BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# FIMI and Collective Security: The Role of Information Manipulation on Contemporary International Relations

**Daniel-Horea BOGDAN***

*MA in security studies, Babes-Bolyai University, Faculty of History and Philosophy, Cluj-Napoca, Romania
e-mail: bogdan.danielh@yahoo.com

## Abstract

This article evaluates the strategic reconfiguration of the European Union, marking the transition from conventional methods of combating disinformation to the implementation of the paradigm of Foreign Information Manipulation and Interference (FIMI). In the current security architecture, this concept becomes the central pillar in the process of securitization of the European information space. The article starts from the assumption that the geopolitical dynamics of 2026 are defined by volatility, and the conclusions of the report of the European External Action Service (EEAS) on the multiplication of hybrid state-origin aggressions validate this hypothesis. Attention is concentrated on Romania's structural vulnerabilities, as state actors can exacerbate internal crises to fragment societal cohesion and induce political instability. The study shows that, in the specific context of the eastern flank, defensive architecture can no longer be limited to an exclusively military or technological response. The results highlight the need for citizen-level cognitive resilience, making media literacy a vital component of national security. It is also necessary to adopt the „whole-of-society" model, supported by inter-institutional cooperation, which guarantees the integrity of democratic processes in the face of an information war in permanent development.

**Keywords:**
Insecurity; Risks; Threats; Vulnerabilities; Hybrid Warfare; Manipulation; Cognitive Resilience.

**Article info**
Received: 13 February 2025; Revised: 25 February 2025; Accepted: 18 March 2025; Available online: 8 April 2026

Citation: Bogdan, D.H. 2026. "FIMI and Collective Security: The Role of Information Manipulation on Contemporary International Relations." *Bulletin of "Carol I" National Defence University*, 15(1): 29-38. https://doi.org/10.53477/2284-9378-26-02

## Preliminary considerations

In the contemporary strategic context, controlling the information field is no longer just an extension of public diplomacy, as it has become a critical component of national security and the strategic sector. The current relevance of the theme is imposed by unpredictable developments in the security environment, where hostile actors have modernized their modes of operation. The scientific novelty of this paper lies in the application of the new FIMI Exposure Framework, introduced in March 2025, on the specific vulnerabilities of the information space in Romania. The central objective is to examine how the EU, through the EEAS, has redefined the fight against disinformation under the integrated concept of FIMI, as well as the way in which aggressor countries adapt their techniques to pass under the radar of responsible institutions, with the main purpose of eroding citizens' trust in national defense and security institutions.

The research question of the paper is the following: to what extent does the adoption of the FIMI structure support the transition to a proactive position in securing the Romanian information space? Methodologically, the study uses a qualitative analysis of strategic documents published by NATO and the EEAS (2022-2025 period) to identify those mechanisms that contribute to reconfiguring national resilience. Thus, the research explains how this theoretical concept is translated into practical mechanisms that strengthen the resilience of the state in the face of external interference. This research method allows identifying the mechanisms by which information is transformed into a weapon by hostile actors, facilitating the securitization of digital space through rigorous attribution methods. The impact assessment is carried out through three operational indicators: the complexity of the technical infrastructure, the mapping of tactics through DISARM (Disinformation Analysis and Risk Management), and the analysis of the impact on the cognitive resilience of the Romanian population.

The practical importance of the study lies in the ability to identify the most important strategic assumptions related to the fight against FIMI that Romania can use as a collective response, together with the organizations it is part of, namely the EU and NATO. From a methodological point of view, the research expands by analyzing statistical data related to the impact of hybrid threats on national stability, providing an applied perspective on how Russian proxies act on the eastern flank. The analysis investigates the mechanisms of content localization and the use of artificial intelligence for the penetration of narratives in the Romanian cognitive space, identifying the vulnerabilities that state actors turn into security vulnerabilities.

The shift from reactive content analysis to proactive identification of handling infrastructures under the DISARM framework is the foundation of a new security culture. The evolution of this new paradigm depends fundamentally on how effectively the "whole-of-society" concept is implemented, which extends protection

beyond the technical barriers of infrastructure to the information security of the population. The research aims to provide answers that could be included in sustainable resilience strategies, and the approach supports efforts to strengthen the security of the digital ecosystem in Romania, adapting it to current challenges.

## Conceptual clarifications

To substantiate the study, it is necessary to delimit the concept of securitization, defined as the act by which a problem is transformed from an ordinary political matter into an existential threat to a related object (Stritzel 2014). In the Strategic Compass 2022 vision, the information space is seen as an area of struggle where the EU must assume a proactive defensive posture (European Council 2022).

Hybrid warfare is a type of conflict that uses conventional operations with subversive, asymmetric, and non-linear methods. This type of conflict requires an instrumentalization of information vectors, which are subordinated to well-defined strategic interests. In this respect, the core of the hybrid conflict lies in the ability to speculate on the internal fragilities of the target states, be they political, social, or technological. They take place in a grey area of security, where the classic distinction between peace and belligerence is deliberately uncertain (NATO 2022), turning uncertainties into a tactical advantage.

The development of the analysis of the phenomenon requires the conceptual clarification of the notions present in the paper, disinformation, and FIMI. Disinformation is false or misleading information spread with the intent to deceive or cause harm. It can occur in the form of deliberately manufactured or manipulated audio/visual content, intentionally created conspiracy theories, or widespread rumors to harm or cause mistrust between citizens (Commons Social Change Library 2023).

As regards the Manipulation and Interference of Foreign Information (IMIF), it can no longer be seen as an isolated phenomenon, but as a systematic threat to the information balance and electoral processes. By deliberately eroding trust in the democratic apparatus, such actions directly target the integrity of the online environment. External actors manage to fracture social cohesion precisely by resorting to a mix of malicious tactics, techniques, and procedures (TTP), strategically disseminating narratives that alter public perception and weaken the foundation of the security of democratic countries (International IDEA).

The evolution from disinformation to FIMI marks a paradigm shift towards the analysis of coordinated manipulative behavior (EEAS 2025). This dynamic fits into the logic of hybrid and non-linear warfare, where the boundary between peace and conflict becomes intentionally uncertain, and national resilience is eroded by non-kinetic means (Global Security Review 2024). As mentioned in the Hybrid CoE report,

these aggressions are turning the entire society into a potential front, where aggression is no longer marked by a formal act of declaring war (Hybrid CoE 2023). State actors invest heavily in reflective control, manipulating the opponent's perception to get him to make decisions that serve his own strategic interests (NATO 2023).

The empowerment of the European institutions and NATO allies to adapt their defensive measures to combat and defend against disinformation facilitated the transition from a descriptive to an operational analysis. The DISARM framework allows handling operations to be broken down into a "kill chain" (attack chain) model, facilitating the reduction of FIMI incidents in their sequential phases (EEAS 2025). By mapping OCTs, ranging from bot creation and web domain acquisition to using AI to impersonate legitimate media sources, raw data is turned into strategic information (Commons Social Change Library 2023). This methodological approach underpins the transition to a proactive defense, giving Romania and European partners the ability to secure the digital space through rigorous attribution and classification methods.

Controlling the information field has thus surpassed the scope of public communication, becoming a critical component of the global information warfare (EEAS 2025). In this context, manipulation of information directly interferes in the internal affairs of countries, autocratic regimes using disinformation as a key non-kinetic activity against liberal democracies (Cenușă 2024). This systemic threat endangers the integrity of electoral processes and social cohesion through manipulative narratives that threaten the structure of the democratic community (International IDEA 2026).

## Operations, architecture, and FIMI exposure framework

The strategic transition operated by the EEAS from the simple monitoring of disinformation content to the proactive identification of technical infrastructures, the introduction of which in 2025 was the FIMI Exposure Framework. It provides a systematic model of classification of sources of influence in four fundamental blocks, allowing decision makers to identify the degree of involvement of a foreign actor in disrupting the information space of a democratic state (EEAS 2025); in this case, the Russian Federation.

At the top of this pyramid are official state channels, representing the direct voice of governments through ministries or diplomatic representations, followed by state-controlled platforms, which are entities that benefit from public funding and government editorial direction, such as RT or Sputnik (EEAS 2025). Much more complex, however, is the basis of this architecture, consisting of channels with hidden state links, identified by technical indicators such as shared IPs (Internet Protocol) or shared hosting services, and non-attributed aligned channels. The latter represent the biggest security challenge, accounting for 76.5% of the investigated architecture,

as they allow the dissemination of malignant narratives without a proven formal link, facilitating "the washing of information" through networks that seem independent (EEAS 2025).

This classification is not only a theoretical exercise, but also a necessary tool for the securitization of digital space, given that FIMI actors systematically exploit anonymity to avoid legal and diplomatic liability. The analysis of manipulative behavior, rather than the truth of the content, allows the identification of coordinated aggression patterns aimed at societal stability (Proto et al. 2025). An eloquent example of this is the Russian Federation, because it is an actor that has developed this multi-level strategy to advance long-term geopolitical goals by creating instability among citizens of the target states (EEAS 2025).

Modern FIMI operations are characterized by outstanding technological adaptability, unfolding on multiple platforms to create "rooms of ideological echo". EEAS data indicates a massive concentration of activity on the X platform (formerly Twitter), which attracted 88% of detected incidents, due to the proliferation of CIB accounts (Coordinated Inauthentic Behavior) and the ease of generating fake accounts. The diversification of OCTs includes the use of AI to automate bot networks and create large-scale content, reducing operational costs for the aggressor. In 2024, the use of AI in creating audio-video deepfakes has become a current method to enhance the emotional impact of disinformation (EEAS 2025).

To increase the credibility of these narratives, aggressors frequently resort to impersonation, which refers to usurping the identity of legitimate media outlets such as the BBC and localizing the content. The latter involves the cultural and linguistic adaptation of messages to resonate with the specific vulnerabilities of the local public, transforming information into a weapon adapted to the national context. The operational analysis of these structures through DISARM enables proactive response to identify bullying in the planning phase (EEAS 2025).

## Collective security and hybrid aggression

Current hybrid activities against NATO member states have moved past classic conflict models, prioritizing the psychological dismantling of public institutions over kinetic destruction. The goal is clear: to compromise the integrity of the rule of law using a calculated mix of disinformation and sabotage. This threat is distinct not just in its intent, but in its execution—the speed and magnitude of today's information activities are a direct result of the pervasive nature of digital platforms and the emergence of disruptive technological tools (NATO 2024).

From the Alliance's perspective, collective security in the 21st century requires an integrated approach centered on societal resilience. Resilience has become NATO's first line of defense, defined by the ability of societies to resist, adapt, and recover

quickly from attacks targeting key state functions (NATO 2024). This layered defense requires close cooperation in the public sector, the private sector, and civil society, and is not limited to post-incidental reactive responses, but invests in strengthening digital literacy and strategic partnerships with the EU. NATO's role in the current collective security architecture is to secure a stability framework that protects not only territorial integrity, but also information flows and democratic processes against any coordinated foreign interference (Homaniuk et al. 2026).

The analysis of Romania's vulnerabilities in the face of foreign manipulation actions requires a direct reporting to the security pillars defined by the National Defence Strategy for the Country 2025-2030. The document bases the process of securitization of the information space, defining disinformation and hybrid actions not only as risks but as direct threats to constitutional stability and social cohesion. An identified critical vulnerability is „the insufficient involvement of resilience in society in front of subversive narratives", which allows FIMI actors to explore citizens' mistrust in state institutions and European values. This weakness is amplified by a heterogeneous level of media literacy, which makes the population an easy target for emotional manipulation campaigns (CSAT 2025).

In the context of coordinated information manipulation, SNAT stresses that „the social and economic cleavages" inside Romania are transformed by Russian proxies into security breaches, used to generate polarization and undermine the national consensus regarding the Euro-Atlantic orientation. Another structural weakness mentioned in the document is „the vulnerability of digital critical infrastructures", which, in the absence of mechanisms for controlling false content, facilitates the rapid propagation of propagandistic messages. This technical vulnerability is associated with „dependence on external technological platforms", where recommendation algorithms may involuntarily favor the distribution of malignant narratives (CSAT 2025).

State actors also promote identity and sovereignty themes to provoke a political and military decision-making deadlock. Thus, the cognitive resilience of the population is a strategic objective, because the attack no longer targets only the physical infrastructure, but the decision-making process. SNAT proposes the transition from a reactive to a preventive approach, focusing on security education as a deterrent against hybrid aggression (CSAT 2025). This vulnerability is at the core of the current hybrid conflict on the eastern flank, requiring close collaboration between the institutions of force and civil society. Romania is a priority target on the eastern flank, as it is the target of complex FIMI operations that reflect the Russian doctrine of "information confrontation".

The role of the Russian Federation as an FIMI actor reflects the perception of the information space as an active area of combat, because it uses official tools (diplomacy, state media) and unofficial (proxy networks, troll farms), and due to these considerations, FIMI tactics are transformed into a major security concern

for Romania and the European Union. Operation Matryoshka is a sophisticated campaign of influence and disinformation coordinated by pro-Russian actors, identified and monitored intensively since 2023 and 2024. It works according to the principle of Russian dolls (a narrative hidden in another) and has as its main objective the flooding of the European information space with messages aimed at undermining support for Ukraine and creating mistrust in democratic institutions (EEAS 2024). The success of the operation Matryoshka is dependent on the degree of preexisting social fragmentation in Romania, because it is posted in the digital space with contradictory narratives, putting the Romanian state in a defensive posture.

In the current geostrategic framework, Romania ceased to be only a country of proximity, becoming a central pillar of the eastern flank and a priority target for hybrid operations carried out under the Russian security doctrine. The analysis reveals a transition to a permanent information confrontation, where information is used as a weapon to erode state cohesion and democratic stability. This strategy is based on the concept of "active measures", adapted to the digital era by the Russian intelligence services, whose purpose is not only to convince the audience of an untruth but to erode the very ability of the company to distinguish reality, thus causing a decision-making block at the political level (Global Security Review 2024; EEAS 2025).

Romania's vulnerability to FIMI is accentuated by the tactical exploitation of internal cleavage points. Russian proxies use content localization to adapt narratives to the national context, instrumenting themes that present NATO as a factor of insecurity. This ecosystem, exemplified by networks such as RT and Sputnik, uses "reflective" control techniques to manipulate public perception. By posting conflicting narratives about national security in the digital space, the aggressor leads Romanian institutions to adopt a defensive, reactive, and inefficient position, transforming a stable ally into an internal fractured state (Cenușă 2024). Moreover, the technique of "mirroring" through false "fact-checking" initiatives, such as the Global Fact-Checking Network, serves to discredit legitimate organizations and official media channels, leaving citizens in a dangerous informational vacuum (Prysiazhniuk 2025).

Romania's resilience cannot be ensured exclusively by technical regulations, but requires a cognitive immunization of the population through a "whole-of-society" approach. The EU has substantiated this response through the Digital Services Act (DSA), which imposes transparency obligations on digital platforms; through operational pillars such as the Rapid Alert System (RAS) and media literacy projects (EDMO) (EEAS 2025; CEDEM 2025). The effectiveness of external interference on the eastern flank is directly proportional to pre-existing cognitive vulnerabilities. The integrity of democratic processes depends on the transition from a "deterrence posture by denying" using political attribution and diplomatic sanctions in fora such as G7 and NATO (International IDEA 2026; NATO 2024). It is necessary to integrate DISARM-based behavioral monitoring into national defense strategies, thereby

ensuring that the information ecosystem is protected from non-linear warfare (Global Security Review 2024; EEAS 2025).

## Conclusions

This article looked at the strategic transition from the simple management of disinformation to the FIMI framework, which is not just a terminological change but a fundamental redefinition of the concept. The analysis of the phenomenon confirms that the information space has become an active operational field, where geopolitical conflicts are carried out through digital tools of "reflective control". From the applied assessment on the national context and recent strategic documents, such as the National Defence Strategy for the Country 2025-2030 and Strategic Compass 2022, the results are derived that confirm the central hypothesis of the research: the adoption of the FIMI framework facilitates the transition from reactive to proactive defense by shifting the focus from content monitoring to identifying manipulative infrastructures.

A fundamental result of the research indicates that the FIMI Exposure Framework may allow Romania to go beyond the traditional "debunking" model in favor of early identification of attack infrastructures. Following the application of operational indicators, technical data, such as common IP addresses and bot networks, can be identified, allowing the phenomenon to be limited before it produces social effects. By applying the "kill chain" methodology within DISARM, institutions with responsibilities in national security can intervene in the early stages of planning. This approach transforms disinformation from a simple miscommunication into a complex hybrid attack, designed to break the cohesion of allied states and undermine the rules-based international order.

The research underlines that cognitive resilience, supported by the expertise of European and national institutions, is currently the fundamental basis of national defense. The results of the analysis indicate that the effectiveness of external interference is directly proportional to pre-existing cognitive vulnerabilities and to the heterogeneous level of media literacy of the population. This requires a paradigm shift, and media literacy needs to be integrated as the central pillar of national security, being the only sustainable barrier against attempts of "reflective" control aimed at decision-making.

The analysis applied to influence and disinformation campaigns, such as Matryoshka, demonstrated that Romania is facing an infrastructure of "permanent information confrontation. The success of Russian campaigns on national territory depends fundamentally on the degree of social fragmentation and the exploitation of radical narratives. Looking towards the strategic horizon of 2026, Romania's stability seems to depend fundamentally on the success of a strategy that is not limited to the institutional level, but to integrate civil society into the defense mechanism

against disinformation. It is not just a simple application of European rules, such as the Digital Services Act (DSA), but a much more complex articulation. This implies, on the one hand, the need for technology platforms to have a real responsibility in limiting disinformation messages and, on the other hand, creating an individual security culture. No regulation, however well-structured, can achieve its goal if there is a lack of public conviction in the reaction capacity of states. This solid trust is the foundation on which the resistance of a society is built in the face of information warfare tactics.

The strategic horizon of Romania depends on the ability to implement early warning mechanisms and facilitate an open dialogue between the state, academia, and the private sector. By adopting measures of "pre-bunking" (inoculation of information), the state can prevent the spread of false information by acting proactively in the face of hybrid destabilization strategies; more specifically, it can limit them before they produce profound effects in society. The FIMI analysis confirms that the information space is an operational field, where geopolitical conflicts are also carried out by digital means. Disinformation is no longer miscommunication, but a hybrid attack designed to break the cohesion of states and undermine the rules-based international order. In the absence of a culture of information resilience, digital vulnerabilities will continue to be exploited by state actors to turn the eastern flank into an area of strategic instability.

The limits of this research lie in the extreme volatility of the technical infrastructures used by FIMI actors, which can change their digital footprint faster than official reports can be updated. Moreover, an important conceptual limitation is the difficulty of isolating the impact of FIMI from organic social cleavages. The data suggest that the success of disinformation is often conditioned by pre-existing internal vulnerabilities, which makes the distinction between an authentic, albeit polarized, opinion and an artificially amplified narrative remain, in some cases, analytically subjective. More than just a theoretical assessment, future studies should assess the pragmatic effectiveness of the EU and NATO response in identifying sources of disinformation and their operational capabilities.

## References

**CEDEM (Centre for Democracy and Rule of Law).** 2025. "What is Foreign Information Manipulation and Interference (FIMI) and how does it affect democracy?" https://cedem.org.ua/en/news/fimi/.

**Cenușă, Denis.** 2024. "Disinformation Narratives Driven or Beneficial to Russia: The Case of Moldova." Policy Paper, Eastern Europe Studies Centre (EESC), pp. 1–21. https://www.gssc.lt/wp-content/uploads/2024/04/v02_Cenusa_Russias-disinformation-in-Eastern_Europe_EN_A4.pdf.

**Commons Social Change Library.** 2023. "Disinformation and 7 Common Forms of Information Disorder." https://commonslibrary.org/disinformation-and-7-common-forms-of-information-disorder/.

**CSAT (Consiliul Suprem de Apărare a Țării).** 2025. "National Defence Strategy of the Country (SNAT) 2025-2030". https://www.presidency.ro/ro/media/csat/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2025-2030.

**EEAS (European External Action Service).** 2024. "2nd EEAS Report on Foreign Information Manipulation and Interference Threats". https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

**___.** 2025. "3rd EEAS Report on Foreign Information Manipulation and Interference Threats." https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

**European Council.** 2022." A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security". https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

**Global Security Review.** 2024. „Hybrid and Non-Linear Warfare Systematically Erases the Divide Between War & Peace." https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/.

**Homaniuk, Oleksandr, Yevheniia Vozniuk, Olena Borysiuk, Viktor Kobets, and Hryhorii Zeleniuk.** 2026. "FIMI VS DISINFORMATION: IMPACT ON DIGITAL SECURITY AND PUBLIC ORDER IN THE EU." *Veredas do Direito* 23 (4): e234678. https://revista.domhelder.edu.br/index.php/veredas/article/view/4678/26742.

**Hybrid CoE.** 2023. "Trends in Hybrid Threats". https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf.

**International IDEA.** 2026. „Foreign Information Manipulation and Interference (FIMI)." https://www.idea.int/theme/foreign-information-manipulation-interference-fimi.

**NATO.** 2022. „Strategic Concept." Adopted by Heads of State and Government at the NATO Summit in Madrid. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2022_06/20220629-220629-strategic-concept.pdf.

**___.** 2024. "Countering Hybrid Threats." https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats.

**NATO Allied Command Transformation.** 2023. "Strategic Concept." https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf.

**NATO CCDCOE.** 2024. "Cyber Defence and Information Operations: Strategic Perspectives". https://ccdcoe.org/uploads/2024/05/CyCon_2024_book.pdf.

Proto, Lucas, Paula Lamoso-González and Luis Bouza García. 2025. "The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight." *Media and Communication* 13 (Article 9474): 1–15. https://doi.org/10.17645/mac.9474.

**Prysiazhniuk, Marianna.** 2025. "Strategic Narratives and Information Warfare: Russian FIMI Campaigns against Ukraine's Armed Forces in the Context of War and Societal Impact." *Culture. Society. Economy. Politics* 5 (1): 88–108. https://doi.org/10.2478/csep-2025-0007.

**Stritzel, Holger.** 2014. *Securitization Theory and the Copenhagen School.* In: *Security in Translation. New Security Challenges Series.* Palgrave Macmillan, London. https://doi.org/10.1057/9781137307576_2.