BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Hybrid Crisis Management: An Integrated Response to Contemporary Asymmetric Threats

Cristiana Maria ALMAȘAN, PhD Candidate*

*Bucharest University of Ec0nomic Studies, Romania
e-mail: cristianaa.almasan@gmail.com
https://orcid.org/0009-0009-6789-9149

Abstract

This article examines the transformation of hybrid conflict over the period 2007-2024 and its impact on the resilience of states within the Euro-Atlantic area, with an emphasis on the interaction among the cyber, information, economic, and legal-political dimensions. Methodologically, the study employs a comparative case-study approach, to highlight variations in vulnerability and institutional responses to hybrid threats. The analysis integrates a resilience-cycle framework, correlated with a multidimensional operational taxonomy. The results indicate a structural mutation of hybrid conflict, in which information and cyber instruments become central to the production of strategic effects. The study also highlights the consolidation of internal mobilisation and offensive legal actions (lawfare) as distinct vectors of hybrid power that are insufficiently integrated into existing theoretical and normative frameworks. The principal conclusion shows that institutional and societal resilience constitutes the essential condition of contemporary deterrence, being determined by the coherence of the normative framework, operational capacity, and the level of investment in cyber and information security. The study proposes an integrated analytical framework for the assessment and management of hybrid threats, with relevance for national and Euro-Atlantic security policies.

Keywords:

Hybrid Conflict; Institutional Resilience; Cybersecurity; Disinformation; Information Warfare; Generative Artificial Intelligence; Euro-Atlantic Security; Prevention; NATO; the European Union.

Article info

Received: 4 April 2026; Revised: 30 April 2026; Accepted: 3 June 2026; Available online: 30 June 2026

Citation: Almașan, C.M. 2026. "Hybrid Crisis Management: An Integrated Response to Contemporary Asymmetric Threats" *Bulletin of "Carol I" National Defence University* 15(2): 285-310. https://doi.org/10.53477/2284-9378-26-29

Introduction

The evolution of the international security environment over the past decade reveals a structural change in the nature of conflict: conventional military means are increasingly replaced or complemented by instruments that operate below the legal threshold of armed conflict, targeting the political, economic, social, and information vulnerabilities of the adversary state. These actions, known in the specialised literature as hybrid conflict, are not a new reality but rather an extension of historic practices of subversion, today amplified by technological advances, by generative artificial intelligence, and by the high degree of interconnection of modern societies (Hoffman 2007; Renz 2016; Cullen and Reichborn-Kjennerud 2017).

What renders this theme acutely topical is the unprecedented simultaneous overlap of hybrid threats of different kinds within the same geographical area and the same temporal interval. The large-scale Russian invasion of Ukraine, launched in February 2022 and ongoing at the time of writing, demonstrated that hybrid and conventional actions are not mutually exclusive but can combine synergistically. In parallel, disinformation campaigns amplified by artificial intelligence, cyber actions directed against NATO critical infrastructure, and proven electoral interference in several member states, including Romania (2024), have shown that no country is sheltered from such aggressions (ENISA 2024; CCDCOE 2024; SRI 2023).

A methodological clarification is required regarding the analytical framework adopted. The specialised literature operates with several competing taxonomic systems: PMESII (Political, Military, Economic, Social, Information, Infrastructure), used in NATO operational planning and in intelligence analysis (Giannopoulos, Smith and Theocharidou 2021; NATO 2022); DIME (Diplomatic, Information, Military, Economic), established in American strategic doctrine (Chambers 2016; Hoffman 2007); and MPECI (Military, Political, Economic, Civil, Information), present in certain European Union documents. At the same time, the term hybrid conflict coexists with competing concepts in academic literature: full-spectrum warfare denotes the synchronised use of all instruments of power across the entire spectrum of conflict (Hoffman 2007; Fridman 2018); parallel warfare describes the simultaneous attack on multiple critical systems of the adversary with the aim of overwhelming its capacity to respond (Warden 1995); and shadow warfare emphasises the deliberately undeclared and ambiguously attributable character of the actions (Mumford 2013; Berzins 2014). The present study employs the term hybrid conflict as a concept established in NATO doctrine, recognising that the three alternative terms are complementary, each illuminating a different dimension of the phenomenon: the breadth of instruments, the logic of their synchronisation, and strategic ambiguity, respectively, all of which dimensions are incorporated into the proposed model. The functional six-domain structure adopted is logically compatible with PMESII, but adapted for operationalisation at the level of crisis management and national institutional resilience.

The present study proceeds from the observation that the academic literature often treats hybrid threats either from an exclusively military perspective or from an exclusively cyber or information one, without proposing an integrated framework of analysis and response. Accordingly, the objectives of the research are: (1) to develop an updated functional taxonomy of hybrid instruments, compatible with contemporary analytical frameworks; (2) to construct a model of crisis management with named actors and quantifiable indicators; (3) to undertake a comparative assessment of Romania's resilience capabilities relative to states with consolidated experience; and (4) to formulate concrete public-policy recommendations. The methodology combines an analysis of strategic documents adopted at the level of NATO, the European Union, and the states examined, a synthesis of recent academic literature, and an analysis of institutional reports published over the period 2022-2024 (Strachan-Morris 2022; Giannopoulos, Smith, and Theocharidou 2021).

The structure of the article reflects these objectives: section 1 elaborates the conceptual framework and the taxonomy of hybrid threats; section 2 proposes the integrated crisis-management model; section 3 analyses six documented cases; section 4 assesses the specific case of Romania; section 5 formulates conclusions and public-policy recommendations.

1. The conceptual framework of hybrid conflict

1.1. The evolution of the concept of hybrid conflict

Although the term hybrid conflict was established in the specialised literature through the work of Hoffman (2007), the phenomenon it describes is not new. The combination of military means with political, economic, and propagandistic pressure has been systematically practised throughout history; the novelty lies in the speed, scale, and degree of coordination with which this combination can today be orchestrated, also through generative artificial intelligence (Fridman 2018; Gioe, Goodman, and Omand 2022). Gerasimov (2013) outlined a doctrinal vision according to which the weight of non-military means had exceeded that of strictly military instruments, inverting the paradigm of the conflicts of the previous century. Galeotti (2018) subsequently tempered this interpretation, noting that Gerasimov's text reflected an observed reality rather than a prescriptive plan of action, while Thomas (2016) demonstrated that the Russian doctrine of reflexive control constitutes the theoretical substratum that unifies hybrid instruments within a coherent strategy. The developments of the period 2022-2024 provided factual confirmation of this doctrinal reading.

At the institutional level, NATO formulated an operational definition in the Warsaw Summit Communiqué (2016), reaffirmed and deepened in the Madrid Strategic Concept (2022): hybrid threats denote actions that articulate military and non-military means, conducted in a coordinated manner to destabilise a state or an alliance without reaching the threshold that would trigger a collective response

under Article 5 of the North Atlantic Treaty. Through the same document, Russia was explicitly designated as the most direct and severe threat to the Alliance, while China was characterised as a source of systemic challenges (NATO 2022). The European Union, through document JOIN (2016)18 and, more recently, through the NIS2/CRA legislative package (2022-2024), has expanded the normative framework for responding to hybrid threats (Fiott and Parreira 2020).

1.2. An updated taxonomy of hybrid threats

The debate concerning the analytical frameworks of hybrid threats reflects the rapid evolution of the field of study. PMESII, developed within the NATO doctrinal environment, structures the variables of analysis along six dimensions: Political, Military, Economic, Social, Information, and Infrastructure. The principal advantage of this framework lies in its comprehensiveness and in its capacity to integrate infrastructure vulnerabilities as an autonomous variable; its limitations relate to the complexity of operationalisation at the level of national planning (Giannopoulos, Smith, and Theocharidou 2021). DIME organises the instruments of state power along four axes: Diplomatic, Information, Military, and Economic. Its advantage consists in strategic clarity; its limitations reside in the subordination of the civil dimension to the military and diplomatic axes (Chambers 2016; Hoffman 2007). MPECI, present in certain European Union documents, explicitly distinguishes the civil component from the military and political ones, but underestimates infrastructure vulnerabilities and does not include a domain dedicated to internal mobilisation and offensive legal actions. The present study adopts a functional six-domain structure, logically compatible with PMESII, but adapted for operationalisation at the level of crisis management and national institutional resilience. This choice does not amount to a reduction of PMESII, but to a reconfiguration oriented towards a precise analytical purpose: the mapping of hybrid-threat vectors in correlation with the response capabilities of a given national framework.

Table 1 sets out the revised taxonomy, organised into six functional domains. Compared with earlier versions (Cullen and Reichborn-Kjennerud 2017; Giannopoulos, Smith şi Theocharidou 2021), the present structure introduces several new elements: the use of generative artificial intelligence in information influence operations, the sabotage of submarine infrastructure, pressure on supply chains as an economic vector, and, as a sixth distinct domain, internal mobilisation and offensive legal actions, instruments empirically confirmed in recent cases but absent from the established taxonomies.

The data in Table 1 show that cyber and information instruments are the most frequently used in the documented hybrid conflicts of recent years, with a significant intensification from 2022 onwards. The use of generative artificial intelligence to produce falsified content at scale and to personalise disinformation messages makes detection and attribution significantly more difficult. The sabotage of physical infrastructure, illustrated by the incidents in the Baltic Sea (2023-2024), indicates a

TABLE 1. Taxonomy of hybrid threats: domains, instruments, and documented cases (2024)

Functional domain	Principal instruments	Recent documented cases
Cyber	Saturation attacks (DDoS); advanced persistent infiltration (APT); sabotage of industrial control systems (ICS)	Estonia (2007); Ukraine power grid (2015-16); Viasat (2022); Sandworm/Industroyer2 (2022)
Informational	Systematic disinformation; AI-generated digital forgeries; amplification through automated networks; electoral influence	Electoral interference Romania (2024); Moldova (2023-24); pro-Russian campaigns EU (2023-24)
Economic	Energy blackmail; selective trade restrictions; hostile acquisitions in sensitive sectors; coordinated diplomatic pressure	Russo-Ukrainian gas blockages (2006, 2009, 2021); reductions in gas deliveries to Europe 2021-22
Sub-threshold military	Unmarked forces; private military companies; support for separatists; physical-infrastructure sabotage	Crimea (2014); eastern Ukraine (2014-22); Baltic submarine cables (2023-24)
Social-political	Financing of extremism; exploitation of identity tensions; corruption of elites; subversion of democratic processes	Financing of European parties; Romania elections 2024
Internal mobilisation / Offensive legal actions	Recruitment of the diaspora and minorities; instrumentalisation of legal rights; orchestrated strikes and judicial blockages	Russian minority in the Baltic states (2007-present); instrumentalised judicial actions in the EU; mobilisations in Romania 2024

Source: Compiled by the author on the basis of the specialised literature (Hoffman 2007; Berzins 2014; Cullen and Reichborn-Kjennerud 2017; IISS 2023) and the reports of ENISA (2024), CCDCOE (2024), and SRI (2023).

shift towards the sub-threshold military domain. A domain insufficiently formalised in earlier taxonomies, but empirically confirmed by recent cases, is that of internal mobilisation and offensive legal actions: the recruitment and activation of a state's own citizens or of minorities within the target state, as well as the instrumentalisation of legitimate legal mechanisms, such as judicial proceedings, the right to strike, and freedom of assembly, in order to paralyse the functioning of democratic institutions (Renz 2016; Giannopoulos, Smith and Theocharidou 2021; Thomas 2016).

1.3. The comparative intensity of hybrid instruments across the cases analysed

Figure 1 presents the evolution of documented hybrid incidents within the Euro-Atlantic area over the period 2015-2024, the author's own processing on the basis of the ENISA cyber threat-landscape reports (2023, 2024) and the cyber-incidents database of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE 2024). Figure 2 presents a radial analysis of instrumental intensity across six selected cases covering the period 2007-2024, on the basis of ENISA (2023, 2024), CCDCOE (2024), SRI (2023), DNSC (2023), and Tikk et al. (2008).

Figure 1 brings into focus three trends of particular significance. On the one hand, the rapid pace of growth in the number of recorded hybrid incidents reflects both the escalation of hostile pressure and the progress achieved in identification and attribution mechanisms. Secondly, the large-scale Russian invasion of Ukraine

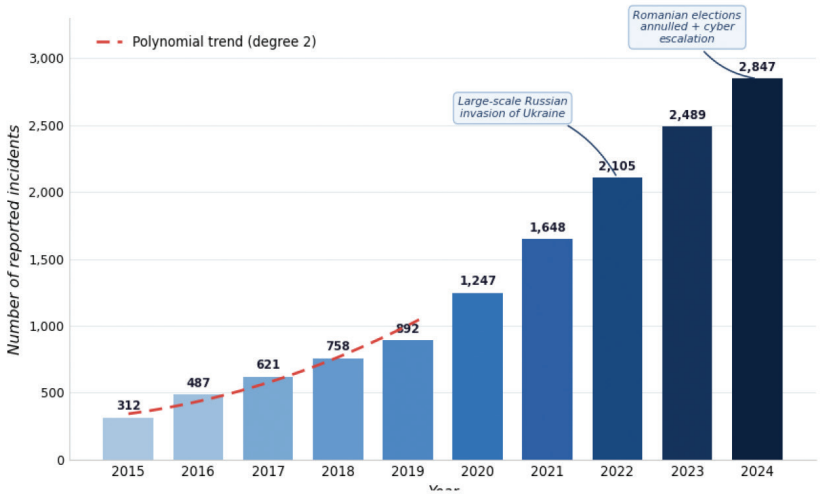

Figure 1 The evolution of hybrid incidents within the Euro-Atlantic area
Source: the author's own processing on the basis of the ENISA Threat Landscape Report (2023, 2024) and the CCDCOE Cyber Incidents Database (2024). 2024 data: preliminary estimate based on the ENISA Q1-Q3 2024 reports.

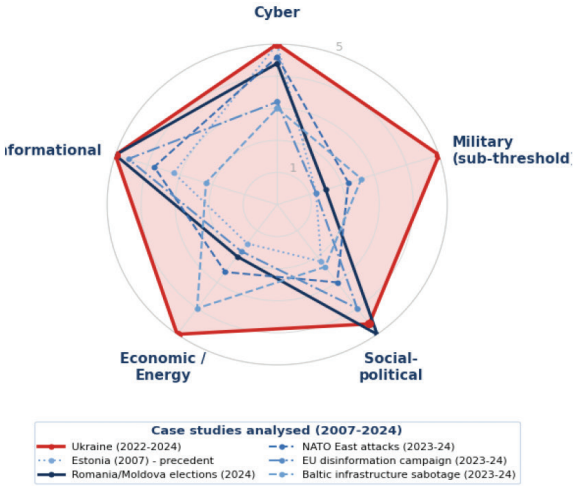

Figure 2 compiled by the author based on ENISA (2023, 2024), CCDCOE (2024), SRI (2023), DNSC (2023), and Tikk et al. (2008).

(2022) marks a qualitative rupture: the annual frequency of incidents doubled compared with 2021, and the typology of attacks diversified towards domains with direct physical impact. Thirdly, the European and national electoral cycle of 2024 confirms that democratic processes constitute a priority target of contemporary hybrid campaigns.

Figure 2 allows the identification of three profiles of hybrid engagement. The first profile, illustrated by the case of Ukraine (2022-2024), is the fully integrated one, with maximum intensity across all six functional domains. The second profile, exemplified by Romania 2024 and Moldova 2023-2024, is of an information-

electoral type, conducted without any explicit military component. It illustrates that hybrid threats are capable of producing strategic-level effects without exceeding the threshold of armed force. The third profile, illustrated by Estonia 2007 and the sabotage of Baltic infrastructure, is the cyber and physical one.

2. The integrated model for managing hybrid crises

2.1. Guiding principles

The literature on crisis management (Boin et al. 2016; Rosenthal, Boin, and Comfort 2001; Ansell, Boin, and Keller 2010) and the doctrinal documents of NATO and the European Union converge on a number of principles whose observance conditions the effectiveness of the response to hybrid threats. The first principle, that of anticipation, proceeds from the observation that hybrid aggressions are built up gradually, through the accumulation of small-scale disturbances which, viewed in isolation, do not exceed the level of a crisis (Giannopoulos, Smith, and Theocharidou 2021). The second principle is inter-institutional coordination: the effectiveness of the response depends on the capacity to synchronise the actions of institutions with different organisational cultures, legal mandates, and chains of command (Strachan-Morris 2022; Chambers 2016). The third principle is that of coherent public communication (Pamment et al. 2018). A fourth principle, absent from the earlier literature, concerns technological adaptability: response structures are required to assimilate artificial-intelligence instruments for the detection, assessment, and attribution of threats (Gioe, Goodman, and Omand 2022).

2.2. The structure of the four-phase model

The construction of the proposed model drew on two reference frameworks well established in the literature of the field. The first is the four-phase crisis-management model elaborated by Boin et al. (2016): crisis identification, decision-making, coordination of actions, and public communication. This model, although comprehensive for classic crises, does not incorporate the cyber dimension as an autonomous prevention phase, does not integrate the recent European normative framework, and does not name responsible actors with measurable performance indicators. The second reference framework is the hybrid-threat management structure proposed by Giannopoulos et al. (2021) at the level of the European Union, organised around the stages of anticipation, prevention, detection, and response, but without an explicit recovery phase and without named actors or quantifiable indicators.

The model proposed in the present study improves on both frameworks by: (a) including the prevention phase as an autonomous stage with dedicated actors and instruments, including Directive NIS2 (2022/2555) on the security of network and information systems and Regulation CRA (2024/2847) on cyber-resilience requirements; (b) treating detection as an autonomous phase, distinct from response, with clear institutional mandates and artificial-intelligence instruments for

signal analysis; (c) naming the actors responsible for each phase; and (d) defining quantifiable and verifiable performance indicators. The treatment of detection as a stage in its own right follows from the fact that, in the earlier models (Boin et al. 2016; Giannopoulos, Smith, and Theocharidou 2021), it was subordinated to the response phase, without defined institutional mandates. The analysis of the cases in section 3 demonstrates that detection deficiencies constitute the principal explanatory factor in response failures, including in the case of the Romanian elections of 2024 (DNSC 2024; BISI 2025).

TABLE 2. The integrated model for managing hybrid crises: phases, objectives, actors, and performance indicators

Phase	Central objective	Principal actors	Performance indicator
PREVENTION	Reduction of systemic vulnerabilities; compliance with NIS2 (2022/2555) and CRA (2024/2847)	Government, DNSC, SRI, critical-infrastructure operators	GCI Index: Tier T1; ≥4 national hybrid exercises/year
DETECTION	Continuous monitoring; predictive (AI) analysis of hybrid indicators	SRI, SIE, DNSC, CRISC, OSINT structures	Detection time under 24 hours; tactical attribution: 72h
RESPONSE	Countering actions; limiting impact; strategic communication	CSAT, MAI, MApN, NATO/EU structures, digital platforms	Impact limitation: < 48h; prevention of crisis escalation
RECOVERY	Restoration of functionality; post-crisis audit; strategic resilience	Public authorities, parliamentary committees, independent auditors	Restoration: 100%; publication of a Lessons Learned report

Source: compiled by the author on the basis of Boin et al. (2016), Giannopoulos et al. (2021), Chambers (2016), and the operational experience documented over the period 2022-2024.

2.3. The NATO and European Union normative and institutional framework for responding to hybrid threats

After 2022, the institutional framework for responding to hybrid threats underwent a process of accelerated strengthening. At the NATO level, the Madrid Strategic Concept (2022) enshrined hybrid conflict as a central planning scenario, while the Vilnius Summit (2023) adopted region-specific defence plans. The relevant centres of excellence, namely the Strategic Communications Centre of Excellence (StratCom COE, Riga), the Cooperative Cyber Defence Centre of Excellence (CCDCOE, Tallinn), and the Counter-Intelligence Centre of Excellence (CI COE, Bucharest), expanded their mandates and operational capabilities. The Tallinn Manual 2.0 (Schmitt 2017) and subsequent allied doctrine incorporate specific operational guidelines for countering cyber-attacks in the context of hybrid conflicts (NATO 2022; European Council 2023).

The European Union accelerated the adoption of its cybersecurity legislative framework: Directive NIS2 (2022/2555) on the security of network and information systems, Directive CER (2022/2557) on the resilience of critical entities, and

Regulation CRA (2024/2847) on horizontal cybersecurity requirements for products with digital elements together currently form the most comprehensive normative framework for responding to hybrid threats in the world (Broeders, Goffin and Groothuis 2023; Fiott and Parreira 2020).

3. Documented cases: lessons for the management of hybrid crises

The six case studies analysed in the present research cover the temporal interval 2007-2024, with an analytical emphasis on recent events, characterised by a high degree of empirical documentation and availability of primary and secondary sources. The conceptualisation of the notion of a "documented case" operationalises the methodological requirements specific to qualitative research in the social sciences, in keeping with the case-study paradigm developed by Robert K. Yin (2018). Within this epistemological logic, each unit of analysis is rigorously delimited from a spatio-temporal perspective and investigated multidimensionally through an analytical grid structured along three complementary levels: (1) the nature, mechanisms, and vectors of the hybrid action; (2) the dynamics, coherence, and effectiveness of the institutional response; and (3) the validation of strategic prescriptions and the identification of lessons learned relevant to the consolidation of institutional and operational resilience.

Each case study is systematically integrated within the proposed conceptual taxonomy, contributing both to testing the internal consistency of the analytical model and to refining its explanatory dimensions. The case-selection strategy was grounded in the criterion of maximum typological diversity, with the aim of ensuring the full representation of the six functional domains identified within the taxonomy. Such a methodological approach facilitates a comprehensive comparative analysis of the manifestations of the hybrid phenomenon and strengthens the internal validity and explanatory capacity of the theoretical-analytical model employed.

3.1. Ukraine (period analysed: 2022-2024)

The large-scale military aggression launched by the Russian Federation against Ukraine in February 2022 represents the most extensive and most rigorously documented example of integrated hybrid conflict of the post-Cold War period. The present analysis delimits the interval 2022-2024 and examines the convergent manifestation of hostilities across three fundamental dimensions: cyber, information, and economic.

In the cyber sphere, technology was used as a multiplier of operational capability, with the aim of disrupting command, control, and communications structures. On the night of 23-24 February 2022, concurrently with the launch of conventional military operations, the Sandworm group, affiliated with Russian military intelligence, carried out a destructive cyber-attack on the Viasat KA-SAT satellite communications network.

By compromising the equipment's embedded firmware, the operation disabled thousands of ground terminals used by Ukrainian governmental institutions and armed forces. The attack was the subject of a coordinated public attribution by the United States, the United Kingdom, and the European Union (CSIS 2022; ENISA 2024). In the same year, the same structure used the Industroyer2 malware to cause damage to a Ukrainian electrical substation, an incident regarded as the first major cyber-attack on Ukraine's energy infrastructure since 2017 (CSIS 2022; Mandiant 2023).

The cyber dimension was complemented by the information component, within which the cognitive confrontation took shape through coordinated disinformation campaigns conducted in at least fifteen European states. These influence operations sought both to fragment the internal social cohesion of Ukraine and to diminish the political and societal support extended to European security in the Western space (East StratCom Task Force 2023, 2024). In parallel, on the economic dimension, the transformation of commercial dependencies into instruments of geopolitical coercion was manifested through the deliberate and asymmetric reduction of natural-gas deliveries to European states over the period 2021-2022. This strategy sought to limit the capacity of the European Union to formulate and implement a firm diplomatic and economic response (Gressel 2022; Meydan 2022).

Compared with the crisis of 2014, the reaction of the North Atlantic Alliance and of the member states demonstrated significant doctrinal and operational progress, reflected in particular in the rapidity of the public attribution processes for cyber-attacks and in the effectiveness of strategic communication. Nevertheless, the conflict highlighted the persistence of structural vulnerabilities in the European security architecture. Among these are the residual energy dependencies of certain member states, the normative and operational fragmentation of national cyber-response mechanisms (Colby and Mitchell 2020; Gressel 2022), as well as the technical limitations associated with the sharing and integration of information at the allied level.

The main conclusion drawn from the analysis of this theatre of confrontation is that societal resilience constitutes the foundation of the modern capacity for deterrence and defence. Recent comparative analyses show that the defensive viability of a state in the face of hybrid threats depends directly on the existence of a robust and redundant industrial capacity for the production of armaments and munitions, on the diversification of energy sources and the reduction of strategic dependencies, as well as on the consolidation of institutional cohesion and of society's capacity to resist actions of information manipulation, propaganda, and psychological warfare (Gressel 2022; IISS 2024).

3.2. Electoral interference in Romania (2024)

The presidential elections in Romania held on 24 November 2024 represented the first case in the history of NATO-member democracies in which a presidential ballot was

annulled after the conduct of the first round of voting. The independent candidate Călin Georgescu, credited with less than 1% in the opinion polls of October 2024, obtained 22.94% of the total votes cast (FPRI 2024; BISI 2025). The documents partially declassified by the Supreme Council of National Defence (CSAT) on 4 December 2024 revealed the existence of three principal lines of hostile action.

In the first place, more than 85,000 cyber-attacks directed against the electoral infrastructure were identified, including the compromise of digital credentials and code-injection attacks on databases (CSAT 2024; BISI 2025). Secondly, the investigations revealed the existence of coordinated networks of accounts on the TikTok and Meta platforms, which generated approximately 179 million impressions for content favourable to the candidate, through the use of automated mechanisms for the promotion and distribution of messages (OECD 2024). Thirdly, the authorities established the existence of mechanisms for the illegal financing of the electoral campaign, given that the candidate had officially declared a nil electoral budget, while subsequent investigations indicated the existence of undeclared contributions estimated at approximately one million euros originating from third-party sources (CSAT 2024; BISI 2025).

The institutional response materialised on 6 December 2024, when the Constitutional Court of Romania unanimously decided to annul the results of the first round of the presidential elections, invoking the provisions of Article 50, paragraph (3) of the electoral legislation. At the European level, the European Commission initiated proceedings against the TikTok platform under the Digital Services Act (DSA 2022). The case is extensively documented both in the specialised literature and in institutional documents drawn up by the Romanian Intelligence Service (SRI 2024), the Supreme Council of National Defence (2024), the National Cyber Security Directorate (DNSC 2024), the Bloomsbury Intelligence and Security Institute (BISI 2025), and the Foreign Policy Research Institute (FPRI 2024).

The analysis of this case empirically demonstrates that a hybrid campaign lacking a military component can generate strategic-level effects, including the annulment of a national ballot, through the exclusive use of cyber, information, and internal-mobilisation instruments. The phenomenon illustrates the sixth domain of the proposed taxonomy, defined by the instrumentalisation of legitimate legal mechanisms and the activation of internal actors in the absence of a normative and institutional framework adequate to counter such threats (DNSC 2024; BISI 2025).

3.3. Cyber-attacks on NATO infrastructure in Eastern Europe (2023-2024)

The reports drawn up by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE 2024) and by the European Union Agency for Cybersecurity (ENISA 2024) document a significant intensification of cyber-attacks against critical infrastructure in the NATO states situated on the eastern flank over the period 2023-2024. These offensive operations systematically targeted the energy,

telecommunications, financial, and transport sectors. In the particular case of Romania, the National Cyber Security Directorate (DNSC 2023, 2024) reported saturation attacks directed against energy and telecommunications networks, actions whose probable attribution points to groups affiliated with the Russian state. From a tactical standpoint, a methodical escalation could be observed, from actions of transient impact towards sustained infiltrations into industrial control networks, a dynamic characteristic of the logic of asymmetric conflicts (Wilner 2020; Lanoszka 2016).

The assessment of institutional performance carried out by the CCDCOE (2024) highlights structural disparities correlated directly with the degree of technological maturity of the defending party. Thus, the data document that states classified in Tier 1 of the Global Cybersecurity Index (GCI) demonstrated superior detection and response capabilities compared with states in Tier 2. This disparity in performance validates the thesis that strategic investments in cyber resilience are reflected directly and measurably in the defensive capacity of security structures in crises.

The escalation trend highlighted in this theatre of operations, manifested through the transition from rudimentary saturation attacks to complex and persistent infiltrations into industrial control infrastructures, generates major doctrinal implications. This evolution of threats makes it imperative to clearly separate the detection phase from the response phase within models for the management of hybrid crises. This functional delimitation constitutes, moreover, the principal foundation of the analytical and operational structure proposed in section 2 of the present research.

3.4. The sabotage of submarine infrastructure in the Baltic Sea (2023-2024)

At least eleven submarine cables and pipelines located in the Baltic Sea region were damaged over the period October 2023 - January 2025, according to documentation published by Reuters and Defense News (2025). Among the most relevant incidents confirmed by official investigations is that of 8 October 2023, when the Balticconnector pipeline, which provides the energy connection between Finland and Estonia over a distance of 152 kilometres, together with several associated telecommunications cables, was damaged by the anchor of the Chinese vessel NewNew Polar Bear, according to the conclusions formulated by the Finnish investigating authorities.

Subsequently, on 18 November 2024, the BCS East-West Interlink submarine cable, which connects Lithuania and Sweden over a distance of 218 kilometres, as well as the C-Lion1 cable, which provides the link between Finland and Germany over a length of 1,173 kilometres, were damaged almost simultaneously. In this context, the Chinese vessel Yi Peng 3 remained for several weeks under the permanent monitoring of the Royal Danish Navy. The series of incidents continued on 25 December 2024, when the Estlink 2 energy cable, which serves the Finland-Estonia

connection, together with four other submarine telecommunications lines, was severed (Reuters 2025; Defense News 2025).

Despite the gravity of these incidents, the official and legal attribution of responsibility remains inconclusive in all the cases investigated. Assessing these developments, the NATO Secretary General, Mark Rutte, highlighted the complexity of the phenomenon without explicitly naming the Russian Federation, stating that hybrid actions are manifested through sabotage, cyber-attacks, and, in the current context, through aggressions directed against the critical submarine infrastructure of the North Atlantic Alliance (NATO, November 2024, cited in Defense News 2025). In response to this emerging vulnerability, the NATO Vilnius Summit initiated a programme dedicated to the protection of critical submarine infrastructure. This undertaking was consolidated in 2025 by the European Commission, which allocated almost one billion euros for the monitoring of submarine cable networks and for the constitution of a specialised fleet of vessels intended for emergency interventions and repairs.

From an analytical perspective, this succession of incidents highlights the fundamental paradox of actions conducted below the threshold of conventional military confrontation and reflects the design logic of contemporary asymmetric threats. The empirical data indicate that operations with major strategic impact on allied security are deliberately conceived so as to preserve ambiguity of attribution. By exploiting evidentiary difficulties and maintaining a high level of legal and operational uncertainty, the actors involved seek to avoid the activation of the collective-defence mechanism provided for by Article 5 of the North Atlantic Treaty.

3.5. The disinformation campaign at the European level (2023-2024)

The flow of disinformation campaigns associated with pro-Kremlin interests in the European space is systematically monitored by the EUvsDisinfo platform, coordinated by the European External Action Service since 2015. The data aggregated in the public database of this structure indicated, as of March 2024, the existence of more than 2,855 cases of disinformation directly correlated with the war in Ukraine, as well as a further 943 cases associated with the COVID-19 pandemic (East StratCom Task Force 2024).

This offensive dynamic intensified significantly in the context of the elections to the European Parliament held over the period 6-9 June 2024. The monitoring carried out by the European Digital Media Observatory (EDMO) and by the European network of fact-checking organisations highlighted a considerable increase in disinformation narratives directed against the European Union in the months preceding the ballot (EDMO 2024). With a view to limiting these threats, the Digital Services Act (DSA 2022) established the obligation for the major technology platforms to assess and mitigate the systemic risks associated with disinformation. On the basis of this normative framework, the European Commission initiated formal investigation

proceedings against the companies X and Meta for possible breaches of the rules concerning the integrity of electoral processes (European Parliament / European Commission 2024).

The response mechanisms activated by the European Union through the Digital Services Act, the EUvsDisinfo platform, and the cooperation agreements concluded with digital-service providers generated relevant operational effects, yet these remain limited relative to the scale and adaptability of the phenomenon. The instruments implemented proved insufficient for the complete neutralisation of disinformation campaigns, in the context of an asymmetric adversary that continually adapts its tactics and operational methods in order to evade the technical mechanisms for the identification, classification, and filtering of manipulative content. This evolution highlights the current limitations of the European defensive structures with respect to the consolidation of a secure and resilient information space.

The analysis of this propagandistic ecosystem offers a strategic conclusion relevant to the management of the contemporary cyber and cognitive space. The empirical data indicate that the effectiveness of information instruments used within hybrid warfare depends directly on the coherence, applicability, and firmness of the normative framework that regulates the activity of digital platforms. Consequently, resilience in the face of subversive actions is not conditioned exclusively by the existence of formal regulations, but also by the development of a robust institutional capacity for the real-time identification, analysis, and countering of manipulative narratives and coordinated influence operations.

3.6. Estonia (2007): the founding precedent and its doctrinal relevance

The cyber-attacks conducted against Estonia over the period 27 April - 18 May 2007 lasted 22 days and systematically targeted, through saturation-type attacks, governmental and ministerial portals, media institutions, internet-service providers, major banking institutions, and small private enterprises (CCDCOE 2024; Ottis 2008; StratCom COE 2019). From a geopolitical perspective, these aggressions coincided with the decision of the Estonian authorities to relocate the Bronze Soldier monument from the centre of the city of Tallinn. The subsequent assessments drawn up by the NATO Cooperative Cyber Defence Centre of Excellence concluded that the entire episode may conceptually be interpreted as a complex information operation coordinated by the Russian Federation, although the technical and judicial investigations did not lead to a definitive and incontestable legal attribution (Ottis 2008).

Although it exposed major structural vulnerabilities, the crisis generated far-reaching doctrinal and institutional reforms both at the national level and within the North Atlantic Alliance. The events of 2007 functioned as a catalysing factor for the elaboration of the Tallinn Manual and contributed decisively to the formal recognition of cyberspace as the fifth operational domain of NATO. These developments were consolidated in May 2008 through the official establishment

of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Domestically, this critical conjuncture accelerated the transformation of Estonia from a vulnerable state into a global reference actor in the field of cybersecurity and institutional resilience, a performance reflected in particular by its attainment of Tier 1 (T1) within the Global Cybersecurity Index (ITU 2024).

The evolution of Estonia after 2007, from the status of a state exposed to significant vulnerabilities to the position of an international benchmark in the field of cybersecurity, constitutes one of the most relevant empirical arguments in support of the idea that a security crisis, managed through coherent public policies and a long-term strategic vision, can be transformed into a durable strategic advantage (Schmitt 2017; Broeders, Goffin and Groothuis 2023). From a comparative perspective, this trajectory represents one of the most valuable doctrinal and institutional lessons for the consolidation of Romania's security architecture in relation to contemporary hybrid threats.

4. The case of Romania: vulnerabilities, institutional framework, and directions for reform

4.1. The risk profile: geopolitical positioning and structural vulnerabilities

Romania cannot be analysed from the perspective of national security without reference to its geopolitical specificity: its positioning on the Black Sea, its immediate proximity to zones of active conflict, the presence of NATO's strategic infrastructure on national territory, and the existence of a population exposed to disinformation flows propagated across two linguistic spaces with cross-border circulation. The events taking place during 2024 empirically demonstrated that Romania does not represent a peripheral actor with respect to hybrid conflict, but rather one of the member states of the Euro-Atlantic area with the highest level of direct exposure to asymmetric threats. In this context, the documented electoral interference definitively transformed Romania from a mere observer of the hybrid phenomenon into a reference case study analysed and invoked at the allied level (SRI 2024; CSAT 2024; DNSC 2024).

The risk analysis highlights the existence of four interdependent structural vulnerabilities that affect national security. The first critical dimension is represented by the cyber component, since the energy infrastructure, the telecommunications networks, and the information systems of the public administration continue to constitute constant targets of hostile cyber activities. In numerous documented situations, intrusion-identification times significantly exceed the reference threshold of 30 days established in NATO standards (DNSC 2023). This technological vulnerability is amplified by a persistent information fragility, reflected in the limited capacity of state institutions to monitor systematically and to counter rapidly the coordinated disinformation campaigns, a reality starkly highlighted in the context of the 2024 electoral process.

The third structural vulnerability concerns the level of social cohesion. Pronounced political polarisation and the persistent deficit of public trust in state institutions create a context favourable to the propagation and amplification of destabilising messages associated with hybrid actions (EIU 2023; SRI 2024). Finally, the fourth vulnerability, empirically confirmed by the political developments of 2024, concerns the limits of the institutional capacity to identify and neutralise in good time the processes of internal mobilisation and the offensive use of legal mechanisms by disruptive actors. The absence of a specific legislative framework adapted to the new forms of hybrid aggression leaves this domain insufficiently protected against strategies of institutional exploitation and political subversion (Renz 2016; Walker 2018).

4.2. An audit of the institutional and normative framework

Assessing Romania's institutional capacity to manage hybrid threats requires the analysis of two complementary and interdependent dimensions: the existence of an adequate normative framework and the effectiveness of the operational structures responsible for its application. From this perspective, institutional resilience is not determined exclusively by the formulation of strategic documents and normative acts, but also by the effective capacity of institutions to integrate, coordinate, and implement response mechanisms adapted to the multidimensional character of contemporary hybrid threats.

TABLE 3. An audit of Romania's institutional framework for the management of hybrid threats

Document / Institution	Year	Principal gap identified
SNA 2020-2024 (National Defence Strategy)	2020	Absence of a dedicated hybrid operational plan. The 2025-2030 Strategy (adopted in 2025) partially remedies this deficit by including explicit hybrid measures.
Cybersecurity Strategy 2022-2027 (GD 963/2022)	2022	Insufficient public funding, situated below the threshold of 0.05% of GDP, compared with the NATO reference threshold of 0.10%.
Law no. 51/1991 on national security (rev. 2014)	1991/2014	Structural failure to adapt to hybrid threats, a concept recognised at EU level since 2014 following the annexation of Crimea.
DNSC: National Cyber Security Directorate	2021	Configured as a coordinating rather than a commanding authority; limited data exchange with the private sector.
SRI: National CYBERINT Centre	2012	Limited flow of information and exchange of technical data with private critical-infrastructure operators.
Participation in **PESCO** (17 projects)	2017-present	Represents a European Union cooperation mechanism rather than a national construct; operational contribution below actual capacity.

Source: Compiled by the author on the basis of official national documents and NATO/EU assessments (SRI 2023, 2024; DNSC 2023, 2024; SEAE 2023).

Table 3 presents a comparative audit of the main strategic documents and of the institutions relevant to the national security architecture, highlighting the structural gaps identified in relation to the standards and practices consolidated at the Euro-Atlantic level. The analysis examines both the degree of conceptual and normative adequacy of the existing framework and the level of institutional interoperability, the capacity for inter-institutional coordination, and the effectiveness of the prevention, detection, and response mechanisms in the face of hybrid threats.

The adoption of the National Defence Strategy for the period 2025-2030, a document that for the first time includes explicit measures dedicated to countering hybrid threats, constitutes a relevant advance in the process of adapting the national security architecture to the new forms of conflict. The explicit introduction of the hybrid dimension within the strategic priorities reflects both the intensification of external pressures on the Euro-Atlantic area and the need to develop institutional mechanisms capable of responding to contemporary multidimensional threats.

Nevertheless, the developments of 2024 empirically confirmed the persistence of major operational vulnerabilities. The first of these concerns the absence of an integrated institutional rapid-reaction mechanism in situations of hybrid electoral interference, capable of ensuring immediate coordination among the security structures, the electoral authorities, and the actors responsible for protecting the digital infrastructure. The second vulnerability relates to the insufficient capacity for real-time monitoring and analysis of the digital space, a limitation that reduces the effectiveness of the early identification of coordinated influence and disinformation campaigns. Finally, the third structural gap consists in the non-existence of a formalised and operationalised framework of cooperation between the national security institutions and the digital platforms operating on Romanian territory, an aspect that affects the capacity for rapid reaction and the efficient exchange of relevant information (DNSC 2024; CSAT 2024).

These deficiencies highlight the fact that the modernisation of the strategic and normative framework, although necessary, is not sufficient in the absence of the development of integrated operational mechanisms, capable of functioning on a permanent basis and of responding to the dynamic and adaptive character of contemporary hybrid threats.

4.3. A comparative analysis of resilience

The table presents a comparative assessment of the principal resilience indicators in relation to hybrid threats, placing Romania's institutional performance within the context of four member states of the North Atlantic Treaty Organization relevant from a strategic and operational perspective. The comparative analysis seeks to highlight the differences in institutional capacity, degree of operational maturity, and level of integration of response mechanisms, in relation to the standards consolidated at the Euro-Atlantic level.

Tabel 4: Comparative indicators of resilience to hybrid threats: Romania and NATO reference states

Indicator	Finland	Estonia	Sweden	Poland	Romania	Ref.
GCI Tier 2024 (ITU)	T1	T1	T1	T2	**T2**	T1
Dedicated hybrid legal framework (year of adoption)	2017	2018	2021	2022	**Absent**	2016*
Cybersecurity budget (% of GDP, GD 963/2022)	n/a	n/a	n/a	n/a	**below 0.05%**	>0.10%
PESCO participation: active projects (SEAE 2023)	12	15	11	14	**17***	-

Sources: ITU Global Cybersecurity Index 2024 (September 2024); SEAE, PESCO Progress Report 2023; GD no. 963/2022.

The data included in the table are drawn exclusively from public, official, and verifiable primary sources, being correlated with strategic documents, institutional reports, and independent assessments available in the academic and security domain. This approach ensures the methodological coherence of the comparison and permits a rigorous interpretation of the performance differences among the states analysed with respect to resilience to hybrid threats.

The data aggregated within the comparative analysis indicate the existence of a systemic gap on the part of Romania relative to the reference states included in the analytical sample. According to the Global Cybersecurity Index 2024 drawn up by the International Telecommunication Union (ITU), Romania is classified in Tier 2 (advanced), while Estonia, Finland, and Sweden are consistently situated in Tier 1 (the benchmark tier), corresponding to the highest level of performance of the index.

The absence of a normative framework dedicated to the integrated management of hybrid threats, in contrast to the institutional and legislative developments recorded in Finland (2017), Estonia (2018), and Poland (2022), represents the principal structural gap of the national security architecture. This deficiency is further highlighted by the administrative difficulties in formulating a coherent preventive response in the context of the developments of 2024.

In financial terms, the vulnerability is amplified by the relatively low level of resources allocated to cybersecurity, which remains below the threshold of 0.05% of gross domestic product (GD 963/2022), a value inferior to the reference threshold of 0.10% used in the comparative assessments of the North Atlantic Alliance.

From this perspective, the conclusion of the comparative analysis highlights that systemic and predictable investment in resilience mechanisms constitutes a fundamental condition of strategic stability, rather than a derived consequence of it.

Conclusions

The present research permits the formulation of conclusions of both theoretical and applied relevance, articulated around three major conceptual axes, which contribute to clarifying the contemporary dynamics of hybrid conflict and to understanding the conditions of systemic resilience within the Euro-Atlantic area.
The first argument concerns the structural transformation of hybrid conflict over the interval 2022-2024, a period in which asymmetric instruments evolved from complementary roles to central positions in the architecture of geopolitical competition. The analysis of the cases investigated confirms the consolidation of an operational model in which cyber, information, economic, and legal actions are integrated within a unitary logic of strategic pressure. In this context, the conceptual debate concerning "full-spectrum warfare", "parallel warfare", and "shadow warfare" does not indicate a mutual exclusion but an analytical complementarity, each paradigm capturing distinct dimensions of the same phenomenon: the breadth of instruments, their operational synchronisation, and the deliberate management of ambiguity of attribution.

At the same time, the results of the research highlight a significant technological discontinuity, determined by the integration of generative artificial intelligence into the ecosystem of information operations. This evolution substantially reduces the production and distribution costs of manipulative content and exponentially amplifies the speed, volume, and granularity of influence campaigns, profoundly altering the balance between institutional defensive capabilities and non-state or state offensive ones.

The second argument focuses on the determinants of national and systemic resilience. The case study concerning the institutional and political dynamics in Romania in 2024 demonstrates that vulnerabilities of a normative nature and deficits of operational capacity do not generate merely localised disturbances, but can produce strategic-level effects, with a direct impact on institutional stability. Within this framework, the research introduces and consolidates the relevance of the domain of internal mobilisation and offensive legal actions (lawfare) as an autonomous vector of hybrid power, capable of producing effects comparable to those of cyber or conventional military instruments, in the absence of the use of kinetic force.

As a counterpoint, the evolutionary trajectory of Estonia after 2007 empirically confirms the possibility of converting a security crisis into a durable strategic advantage, provided there exists coherent institutional learning and a consistent transposition into public policy. This experience constitutes a doctrinal benchmark with a high value of transferability for the processes of consolidating resilience in states exposed to hybrid threats.

The third argument validates the analytical contribution of the model proposed within the research. The application of a management cycle structured around four interdependent phases, namely prevention, detection, response, and recovery, in correlation with an operational taxonomy extended to six functional domains, made it possible to systematically identify the institutional deficits specific to each unit of analysis. The results indicate the existence of a persistent structural risk in the case of Romania across the entire crisis-management chain, with pronounced vulnerabilities in the detection and response stages, relative to the standards consolidated at the level of the North Atlantic Treaty Organization.

In summary, the research highlights the imperative necessity of adopting a unitary and specialised normative framework for the management of hybrid threats, one that explicitly integrates the cyber, information, economic, and legal-political dimensions, including the emerging components of internal mobilisation and offensive legal actions. The consolidation of such an institutional architecture constitutes an essential condition for increasing strategic resilience and for full alignment with the security standards of the Euro-Atlantic area.

Public-Policy Recommendations

The recommendations formulated in the present work are calibrated in relation to a medium- and long-term strategic-planning cycle and fall within the commitments assumed by Romania as a member state of the North Atlantic Treaty Organization and the European Union. These lines of action aim at the coherent consolidation of the national resilience architecture in the face of hybrid threats, through the integration of the normative, institutional, operational, and societal dimensions within a unitary framework of response.

The first line of action consists in the elaboration of a normative framework dedicated to hybrid threats, one that includes explicit provisions concerning the prevention and countering of electoral interference, the sabotage of critical infrastructure, and influence operations assisted by artificial intelligence. This legal framework must explicitly include the recognition of internal mobilisation and offensive legal actions (lawfare) as autonomous vectors of threat to national security. Although the National Defence Strategy 2025-2030, adopted in 2025, includes general guidelines concerning the countering of hybrid threats, its operationalisation through sectoral action plans is necessary. These subsequent instruments should define detailed crisis scenarios, clearly assigned institutional responsibilities, and pre-established escalation thresholds for the activation of response mechanisms.

The second recommendation concerns the constitution of an integrated national centre for the fusion and analysis of information flows, with the mandatory participation of the Romanian Intelligence Service, the Foreign Intelligence Service, the National Cyber Security Directorate, the Ministry of Internal Affairs, and the

Ministry of National Defence. In order to ensure operational effectiveness, this structure must be supported by an explicit legal mandate, regulating the secure exchange of classified information and the rapid-activation protocols in situations of multidimensional crisis.

The third recommendation concerns the consolidation of cooperation between the public sector and the private sphere in the field of cybersecurity, through the formal integration of critical-infrastructure operators into the national detection and response mechanisms. This approach entails adapting models of the sectoral information-sharing and analysis-centre type to the national legal and institutional framework, with a view to ensuring a bidirectional, secure, and operational flow of technical data between the state and the economic actors of the essential sectors.

The fourth recommendation concerns the consolidation of information resilience at the societal level through the introduction of education for media security into compulsory schooling, as a structural instrument for the long-term countering of disinformation and cognitive-influence operations. In a complementary respect, this measure must be supported through the development of a national programme for the certification and validation of information sources, inspired by European good practices, including the experience of Finland.

The fifth recommendation concerns ensuring the financial and human sustainability of the cybersecurity system, through the progressive alignment of budgetary allocations with the reference threshold of 0.10% of gross domestic product, used in the comparative assessments at the level of the North Atlantic Treaty Organization. This increase must be correlated with the implementation of a national programme for the training, retention, and motivation of digital-security specialists, intended to reduce the deficit of critical competences in the public sector and to consolidate the operational capacity of the responsible institutions.

FUNDING STATEMENT
The present study did not benefit from any external funding, whether public or private. The research was carried out exclusively on the basis of the author's own resources.

CONFLICT OF INTEREST STATEMENT
The author declares that there is no conflict of interest of a financial, professional, or personal nature that may have influenced the preparation of the present article.

References

Ansell, Chris, Arjen Boin, and Ann Keller. 2010. "Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System." *Journal of Contingencies and Crisis Management* 18 (4): 195-207. https://doi.org/10.1111/j.1468-5973.2010.00620.x.

Bachmann, Sascha-Dominik, and Hakan Gunneriusson. 2015. "Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere." *Georgetown Journal of International Affairs* 16: 198-211.

Berzins, Janis. 2014. *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy.* Policy Paper No. 02. Riga: National Defence Academy of Latvia. https://www.nda.mil.lv/wp-content/uploads/2020/04/PP02_Berzins_Russia_Hybrid_Warfare.pdf.

Bloomsbury Intelligence and Security Institute (BISI). 2025. *Invisible Influence: Romania's Presidential Election Crisis*. Londra: BISI. https://bisi.org.uk/reports/invisible-influence-romanias-presidential-election-crisis.

Boin, Arjen, Paul't Hart, Eric Stern, and Bengt Sundelius. 2016. *The Politics of Crisis Management: Public Leadership under Pressure*. Ed. a 2-a. Cambridge: Cambridge University Press.

Broeders, Dennis, Hadrien Goffin și Bart Groothuis. 2023. "Governing Cybersecurity through Resilience: The European Approach to Systemic Risk in Critical Infrastructure." *Journal of Common Market Studies* 61 (4): 901-919. https://doi.org/10.1111/jcms.13442.

CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence). 2024. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Tallinn: CCDCOE.

Chambers, John (ed.). 2016. *Countering Hybrid Warfare. MCDC Project Report*. Londra: Multinational Capability Development Campaign. https://assets.publishing.service.gov.uk/media/5a82499340f0b62305b91b2a/concepts_mcdc_countering_hybrid_warfare.pdf.

Colby, Elbridge, and A. Wess Mitchell. 2020. "The Age of Great-Power Competition." Foreign Affairs 99 (1): 118-130.

CSAT (Supreme Council of National Defence). 2024. "Synthesis concerning the hybrid influence campaign in the Romanian presidential elections of 2024 (partially declassified document)." Bucharest: CSAT.

CSIS (Center for Strategic and International Studies). 2022. Cyber Operations Tracker: Russia-Ukraine Conflict 2022. Washington: CSIS. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Cullen, Patrick J., and Erik Reichborn-Kjennerud. 2017. *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*. London: Multinational Capability Development Campaign. https://assets.publishing.service.gov.uk/media/5a82499340f0b62305b91b2a/concepts_mcdc_understanding_hybrid_warfare.pdf.

Defense News. 2025. "At Least 11 Cables and Pipelines Damaged in Baltic Sea Since October 2023." *Defense News*. https://www.defensenews.com/naval/2025/01/28/at-least-11-cables-and-pipelines-damaged-in-baltic-sea-since-october-2023/.

DNSC (National Cyber Security Directorate). 2023. *Annual report on the state of cybersecurity in Romania: 2023*. Bucharest: DNSC.

___. 2024. Report on cyber threats against electoral processes: 2024. Bucharest: DNSC.

East StratCom Task Force (EEAS). 2023. *EUvsDisinfo Database: Annual Report 2023*. Brussels: European External Action Service. https://euvsdisinfo.eu/reports/.

___. 2024. *EUvsDisinfo Database: Quarterly Report Q1 2024*. Bruxelles: EEAS. https://euvsdisinfo.eu.

EDMO (European Digital Media Observatory). 2024. *EU Elections 2024: Disinformation Monitoring Report*. Florence: EDMO / European University Institute.

EEAS (European External Action Service). 2023. *PESCO: Progress Report 2023*. Brussels: EEAS.

EIU (Economist Intelligence Unit). 2023. *Democracy Index 2023: Age of Conflict*. London: EIU.

ENISA (European Union Agency for Cybersecurity). 2023. *ENISA Threat Landscape 2023*. Heraklion: ENISA. https://doi.org/10.2824/782573.

___. 2024. *ENISA Threat Landscape 2024*. Heraklion: ENISA.

European Council. 2023. "Joint Declaration on EU-NATO Cooperation." 10 January 2023.

European Parliament / European Commission. 2024. *Investigation of digital platforms concerning electoral integrity in the context of the European elections of June 2024 (DSA proceedings)*. Brussels: European Parliament. https://www.europarl.europa.eu/news/en/press-room.

European Union. 2022a. "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)." Official Journal of the European Union L 333: 80-152.

___. 202b2. "Directive (EU) 2022/2557 on the resilience of critical entities (CER)." Official Journal of the European Union L 333: 164-198.

European Union. 2024. "Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (CRA)." Official Journal of the European Union L.

Fiott, Daniel, and Raluca Parreira. 2020. *Protecting Europe: The EU's Response to Hybrid Threats*. Chaillot Paper No. 151. Paris: EU Institute for Security Studies.

Foreign Policy Research Institute (FPRI). 2024. *Romania's Electoral Crisis: A Blueprint for Defending Democracy*. Philadelphia: FPRI.

Fridman, Ofer. 2018. *Russian Hybrid Warfare: Resurgence and Politicisation*. London: Hurst. https://doi.org/10.1093/oso/9780190877095.001.0001.

Galeotti, Mark. 2018. *I'm Sorry for Creating the Gerasimov Doctrine*. Foreign Policy, 5 March 2018.

Gerasimov, Valery. 2013. "Tsennost' nauki v predvidenii [The Value of Science in Anticipation, translated by Robert Coalson]." Voenno-promyshlennyi kur'er 8 (476): 1-3.

Giannopoulos, Georgios, Helen Smith, and Marianthi Theocharidou. 2021. *The Landscape of Hybrid Threats: A Conceptual Model*. Luxembourg: Publications Office of the European Union. https://doi.org/10.2760/019854.

Gioe, David V., Michael S. Goodman, and David Omand (eds.). 2022. *The Routledge Companion to Intelligence Studies*. London: Routledge.

Government Decision no. 963/2022 on the approval of the Cybersecurity Strategy of Romania 2022-2027. Official Gazette of Romania, Part I, no. 1029, 19 October 2022.

Gressel, Gustav. 2022. *Armies of Russia's War in Ukraine*. London: European Council on Foreign Relations. https://ecfr.eu/publication/armies-of-russias-war-in-ukraine/.

Hoffman, Frank G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.

IISS (International Institute for Strategic Studies). 2023. *The Military Balance 2023*. London: Routledge / IISS.

___. 2024. *The Military Balance 2024*. London: Routledge / IISS.

ITU (International Telecommunication Union). 2024. *Global Cybersecurity Index 2024*. 5th ed. Geneva: ITU. https://www.itu.int/hub/publication/d-hdb-gci-01-2024/.

JOIN(2016)18. European Commission and High Representative of the Union. 2016. "Joint Framework on countering hybrid threats: a European Union response. JOIN(2016)18 final." Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2016:18:FIN.

Lanoszka, Alexander. 2016. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe." International Affairs 92 (1): 175-195.

Mandiant. 2023. *Industroyer2: Industroyer Reloaded. Technical report*. Reston: Mandiant / Google Cloud. https://www.mandiant.com/resources/reports/industroyer2-industroyer-reloaded.

Meydan, Timur. 2022. "Hybrid Warfare and the Changing Nature of Conflict: Implications for NATO's Deterrence Posture." Journal of Strategic Studies 45 (5): 721-748. https://doi.org/10.1080/01402390.2021.1972484.

Mumford, Andrew. 2013. *Proxy Warfare*. Cambridge: Polity Press.

NATO. 2022. *NATO 2022 Strategic Concept*. Adopted at the Madrid Summit, 29-30 June 2022. Brussels: NATO.

OECD (Organisation for Economic Co-operation and Development). 2024. *AI Incidents Monitor: Case Study - Romanian Presidential Elections 2024*. Paris: OECD. https://oecd.ai/en/incidents.

Ottis, Rain. 2008. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Tallinn: CCDCOE.

Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjallhed. 2018. *Countering Information Influence Activities: A Handbook for Communicators*. Lund: Lund University.

Presidential Administration of Romania. 2020. "National Defence Strategy for the period 2020-2024." Bucharest: Presidential Administration.

___. 2025. "National Defence Strategy for the period 2025-2030." Bucharest: Presidential Administration.

Renz, Bettina. 2016. "Russia and Hybrid Warfare." *Contemporary Politics* 22 (3): 283-300.

Reuters. 2025. "Baltic Sea Underwater Infrastructure: Timeline of Incidents 2023-2025." *Reuters.* https://www.reuters.com/world/europe/baltic-sea-cable-damage-timeline-2025-01/.

Rosenthal, Uriel, Arjen Boin, and Louise K. Comfort (eds.). 2001. *Managing Crises: Threats, Dilemmas, Opportunities*. Springfield, IL: Charles C Thomas.

Schmitt, Michael N. (ed.). 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

SRI (Romanian Intelligence Service). 2023. *Activity report: 2023*. Bucharest: SRI.

___. 2024. *Report on hybrid threats to the electoral process in Romania (2024)*. Bucharest: SRI.

Strachan-Morris, David. 2022. "Understanding Hybrid Warfare: Lessons for Intelligence Analysis." *Intelligence and National Security* 37 (3): 389-405. https://doi.org/10.1080/02684527.2021.2016672.

StratCom COE. 2019. *Hybrid Threats: 2007 Cyber Attacks on Estonia*. Riga: NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

Thomas, Timothy. 2016. "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and Ambiguous Warfare." *Journal of Slavic Military Studies* 29 (1): 147-174.

Tikk, Eneken, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharma, and Liis Vihul. 2008. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn: CCDCOE.

Walker, Christopher. 2018. "What Is Sharp Power?" *Journal of Democracy* 29 (3): 9-23. https://doi.org/10.1353/jod.2018.0041.

Warden, John A. 1995. "Enemy as a System." *Airpower Journal* 9 (1): 40-55.

Wilner, Alex S. 2020. "US Cyber Deterrence: Practice Guiding Theory." *Journal of Strategic Studies* 43 (2): 245-280. https://doi.org/10.1080/01402390.2018.1563779.

Yin, Robert K. 2018. *Case Study Research and Applications: Design and Methods*. 6th ed. Thousand Oaks: SAGE.