CYBER DIPLOMACY IN NATO 3.0 ARCHITECTURE: ROMANIA AS A REGIONAL HUB AND VECTOR OF RESILIENCE IN THE BLACK SEA

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

Abstract: In the context of the transition to NATO 3.0 doctrine and the reconfiguration of the security equation on the Eastern Flank, this paper analyzes Romania's strategic role as a regional hub of cyber diplomacy and technological resilience in the Black Sea basin. The research assesses how the digital dimension and international cooperation can support the defense effort against hybrid threats and asymmetric attacks below the threshold of NATO Article 5. Using a mixed methodology, the paper combines discourse and diplomatic process analysis with stochastic modeling of cyber risks on dual critical infrastructures. In this regard, three fundamental hypotheses regarding strategic cyber deterrence, international legislative harmonization and public-private partnerships in defense technology research and development are analyzed. The results highlight a direct dependence between the speed of diplomatic reaction and limiting the degradation of the capacity of command and control (C2) systems, while also highlighting the vulnerabilities caused by the gaps in domestic innovation and infrastructure. Based on the results obtained, it is proposed to adopt a phased framework until 2035, based on the transition from a reactive to a proactive cyber diplomacy posture, which would strengthen national and regional resilience, in accordance with the commitments assumed by Romania within the North Atlantic Alliance and the European Union
Keywords: Black Sea, cyber diplomacy, cybersecurity, digital resilience, hybrid threats, NATO 3.0.

INTRODUCTION AND STRATEGIC CONTEXT

The NATO Strategic Concept 3.0 has reconfigured the Euro-Atlantic security architecture and shifted the focus of strategic deterrence beyond the administrative borders of NATO member states, establishing cyberspace as a priority operational domain. This transitional stage marks the abandonment of the traditional model of asymmetric support in favor of an approach based on deterrence through shared responsibility, high availability. In this framework, security management is no longer a strict responsibility of the military sphere, but an essential component of international relations, governed by norms and mechanisms specific to cyber diplomacy (Vevera, Vasiloiu & Stoica, 2025). In this paper, the term "NATO 3.0" is used as an analytical and conceptual framework to describe the transition toward a digitally integrated advanced defense; it does not represent an official designation found in the Alliance's documents or formal decisions.

Looking back, for decades NATO's security equation was based on a relatively simple premise. The frontline states provided buffer zones and constituted the early sensors of the Alliance. The real capacity to deter and repel aggression depended almost exclusively on the rapid mobilization of conventional forces in the transatlantic space, mainly from the United States. Against the backdrop of accelerated digitalization and rapid modernization of military operations, this external "backstop" model has become unsustainable in the current context, characterized by deep geopolitical fragmentation. The lessons learned from the large-

scale strategic exercises conducted by NATO (the series of complex exercises Steadfast Deterrence, Steadfast Dart and Trojan Footprint), have imposed the transition from deterrence by punishment to deterrence by denial. The new doctrine requires the European pillar to assume the role of "first responder" in the event of a high-intensity conflict.

This structural reconfiguration stems from the need for the US to reorganize its defensive resources to manage the situation in the Indo-Pacific theater, in order to maintain global stability in the face of the challenges of multipolar rivalries. Although the US commitment to security towards European partners remains firmly in the nuclear and advanced cyber security directions, the European allies are tasked with generating robust conventional capabilities, regional logistics and resilience of critical infrastructures necessary to sustain a prolonged conflict. Operating effectively on the Eastern Flank requires an enormous density of armed forces, mobile and interoperable. Digital systems and logistics chains must be complete and capable of operating without syncope in hostile environments.

In order to avoid major problems resulting from NATO exercises conducted to date and for the transition to an effective forward defense should:

- Cross-border bureaucracy eliminated: Extensive cross-border maneuvers have demonstrated that obtaining state border crossing permits on time is an obstacle that requires a military Schengen area;
- Strengthened critical infrastructure of member states, especially road and rail, which causes vulnerabilities in logistics chains to the Eastern Flank countries;
- Urgent transition from support to forward defense: Currently, a military brigade can be formed in approximately 10 days. To shorten this time, component forces must be pre-positioned, operationalized and authorized to action in just a few hours;
- Decentralized command and advanced technologies: New battle groups require decentralized commands that can deal with multi-domain threats (Finland model);
- Established and achieved an effective control of autonomous defense zones: Implementation of new defense technologies capable of effectively intercepting drone swarms and other strike vectors (based on the Ukraine war lessons learned);
- Establish cooperation mechanisms adapted to the current context: Inter-agency cooperation must be optimized to effectively combat disinformation and other hybrid activities, especially at the level of the civilian population.

For this, at the NATO Summit for the Defense Industry Forum (2026), the states from the NATO space are called to build their own digital resilience, while ensuring, at the same time, solid channels of cooperation and technological interoperability with all allies, by creating a cloud-enabled digital enterprise (NATO, 2026). In this geostrategic ecosystem, the Black Sea has become an essential testing space for hybrid operations, often below the threshold of NATO Article 5, where sophisticated cyber-attacks, electronic jamming and disinformation directly affect regional stability. Beyond the military dimension, the Black Sea represents a vital node for trade, energy and data routes between Europe and Asia. Any hybrid challenge, without exceeding the critical threshold of triggering Art. 5, must be approached as a test of the Alliance's cohesion.

Whoever controls or destabilizes the Black Sea geostrategic space can obtain access to the data and information routes that connect Central Europe with the Middle East and Central Asia.

The main security challenges related to this space are:

- Electronic jamming (intense and persistent) on GPS signals. These affect military and civil flights, maritime navigation and the functionality of critical infrastructures in the coastal space. The jamming actions come mainly from the Crimea area and from Russian military ships (Iancu & Mândraș, 2024);
- Advanced Persistent Threat (APT) cyber operations executed by state actors on communication and transport networks, on port infrastructures and logistics systems, on other critical infrastructures etc. (Todorov, 2024);
- Manipulation and cognitive warfare campaigns to erode public trust in transatlantic alliances and in national security decisions, based on various divergent currents of opinion and internal social faults of the riverain countries (Chiriac, 2021).

The pressure on the security systems of the dual critical infrastructures of the riverain countries is at an unprecedented level. Therefore, the new model of the security equation must also integrate the cybersecurity parameters specific to inter-state connections. Strategic deterrence can no longer be credible if it is limited to a purely military approach manifested by the presence of combat ships and coastal artillery and missile systems. It must integrate digital resilience and cyber diplomacy to guarantee the continuity of governance and defense management in conditions of prolonged war.

ROMANIA IN THE NEW STRATEGIC CONTEXT

In this new security architecture, Romania occupies a key position, acting as a NATO outpost on the Eastern Flank for managing possible regional crises along the Black Sea. Within this doctrinal reconfiguration, the Black Sea basin has ceased to be viewed as a secondary border area or as a theater for monitoring the risks determined by the competition between the great Eurasian powers.

However, between Romania's strategic intention to become a regional technological, military (Dușescu, 2025) and diplomatic hub and the operational reality, some significant structural gaps persist, visible in the reduced capacities of logistics infrastructures, the dependence on military import purchases and the limited degree of connection of local digital systems.

It is known that the firm political commitment of the Romanian government has been translated into substantial budgetary allocations for defense. Romania allocates 2.45% of GDP to defense (Lupițu, 2026), specifically 49.426 billion lei, in accordance with Law No. 43/2026 on the state budget for the year 2026. Thus, financial predictability was ensured that allowed the initiation of major military equipment programs and the consolidation of the infrastructure to host multinational, brigade-level battle groups. Moreover, the confidence of the allied states in the national security and defense capabilities also derives from Romania's inclusion in the NATO initiative known under the code name Eastern Flank Defense Initiative (EFDI), for the creation of an integrated system of satellites, drones, ground sensors and robotic platforms, for the purpose of monitoring activity along the Eastern Flank (Eastern Flank Institute, 2026). The collected data will be analyzed quickly using artificial intelligence and will be shared securely to all members of the alliance through the 'Kill Web' network

(Hoffmann, 2026). The concept integrates reconnaissance and monitoring systems with fire control and other physical actions into a single network, allowing for the optimization of the OODA (Observe, Orient, Decide, Act) loop. The novelty of this approach is determined by the formation of an advanced defense zone, where combat drones, unmanned ground platforms and other remotely controlled fire systems will engage in combat from the first moments. The role of this integrated system is not only to compensate for the technological advantage of a hypothetical enemy, but also to "deterrence by denial", being able to quickly determine the type of threat, identify and propose which member state and with which type of weapon system should respond to effectively intercept and neutralize it. Even though conventional capabilities will remain the main pillar of NATO defense, the new system "is designed to help preserve their combat power and give commanders more time and decision advantage", as said Maj. Matt Blubaugh, a spokesman for US Army Europe and Africa (Hoffmann, 2026).

Thus, the structural gap between intention and reality risks compromising not only the efficiency of national defense but also of the entire region. In terms of security and defense infrastructure, the Constanța port and the Mihail Kogălniceanu air base offer remarkable transport, storage and transfer capacities of equipment both within the country and towards the borders. However, the functional capacities of the national road and rail networks currently produce delays due to the low average speed of trains, tonnage limits for bridges over the Danube and due to the railway gauge differences at the EU's external borders, all of which transform military mobility into a major challenge. Any exceeding of the planned operational time window directly reduces the strategic deterrence capacity and exposes the Eastern Flank to a multitude of asymmetric risks (JOIN, 2025).

Another relevant aspect concerns the budget allocated to defense equipment. Even though, at the national level, the budget is quite large, a very small percentage of these funds goes back to the domestic defense industry (Grădinaru, 2025). Most of the acquisitions are imports of complex military equipment, at turnkey. The advantage of this approach is that it offers speed in reaching operational standards. However, there are no national capacities to ensure long-term maintenance, local technological modernization or domestic production for consumables and ammunition, essential capacities especially in the event of a prolonged and high-intensity conflict.

Regarding cyber resilience, the transition to NATO 3.0 requires fully integrated, secure command and control (C2) systems capable of withstanding massive cyber-attacks. There are initiatives in this direction for the development of dual-use software solutions, especially through public-private partnerships (Ion, 2026). However, a major problem that can turn into a systemic vulnerability is the retention of cybersecurity specialists, especially in the public sector.

The objective of this research is to investigate the concrete way in which the identified internal limitations can be overcome, providing an empirically based assessment and a strategic perspective oriented towards a ten-year horizon. The investigation into how Romania can overcome these barriers to become a functional regional hub will not evaluate national policy decisions, adopted following NATO and B9 summits or within regional cooperation initiatives.

Therefore, the research question of this study is: To what extent do the effectiveness of cyber diplomacy mechanisms and normative-diplomatic response measures determine the level of cyber resilience (R_h) of Romania's dual-use critical infrastructures in the face of hybrid threats in the Black Sea region?

WORKING HYPOTHESES, THEORETICAL FRAMEWORK AND RESEARCH METHODOLOGY

The analytical approach tests three fundamental hypotheses to ensure the rigor and falsifiability of the thematic directions:

Hypothesis 1 (H1): The effectiveness of diplomatic coordination in cyber deterrence is directly conditioned by the existence of common and recognized threat intelligence sharing protocols between partner states. Reducing the diplomatic notification time (D_p) below the 5 minutes threshold reduces the C2 systems compromise rate below the critical threshold of 10% in the case of complex APT attacks.

Hypothesis 2 (H2): The efficiency of the response to hybrid disinformation campaigns and cognitive attacks is directly conditioned by the existence of this cross-border regulatory framework for cooperation with Big Tech platforms, the reduction of institutional reaction time being determined mainly by the application of EU/NATO norms and secondarily by the isolated acquisition of modern monitoring technologies.

Hypothesis 3 (H3): Structural dependence on external supply chains and unreliable technologies, the low share of domestic production of dual technologies and R&D in the security and defense sector (< 15%) limits national operational resilience (R_h), directly and proportionally increasing the time required to perform reverse engineering/patching in conditions of crisis and war.

From a methodological point of view, the research adopts a mixed design (qualitative - quantitative) that combines qualitative analysis with stochastic modeling to ensure data triangulation.

The theoretical framework of this research is anchored in the theory of international security governance (Kello, 2017) and in the literature on cyber deterrence, examined through the lens of complex interdependencies and neoclassical realism. Unlike the nuclear or conventional domain, where deterrence is based on the credible representation of massive reprisals, deterrence in cyberspace is based on denial and normative-diplomatic attribution. (Nye, 2011).

To explain how systemic pressures, translate into internal operational resilience, the analysis articulates three complementary paradigms from the field of International Relations as follows:

- International security governance establishes that cyber resilience is a collective public good; this underpins H1, demonstrating that the technical protection of C2 systems depends directly on shared threat intelligence protocols and rapid diplomatic notification mechanisms;
- Complex interdependence highlights the role of non-state actors and transnational networks, forming the basis for H2; neutralizing AI-generated cognitive threats depends primarily on common EU/NATO regulatory frameworks regarding big tech platforms and, secondarily, on national monitoring tools;
- Neoclassical realism links external structural threats with internal state variables (public procurement, the national Research, Development and Innovation base); this informs H3, arguing that a heavy reliance on imported technologies (with domestic production below 15%) limits operational autonomy and extends patching/reverse engineering times, during crises.

In a deeply interconnected digital environment, the state security can no longer be in isolation conceptualized or managed. The cyber vulnerability of an ally on the Eastern Flank has the potential to compromise all integrated command and control systems of the entire Alliance, transforming individual resilience into a collective imperative.

Qualitative component and sampling

Process-tracing evidence was selected based on its direct relevance to B9/NATO decisions and the adopted EU/national norms. The evidence was evaluated using causal inference tests (hoop tests and smoking-gun tests) to establish the link between bureaucratic/normative gaps and the speed of response to hybrid attacks.

The normative-diplomatic dimension is complemented by a purposive sampling consisting of 15 semi-structured interviews, conducted in a hybrid format (in-person and online), conducted with diplomats, cybersecurity specialists, experts and researchers from profile think tanks. The selection of specialists was based on at least 5–8 years of experience in the fields of cybersecurity, foreign policy, or critical infrastructure. In order to comply with ethical and confidentiality norms (GDPR), the participants were coded anonymously (EXP 01 – EXP 15). Content analysis was conducted using inductive thematic coding, and the anonymized data were stored in encrypted form, free of identifying information.

The profile of the expert sample is presented in table 1. To prevent the identification of individuals within the small sample (15 experts), individual roles are aggregated into broader categories as follows:

Table 1. The profile of the expert sample

Selected category	No. of participants (codes)	Intermediate level of experience
Digital diplomacy and international cooperation	3 (EXP-01, EXP-08, EXP-15)	12 years
National Defense and Security (Ministry of National Defence - MApN, National Cyber Security Directorate - DNSC, Ministry of Internal Affairs - MAI)	3 (EXP-02, EXP-03, EXP-04)	12 years
Critical infrastructure / Rail transport	2 (EXP-09, EXP-10)	11 years
Research, Academia, and Think Tanks	3 (EXP-07, EXP-12, EXP-13)	10 years
Private sector and technological environment	4 (EXP-05, EXP-06, EXP-11, EXP-14)	8 years

Stochastic component and mathematical formula

The qualitative approach is complemented by a technical security component that uses stochastic Monte Carlo simulations to measure the responsiveness and resilience of networks to coordinated cyberattacks. We accept Terje Aven's justification that qualitative assessment alone is not sufficient for national security decisions (Aven, 2009).

The mathematical model used evaluates the dynamic balance between internal detection and response capabilities, the level of technological interoperability and the efficiency of cyber diplomacy mechanisms, related to the frequency and structural vulnerability to digital aggression. Starting from the analytical model developed by Anthony Cox (Cox, 2008), regarding the limitations of qualitative risk matrices (the possibility of inducing serious decision errors in the absence of the use of mathematical equations based on attack frequencies

- λ and vulnerability - V), as well as the time integral of internal security vectors, cumulated with the sum of the impact of exogenous risks - the weighted sum of risks (Giannopoulos, Dorneanu & Jonkeren, 2013), we defined the dynamic resilience of the regional hub (R_h), on a time horizon T (modeled until 2035), in the following form:

$$R_h(T) = \int_0^T [w_1 C_a(t) + w_2 I_t(t) + w_3 D_p(t)]dt - \sum_{i=1}^{n} \lambda_i V_i \quad (1)$$

Where:

$R_h(T)$ measures the aggregate dynamic resilience index (values between 0 and 1); a value close to 1 indicates a high capacity for network absorption and recovery;

$C_a(t) \in (0, 1)$ represents the dynamic early warning and incident response capability at the time „t";

$I_t(t) \in (0, 1)$ measures the level of technological integration and interoperability with other NATO/EU networks;

$D_p(t) \in (0, 1)$ represents the efficiency of cyber diplomacy mechanisms (regulatory speed, existence of mutual assistance and data sharing agreements; it is a function inversely proportional to the type of diplomatic notification/sharing; as the notification time decreases (e.g., below 5 minutes), the D_p value rises towards 1, maximizing the resilience integral;

$w_1, w_2, w_3 \in (0, 1)$ there are coefficient assigned to each security vector ($\Sigma w_k = 1$, $w_k = 1/3$); reflects the hypothesis that cyber architecture depends equally on internal capabilities (C_a), technical interoperability (I_t) and the regulatory/diplomatic framework (D_p);

$\lambda_i > 0$ represents the incidence rate (frequency) of type „i" cyberattacks (drones, ransomware, APT, jamming etc.); data on the attacks frequency become from DNSC and ENISA reports;

$V_i \in (0, 1)$ measures the structural vulnerability associated with systems to attacks of the type „i".

To assess the systemic uncertainty, the equation was subjected to N = 1000 iterations. The parameterization of the variables λ_i followed a Poisson distribution (λ_{APT} = 12.4/year, $\lambda_{Ransomware}$ = 8.1 /year, λ_{GPS} = 45.2 events /year), based on incidence data extracted from DNSC, ENISA reports and from critical infrastructure operators.

This methodological blend allows one to go beyond purely qualitative assessments, providing a rigorous analytical basis for underpinning strategic decisions, and follows Joseph Nye's way of explaining cyber deterrence as achieved not through unilateral accumulation of force, but through diplomatic networks and cooperation (Nye, 2011).

In this context, the concept of NATO 3.0 represents the third evolutionary stage of the North Atlantic alliance and the transition from classical collective defense (NATO 1.0 – Cold War period, NATO 2.0 – post-1991 crisis management operations), to an integrated, multi-domain model, based on forward defense, native digital interoperability and shared civil-military resilience. In the NATO 3.0 architecture, cyberspace is a priority operational domain, in which the delimitations between peace, crisis and conflict are permanently fluid. The Black Sea space thus becomes a main theater of manifestation of hybrid warfare under the Article 5, where the cyber resilience posture of each ally directly conditions the deterrence capacity

of the entire Eastern Flank. Therefore, it is important to introduce the variable D_p (efficiency of cyber diplomacy mechanisms) into the core of the resilience function.

Research and analysis on the systemic digital infrastructure resilience and civil-military cooperation on NATO's Eastern Flank, underlines the need for a robust framework to prevent disruption of critical networks, determined by the level of technological integration and interoperability (I_t), across the Alliance (NATO, 2024). Therefore, the vulnerability variables V_i and the capabilities C_a, I_t, D_p were modeled by beta distributions ($\alpha = 2$, $\beta = 5$), adjusted based on empirical assessments obtained from the expert sample. These distributions were selected to reflect risk asymmetry (a higher probability of moderate-to-high vulnerability in legacy dual-use infrastructures) and were calibrated based on the consensus of the experts in the sample.

ANALYSIS AND DISCUSSIONS

The results obtained by triangulating stochastic simulations with qualitative analysis confirm the thesis that cyber resilience on the Eastern Flank is not a simple matter of modern technology acquisitions but a direct function of the speed of diplomatic and normative reaction. Although, Romania has taken important steps to transpose European legislation and create institutions with functions in ensuring cybersecurity, there are significant discrepancies between the objectives assumed by the diplomatic security discourse and the technical realities on the ground. Stochastic simulations conducted based on incident reports show a significant increase in persistent and asymmetric attacks on critical infrastructures in the eastern region of the country. At the same time, the qualitative assessment through interviews confirms the existence of structural limits to the development of public-private partnerships in the defense technology sector (frequently reported in the ICI Bucharest and ARASEC reports), which validates the limits of innovation capacities at the local level.

Testing the first hypothesis highlights a direct and non-linear correlation between the density of threat intelligence sharing protocols and the success rate of APT attacks against national critical infrastructures. The data analyzed for the period 2024-2026 indicate a massive intensification of cyber intrusion campaigns coordinated by groups with links to states in the eastern proximity (actors associated with APT28 and APT29 entities). These campaigns mainly targeted communication systems in eastern Romania, in the Constanța port, logistics systems and railway transport networks (DNSC, 2024).

In the scenarios modeled for the C2 traffic infrastructures, indicates the existence of a critical alert threshold, which is established by operational norms and procedures. In situations where the communication of data about the indicators of compromise (diplomatic and technical notification time, as well as the sharing of cyber-attack indicators to NATO counterparts) is delayed beyond the 15 min. threshold, the rate of damage to adjacent systems increases exponentially (by approx. 150%), degrading the response capacity (according to Table 2).

Table 2. Impact of data exchange delay on C2 systems compromise rate

Notification/sharing delay (min)	Compromise rate (%)	Operability/resilience level
Under 5 min	8%	High resilience/ Automated response
5 – 15 min	22%	Reduced degradation / Controlled response
15 – 30 min	54%	Significant network degradation
Over 30 min	80 %	Major compromise of C2 systems

Note: The values obtained from the outputs of the stochastic Monte Carlo scenario modeling (N=1000 iterations) represent simulated projections and not direct empirical measurements.

Data shows that reducing notification time below the 5 min. threshold keeps system degradation to a minimum of 8%. In contrast, a delay of more than 15 min. causes an exponential increase in the compromise rate of 54%, reaching 80% after 30 min.

Stochastic modeling has shown that the introduction of cross-border cyber assistance protocols (variable D_p in the resilience formula) will significantly reduce the value of the hub's structural vulnerability (V_i) by over a third (approx. 65%). However, interview data indicate that the main problem is not technological but administrative-procedural (rigid bureaucratic procedures, especially at the level of data flows with non-NATO regional partners, such as the Republic of Moldova and Ukraine).

EXP-02 emphasized that: "our technical systems can send a compromise indicator within seconds to NATO structures. However, if that indicator is classified as a classification that requires manual inter-institutional approvals, the transfer can exceed 24 hours." Therefore, although tactical cyber exercises (such as Locked Shield) technically validate the rapid transfer of data, often national information classification protocols block the technical capacity. Harmonizing these frameworks through cyber diplomacy tools becomes an essential condition for ensuring credible deterrence, limiting delays and harmonizing asymmetries in security legal regimes.

This empirically validates H 1 and extends Todorov's (2024) conclusions on the vulnerability of the Black Sea space, showing that, at least at the regional level, national bureaucratic bottlenecks represent a vulnerability as critical as the cyberattack itself. Integrated cyber deterrence in the Black Sea region can only be credible through cyber diplomacy.

The qualitative analysis of efforts to neutralize cognitive hybrid attacks (H 2), during the period of frequent use of generative artificial intelligence (AI), highlights the need for a profound structural change to block societal disinformation, to limit social faults in times of crisis or during large-scale military exercises. In the period 2025-2026 were identified a series of complex deepfake campaigns. These exploited the emotional tensions caused by the presence of allied troops on Romanian territory, as well as the strategic decisions communicated through the voice of various political leaders, regarding the evolution of the international geopolitical situation. Through the process tracing method, it was demonstrated that cognitive attacks are no longer just a classic propaganda campaign, but cyber operations. They use networks of AI coordinated bots to simplify messages and adapt them to the level of perception of the auditor, in order to generate or amplify panic in times of crisis, such as the governmental one of 2026, or during the conduct of complex military exercises, planned within the Alliance.

Despite these challenges, Romania's current digital diplomacy mechanisms operate in a predominantly reactive regime. Interviewed experts emphasize that technical monitoring tools are insufficient if they are not complemented by regulatory diplomatic actions. In the absence of an adequate regulatory framework, the gap between the moment of identifying a massive disinformation campaign recognized by the national cybersecurity authority (DNSC) and the moment of limiting its propagation on social media platforms can vary between 24 and 72 hours. This interval provides sufficient time for the negative impact on public perception to already be produced. "Digital diplomacy is not just about presence on social networks (...) In the absence of a clear mandate framework at EU and NATO level, this process takes days, during which time the societal effect is already produced." (EXP-08)

Therefore, limiting these risks does not depend exclusively on the acquisition of technical monitoring tools, but on the ability to promote regular standards at European level and to develop cognitive resilience of the population.

These results partially validate H 2: the success of limiting hybrid attacks is also strongly dependent on Romania's diplomatic capacity to promote normative standards (European Union and NATO level), as well as on the level of education of citizens in the field of cybersecurity. Only in this way will major technology providers be forced to integrate rapid mechanisms for real-time response to hybrid attacks and neutralization of information manipulation on the Eastern Flank.

The analysis of H 3 highlights a major imbalance between the level of investment in technological independence (domestic innovation) and applied research, compared to the volume of resources allocated to the acquisition of imported military equipment. Stochastic simulations performed on IT, logistics and railway networks serving the Constanța port indicate that the physical-digital vulnerabilities of dual infrastructures remain high ($V_i > 0.65$), at the local level. A paradox emerges: the acquisition of advanced systems, with Romania assuming ambitious budgetary targets for defense financing, without reverse engineering rights or access to source code creates critical dependencies in supply chains (the analysis of economic flows shows a major gap between the level of investment for the acquisition of imported defensive systems and that of investment in the development of a technological and industrial defense base, at the national level). The share of equipment and systems in the Romanian-made army's equipment is below the critical threshold of 15%.

In the event of large-scale cyber-attacks on firmware from the strategic equipment, the lack of internal analysis components, reverse engineering and independent maintenance capabilities forces increased remediation times and degradation of the value of the digital resilience function with a particular impact on early warning and incident response capacity (C_a).

A direct causal factor is the operation of national transport systems on predominantly technologically outdated infrastructures (legacy systems), vulnerable to ransomware cyber-attacks or database alterations, such as the cyber-attack on the National Agency for Cadastre and Real Estate Advertising (IntelliNews, 2026). Such events contradict the desired state of a regional cybersecurity hub. Any modern logistics system and any armed force equipped with state-of-the-art technology become ineffective if the digital networks through which troop movements are coordinated can be blocked by a ransomware attack or if traffic monitoring sensors can be jammed.

For Romania to become a real regional hub, under the NATO 3.0 doctrine, the main digitalization program must go beyond the level of accumulation of conventional equipment and move to that of securing the dual national digital ecosystem, in accordance with the EU directive on data and technology sovereignty (Directorate General for Communication, 2026). This direction can be followed if public-private partnerships become truly functional and are able to attract highly qualified human capital in the government cybersecurity domain. At the same time, a solid domestic R&D base must be provided capable of ensuring Romania's technological sovereignty in the coming period. Maintaining the share of national defense equipment production below a minimum threshold creates critical dependencies on external supply chains. This reality is criticized by experts in the R&D sector and private industry.

"We buy highly advanced military equipment with integrated software. But if we suspect a vulnerability or malicious code, we do not have the right or technical capability to reverse engineer it. Dependence on external manufacturers nullifies the notion of strategic autonomy." (EXP-06)

"Romania has extraordinary human capital in IT and cybersecurity, but national public acquisition mechanisms are designed for the industrial age. If a start-up developing an AI algorithm for drone detection cannot participate in public tender due to its low turnover in recent years." (EXP -14)

It is observed that, in the event of major disruptions or massive cyberattacks on the software components of critical infrastructures, the lack of local maintenance and analysis capabilities prolongs remediation times and reduces national operational resilience.

These findings validate H 3 and are in direct agreement with the European Commission's (2026) analyses on technological sovereignty, highlighting that Romania's regional hub status remains only theoretical in the absence of stimulating domestic R&D for flexible public procurement mechanisms.

The simulation's limitations are determined by the Poisson distribution established for cyberattacks and do not account for "Black Swan" events (unforeseen cascading systemic failures) or major geopolitical shifts in doctrine. Furthermore, sensitivity analysis demonstrates that the Dp parameter (diplomacy/rapid sharing) has the greatest elasticity regarding Rh; a fluctuation of approximately 20% in the notification method alters the C2 system compromise rate by more than 35%, confirming that the bureaucratic actor is the most sensitive vector in the model.

CONCLUSIONS AND STRATEGIC DIRECTIONS

The research conclusions reconfirm that, within the NATO 3.0 doctrine, the geopolitical role of a state cannot be estimated only by assessing conventional military capabilities, but by its ability to project digital resilience, secure critical infrastructures and achieve sustainable technological alliances. In a security environment characterized by complex interdependencies and persistent hybrid threats, cyberspace represents an integrated dimension of collective defense, where perseverance and timely response are as important as classical deterrence.

One of the main functions of diplomacy is the initiation, negotiation and consolidation of international treaties and agreements that regulate cooperation between states. In the field of cybersecurity, the development of international, bilateral and regional cooperation mechanisms is essential for the early identification of cyber incidents and for the effective management of cross-border events.

In this context, cyber diplomacy contributes to strengthening national resilience by promoting norms, mechanisms and cooperation instruments that facilitate the attribution of responsibilities for activities carried out in cyberspace. Against the background of the evolution of the conflict in Ukraine, identifying of a cyber incident authors, by correlating all the information obtained at regional level, will allow substantiating the attribution of hybrid attacks, assessing threats

and developing the institutional capacities of states to recognize operational patterns associated with certain actors, as well as identifying incipient manifestations of new attacks to optimize prevention and response mechanisms. Ongoing developments within the UN regarding the consolidation of the Open-Ended Working Group (OEWG) with the Global Mechanism on ICT security indicate the certainty of international efforts to create a permanent body to regulate responsible behavior in cyberspace.

The main conclusions of the research emphasize that, in order for Romania to consolidate its position as a regional hub for security and digital diplomacy in the NATO 3.0 architecture, a strategic reorientation structured along the following directions is necessary:

1. Institutionalizing a regional dialogue format dedicated to cybersecurity in the Black Sea, in which Romania would take the diplomatic initiative by creating a permanent platform for cooperation in the field of cybersecurity. This should facilitate the standardization of procedures for analysis and the provision of rapid technical assistance in crisis situations, bringing together allied and partner states in the region.

2. Stimulating domestic innovation and technological development by attracting NATO and EU funds: For this, the accelerated use of programs such as DIANA (Defence Innovation Accelerator for the North Atlantic) is essential, especially for financing Romanian startups developing emerging technologies and AI. This direction will reduce dependence on technological solutions from external suppliers and will give substance to the status of a technological hub.

3. Supporting a body of experts specialized in cyber diplomacy: The Ministry of Foreign Affairs, in close cooperation with recognized institutions (DNSC, ICI Bucharest etc.), must invest in continuous training of diplomats in the field of Internet governance, the norms of responsible behavior of states in cyberspace and international law applicable to the digital environment. They will ensure the link between political decisions and technical cybersecurity requirements. Currently, by applying the provisions of Law no. 114/2026 (Art. 2, point 13), the Body of potential expert evaluators of a CDI project competition can be established, which will also become the core of the training of this group of experts. This can be coordinated by the Observatory for Research, Development and Innovation (OCDI), which has the role of ensuring and developing the expertise acquired through the implementation of the milestones and targets associated with the National Recovery and Resilience Plan (Art. 3, point 1), if responsibilities are established in this regard.

Romania's transformation into a Black Sea regional hub directly depends on the maturity of its cyber diplomacy tools. Cyber diplomats will be involved in negotiations on establishing the norms of responsible behavior of states in cyberspace and in defining the norms of application of international law in cyberspace.

We believe that reducing the gaps between the political decision-making process and the implementation of technical measures, while promoting a stable regional framework for digital cooperation, is an essential condition through which national security and that of the entire Eastern Flank of NATO can be guaranteed in the long term.

REFERENCE LIST

Aven, T. (2009), *A new scientific framework for quantitative risk assessments*, Int. J. Business Continuity and Risk Management, Vol.1, No.1, pp. 67 – 77, DOI: 10.1504/IJBCRM.2009.028951

Chiriac, O., R. (2021), *Cognitive Warfare in the 21st Century Great Power Competition – Framing of Military Activity in the Black Sea*, Romanian Military Thinking International Scientific Conference, no. 4: 54 - 71, DOI: 10.55535/RMT.2021.4, https://en-gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2021/4/CHIRIAC.pdf at 29.07.2026

Cox, A.L.Jr. (2008), *What's Wrong with Risk Matrices?*, Risk Analysis, vol. 28, pp. 49-512, https://doi.org/10.1111/j.1539-6924.2008.01030.x

Direcția Generală Comunicare. (2026), *Consolidarea suveranității tehnologice a Europei*, Comisia Europeană, https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03_ro at 30.07.2026

DNSC. (2024), *Raport anual de activitate 2024 (aprobat prin HCSAT nr. 7/30.06.2025), Document destinat publicării*, Directoratul Național de Securitate Cibernetică, pp 6 - 8, https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024 at 30.07.2026

Duțescu, I. (2025), *Negrescu: România poate deveni un hub tehnologic și militar pentru sud-estul Europei*, Mediafax, https://www.mediafax.ro/politic/negrescu-romania-poate-deveni-un-hub-tehnologic-si-militar-pentru-sud-estul-europei-23528251 at 29.07.2026

Eastern Flank Institute. (2026), *Eastern Flank Review, 13.05-19.05.2026, EFI review of the past week in Central and Eastern Europe*, https://easternflank.org/eastern-flank-review-13-05-19-05-2026/ at 29.07.2026

Giannopoulos, G., Dorneanu, B. and Jonkeren, O. (2013), *Risk Assessment Methodology for Critical Infrastructure Protection, JRC Scinetific and Policy Reports*, European Commission, Chap. 3 (pp. 27- 43), doi:10.2788/78850

Grădinaru, A. (2025), *Industria de apărare a statului român are în 2025 un miliard de lei în pus de la buget. Cum îl cheltuiește?*, Europa Liberă Romania, Interviurile ONE2ONE, https://romania.europalibera.org/a/industria-de-aparare-de-stat-are-in-2025-un-miliard-de-lei-de-la-buget-cum-il-cheltuieste-/33345457.html at 26.07.2026

Hoffmann, L.-M. (2026), *NATO is building an AI 'Kill Web' to stop Russian attackers in their tracks*, Business Insider, Military & Defense, https://www.businessinsider.com/nato-builds-ai-kill-web-to-stop-russian-attackers-2026-7 at 29.07.2029

Iancu S. and Mândraș, P. (2024), *Cât de periculoase sunt atacurile electromagnetice ale Federației Ruse pentru aviația civilă?*, Euro-Atlantic Resilience Centre, Bucharest, https://e-arc.ro/wp-content/uploads/2024/05/Text_GPS-Jamming_Iancu_Mandras.pdf at 29.07.2026

IntelliNews. (2026), *Cyberattack cripples Romania's land registry, freezing property market before VAT deadline*, bne-Intellinews, https://www.intellinews.com/cyberattack-cripples-romania-s-land-registry-freezing-property-market-before-vat-deadline-455796/ at 23.07.2026

Ion, T. (2026), *ICI București anunță „un rezultat important" pentru România: A fost aprobată propunerea privind includerea a cinci noi Centre de Testare DIANA în România în bugetul de anul viitor*, Calea Europeană, https://www.caleaeuropeana.ro/ici-bucuresti-anunta-un-rezultat-importat-pentru-romania-a-fost-aprobata-propunerea-privind-includerea-a-cinci-noi-centre-de-testare-diana-in-romania-in-bugetul-de-anul-viitor/ at 29.07.2026

JOIN. (2025), *Joint Communication to the European Parliament and the Council on Military Mobility*, European Commission, High Representative of the Union for Foreign Affairs and Security Policy, Brusseles, JOIN (2025) 846 final, https://transport.ec.europa.eu/document/download/4466a1dc-49d8-459f-9afa-d93c4346c26a_en?filename=JOIN_2025_846.pdf at 29.06.2026

Kello, L. (2017), Cyber Security, Gridlock and Innovation, in book: Hale T. and Held, D. (201) *Beyond Gridlock*, Cambridge: Polity, pp 205 – 228, ISBN-13: 98-1-5095-15714; ISB-13: 978-1-5095-152-1(pb), https://ora.ox.ac.uk/objects/uuid:adac6b9a-ccdc-4d8b-b02a-cfbca849072f/files/m34094ee8ba2aab54d4f3eb74c7ef980e at 30.07.2026

Lupițu, R. (2026), *Bugetul militar crește în 2026: România alocă 2,45% din PIB pentru apărare. 38% din fonduri, pentru înzestrare*, Calea europeană, https://www.caleaeuropeana.ro/bugetul-militar-creste-in-2026-romania-aloca-245-din-pib-pentru-aparare-38-din-fonduri-pentru-inzestrare/ at 28.07.2026

NATO. (2024), *Cyber defence, Deterrence and defence*, https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence at 16.07.2026

NATO. (2026), *NATO builds a more agile and resilient digital infrastructure*, https://www.nato.int/en/news-and-events/articles/news/2026/07/07/nato-builds-a-more-agile-and-resilient-digital-infrastructure at 20.07.2026

Nye, J. S. Jr. (2011), *The Future of Power*, Public Affairs, New York, https://www.academia.edu/23946693/THE_FUTURE_OF_POWER at 16.07.2026

Parlamentul României. (2026). Monitorul Oficial al României, nr. 588 din 20.07.2026, *Legea nr. 114 din 20 iulie 2026 privind unele măsuri pentru digitalizarea activității și stimularea investițiilor publice și private în domeniul cercetare-dezvoltare și inovare,* în vigoare din data de 23.07.2026, lege5.ro

Todorov, Y. (2024), *Navigating Uncharted Waters: Tackling Maritime Cybersecurity Challenges in the Black Sea Region*, Information & Security, vol. 55, no. 3: 113-132, DOI: 10.11610/isij.5509

Vevera, A.-V., Vasiloiu, I.-C. and Stoica, M. (2025), *An AI-based OSINT framework for fake news detection and economic impact assessment in cyber diplomacy*, Romanian Journal of Information Technology and Automatic Control, ISSN 1220-1758, vol. 35 (4), pp 63-77, https://doi.org/10.33436/v35i4y202505



Sorin TOPOR is a cyber security specialist at the Critical Infrastructure Protection Service, at the National Institute for Research and Development in Informatics – ICI Bucharest, specializing in security studies, electronic warfare and defense against terrorism. He graduated his Ph.D. in Military Sciences at the "Carol I" National Defense University, in 2000. In the last 20 years, he has held various leadership positions in academic education. He was project director and member of various research teams for international and national projects. He has also published 10 books and over 100 specialist works..



This is an open access article distributed under the terms and conditions of the
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.