BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Security Culture and Organizational Resilience in the Context of Cyberwarfare: the Case of Romania

Mihail-George GURANDA*
Dănuț MAFTEI, Ph.D.**

*Senior Legal and Regulatory Affairs Expert | EU-Level Cybersecurity Policy Specialist | Strategic Advisor in Public Policies
e-mail: mihaigu@riseup.net
**National Cyber Security Directorate, Bucharest, Romania
e-mail: dn.maftei@gmail.com

Abstract

This article examines the relationship between Cyber Warfare, security culture, and organizational resilience in Romania through the interaction of the legal framework, institutional architecture, and public governance practices. In the context of expanding hybrid conflicts and the convergence of technical, strategic, and cognitive threat dimensions, security culture can no longer be treated as a secondary issue, but as a condition for organizational and state resilience. Methodologically, the study relies on qualitative research combining doctrinal analysis, legal-institutional analysis, and a case study of Romania, drawing on relevant national legislation, the European Union acquis, institutional documents issued by DNSC, ENISA, and NATO, as well as relevant academic literature. The central argument is that Romania's recently developed normative and institutional architecture, particularly Law no. 58/2023, G.E.O. no. 155/2024, the operationalization of SNAC, and integration with NIS2 mechanisms, creates premises for strengthening security culture and resilience, without automatically guaranteeing the internalization of security behaviours.

Keywords:
Cyber Warfare; Security Culture; Cybersecurity; Cyber Defense; Cyber Crisis; Threats; Resilience; Cyber Governance.

Article info
Received: 13 February 2026; Revised: 23 February 2026; Accepted: 17 March 2026; Available online: 8 April 2026

Citation: Guranda, M.G., and D. Maftei. 2026. "Security Culture and Organizational Resilience in the Context of Cyberwarfare: the Case of Romania." *Bulletin of "Carol I" National Defence University* 15(1): 252-265. https://doi.org/10.53477/2284-9378-26-15

Introduction

Over the past decade, cyber warfare has profoundly altered the way states perceive the relationship between security, conflict, and the functioning of public institutions. Unlike traditional cyber threats, which are primarily associated with criminal activities or the technical protection of networks, cyber warfare is part of a broader strategic framework in which digital operations can be used for espionage, disruption of critical services, coercion, foreign influence, and the erosion of public trust in democratic institutions (Lin 2012).

An analysis of threats attributed to APT (*Advanced Persistent Threat*) groups illustrates the high degree of sophistication of cyber operations carried out by various state actors. Thus, the APT43 group (alias *Kimsuky*), supported by North Korea, has become a symbol of this evolution, carrying out complex espionage and strategic intelligence-gathering activities in the diplomatic, technological, and defense sectors (Mishra 2025). This malicious group combines advanced persistence techniques with the exploitation of legitimate operating system tools, bypassing conventional detection methods and targeting government institutions, think tanks, research centers, and critical information infrastructure in EU member states (MS), the United States, Japan, and South Korea.

A similar trend can be observed in the capabilities of the Russian group *Curly COMrades* (Lyons 2025), which uses virtualization technologies to hide malicious code within an isolated environment, drastically reducing the likelihood of detection. This offensive innovation demonstrates the creative use of legitimate technologies for hostile purposes and marks a shift in the defensive paradigm: simple endpoint-level detection becomes insufficient in the face of threats that exploit virtualized architectures and dynamic persistence mechanisms.

This transformation has direct consequences for security culture. In the classical paradigm, cybersecurity was frequently treated as a technical specialty. In contrast, in the current paradigm, it has become a matter of governance, organizational behavior, inter-institutional coordination, and societal resilience. Several reports highlight the fact that a mature cybersecurity culture involves not only rules and controls, but also values, attitudes, practices, and learning mechanisms that influence the actual behavior of organizational actors (Huang and Pearlson 2019).

In the case of Romania, this evolution is particularly relevant. The transition from a fragmented approach to cybersecurity toward a more coherent model of crisis governance and cyber alerting is indicated by:

- Recent legislative developments, such as Law No. 58/2023 on Romania's cybersecurity and cyber defense, and Government Emergency Ordinance (G.E.O.) No. 155/2024 establishing a framework for the cybersecurity of networks and information systems in the national civilian cyberspace (Romanian Government 2024);

• Institutional developments such as the establishment of the National Cyber Security Directorate (DNSC), the operationalization of the National Cyber Alert System (SNAC), as well as integration into the mechanisms of the Directive (EU) 2022/2555 - NIS2 (EUR-Lex 2022) and the *European Cyber Crisis Liaison Organisation Network* (EU-CyCLONe).

However, the existence of a more robust regulatory and institutional architecture does not automatically solve the central issue of resilience: the way in which rules, procedures, alert mechanisms, and inter-institutional cooperation are transformed into stable practices, organizational reflexes, and public trust. This is, in essence, the issue of security culture.

This paper begins with the following research question: **To what extent and through what mechanisms does Romania's regulatory and institutional framework for cybersecurity contribute to the development of a security culture and organizational resilience in the context of cyber warfare?**

In relation to this question, the article formulates three working hypotheses:

- Hypothesis 1: Normative clarity and the formal distribution of competencies enhance coordination capacity in cyber crises.
- Hypothesis 2: Alert mechanisms, inter-institutional cooperation, and public communication can foster the internalization of security behaviors.
- Hypothesis 3: In the absence of implementation indicators and systematic data on compliance and institutional learning, the effect of the legal framework on security culture remains plausible but only partially demonstrable.

Given the circumstances described, this article proposes, on the one hand, a conceptual reordering of the relationship between cyber warfare, security culture, and organizational resilience, and, on the other hand, it offers a structured analysis of the Romanian case, placing domestic regulatory and institutional developments within the context of the EU – NATO convergence and of the recent European requirements regarding the management of cyber incidents and crises.

1. Conceptual framework

Conceptual clarity is essential for any scientific analysis of cybersecurity. In the absence of a rigorous definition, terms such as "cyber warfare," "security culture," and "organizational resilience" tend to be used metaphorically or interchangeably, which affects both the coherence of the argument and the possibility of empirical evaluation.

1.1. Cyber Warfare

According to several reports, *Cyber Warfare* is not reduced to the mere existence of cyberattacks. It involves the use of cyber capabilities within a strategic logic of conflict, particularly by states or actors sponsored by various countries and governments, to produce negative political, military, economic, or psychological

effects on an adversary. Analyses of cyber conflicts highlight precisely the difficulty of separating the technical dimension of the attack from its strategic purpose and its effects on the political order and institutions (Sutton and Tompson 2023).
For this article, Cyber Warfare could be defined as the set of offensive, defensive, and influence operations conducted in and through cyberspace to impair the operational capacity, decision-making, trust, or resilience of a state, certain institutions, or critical information infrastructure. It takes place in the information environment, with actors and targets in both the physical and non-physical domains, and the level of violence may vary depending on the circumstances (Taddeo 2012). This definition allows for the inclusion of both the technical and the cognitive and institutional dimensions.

1.2. Security Culture

The concept of *Security Culture* must be distinguished from mere formal compliance. The relevant reports in the field specify that a security culture involves a set of shared values, beliefs, attitudes, and behaviors that influence the way in which members of an organization understand risks, respond to rules, and participate in the protection of digital assets. Recent models emphasize the link between culture and behavior, with education, leadership, group norms, communication, and reward systems directly influencing security conduct.
Security culture is defined in Romania by the *National Defense Strategy Guide for the period 2015-2019*. This document defines security culture as the totality of those values, norms, attitudes, or actions that determine a society's understanding and assimilation of the concept of security and its derivatives (national, international, and collective security; insecurity; security policies, etc.) (Presidency 2015). Thus, relevant actors (institutions, organizations, and citizens) perceive cyber risks, prioritize security, and act consistently to prevent, report, and manage incidents.
For this article, it is also important to highlight the existence of a *Cybersecurity Culture*, which is represented both by the norms and values that members of an organization hold regarding cybersecurity and by the way these are manifest in their behavior (Sutton and Tompson 2023).

1.3. Organizational Resilience

The concept of *Organizational Resilience* is frequently used in security discussions, but often without being operationalized. It is described in recent academic literature as a *multifaceted capability* that includes anticipation and preparation, endurance and response, recovery, and subsequent learning.
According to the definition provided by the British Standards Institution (BSI), organizational resilience is the ability of an organization to anticipate, prepare for, respond to, and adapt to sudden changes and disruptions in order to survive and thrive (Hilio 2025). In the case of Cyber Warfare, this entails flexibility, agility, and innovation in the face of challenges, as well as maintaining essential functions during a cyber incident, recovering within a reasonable timeframe, and integrating lessons learned into future policies, procedures, and architectures.

1.4. The Relationship Between Concepts

The relationship between the three concepts can be formulated as follows: *Cyber Warfare* represents the conflict environment and the type of strategic pressure; *Security Culture* represents the socio-organizational dimension through which actors perceive and internalize risk; *Organizational Resilience* represents the actual capacity to cope with disruption. In this context, security culture is not synonymous with resilience, but it constitutes one of the essential prerequisites for achieving it.

2. Methodology

The article employs a qualitative methodology structured around three complementary methods: doctrinal analysis, legal-institutional analysis, and case study. This methodological approach is appropriate because the research does not aim to statistically measure individual behaviors, but rather to examine the relationship between norms, institutions, coordination mechanisms, and security concepts within a specific national context.

The doctrinal analysis aims to define key concepts and situate them within the specialized literature on *Cyber Warfare, Security Culture*, and *Organizational Resilience*. The legal-institutional analysis examines the relevant legislation and documents that define competencies, alert mechanisms, and the coordination architecture at the national and European levels. The case study applies these frameworks to Romania, with a focus on the DNSC, SNAC, the Cyber Security Operational Council (COSC), the National Center for Cyber Security Crisis Management (CNGCSC), and integration with the European mechanisms provided for by the NIS2 Directive.

The analyzed corpus includes national legislation, administrative norms and methodologies, European documents, institutional sources from ENISA (ENISA 2026), DNSC (DNSC 2026) and NATO (NATO 2026b), as well as academic works relevant to security culture and resilience. From a research design perspective, Romania is treated as a "*most likely case*" for analyzing how legal and institutional consolidation can create the conditions for the maturation of security culture, without this automatically proving the existence of a fully empirically validated causal relationship.

To avoid speculative claims, this paper employs an explicit set of analytical criteria to assess the contribution of the regulatory and institutional framework to the culture of security and resilience: the clarity of roles and responsibilities; the existence of alert and escalation mechanisms (DNSC 2025); the capacity for inter-institutional coordination; the integration of public communication; the inclusion of exercises, planning, and learning; the alignment with European and Euro-Atlantic mechanisms.

The limitations of the research stem from the fact that the scientific study did not include interviews, sociological surveys, sets of quantitative indicators, or systematic comparisons across multiple countries. For this reason, conclusions regarding the effects on security culture are formulated cautiously, in terms of "institutional premises," "enabling mechanisms," or "conditions of possibility," rather than as definitive empirical demonstrations.

3. The European architecture of cyber resilience

In recent years, the European Union has shifted from an approach centered predominantly on technical cooperation to a more complex architecture for managing cyber incidents and crises (ENISA 2026). In this evolution, ENISA, the EU Network of *Cyber Security Incident Response Teams* (CSIRTs Network), and, more recently, EU-CyCLONe have become central elements of a multi-level governance framework oriented not only toward technical response, but also toward strategic coordination and shared situational awareness (EUR-Lex 2022).

The NIS2 Directive is particularly relevant, as it contains provisions that structure cooperation among EU MS around clearer obligations regarding risk management, incident notification, coordination, and preparedness. Article 16 of the NIS2 Directive establishes the role of EU-CyCLONe in the strategic coordination of large-scale cyber incidents and crises, complementing the more technical role of the CSIRTs Network.

This technical-strategic duality is important for the subject under study. It suggests that cyber resilience can no longer be reduced solely to the technical capability of detection and remediation (EUR-Lex 2024), but it also entails institutional mechanisms for interpretation, decision-making, communication, and cooperation across different levels of governance. From this perspective, the European model offers a useful framework for understanding how cybersecurity is progressively integrated into the broader logic of democratic and institutional resilience.

Furthermore, European initiatives regarding crisis exercises, the cybersecurity reserve, and cross-border interoperability point to a significant doctrinal shift: the focus is shifting from securing infrastructure to preparing public systems for continuity, cooperation, and recovery. This shift has direct consequences for EU MS, including Romania, as it compels national institutions to develop mechanisms that are compatible both technically and procedurally.

4. The Regulatory and Institutional Framework in Romania

4.1. From fragmentation to coordination

At the national level, recent developments point to a consolidation of the cybersecurity and defense architecture. Through G.E.O. No. 104/2021 (Art. 3(o) and

Art. 17) (Romanian Government 2021), the role of the DNSC in managing cyber crises during peacetime was strengthened, and the institutional foundations were laid for the operation of a national cyber security crisis management center.
Law No. 58/2023 has further developed this framework, establishing an integrated institutional framework for the management of cyber risks, incidents, and crises. From the perspective of this study, the law's significance lies not only in the introduction of obligations and competencies, but also in the formalization of a logic of strategic coordination among different institutional levels (Romanian Parliament 2023).
The role of the COSC, its relationship with the DNSC, and the Supreme Council for National Defense (CSAT) (CSAT 2026), as well as the mechanisms associated with cyber alert levels, indicate an attempt to overcome the traditional fragmentation of responsibilities. In analytical terms, this can be interpreted as a favorable condition for a security culture, as clarity of responsibilities and the existence of a decision-making chain reduce organizational ambiguity and increase the predictability of the response.

4.2. Operationalization of the SNAC

The implementation of the National Cyber Alert System, pursuant to DNSC Order No. 180/2024 approving the Methodology on cyber alert levels and procedures for action in cyber alert situations (DNSC 2024) is one of the most relevant aspects of the topic addressed in this article. The SNAC is not merely a technical tool for risk reporting, but also a mechanism with cultural and organizational potential, as it connects technical analysis, institutional decision-making, and public communication.
From the perspective of security culture, the relevance of SNAC stems from three elements: the standardization of the response through alert levels and associated action plans; the inclusion of private and sectoral actors in the logic of alerting and preparedness; and the public communication dimension, which creates the possibility of transitioning from exclusively technical governance to one that addresses social behaviors and perceptions.
However, it is important to make the following methodological clarification: the fact that the SNAC is designed to contribute to awareness and coordination does not automatically demonstrate its actual effect on security culture. In the absence of data regarding the public's understanding of alerts, the level of compliance among targeted actors, or the impact of exercises and notifications on behavior, the appropriate conclusion is that SNAC establishes a mechanism with the potential to foster a security culture, not that it has already demonstrably produced societal maturation.

4.3. Integration with European mechanisms

An important aspect of the Romanian case is synchronizing the national architecture with the mechanisms outlined in the NIS2 Directive. G.E.O. No. 155/2024 and its subsequent approval by Law No. 124/2025 (Romanian Parliament 2025) consolidated this synchronization by establishing DNSC as the national authority for managing cyber crises in peacetime and as the contact point for EU-CyCLONe.

In 2024, Romania demonstrated the practical application of this framework by activating the relevant procedures in the context of election security. In this context, the DNSC operated simultaneously in coordination with:

- ENISA, for strategic support and information-sharing tools;
- EU-CyCLONe, where the network level was escalated to *Warning Mode*, activating dedicated channels and operational cooperation;
- the ENISA Network of Liaison Officers (NLO Network), for briefings and information requests;
- EU CSIRTs Network, where the transition to *Alert Cooperation Mode* was discussed, and relevant technical data was shared.

This example is significant because it highlights the shift from mere legislative transposition to the operational use of cooperation channels.

From an analytical perspective, these aspects support the idea that resilience is not merely an internal attribute of the state but also the result of being part of a broader cooperative framework. In this sense, the culture of institutional security must also be understood as a culture of interoperability, information sharing, and shared reflexes for action (Cheng 2023).

From the same perspective, EU-NATO convergence complements the European dimension of cyber resilience. For Romania, NATO's relevance lies not only in the strictly military dimension but also in the civil–military integration of planning, exercises, and strategic risk assessment. Mechanisms such as the *Cyberspace Operations Centre* (CyOC), the *NATO Integrated Cyber Defence Centre* (NICC), and the *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) provide a useful framework for lessons learned, exercises, and doctrinal interoperability, while initiatives such as the *Defence Innovation Accelerator for the North Atlantic* (DIANA 2026) and the *NATO Innovation Fund* (NATO 2026a) indicate that technological innovation and cooperation with the civilian sector are becoming part of the broader ecosystem of defense and digital resilience (NATO 2025). In this sense, this convergence reinforces the idea of resilience as a product of multi-level cooperation, not just national capability.

4.4. Democratic oversight and constitutional legitimacy

The case law of the Constitutional Court of Romania (CCR) (CCR 2026) establishes a clear framework: **the security of networks and information systems is no longer a purely technical field, but one of general interest, closely intertwined with national security**.

This issue is relevant not only from a legal standpoint but also from a conceptual one. In Decision No. 17/2015 (CCR 2015), the Constitutional Court of Romania draws a clear political and institutional line: **the coordination of cybersecurity at the national level must be exercised by a civilian body, under democratic control, not by intelligence, law enforcement, or defense agencies**.

The choice of who coordinates cybersecurity at the national level matters for the security culture for at least two reasons. First, legitimacy and public trust can

be affected by perceptions of the institutions coordinating security. Second, a democratic security culture cannot be built sustainably outside the requirements of normative clarity, proportionality, and the protection of fundamental rights.
Therefore, the constitutional and conventional framework is not external to resilience but is part of its conditions. Resilience built through opaque, disproportionate, or insufficiently controlled measures can generate reactions of distrust that weaken the very security culture it claims to strengthen.

5. The impact on security culture and organizational resilience

Cyber warfare has effects that extend beyond the strictly technical realm of securing networks and information systems, influencing security culture, institutional coordination, and organizations' ability to function under pressure and in stressful conditions. In this context, organizational resilience must be understood not only as the ability to ensure operational continuity but also as the capacity to anticipate, absorb, adapt to, and integrate the lessons learned from cyber incidents, hybrid campaigns, and disruptions encountered at the strategic level. In Romania's case, recent legislative and institutional developments suggest a shift from a predominantly technical approach to one of strategic governance, in which security culture becomes the connecting variable between norms, institutions, and organizational behaviors.

5.1. From technical protection to organizational security culture

One of the main consequences of cyber warfare is the shift in emphasis from exclusively technical protection toward organizations' ability to react coherently and adaptively under conditions of persistent stress. Sophisticated attacks, supply chain exploitation, and influence campaigns show that vulnerability stems not only from a lack of technical controls but also from deficiencies in coordination, communication, and institutional learning. From this perspective, a security culture entails more than formal compliance: it involves organizational reflexes, clear decision-making, and the transformation of rules into repetitive and internalized practices.

5.2. Institutional architecture and its impact on resilience

In Romania, Law No. 58/2023, G.E.O. No. 155/2024, the operationalization of the SNAC, and the integration with NIS2 mechanisms create important conditions for strengthening organizational resilience. This framework reduces fragmentation, clarifies roles, and introduces a logic of alerting, escalation, and coordination that can standardize the institutional response in crisis situations. However, the relationship between institutional architecture and security culture must be framed cautiously: the existence of procedures and competencies is a necessary condition, but not sufficient proof that organizations have internalized stable security behaviors.

5.3. The Societal and Cognitive Dimensions of Security Culture

The impact of cyber warfare is not limited to institutions but extends to how society

perceives risk and reacts to digital crises. In practice, the most significant effects occur when cyber incidents are accompanied by disinformation, information pressure, and the erosion of trust in institutions (Maftei 2025). In this context, the public communication component associated with SNAC is important because it can support faster and more proportionate responses, without, however, automatically transforming cybersecurity into a mature societal culture. The outcome will depend on the continuity of communication, institutional credibility, and the public's ability to interpret risk signals (Fomnya 2024).

5.4. The skills, the human factor, and the challenge of the Artificial Intelligence era

Another major effect of the transformation of the security environment is the growing importance of digital skills. The accelerated integration of Artificial Intelligence (AI) into operational and decision-making processes compels organizations to simultaneously manage classic cyber risks and risks associated with the interaction between people, data, and automated systems (Palma 2026). In this context, resilience depends not only on technology but also on having personnel capable of understanding the limits of automation, critically using digital tools, and maintaining human control over sensitive processes (Maftei 2024).

5.5. Implications for Romania

For Romania, the impact of cyber warfare on security culture and organizational resilience must be understood at the intersection of governance, administrative capacity, and professional training. The recent regulatory framework, the role of the DNSC, the functioning of the SNAC, and European interoperability provide a more robust coordination infrastructure than in the previous phase, but its lasting effect depends on recurring exercises, evaluation, continuous training, and the integration of lessons learned into institutional practices.

Consequently, strengthening the security culture cannot be treated as an automatic result of legislative reform, but rather as a continuous process of operationalization, coordination, and learning. This process requires clear planning mechanisms, the distribution of responsibilities among public and private actors, and the transformation of legal norms into verifiable organizational routines.

In practical terms, developing organizational resilience requires the consistent implementation of crisis planning, the regular conduct of interagency exercises, the integration of lessons learned into procedures, and the strengthening of public communication during alerts. At the same time, responsibility does not lie exclusively with central authorities but must be shared among competent public institutions, operators of essential services, private organizations, and actors involved in professional training.

In this context, a culture of security functions not merely as a regulatory requirement, but as a social and organizational practice, dependent on the continuity of institutional operations, the clarity of the decision-making chain, and the ability of relevant actors to cooperate under conditions of pressure and uncertainty.

Precisely for this reason, the essential step for Romania is not merely to strengthen the legal framework but to transform it into an effective mechanism for adaptation, coordination, and resilience.

Conclusions

This analysis shows that Romania is in a phase of significant regulatory and institutional consolidation in the field of cybersecurity and cyber defense. Recent legislative and administrative developments indicate the existence of a clearer architecture for European alerting, coordination, and interoperability compared to the previous period, particularly through the role of the DNSC, the operationalization of the SNAC, and integration into the mechanisms associated with the NIS2 Directive.

The answer to the research question is, however, nuanced. Romania's regulatory and institutional cybersecurity architecture contributes to the development of a security culture and organizational resilience by clarifying roles, standardizing alerts, strengthening coordination, and connecting to European and Euro-Atlantic cooperation networks. However, these developments must be interpreted cautiously. They create solid premises for strengthening security culture, but do not, by themselves, equate to demonstrating full internalization of security behavior at the organizational and societal level.
The main finding of the scientific study is, therefore, conditional. Romania has more robust legal and institutional foundations for strengthening resilience, but the lasting effects of this framework remain dependent on the implementation and transformation of norms into stable institutional practices.

The study also suggests that organizational resilience should be viewed within a broader framework than that of technical security. It includes institutional coordination capacity, public communication, European and Euro-Atlantic interoperability, as well as the preparation of a workforce capable of operating in an environment characterized by the convergence of cyber threats, information pressure, and the widespread use of AI.

In terms of public policy, four priority areas emerge. **The first** of these relates to the development of maturity indicators for security culture and organizational resilience in the public sector and in critical sectors. **The second** priority area concerns the strengthening of national exercises and interoperability with European and NATO mechanisms, with the integration of lessons learned into the regulatory and operational cycle. **The third** priority area is the one of strengthening public communication and digital literacy, with a focus on prevention and proportionate response. **The fourth** one involves adapting professional training to the new risks associated with the use of AI, automation, and human-system interaction in critical processes.

Therefore, the main challenge for cybersecurity and cyber defense in Romania is not merely the development of superior technical capabilities, but transforming these into an institutional and organizational culture robust enough to support resilience in a persistently contested strategic environment.

References

CCR. 2015. „Decizia nr. 17 din 21 ianuarie 2015 asupra obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României." https://www.ccr.ro/wp-content/uploads/2020/07/Decizie_17_2015.pdf.

___. 2026. *Curtea Constituțională a României.* https://www.ccr.ro/.

Cheng, Joseph. 2023. „Building Cyberresilience From Collaborative Culture." *ISACA*. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/building-cyberresilience-from-collaborative-culture.

CSAT. 2026. *Consiliul Suprem de Apărare a Țării.* https://csat.presidency.ro/.

DIANA. 2026. *Defence Innovation Accelerator for the North Atlantic.* https://www.diana.nato.int/.

DNSC. 2024. *ORDIN nr. 180 din 21 februarie 2024 pentru aprobarea Metodologiei privind nivelurile de alertă cibernetică și modalitățile de acțiune în situații de alertă cibernetică.* https://legislatie.just.ro/Public/DetaliiDocument/279736.

___. 2025. „Raport anual de activitate 2024." https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024.

___. 2026. *Directoratul Național de Securitate Cibernetică.* https://www.dnsc.ro/.

ENISA. 2026a. *EU incident response and cyber crisis management.* https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management.

___. 2026b. *European Union Agency for Cybersecurity.* https://www.enisa.europa.eu/.

EUR-Lex. 2022. „Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

___. 2024. „Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale." *Cyber Resilience Act*. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

Fomnya, Hyelda Joseph. 2024. „The Influence of Cybersecurity. Risk Management Practices on Organizational Resilience." *Hallford Education.* https://hallford.education/wp-content/uploads/2026/01/The-Influence-of-Cybersecurity-Risk-Management-Practices-on-Organizational-Resilience.docx.pdf.

Hilio. 2025. *Reziliența individuală și organizațională – Definiție, rol și strategii de dezvoltare.* https://hilio.com/ro/blog/humancapital/ce-este-rezilienta-organizationala.

Huang, Keman, and Keri Pearlson. 2019. "For What Technology Can't Fix:Building a Model of Organizational Cybersecurity Culture." *Proceedings of the 52nd Hawaii International Conference on System Sciences.* doi:https://doi.org/10.24251/HICSS.2019.769.

Lin, Herbert. 2012. „Cyber conflict and international humanitarian law." *International Review of the Red Cross* 94 (886): 515-531. https://international-review.icrc.org/sites/default/files/irrc-886-lin.pdf.

Lyons, Jessica. 2025. *Russian spies pack custom malware into hidden VMs on Windows machines.* https://www.theregister.com/2025/11/04/russian_spies_pack_custom_malware/?cid=soc%7Cn%7Csprout%7Cemp&blaid=8069358.

Maftei, Dănuț. 2024. „The Cyber Competences Act - a Vital EU Regulation Concerning Mandatory Certification of Critical Network and Information Systems' Operators across the European Union." *Informatica Economică* 28 (2): 45-60. doi:10.24818/issn14531305/28.2.2024.04.

___. 2025. „"Three Warfares" versus "Hybrid Warfare". New Generation Warfare – New Approaches and Challenges." *Revista GeoPolitica.* https://www.geopolitic.ro/in/topics/geointellicence/page/2/.

Mishra, Siddhant. 2025. *Inside the Shellcode: Dissecting North Korean APT43's Advanced PowerShell Loader.* https://systemweakness.com/inside-the-shellcode-dissecting-north-korean-apt43s-advanced-powershell-loader-e6c51b77f486.

NATO. 2026a. *NATO Innovation Fund.* https://www.nif.fund/.

___. 2026b. *North Atlantic Treaty Organization.* https://www.nato.int/en.

___. 2025. „Request for Information (RFI) to engage with industry, academia and nations." https://www.act.nato.int/wp-content/uploads/2025/12/rfi025112.pdf.

Palma, Bryan. 2026. *The cybersecurity paradox: training the next generation workforce.* https://www.weforum.org/stories/2026/01/cybersecurity-paradox-training-the-next-generation-workforce/.

Presidency. 2015. „Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019." https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019.

Romanian Government. 2021. *ORDONANȚĂ DE URGENȚĂ nr. 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică.* https://legislatie.just.ro/Public/DetaliiDocumentAfis/246652.

___. 2024. *Ordonanță de urgență nr. 155 din 30 decembrie 2024 privind instruirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil.* https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121.

Romanian Parliament. 2025. *Lege nr. 124 din 7 iulie 2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil.* https://legislatie.just.ro/public/DetaliiDocument/299675.

___. 2023. *Lege nr. 58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.* https://legislatie.just.ro/Public/DetaliiDocument/265677.

Sutton, Anna, and Lisa Tompson. 2023. "Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review." https://doi.org/10.31234/osf.io/h4uby.

Taddeo, Mariarosaria. 2012. „An analysis for a just cyber warfare." *2012 4th International Conference on Cyber Conflict (CYCON 2012).* Tallinn, Estonia. https://ieeexplore.ieee.org/document/6243976.