Research and Science Today
WWW.RSTJOURNAL.COM

DOI: 10.38173/RST.2025.30.2.8:87-106

Title:	*ROMANIA FACING NEW VECTORS OF INSECURITY: HYBRID WARFARE AND ARTIFICIAL INTELLIGENCE*
Author:	Cătălin PEPTAN

Section: Social Sciences and Humanities
Issue: 2(30)/2025

Received: 2 August 2025	**Revised:** 25 September 2025
Accepted: 3 October 2025	**Available Online:** 3 October 2025

How to cite: Cătălin PEPTAN, "Romania Facing New Vectors of Insecurity: Hybrid Warfare and Artificial Intelligence", *Research and Science Today, 2(30)/2025, pages 87-106, DOI: 10.38173/RST.2025.30.2.8:87-106*

RST Research and Science Today
WWW.RSTJOURNAL.COM
AUTUMN 2025
No. 2(30)/2025
ISSN-E: 2285-9632

ROMANIA FACING NEW VECTORS OF INSECURITY: HYBRID WARFARE AND ARTIFICIAL INTELLIGENCE

Cătălin PEPTAN [1]

ABSTRACT:
THIS PAPER EXAMINES ROMANIA'S CAPACITY TO ADDRESS CONTEMPORARY INSECURITY DYNAMICS SHAPED BY THE INTERSECTION OF HYBRID WARFARE AND THE RAPID ADVANCEMENT OF ARTIFICIAL INTELLIGENCE (AI), WITHIN THE STRATEGIC CONTEXT OF THE WAR IN UKRAINE AND THE PARTICULARITIES OF THE BROADER BLACK SEA REGION. HYBRID WARFARE IS CONCEPTUALIZED AS A COORDINATED USE OF CONVENTIONAL AND NON-KINETIC TOOLS - DISINFORMATION, CYBER OPERATIONS, ECONOMIC AND DIPLOMATIC PRESSURE, AND PROXY ACTORS - AIMED AT ERODING SOCIAL COHESION AND DELEGITIMIZING INSTITUTIONS RATHER THAN PURSUING TERRITORIAL CONQUEST. AI ACTS AS A POWER MULTIPLIER, ENHANCING HOSTILE ACTORS' ABILITY TO GENERATE SYNTHETIC CONTENT (DEEPFAKES), CONDUCT PERSUASIVE MICROTARGETING, AND AUTOMATE OFFENSIVE OPERATIONS IN CYBERSPACE.
THE ANALYSIS HIGHLIGHTS ROMANIA'S STRUCTURAL VULNERABILITIES: LOW LEVELS OF DIGITAL AND MEDIA LITERACY, FRAGMENTATION OF PUBLIC CYBER INFRASTRUCTURE, REACTIVE INSTITUTIONAL MECHANISMS, AND REGULATORY GAPS CONCERNING AI USE IN SECURITY AND DEFENSE. DESPITE EXISTING STRATEGIC FRAMEWORKS (NATIONAL DEFENSE STRATEGY, CYBERSECURITY STRATEGY, NATIONAL AI STRATEGY) AND SPECIALIZED INSTITUTIONS (NATIONAL CYBER SECURITY DIRECTORATE, ROMANIAN INTELLIGENCE SERVICE, CYBERINT CENTER, MINISTRY OF NATIONAL DEFENSE, MINISTRY OF INTERNAL AFFAIRS, NATIONAL AUDIOVISUAL COUNCIL), INTERAGENCY COORDINATION AND THE INTEGRATION OF COGNITIVE SECURITY REMAIN LIMITED. NATO AND EU MEMBERSHIP PROVIDES OPPORTUNITIES FOR INTEROPERABILITY, YET ROMANIA REMAINS PRIMARILY A SECURITY RECIPIENT RATHER THAN A PROACTIVE CONTRIBUTOR.
THE STUDY PROPOSES SEVERAL POLICY-ORIENTED RECOMMENDATIONS: ADOPTION OF A NATIONAL STRATEGY FOR HYBRID WARFARE AND COGNITIVE SECURITY; ESTABLISHMENT OF A DEDICATED AI LEGISLATIVE FRAMEWORK; CREATION OF AN INTERAGENCY ALERT AND RESPONSE PLATFORM; SYSTEMATIC EDUCATION PROGRAMS TO STRENGTHEN COGNITIVE RESILIENCE; AND REINFORCEMENT OF CYBER DEFENSE AND TECHNOLOGICAL DIPLOMACY. THE OVERARCHING OBJECTIVE IS TO SHIFT FROM A FRAGMENTED, REACTIVE POSTURE TO A PROACTIVE, INTEGRATED, AND EURO-ATLANTIC-ALIGNED SECURITY PARADIGM.

KEY WORDS: HYBRID WARFARE; ARTIFICIAL INTELLIGENCE; NATIONAL SECURITY; COGNITIVE RESILIENCE; CYBER DEFENSE.

[1] University lecturer PhD, „Constantin Brâncuși" University of Târgu Jiu, Romania, catalin.peptan@e-ucb.ro

1. INTRODUCTION

The international environment in the first half of the 2020s has been marked by the unprecedented proliferation of non-conventional conflicts, particularly in Eastern Europe and the wider Black Sea region. Russia's military invasion of Ukraine on 24 February 2022, launched under the pretext of a „special military operation", became both a catalyst for regional instability [1] and a paradigmatic case of large-scale hybrid warfare [2]. In parallel, the rapid development of AI has introduced new dimensions of security threats, ranging from sophisticated information manipulation to the automation of decision-making processes in cyber and military domains [3; 4].

As a NATO and EU member state located on the Union's eastern frontier, Romania faces multidimensional hybrid challenges: cyberattacks targeting critical infrastructures [5], disinformation campaigns with geopolitical implications [6], attempts to influence public opinion and democratic processes [7], and risks arising from the unregulated use of emerging technologies [8]. Romania's geostrategic position in the Black Sea region provides it with heightened strategic importance but also exposes it to asymmetric conflicts and hybrid operations linked to the war in Ukraine [9].

The central research question is whether Romania is adequately prepared to address these new architectures of insecurity generated by the intersection of hybrid warfare and AI advancements. The paper analyzes the implications for national security paradigms, institutional capacity, and societal resilience, while emphasizing the need for doctrinal, legislative, and technological adaptation.

The analytical approach will employ an exploratory methodology, combining content analysis of official strategic documents adopted by state authorities up to the present (September 2025) with relevant case studies from the Romanian context. The study will draw on both academic sources and reports issued by European institutions, NATO structures, and specialized think tanks in the fields of security and technology. Its structure will follow a logical progression, beginning with the conceptual delineation of hybrid warfare and artificial intelligence, continuing with their adaptation to the Romanian context, and concluding with strategic proposals aimed at strengthening national security within a rapidly evolving global environment.

2. HYBRID WARFARE – GENERAL CONCEPTS AND ADAPTATION TO THE ROMANIAN CONTEXT

The term *hybrid warfare* refers to a complex form of conflict that combines conventional and unconventional, military and non-military, overt and covert means, with the purpose of destabilizing an adversary state without necessarily escalating into a declared military confrontation [10, 11]. This type of warfare is marked by strategic complexity, operational deniability, and the synchronization of multiple non-kinetic tools such as cyberattacks, disinformation, economic and diplomatic pressure, sabotage, proxy actors, and identity manipulation [12].

Conceptually, hybrid warfare differs from traditional war through its core objective: undermining the target state from within by fragmenting social cohesion, discrediting institutions, and challenging democratic order, rather than occupying territory [13]. In this logic, the „frontline" is no longer a physical line of battle but a complex network that includes mass media, social networks, state institutions, critical infrastructures, as well as religious or minority communities [14; 15].

In Romania, hybrid warfare manifests predominantly in three interconnected areas: the informational space, the cyber domain, and the socio-political sphere. Nevertheless, Romania's national defense strategies to date have not explicitly addressed the risks and vulnerabilities associated with hybrid warfare, instead adopting general formulations that lack adaptation to the country's specific societal context [16].

The informational space represents a preferred target for disinformation and influence campaigns conducted by hostile actors, particularly those originating from the Russian Federation. These operations have intensified over the past decade, reaching critical peaks during electoral periods [17] or in times of crisis such as the COVID-19 pandemic, economic contraction, the war in Ukraine, or natural disasters [18; 19]. The narratives promoted include anti-NATO, anti-EU, and anti-vaccination messages, as well as identity-based and conspiratorial themes, all designed to erode public trust in state institutions. The instruments employed range from networks of obscure websites and fake social media pages to ideologically affiliated influencers and even mainstream media outlets prone to political partisanship.

The cyber dimension of the threat stems from the fact that Romania has been repeatedly targeted by cyberattacks in recent years, including those against critical infrastructures and governmental IT systems. The National Cyber Security Directorate (NCSD) emphasizes Romania's heightened vulnerability to such attacks, driven by its large number of internet users combined with insufficient levels of digital protection. The most exposed sectors are healthcare - managing vast amounts of sensitive data on poorly secured infrastructures - public administration, where attacks seek to disrupt services and undermine citizens' trust, and energy, subjected to constant threats targeting Information Technology (IT)/Operational Technology (OT) networks with potentially severe national security implications [5]. Overall, Romania is perceived as having an extensive „attack surface", which necessitates both stronger defense mechanisms and reinforced international cooperation. These incidents highlight the digital fragility of public institutions, as the rapid pace of digitalization has not been accompanied by adequate security measures.

Hybrid influence in the political and social domain is reflected in attempts to manipulate the political climate and public life, manifesting through the covert support of radical or anti-system movements, the promotion of nationalist or anti-globalist discourse, and the exploitation of social, economic, or identity-based tensions [20; 21]. Furthermore, the dissemination of false information - deliberately amplified by informational „boosts" orchestrated by foreign entities with vested interests - fuels hostility between Romanian citizens and state officials [22].

In this context, Romania faces not only external threats but also an instrumentalized form of internal contestation. Hybrid warfare thus emerges as a systemic challenge that undermines political stability, disrupts institutional functioning, and erodes citizens' trust in the democratic order.

3. ARTIFICIAL INTELLIGENCE AS A MULTIPLIER OF INSECURITY

The accelerated development of AI has opened new frontiers not only in the economic and technological spheres but also in the domain of security. Alongside AI's transformative potential in enhancing operational efficiency and data analysis, significant strategic risks have emerged [23], particularly when such technologies are employed in hostile contexts such as hybrid conflicts or cyber operations [24]. In this regard, AI functions as a power multiplier, enabling state and non-state actors to conduct influence campaigns, espionage, and destabilization efforts on a large scale, at low cost and with a high degree of anonymity.

One of the most concerning applications of AI in the security realm is the generation of fabricated content - ranging from video and audio deepfakes to persuasive texts produced by advanced algorithmic models [25]. These tools are already being used to fabricate statements attributed to political leaders, simulate protests, or spread panic among populations at critical moments. Romania has not been spared from such attempts, particularly in the context of the war in Ukraine, when certain fake social media accounts disseminated carefully crafted content - which was then automatically redistributed - in order to suggest the imminent danger of our country's direct military involvement in the conflict [26].

Another area of risk is predictive intelligence, used to analyze population behaviors, anticipate social or political movements, and customize influence messages [27]. This type of AI-driven microtargeting can be exploited to sow distrust, polarization, and identity-based tensions in societies that are informationally vulnerable.

Romania is not currently a significant actor in the development of AI technologies, but rather a vulnerable recipient of their effects. The low level of digital and media literacy among the general population, coupled with insufficient regulation of AI use in the public sphere compared to other European states [28], creates a favorable context for manipulation campaigns, influence operations, and efforts to undermine social cohesion. Although Romania has adopted the National Strategy on Artificial Intelligence (NS-AI) for the period 2024-2027 [29], in the field of national security the country remains in a reactive position, lacking coherent tools for prevention and response.

Moreover, while other European states have begun implementing the principle of meaningful human control (*Human-in-the-Loop*) in the use of AI within the military and security sectors [30], Romania has not yet adopted concrete institutional measures in this regard. This gap may generate risks in the context of accelerated digitalization of the national defense system and Romania's increasing integration into NATO and EU common infrastructures.

In response to these challenges, Romania has set the objective of developing a robust institutional and doctrinal capacity for the use of AI in the security domain. This involves: drafting a national legislative framework for AI regulation, aligned with European Union legislation [31; 32] and the National Strategy on Artificial Intelligence (2024-2027); strengthening international partnerships with NATO and the EU for best practice exchange, interoperability, and joint responses to emerging threats [33]; and establishing interdisciplinary centers of excellence that integrate military, cyber, and academic expertise.

Romania is currently at a delicate juncture, where strategic inaction regarding AI could lead to an accelerated increase in internal vulnerabilities and a diminished capacity for regional projection.

4. ROMANIA'S SPECIFIC VULNERABILITIES TO EMERGING THREATS

Romania faces a set of structural vulnerabilities that amplify its exposure to the new forms of insecurity generated by hybrid warfare and AI. These vulnerabilities are systemic in nature and manifest across the institutional, technological, educational, and societal domains. In a continuously evolving security environment, Romania's ability to prevent, detect, and respond to emerging threats depends directly on its level of internal resilience and strategic adaptability.

One of the most significant vulnerabilities is *the low level of digital* and media literacy among the population. Recent studies place Romania at the bottom of the EU rankings in terms of understanding the societal impact of digitalization and possessing basic digital skills [8]. At the same time, Romania faces heightened susceptibility to disinformation, which requires

coordinated responses from government institutions, academia, civil society, the media, and private-sector initiatives. These actors play a crucial role in countering toxic narratives, conspiracy theories, and social polarization - classic instruments in the arsenal of hybrid warfare [34].

The fragmentation of Romania's public cyber infrastructure constitutes another major vulnerability. Despite ongoing efforts to digitalize public administration and enhance cyber infrastructure, Romania ranks last in the EU in terms of digital public services [35]. The absence of a centralized risk-monitoring system and standardized response procedures leaves many public institutions - including hospitals, local authorities, and government agencies - exposed as soft targets for cyberattacks. In particular, the information systems of local administrations are frequently exploited by hostile actors, who take advantage of limited resources and inadequate IT expertise at the local level.

An often-overlooked vulnerability lies in *the fragility of social cohesion* in the face of external influence. Vulnerable groups - such as young people without access to quality education, ethnic minorities, or poorly connected rural communities - are frequently targeted by manipulation campaigns, designed either to erode trust in state institutions or to fuel cultural and ethnic antagonisms [36]. Moreover, certain themes - such as sovereigntism, politicized Orthodoxy, or Euroscepticism - are systematically instrumentalized in the online sphere, exerting a significant impact on public opinion.

Despite the existence of specialized entities - such as the National Cyber Security Directorate (NCSD) and the National CYBERINT Center - and the adoption of the National Strategy for Strategic Communication and Countering Disinformation [37], Romania continues to suffer from a *fragmented institutional response.* Moreover, cooperation between the public sector, academia, and the private sector remains insufficient, lacking a functional platform for sharing data, analyses, and best practices. Under these circumstances, the effectiveness of prevention and response measures to hybrid attacks is limited.

5. ROMANIA AS A TESTING GROUND FOR HYBRID OPERATIONS

Romania's geostrategic position at NATO's and the EU's eastern frontier, in close proximity to conflict-prone areas (Ukraine, Transnistria, the Black Sea), has transformed the country into a testing ground for hybrid operations conducted by actors hostile to Western interests. In recent years, Romania has been subjected to a continuous informational and cyber assault targeting both public opinion and state institutions, orchestrated according to a strategic pattern aimed at weakening internal cohesion, discrediting Euro-Atlantic orientation, and undermining confidence in democracy.

Since 2014 - and with greater intensity after 2022 - Romania has been the target of *hostile information campaigns and narratives,* disseminated through disinformation and carried across multiple channels: so-called „alternative news" websites, social media platforms, and local influencers with conspiratorial or anti-Western orientations. The narratives promoted range from anti-NATO and anti-EU themes to conspiracy theories related to the pandemic, the war in Ukraine, or the so-called „globalist dictatorship." Some of these messages are conceived and distributed by networks affiliated with the geopolitical interests of the Russian Federation [22; 18; 21].

A distinctive feature of hybrid operations conducted in Romania is *the exploitation of religious, historical, and cultural themes,* aimed at activating collective emotions and mobilizing vulnerable segments of the population. Orthodox values, sovereigntism, and the notion of a „besieged nation" are frequently instrumentalized to create divisions among citizens and to delegitimize the state's pro-Western orientation [38]. Furthermore, radical conservative

discourse, promoted in recent years by certain political formations and influence groups, is often synchronized with messages from Russian propaganda, even though no direct connection between the sources has been formally established. In this context, Romania is perceived by hostile actors as fertile ground for digital social engineering, where cultural and historical divisions can be artificially stimulated for destabilizing purposes.

It is also *noteworthy that certain moments of social crisis in Romania have been artificially amplified* in the online environment through networks of fake accounts, bots, and websites disseminating emotional, unverified, or alarmist content. Examples include the COVID-19 pandemic crisis in Romania [39], the so-called foreign interference in national politics [40], and attempts to influence Romanian elections [41]. The strategy sought to artificially escalate social tensions, with the aim of either triggering mass mobilization against the state or provoking a disproportionate institutional response that could subsequently be exploited for propaganda purposes.

6. NATIONAL LEGAL AND INSTITUTIONAL FRAMEWORK

Romania's response to the new security challenges posed by hybrid warfare and emerging technologies is articulated through a set of strategic documents, normative acts, and specialized institutional structures.

The primary normative reference is the *National Defense Strategy of Romania for 2020-2024*, which explicitly acknowledges hybrid, cyber, and technological threats as integral components of the new insecurity paradigm [42]. Nevertheless, the strategy provides more of a declarative vision than a coherent operational plan, lacking measurable performance indicators and a clear delineation of inter-institutional responsibilities.

In addition, the *Cybersecurity Strategy of Romania (2022-2027)* represents an important step forward in the field of digital protection. However, it insufficiently addresses the dimension of artificial intelligence or the challenges of information manipulation [43].

Moreover, the *National Strategy on Artificial Intelligence (NS-AI) for 2024-2027* positions artificial intelligence as a driver of economic development and social progress. Its major objectives include: education and skills development, infrastructure and datasets, strengthening research and innovation, technology transfer, societal adoption of AI, and appropriate governance [29]. Furthermore, the strategy underscores the role of standardization through the involvement of the *Romanian National Standardization Body* (SR EN ISO/IEC 23053), in order to ensure the compatibility and competitiveness of solutions at both the European and international levels [44].

Last but not least, *Government Emergency Ordinance no. 155/2024* [45] transposes the NIS 2 Directive [46] into Romanian legislation and establishes a unified framework for strengthening cybersecurity at the national level. The normative act expands the range of entities required to adopt protective measures and introduces strict requirements for incident reporting and auditing. Through its firm sanctions and imposed responsibilities, the ordinance fosters investment in digital resilience and aligns Romania with European standards, generating an impact both on state-entity relations and on contractual arrangements and civil liability.

From an institutional perspective, Romania has several entities tasked with managing hybrid threats:

The *National Cyber Security Directorate (NCSD)*, created through the reorganization of the National Computer Security Incident Response Team (CERT-RO), has as its primary mission the protection of national cyber infrastructures and the coordination of cybersecurity measures at the national level [47].

While the institution does not hold direct responsibilities regarding the regulation of media content, it plays a significant role in the prevention, identification, and counteraction of disinformation campaigns carried out in the online environment, insofar as these intersect with cybersecurity and the protection of critical digital infrastructures. NCSD's activity focuses on detecting and reporting coordinated information manipulation campaigns in the digital sphere, working in cooperation with communication service providers, private stakeholders, as well as international organizations such as the EU and NATO. In addition, the institution fulfills an important role in public education and awareness-raising, promoting information campaigns aimed at strengthening the resilience of citizens and organizations against online manipulation attempts. In this respect, NCSD positions itself as an institutional actor with indirect responsibilities in the fight against disinformation, primarily through the cybersecurity lens, while complementing the mandates of other institutions engaged in strategic communication and national security [5; 47].

The *Romanian Intelligence Service (SRI)*, through its *National CYBERINT Center*, acts as the national authority in the field of cybersecurity, with extensive responsibilities for the prevention, identification, and counteraction of cyber threats to national security. Within this framework, disinformation is addressed as a component of information warfare and hybrid campaigns, insofar as it unfolds through digital channels and undermines the security of critical infrastructures or the resilience of state institutions [48]. Pursuant to its legal mandate, the CYBERINT Center is tasked with monitoring cyberspace, detecting coordinated influence campaigns, and analyzing how such operations may be exploited by state or non-state actors to weaken national security. The center also contributes to informing decision-makers and supporting public policies on information security by providing strategic reports and assessments.

In addition, CYBERINT plays an active role in international cooperation formats within NATO and the EU, where disinformation is recognized as a transnational threat with significant implications for democratic stability and decision-making processes [48]. Consequently, its role is predominantly technical and analytical, embedded within the broader national security mechanisms and complementary to other institutions responsible for strategic communication and the regulation of the public sphere.

The *Ministry of National Defense (MoND)* holds specific competences within the broader framework of national security concerning the countering of disinformation, being responsible for ensuring the resilience of the military environment and protecting operational structures against information manipulation. In recent strategic planning documents, such as the *White Paper on Defense 2021-2024* [49] and the *National Defense Strategy of Romania 2020-2024* [42], disinformation is addressed as part of the broader spectrum of hybrid threats and information warfare, with a direct impact on both national and collective security within NATO and the EU.

At the operational level, the MoND relies on specialized structures in strategic communication, psychological operations, and public relations, tasked with identifying, analyzing, and countering hostile narratives in the military domain. Furthermore, the ministry participates in allied initiatives and exercises in the field, contributing to the development of information defense capabilities. In this regard, the role of the MoND is predominantly defensive and operational, focused on securing the military environment and strengthening institutional resilience.

The *Ministry of Internal Affairs (MoIA)* holds indirect competences in the field of countering disinformation, derived from its fundamental role as guarantor of public order, citizens' safety, and the state's internal security [50; 51]. Disinformation is primarily addressed

by the MoIA as a threat to social stability and public security, particularly when hostile information campaigns aim to destabilize communities, generate panic, or undermine trust in state institutions.

At the operational level, MoIA structures - most notably the Romanian Police, the Gendarmerie, and the Department for Emergency Situations - act through monitoring and managing the effects of disinformation in the public sphere, in close cooperation with the Romanian Intelligence Service and other competent institutions. In addition, the MoIA is engaged in prevention and public awareness campaigns designed to mitigate the impact of manipulative messages on the population, especially in times of crisis (e.g., pandemics, natural disasters, terrorist threats).

Thus, although it does not exercise direct authority over media content regulation, the MoIA plays a key role in managing the social consequences of disinformation and strengthening community resilience, thereby contributing to a coordinated state response to this type of threat.

The *National Audiovisual Council (CNA)*, as the sole regulatory authority for the audiovisual sector in Romania, holds significant responsibilities in preventing and sanctioning disinformation in the public sphere. Under Law No. 504/2002 on Audiovisual Broadcasting, the CNA is tasked with ensuring a balanced informational environment and safeguarding the public's right to accurate information [52]. Within this framework, disinformation is regarded as a violation of the public interest, through the dissemination of false, manipulative, or unverified content.

In practice, the CNA's competences are exercised through the monitoring of audiovisual content and the imposition of sanctions in cases of breaches of legal provisions on accurate reporting. The *Audiovisual Content Regulation Code* further details the professional standards that explicitly prohibit the broadcasting of false or biased news [53].

Although the CNA does not hold authority over the regulation of online platforms or social networks, its role remains essential in curbing the spread of disinformation through audiovisual channels (radio and television), thereby contributing to the resilience of the media space and the protection of the public interest.

The National Authority for Management and Regulation in Communications (ANCOM) plays a significant role in countering disinformation, not as an institution that censors or controls online content, but rather as a regulatory actor facilitating a secure framework for electronic communications. On the one hand, ANCOM supports the development of a resilient digital ecosystem by regulating communication networks and services, which includes ensuring transparency of internet providers, guaranteeing non-discriminatory access to information, and protecting users against abuses such as false or manipulative content disseminated through digital platforms. On the other hand, the institution is responsible for implementing both European and national legislation on digital services, working in cooperation with other authorities to oversee online platforms and counter disinformation campaigns. Thus, ANCOM's role is not to assess the veracity of information, but to ensure a transparent, secure, and properly regulated electronic communication framework in which public and private actors operate, thereby indirectly contributing to limiting the impact of disinformation and strengthening trust in the digital space [54].

The National Agency for Romania's Digitalization plays a complementary role in strengthening the country's resilience to hybrid threats and disinformation, contributing to the development of secure digital infrastructures, the implementation of European digital transformation policies, and the provision of technological foundations for a protected information space. Within its structure operate the *Intermediate Body for the Promotion of the*

Information Society (OIPSI) and the *National Cyber Coordination Center (NCC-RO),* both tasked with monitoring, analysis, and coordinating responses to cyber incidents, including online information manipulation campaigns [55].

In light of the foregoing, we contend that a major obstacle to the effective management of risks and threats posed by emerging challenges lies in the absence of coherent legislation on hybrid warfare and the use of AI in the security domain. At present, Romania lacks a dedicated law defining and sanctioning acts of information warfare, foreign interference in democratic life, or the use of AI in sensitive operations. In the absence of such a normative framework, institutions remain confined to traditional instruments, which often prove inadequate when confronted with these new types of threats.

Moreover, Romania has not yet fully transposed the provisions of European legislation on AI, despite ongoing efforts to adopt a national strategy in the field [32]. This delay has generated setbacks in the ethical and operational standardization of artificial intelligence - based technologies.

Against the backdrop of a rapidly evolving security environment, the imperative of institutional and doctrinal reform becomes evident. In this context, we consider it necessary for Romanian authorities to adopt the following measures: a national strategy for countering hybrid threats, integrating informational, cyber, psychological, and social components; an updated legislative framework on the use of AI in security and defense, aligned with NATO and EU standards; the institutionalization of a national inter-institutional platform to coordinate responses to hybrid operations; and the development of a national system for rapid alert and response to information manipulation, in cooperation with digital platforms and civil society.

7. ROMANIA'S ROLE IN NATO AND THE EU IN THE CONTEXT OF EMERGING THREATS

Romania's membership in NATO and the EU constitutes the main pillar of strategic stability and security in the face of hybrid threats and new technological challenges. Nevertheless, despite its active participation within Euro-Atlantic structures, Romania remains largely a security consumer rather than a regional provider of expertise and initiative in emerging domains such as artificial intelligence and information warfare [56].

Participation in NATO exercises and initiatives. Romania has been actively involved in international cyber defense and hybrid attack response exercises, such as *Locked Shields*, organized by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). The aim of this exercise is to provide a practical training platform for member nations and to assist them in developing their capabilities to counter cyber threats [57]. At the same time, national security structures cooperate within NATO with the Joint Intelligence and Security Division at NATO Headquarters, which enhances situational awareness and the analysis of information concerning hybrid threats, particularly in the Black Sea region [58]. Romania also participates in the *Hybrid Warfare Centre of Excellence*, whose mission is to strengthen the security of participating states by providing expertise and training for countering hybrid threats, as well as by fostering EU-NATO cooperation in this regard [59].

Despite these engagements, Romania's doctrinal and technological integration within NATO remains relatively modest. The absence of a clear and coherent legislative framework on AI in the field of defense reduces the country's capacity to actively contribute to shaping the Alliance's policies in this domain.

Engagement in European Union Security Policies. At the European level, Romania participates in mechanisms such as the *EU Cyber Diplomacy Toolbox* - which contributes to conflict prevention, mitigation of cybersecurity threats, and the strengthening of stability in

international relations [60]; the *StratCom Task Forces* - operating under the European External Action Service, focused on „effective communication" and the promotion of EU activities in Eastern Europe in response to disinformation campaigns conducted by hostile entities [61]; and *Permanent Structured Cooperation (PESCO) projects* - which provide the necessary framework for deepening defense cooperation, delivering the capabilities required to enhance EU citizens' security, including in the fields of cybersecurity and counter-disinformation [62].

Romania also supports, both declaratively and operationally, initiatives such as the *EU Artificial Intelligence Act* - legislation classifying AI applications into three categories of risk (applications and systems that create an unacceptable risk, high-risk applications, and applications not explicitly prohibited or listed as high risk) [31]; and the *Digital Services Act* - the EU regulation on digital services, which addresses illegal content, transparent advertising, and the fight against disinformation [63].

In addition, Romania contributes to the *EU Defence Fund* by participating in research, innovation, and industrial cooperation projects aimed at modernizing the national defense industry and integrating it into European value chains. This engagement supports interoperability, the development of advanced technologies, and the strengthening of European security, reflecting both EU solidarity and Romania's national strategic interests [64].

Equally important, Romania is an active participant in *Horizon Europe*, the EU's flagship funding program for research and innovation in areas critical for adapting to new technological paradigms [65].

The tense regional context, exacerbated by the war in Ukraine and instability in the Black Sea region, has significantly increased Romania's strategic relevance for NATO's eastern flank and for the EU's energy and logistical security. The Port of Constanța, the military bases at Mihail Kogălniceanu and Cincu, as well as dual-use civil-military infrastructure, have become key assets supporting NATO's regional efforts. However, this geographic relevance is not yet matched by autonomous strategic capacity. Romania lacks consolidated expertise in analyzing and countering information warfare, nor does it possess a comprehensive legal framework for cognitive defense. Furthermore, its position within European decision-making bodies is often passive, with participation that is reactive to initiatives launched by other actors (Germany, France, Poland).

To harness its potential within NATO and the EU and to develop genuine strategic capacity, Romania must adopt a more proactive profile in the following directions: establishing a national structure dedicated to international cooperation on AI and hybrid security; strengthening technological diplomacy through digital and security attachés in Brussels and other key NATO capitals; developing a domestic legislative framework harmonized with the EU Artificial Intelligence Act and NATO policies on the responsible use of AI; and creating regional centers of excellence in information and cyber defense, in partnership with other states on the eastern flank. In this way, Romania can consolidate its status as an active generator of security at the regional level.

8. THE IMPACT OF THE WAR IN UKRAINE ON ROMANIA'S SECURITY ARCHITECTURE

The war launched by the Russian Federation against Ukraine on 24 February 2022 has triggered a rapid reconfiguration of security paradigms in Eastern Europe, with direct consequences for Romania's security architecture. As a state located on NATO's and the EU's eastern flank, Romania has become a key hub in logistical, intelligence, and collective defense chains, while simultaneously representing a potential indirect target of hybrid operations carried out by the Russian Federation in the region [66].

Romania's geographical proximity to the theater of operations in southern Ukraine (particularly the Odesa region) has exposed the country to collateral effects of the conflict, including kinetic-type incidents. Clear examples include the repeated fall of fragments from Russian drones on Romanian territory in the Danube Delta area (Tulcea County), officially confirmed by the Ministry of National Defense and NATO, and widely reported in the Romanian media. Although isolated, such incidents have raised concerns about the unintended spillover of the conflict and the testing of NATO's thresholds of response. In this context, Romania has regulated the legal framework concerning the control of its national airspace [67] as well as the conduct, in peacetime, of military missions and operations on Romanian territory [68].

In parallel, Romania has also faced an intensification of hybrid operations: cyberattacks targeting government critical infrastructure [43], disinformation campaigns regarding the country's military involvement [26], and the polarization of public discourse surrounding support for Ukraine [69].

On the other hand, the war in Ukraine has placed significant strain on Romania's critical infrastructures, particularly in the areas of transport, energy, and communications. The Port of Constanța, the railway network, and border crossing points have been heavily utilized for the transit of grain, fuel, equipment, and humanitarian aid to and from Ukraine. This pressure has exposed major vulnerabilities in the national logistics infrastructure, while also underscoring the need to strengthen crisis-response capacities in the context of protracted emergencies.

At the same time, the heightened risk of sabotage and espionage targeting critical infrastructure has prompted a review of security measures in the energy sector, especially in Dobrogea and the Black Sea coastal region. In this regard, the *Romania's Energy Strategy 2025-2035, with a 2050 Outlook*, was shaped in the aftermath of the outbreak of the war in Ukraine. The document emphasizes the imperative of ensuring energy security, diversifying supply sources, promoting renewables, expanding energy storage, and enhancing energy efficiency [70]. Similarly, the *Strategic Institutional Plan of the Ministry of Energy 2024-2027* identifies the effects of the war in Ukraine on the energy sector and highlights the need for a stimulating legislative framework aimed at accelerating investments in renewable energy production and strengthening Romania's energy security [71].

In response to the new security context, Romania has accelerated the modernization of its military capabilities and deepened cooperation with strategic partners. Announced measures include participation in the implementation of the IRIS-T air defense system [72], the expansion of military bases at Mihail Kogălniceanu and Cincu, the reinforcement of NATO contingents stationed in Romania [73], and an increase in the defense budget to over 2.5% of GDP starting in 2023 [74].

Doctrinally, however, Romania remains behind in integrating hybrid, informational, and AI dimensions into its national security strategy. The war in Ukraine has demonstrated that success on the battlefield is closely linked to superiority in the information domain, and Romania must learn from these lessons to consolidate its own capabilities.

The conflict in Ukraine has also highlighted social and cognitive divisions within Romania, between groups supportive of Ukraine and segments influenced by Russian propaganda, Euroscepticism, or conspiracy theories. In this context, cognitive security has emerged as a critical component of the national security architecture. The absence of a sustained strategic communication campaign and media education initiatives leaves these divisions vulnerable to exploitation by hostile actors.

9. THE CYBER DIMENSION OF NATIONAL INSECURITY

In the digital era, cyberspace has become a strategic conflict zone in its own right, and national security can no longer be conceived without the adequate protection of IT networks, sensitive data, and critical infrastructures. For Romania, exposure to cyber threats is steadily increasing, as the accelerated digitalization of public services and institutions has not been matched by a proportional strengthening of defense capabilities and the training of specialized personnel.

In recent years, Romania has been the target of several large-scale cyberattacks, some of which have directly affected the functioning of public institutions or public trust. Among the most notable incidents are: ransomware attacks against several hospitals in Romania [75] and the Chamber of Deputies [5]; DDoS attacks claimed by the pro-Russian group *Killnet*, targeting the websites of the Government, the Ministry of National Defense, the Ministry of Foreign Affairs, and other institutions in 2022, in the context of Romania's support for Ukraine [76]; as well as phishing campaigns and data exfiltration operations attributed to the group *Scattered Spider*, which compromised IT networks of hospitals and local municipalities, revealing widespread vulnerabilities at the territorial level [77].

These attacks demonstrate not only the existence of hostile capabilities aimed at destabilizing Romania but also the absence of uniformly protected cyber infrastructures, particularly within the public sector.

Romania faces several structural challenges in the cyber domain: a shortage of qualified IT security personnel, especially within non-military institutions; fragmentation of IT systems between central and local authorities; dependence on outdated or unsecured software solutions; and the absence of regular IT infrastructure audits across many institutions.

Moreover, the culture of cybersecurity remains underdeveloped at the institutional level. Many entities lack clear incident-response procedures, while inter-agency communication is often delayed or ineffective. In this context, the development of comprehensive educational programs and the integration of cyber diplomacy concepts into university-level curricula on cybersecurity are strongly recommended [78].

We note that Romania has made significant progress in developing a dedicated normative framework for cybersecurity. The *National Cybersecurity Strategy 2022-2027* [43] and *Law No. 58/2023 on Romania's Cybersecurity* [79] provide an updated framework for action. Nevertheless, the implementation of strategic provisions remains slow, while the absence of an integrated digital security culture continues to pose a major obstacle.

At the international level, Romania is an active participant in global cyber defense efforts, being a member of NATO's *Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, whose mission is „to support NATO and member nations with unique interdisciplinary expertise in cyber defense research, training, and exercises" [80]. Romania also takes part in international exercises such as *Cyber Europe* - large-scale, cross-border cyber crisis management simulations [81] - and *Locked Shields*, which „allow cybersecurity experts to enhance their skills in defending national IT systems and critical infrastructures against real-time attacks" [82]. In addition, the *National Cyber Security Directorate (NCSD)* cooperates with *ENISA* (the European Union Agency for Cybersecurity) and with national Computer Security Incident Response Teams (CSIRTs) across other EU states [5; 45].

However, in order to face the new generation of threats - including AI-driven automated attacks, disinformation operations integrated into cyber actions, and digitalized critical infrastructures - Romania must: consistently invest in the training of cybersecurity experts; support the creation of a public–private innovation ecosystem in cyber defense; and develop

an integrated strategy for cognitive-digital defense, one that brings together IT, AI, and psycho-informational components.

10. SOCIETAL RESILIENCE AND COGNITIVE SECURITY

Within the contemporary architecture of insecurity, cognitive security has emerged as a fundamental component. It refers to a society's ability to safeguard its processes of thinking, decision-making, and perception against external or internal manipulation, hostile influence, and information attacks [83]. In parallel, societal resilience entails the collective capacity of a population to withstand crises, propaganda, polarization, and attempts at destabilization. For Romania, these dimensions are becoming increasingly relevant amid the proliferation of information warfare and the deepening of social fragmentation.

Romania is currently facing significant cognitive vulnerabilities, as it records a low level of media and digital literacy - a fact confirmed by reports from European institutions [84]. Many segments of the population - particularly those in rural areas, the elderly, and individuals with limited education - lack the cognitive tools necessary to distinguish between verified information and manipulative content. At the same time, a significant portion of the public shapes its political and social views based on informal sources (social media groups, YouTube, unverified blogs), without the filter of critical thinking [18].

This situation creates fertile ground for hostile propaganda, fake news, conspiracy theories, and anti-Western narratives. The existence of an „alternative information bubble" is an increasingly tangible reality, with direct consequences for electoral choices, trust in state institutions, and national cohesion.

One of the consequences of this reality is the instrumentalization of fear, religion, and identity by hostile actors targeting Romania - particularly in the online sphere - who exploit emotional and symbolic themes to influence public perceptions. The predominant narratives used include: fear of war and the notion of Romania being „sacrificed" by NATO [85]; the defense of traditional values against the EU's so-called „progressive dictatorship" [86]; and the idealization of a lost sovereignty, coupled with distrust in external partners [87]. These messages are disseminated in a coordinated manner by seemingly independent pages and influencers, yet their rhetoric is strikingly synchronized. Their impact is twofold: undermining democratic consensus and fueling heightened social polarization, especially during electoral campaigns.

The absence of a national cognitive security strategy - despite the official acknowledgment of disinformation and mass manipulation as critical challenges - hampers institutional efforts to counter hostile propaganda, which are carried out in a fragmented, reactive manner, often with limited resources. These efforts are further constrained by the lack of a central authority to coherently coordinate public policies on media literacy, strategic communication, and responses to information attacks. Moreover, the education system does not systematically incorporate courses on critical thinking, source evaluation, or the responsible use of digital networks. Such initiatives remain isolated, typically undertaken by NGOs or academic institutes, without consistent institutional support.

We contend that in order to strengthen societal resilience and cognitive security, Romania must adopt a coherent approach that includes: the creation of a national strategy for media literacy and cognitive protection, coordinated across institutions; the integration of critical thinking into school curricula starting from lower secondary education; the development of proactive strategic communication campaigns to explain public policies and counter disinformation; public–private partnerships with social media and broadcasting platforms to detect and limit manipulative content; and the support of academic research on

digital propaganda and the psychosocial impact of disinformation. Without strengthening this dimension, national security will remain vulnerable to threats that require no military force - only control over public perception.

11. ETHICAL AND REGULATORY CHALLENGES OF AI IN ROMANIA

Artificial intelligence (AI) is among the most disruptive technologies of the 21st century, with immense potential in the field of security but also with significant ethical and regulatory risks. As a member state of both the EU and NATO, Romania is obliged to comply with an emerging set of international norms governing the responsible use of AI. Nevertheless, at the national level, the regulatory framework and public debate on the implications of AI for security remain at an early and fragmented stage.

Romania currently lacks a dedicated AI law - despite the adoption of the *National Artificial Intelligence Strategy 2024–2027* - and the use of such technologies is regulated only indirectly, through general legislation on data protection, public procurement, or cybersecurity. This legislative gap creates uncertainty regarding legal liability in cases where decisions are made by automated systems, ethical standards for the use of AI in national security, justice, or public order, and the limits of algorithmic surveillance in relation to fundamental rights [88; 89; 90]. In addition, Romania lags behind in implementing the requirements of the *EU Artificial Intelligence Act*, which introduces a risk-based classification and strict regulations for AI in sensitive domains, including defense.

A key principle promoted at the international level is that of *meaningful human control* over AI-based systems, particularly those employed in military contexts [91]. While Romania has endorsed this principle within NATO, it has not yet formulated clear regulations for its concrete application in military operations or procurement. This gap becomes increasingly dangerous given the growing use of AI in surveillance systems based on facial recognition, automated decision-making for threat prioritization, and autonomous platforms. The absence of clarity regarding legal responsibility in the event of algorithmic error in an operational context generates major ethical and strategic risks.

One of the most sensitive issues is *the balance between security and the protection of citizens' rights*, particularly the right to privacy, freedom of expression, and the protection of personal data. There is a risk that AI tools deployed for legitimate defense or preventive purposes (e.g., combating radicalization, detecting abnormal behaviors) could be diverted toward excessive surveillance or abusive profiling. In the absence of democratic control mechanisms - such as independent oversight authorities, ethical audits of algorithms, and transparency of code and training data - AI may come to be perceived not as an instrument of protection, but rather as a source of intrusion into private life, a risk against which preventive measures have already been adopted at the European and international levels [90; 92; 93].

To mitigate these risks and harness the technological potential, Romania needs an ethical and institutional architecture for AI that, beyond the *National Artificial Intelligence Strategy 2024–2027*, should include: the establishment of a National Committee on AI Ethics with advisory and supervisory functions; the integration of AI into the training curricula of military, judicial, and administrative personnel; and partnerships with academic centers and think tanks to assess the social and political impact of AI. Only through a clear, transparent, and participatory regulatory framework will Romania be able to employ AI responsibly and effectively, while avoiding a slide toward authoritarian or abusive practices.

12. CONCLUSIONS AND RECOMMENDATIONS

The accelerated transformations of the international and regional security environment - driven by the rise of disruptive technologies and the intensification of hybrid operations - require a profound rethinking of national defense and resilience paradigms. For Romania, its proximity to the Ukrainian conflict zone, its geostrategic position in the Black Sea region, and its status as a NATO and EU member amplify both its responsibilities and vulnerabilities.

The analysis conducted in this paper highlights a series of strategic, institutional, and doctrinal shortcomings, including: the absence of an integrated strategy for countering hybrid threats; the population's low level of digital and media literacy; the lack of a legislative framework on the responsible use of artificial intelligence in the security domain; and a fragmented, reactive institutional response to non-conventional threats.

The study relies primarily on sources (strategic documents, institutional reports, academic studies), which may reflect a perspective partially dependent on the official framework. Limited access to classified data constrains the possibility of fully assessing internal response mechanisms. Moreover, the exploratory nature of the research means that its findings are indicative -intended to outline strategic directions rather than provide definitive solutions.

Given that Romania has real opportunities to strengthen its security - through anchoring in Euro-Atlantic structures, through its assumed strategic role in the region, and through access to funding and partnerships for technological innovation and institutional reform - we argue that effectively addressing the new vectors of insecurity requires a qualitative leap in strategic thinking, translated into a set of concrete measures:

✓ *Drafting a National Strategy on Hybrid Warfare and Cognitive Security* as a distinct strategic document, complementary to the National Defense Strategy, integrating informational, cyber, social, and psychological dimensions, along with coordination mechanisms among security, education, culture, technology, and media institutions.

✓ *Adopting a national legislative framework on AI in security*, complementary to the *National Artificial Intelligence Strategy 2024–2027*, by transposing and adapting the provisions of the *EU Artificial Intelligence Act* and introducing the principle of *meaningful human control* into military doctrine, in order to clarify legal responsibility for automated decisions.

✓ *Establishing an Interinstitutional Committee on Information and Digital Security*, as a permanent platform for cooperation among the MoND, the SRI, the DNSC, the NGOs, and academia, for continuous monitoring of the information space and social networks, and for coordinating rapid responses to hostile campaigns.

✓ *Investing in education for cognitive resilience,* through: integrating critical thinking and media literacy into school curricula; developing national training programs for civil servants, teachers, and journalists; and conducting proactive strategic communication campaigns supported by state institutions.

✓ ***Strengthening cyber defense capabilities*** through: expanding cooperation with NATO and ENISA; establishing a national fund for innovation in cybersecurity; and conducting regular audits of critical digital infrastructures and public applications.

Romania stands at a turning point: it can either continue to manage insecurity through fragmented, reactive instruments, or it can become an active, forward-looking, and innovative actor within the Euro-Atlantic security architecture. The choice between vulnerability and resilience is not an abstract one; it is reflected in legislation, education, technology, institutions, and ultimately in the trust that citizens place in the Romanian state. Confronted with a war waged not only with conventional weapons but also with data, perceptions, and algorithms,

Romania must adopt a form of security that is smart, ethical, and democratic - adapted to the realities of the 21st century.

REFERENCES

[1]. Peptan, C. (2022). Considerations regarding the reconfiguration of the new geopolitical architecture in the context of the crisis in Ukraine. *Analele Universitatii „Constantin Brancusi" din Targu Jiu - Seria Litere si Stiinte Sociale*, (01), 65-75.
[2]. Ioniță, C. C. (2023). Conventional and Hybrid Actions in the Russia's Invasion of Ukraine. *Security and Defence Quarterly*, *44*(4), 5-20.
[3]. Feldman, P., Dant, A., & Foulds, J. R. (2024). Killer Apps: Low-Speed, Large-Scale AI Weapons. *arXiv preprint arXiv:2402.01663*.
[4]. Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Srikumar, M. (2020). Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. *Berkman Klein Center Research Publication*, (2020-1).
[5]. DNSC. Raport anual privind starea securității cibernetice în România, 2024 (aprobat prin HCSAT nr. 77/30.06.2025). Available at: https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024. Accessed: 15.08.2025.
[6]. Toma, B., Suciu, M. (September, 2024). România and the 2024 elections: EU related disinformations – Targets and challenges. Available at: https://www.crpe.ro/wp-content/uploads/2024/10/CRPE-Disinformation-2024-Report-ENG.pdf. Accessed: 15.08.2025.
[7]. MAE. (May 22, 2025). Precizări de presă. Available at: https://www.mae.ro/node/66801. Accessed: 17.08.2025.
[8]. Sfetcu, N. (2024). Information and Communications Technology in Romania-Comparative Analysis with the EU, Social Impact, Challenges and Opportunities, Future Directions. Pp. 52-68.
[9]. ROGOZAN, A. P. C. C. C., & LEARSCHI, I. C. I. C. S. (2023). Reziliența maritimă a României în era amenințărilor hibride și importanța unei Strategii de Securitate Maritimă. Pp. 25-28.
[10]. Wither, J. K. (2016). Making sense of hybrid warfare. *Connections*, *15*(2), 73-87.
[11]. Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars* (p. 51). Arlington, VA: Potomac Institute for Policy Studies.
[12]. Solmaz, T. (2022). Hybrid warfare': one term, many meanings. *Small Wars Journal*, *25*.
[13]. Reichborn-Kjennerud, E., & Cullen, P. (2022). *What is Hybrid Warfare?* Norwegian Institute for International Affairs (NUPI).
[14]. Svetoka, S. (2016). *Social media as a tool of hybrid warfare*. NATO Strategic Communications Centre of Excellence.
[15]. Nikolov, O. (2018). Building societal resilience against hybrid threats. *Information & Security*, *39*(1), 91-109.
[16]. Dumitru, I. R. (2022). EVOLUȚIA CONCEPTULUI DE RĂZBOI HIBRID ÎN STRATEGIILE NAȚIONALE DE APĂRARE ALE ROMÂNIEI. *Buletinul Universității Naționale de Apărare «Carol I»*, *11*(03), 24-34.
[17]. Stanescu, G. C. (2024). Fake news, bots, and influencers: The impact of social media on Romania's 2024 elections. *Social Sciences and Education Research Review*, *11*(2), 361-366.
[18]. Peptan, C., Mărcău, F., C. (2024). *Impactul informațiilor de tip fake news asupra problematicilor securitare*. Editura Sitech, Craiova.
[19]. Mărcău, F. C., Peptan, C., Băleanu, V. D., Holt, A. G., Iana, S. A., & Gheorman, V. (2023). Analysis regarding the impact of 'fake news' on the quality of life of the population in a region affected by earthquake activity. The case of Romania–Northern Oltenia. *Frontiers in public health*, *11*, 1244564.
[20]. Vladu, L., Bârgăoanu, A., & Nastasiu, C. (2025). Information Warfare: Adapting to the Ever-Changing Nature of War. *International Journal of Intelligence and CounterIntelligence*, *38*(2), 348-368.
[21]. Lovi, S. (2025). How Disinformation Can Influence a Nation: The Case of Romania. *Studia i Analizy Nauk o Polityce*, (1), 27-44.
[22]. Pop, A. M. (December, 2022). STRENGTHENING ROMANIAS'RESILIENCE TO RUSSIAN DISINFORMATION. In *PROCEEDINGS OF THE INTERNATIONAL SCIENTIFIC CONFERENCE STRATEGIES XXI. VOLUME XVIII* (pp. 429-438). Carol I National Defence University Publishing House.
[23]. Osoba, O. A., & Welser, W. (2017). *The risks of artificial intelligence to security and the future of work*. Santa Monica, CA: RAND.
[24]. Budacu, D. (2024). The impact of the artificial intelligence on hybrid conflicts in the 21st century. *Studia Securitatis*, *18*(2), 87-108.

[25]. Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. *Applied intelligence*, *53*(4), 3974-4026.
[26]. INFORADAR. (Iuly 29, 2025). Dezinformare în mediul online cu privire la așa-zisa intrare a României în război. Available at: https://inforadar.mapn.ro/. Accessed: 03.09.2025.
[27]. KAKULAPATI, V. (2023). ARTIFICIAL INTELLIGENCE-BASED PREDICTING PATTERN ANALYSIS. *Pattern Analysis of Personality Dimensions Using Artificial Intelligence*, 1.
[28]. Pop, M. (2024). Legal Frameworks for Artificial Intelligence: A Comparative Analysis of Romania, the European Union, and International Perspectives. *Jurnalul de Drept si Stiinte Administrative*, *1*(21), 75-87.
[29]. Strategia Națională în domeniul Inteligenței Artificiale. Available at: https://www.adr.gov.ro/wp-content/uploads/2024/03/Strategie-Inteligenta-Artificiala-22012024-1.pdf. Accessed: 04.09.2025.
[30]. Davidovic, J. (2023). On the purpose of meaningful human control of AI. *Frontiers in big data*, *5*, 1017677.
[31]. The EU Artificial Intelligence Act. Available at: https://artificialintelligenceact.eu/. Accessed: 05.09.2025.
[32]. REGULAMENTUL (UE) 2024/1689 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 13 iuny 2024. Available at: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R1689. Accessed: 05.09.2025.
[33]. De Maio, G. (2021). Opportunities to deepen NATO-EU cooperation. *Brookings, De-cember*, *202*(1).
[34]. Bălan, C. (2025). Romania's Susceptibility to Hybrid Threats related to Disinformation. *Romanian Military Thinking*, (1), 78-91.
[35]. Voinea, R. C. (2024). Digital Performance Analysis of Public Administration: Romania's Ranking in DESI. *Revista de Științe Politice. Revue des Sciences Politiques*, (81), 223-234.
[36]. Corbu, N., Oprea, D. A., & Frunzaru, V. (2022). Romanian adolescents, fake news, and the third-person effect: A cross-sectional study. *Journal of children and media*, *16*(3), 387-405.
[37]. Strategia Națională de Comunicare Strategică și Combatere a Dezinformării, (2021). București, aprobată prin Hotărârea CSAT nr. 113 din 18.08.2021.
[38]. Lupulescu, G. D. (2024, May). Revealing Hybrid Threats: Vulnerability Exploitation in Romania's. In *11th European Conference on Social Media: ECSM 2024*. Academic Conferences and publishing limited.
[39]. „ADEVĂR SAU PROVOCARE? - Despre dezinformare și efectele sale în contextul pandemiei de coronavirus", Raport realizat de Asociația de Investigații Media în Balcani (BIRN România), în cadrul proiectului „Don't Spread the Virus", aprilie - decembrie 2020. Available at: https://sinopsis.info.ro/wp-content/uploads/2021/01/ASP.pdf. Accessed: 05.09.2025.
[40]. Associated Press. (April 27, 2025). *Romanians confront a deluge of online disinformation ahead of a presidential election rerun*. AP News. Available at: https://apnews.com/article/2cae1b28b5059b7cee228142eadaca78. Accessed: 05.09.2025.
[41]. Cyabra (2025). *Coordinated Disinformation Targeting Romania's Election*. Available at: https://cyabra.com/reports/coordinated-disinformation-targeting-romanias-election/. Accessed: 03.09.2025.
[42]. Președinția României. *Strategia Națională de Apărare a Țării pentru perioada 2020–2024*. Monitorul Oficial al României, Partea I, nr. 574/1 iulie 2020.
[43]. Strategia de Securitate Cibernetică a României, pentru perioada 2022-2027. Available at: https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf. Accessed: 08.09.2025.
[44]. SR EN ISO/IEC 23053, standardul care ghidează lumea Inteligenței Artificiale. Available at: https://www.asro.ro/sr-en-iso-iec-23053-standardul-care-ghideaza-lumea-inteligentei-artificiale/. Accessed: 08.09.2025.
[45]. ORDONANȚĂ DE URGENȚĂ nr. 155 din 30 decembrie 2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil. Publicat în MONITORUL OFICIAL nr. 1332 din 31 decembrie 2024.
[46]. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng. Accesed: 18.09.2025.

[47]. Legea nr. 11/2022 pentru aprobarea Ordonanței de Urgență nr. 104/2021. Publicat în MONITORUL OFICIAL nr. 25 din 7 ianuarie 2022.
[48]. Cyber intelligence. Available at: https://www.sri.ro/cyberint. Accessed: 08.09.2025.
[49]. Guvernul României, *Carta Albă a Apărării 2021–2024*, București, 2021.
[50]. Legea nr. 218/2002 privind organizarea și funcționarea Poliției Române, Monitorul Oficial al României, Partea I, nr. 307/2002.
[51]. Legea nr. 550/2004 privind organizarea și funcționarea Jandarmeriei Române, Monitorul Oficial al României, Partea I, nr. 1175/2004.
[52]. Legea nr. 504/2002 a audiovizualului, Monitorul Oficial al României, Partea I, nr. 534/22 iulie 2002.
[53]. CNA. DECIZIE nr. 573 din 25 iunie 2025 privind Codul de reglementare a conținutului audiovizual Publicată în Monitorul Oficial al României, Partea I, nr. 641 din 8 iulie 2025.
[54]. ANCOM (Autoritatea Națională pentru Administrare și Reglementare în Comunicații). Available at: https://www.ancom.ro/. Accesed: 18.09.2025.
[55]. Agenția Națională pentru Digitalizare a României. Available at: https://www.adr.gov.ro/ Accesed: 18.09.2025.
[56]. OECD (2025). *Emerging divides in the transition to artificial intelligence*. OECD Publishing. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/emerging-divides-in-the-transition-to-artificial-intelligence_eeb5e120/7376c776-en.pdf. Accessed: 10.09.2025.
[57]. Cooperative Cyber Defence Centre of Excellence: Locked Shields Exercise Showcased the Power of Cooperative Defence. (26 iuly 2024). Available at: https://www.act.nato.int/article/ccd-coe-2024/ Accessed: 10.09.2025.
[58]. Countering hybrid threats. (May 07, 2024). Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm. Accessed: 10.09.2025.
[59]. Hybrid CoE. Available at: https://www.hybridcoe.fi/ Accessed: 05.09.2025.
[60]. The Cyber Diplomacy Toolbox. Available at: https://www.cyber-diplomacy-toolbox.com/ Accessed: 05.09.2025.
[61]. EEAS Strategic Communication Task Forces. (May 05, 2025). Available at: https://www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en?s=2803. Accessed: 012.09.2025.
[62]. Permanent Structured Cooperation (PESCO). Available at: https://www.pesco.europa.eu/. Accessed: 05.09.2025.
[63]. Digital Services Act (DSA) | Updates, Compliance. Available at: https://www.eu-digital-services-act.com/. Accessed: 12.09.2025.
[64]. EDF | Developing tomorrow's defence capabilities. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en. Accessed: 12.09.2025.
[65]. Horizon Europe. Available at: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en. Accessed: 15.09.2025.
[66]. SIMILEANU, V. (2021). România în jocul Federației Ruse. *STRATEGII XXI - Colegiul Național de Apărare* , *1* (72), 284-302.
[67]. Legea nr. 73/2025 privind controlul utilizării spațiului aerian național. Publicată în *Monitorul Oficial, Partea I nr. 462 din 19 mai 2025*.
[68]. Legea nr. 72/2025 privind desfășurarea pe timp de pace a misiunilor și operațiilor militare pe teritoriul statului român. Publicată în Monitorul Oficial, Partea I nr. 462 din 19 mai 2025.
[69]. Boboc, R. V., & Baciu, R. C. (2025). Populist Narratives on Facebook: How the Far-Right Hijacks the Romanian Discourse on the Russo-Ukrainian War. *Romanian Journal of Communication and Public Relations*, *27*(1), 25-51.
[70]. Ministerul Energiei. Strategia Energetică a României 2025–2035, cu perspectiva anului 2050. Available at: https://sgg.gov.ro/1/wp-content/uploads/2024/11/ANEXA-34.pdf. Accessed: 15.09.2025.
[71]. Ministerul Energiei. Planul Strategic Instituțional al Ministerului Energiei 2024 -2027 Available at: https://energie.gov.ro/wp-content/uploads/2023/08/Planul-Strategic-Institutional-al-Ministerului-Energiei.pdf. Accessed: 15.09.2025.
[72]. Defenseromania.ro. (Iuly 25, 2023). Un nou stat se alătură „scutului" european IrisT - Arrow 3 - Patriot condus de Germania. România participă și ea în program. Available at: https://www.defenseromania.ro/un-nou-stat-se-alatura-scutului-european-irist-arrow-3-patriot-condus-de-germania-romania-participa-si-ea-in-program_623413.html. Accessed: 07.09.2025.

[73]. Planul NATO în România. 20.000 de soldați la Constanța: numărul militarilor de la baza Kogălniceanu ar putea fi dublat. (Septembrer 04, 2025). Available at: https://www.digi24.ro/stiri/actualitate/social/planul-nato-in-romania-20-000-de-soldati-la-constanta-numarul-militarilor-de-la-baza-kogalniceanu-ar-putea-fi-dublat-3398989. Accessed: 15.09.2025.
[74]. Angajamentul privind creșterea cheltuielilor pentru apărare. (August, 2024). Available at: https://nato.mae.ro/node/1012. Accessed: 15.09.2025.
[75]. DNSC. (February 15, 2024)). UPDATE: Un atac cibernetic de tip ransomware a afectat spitale din România. Available at: https://www.dnsc.ro/citeste/atac-cibernetic-ransomware-spitale-Romania. Accessed: 18.09.2025.
[76]. Cine este Killnet, gruparea de hackeri pro-ruși care a atacat cibernetic România. (May 02, 2022). Available at: https://www.euronews.ro/articole/cine-este-killnet-gruparea-de-hackeri-pro-rusi-care-a-atacat-cibernetic-romania. Accessed: 18.09.2025.
[77]. DNSC. (Iuly 31, 2025). AVERTIZARE: Amenințările cibernetice asociate grupării Scattered Spider. Available at: https://www.dnsc.ro/citeste/avertizare-amenintarile-cibernetice-asociate-gruparii-scattered-spider. Accessed: 18.09.2025.
[78]. VEVERA, A. V., CÎRNU, C. E., & VASILOIU, I. C. Enhancing cyber security education in Romania: integrating cyber diplomacy concepts into universities curricula. *ON VIRTUAL LEARNING*, 53.
[79]. Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative. Text publicat în Monitorul Oficial, Partea I nr. 214 din 15 martie 2023.
[80]. The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. Available at: https://ccdcoe.org/. Accessed: 18.09.2025.
[81]. Cyber Europe. Available at: https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe. Accessed: 18.09.2025.
[82]. Locked Shields. Available at: https://ccdcoe.org/locked-shields/. Accessed: 20.09.2025.
[83]. Huang, L., & Zhu, Q. (2023). *Cognitive security: a system-scientific approach*. Springer Nature.
[84]. Digital skills &jobs.europa. (Iuly 30, 2024). Romania: a snapshot of digital skills. Available at: https://digital-skills-jobs.europa.eu/en/latest/briefs/romania-snapshot-digital-skills. Accessed: 20.09.2025.
[85]. HOSTILE NARRATIVE BRIEF WAR IN UKRAINE Overview of a Year of Aggression February 2022-2023 R O M A N I A. Available at: https://expertforum.ro/en/files/2023/04/HOSTILE-NARRATIVES-1-YEAR-OF-WAR-2.pdf. Accessed: 20.09.2025.
[86]. Hyve Mind. (October 16, 2024). "Gender Ideology" as a Tool of Disinformation in Romania. Available at: https://en.hive-mind.community/blog/951%2Cgender-ideology-as-a-tool-of-disinformation-in-romania. Accessed: 20.09.2025.
[87]. Ceuca, R. (2021). The Kremlin's Malign Influence Through Strategic Narratives: Sputnik's Discourse on the Relation Between Romania and NATO. The Kremlin's Influence Quarterly.
[88]. Nahoi. O. (May 12, 2023). O provocare în fața UE: reglementarea inteligenței artificiale, Available at: https://www.rfi.ro/politica-social-155762-provocare-fata-ue-reglementare-inteligenta-artificiala. Accessed: 07.02.2025
[89]. Peptan, C., Gavrilă, C., Sîrbu, L., & Mărcău, F. C. (2023). CONSIDERATIONS ON THE IMPACT OF ARTIFICIAL INTELLIGENCE ON TERORISM. *Annals of the Constantin Brancusi University of Targu Jiu-Letters & Social Sciences Series*, (1).
[90]. Carta Etică Europeană în privința utilizării inteligenței artificiale în sistemele judiciare și domeniile adiacente. Available at: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c. Accessed: 07.09.2025.
[91]. Trabucco, L. (September 21, 2023). What is Meaningful Human Control, Anyway? Cracking the Code on Autonomous Weapons and Human Judgment. Available at: https://mwi.westpoint.edu/what-is-meaningful-human-control-anyway-cracking-the-code-on-autonomous-weapons-and-human-judgment/ Accessed: 07.09.2025.
[92]. Vidu, V., Comisia Europeană anunță interzicerea în Uniunea Europeană a opt utilizări ale inteligenței artificiale, de la supravegherea în masă, la recunoașterea emoțiilor și clasificarea socială. Available at: https://www.news.ro/externe/comisia-europeana-anunta-interzicerea-in-uniunea-europeana-a-opt-utilizari-aleinteligentei-artificiale-de-la-supravegherea-in-masa-la-recunoasterea-emotiilor-si-clasificarea-sociala1922405705002025021021923593. Accessed: 07.09.2025.
[93]. Recomandarea privind etica inteligenței artificiale. UNESCO. Available at: https://www.cnrunesco.ro/uploads/media/f1077_recomandari-unesco-ai-site.pdf. Accessed: 07.09.2025.