Revista de Științe Politice. Revue des Sciences Politiques • No. 90 • 2026: 188 – 200

ORIGINAL PAPER

Cybersecurity and institutional trust in digital governance: lessons from Romania and the European Union

Diana-Maria Grosu[1)]

Abstract: The accelerated digitalization of public administration in Romania and the European Union offers new perspectives for efficiency, but simultaneously intensifies structural risks associated with cybersecurity. The scope of this research is to evaluate the interdependence between cybersecurity performance and the dynamics of institutional trust. The central question guiding this research examines to what extent cybersecurity acts as a pillar for strengthening trust or, conversely, generates new forms of vulnerability and institutional exclusion. To this end, the research employs a comparative policy analysis framework, triangulating data from public policy documents, institutional reports, and national and European cyber incident databases. The study highlights the main threats (ransomware, DDoS, cyber espionage) and structural vulnerabilities affecting institutional response. The analysis answers the central question by demonstrating that in Romania, trust is undermined not by the threats themselves, but by institutional and coordination deficiencies. Drawing from these findings, the study concludes that personal data protection is an implicit pact whose breach directly affects the legitimacy of institutions. Finally, the research argues for strategic alignment with European directives (NIS 2, GDPR) to reposition cybersecurity as a tool for institutional integrity rather than a systemic vulnerability. Ultimately, the research concludes that a robust cybersecurity posture serves as the essential guarantor of digital sovereignty, transforming administrative modernization into a sustainable engine for public trust and democratic resilience.

Keywords: *digital governance; public administration; democratic accountability; public policy; cyber vulnerability*

[1)] PhD student, Department of Political Sciences, International Relations and European Studies, Faculty of Philosophy and Social Political Sciences, "Alexandru Ioan Cuza" University of Iași, Address: Carol I Boulevard no. 11, 700506, Iasi, Romania; Phone: 0741 738 571; E-mail: dianagrosum@yahoo.com; ORCID ID: 0009-0002-8256-7600.

Cybersecurity and institutional trust in digital governance: lessons from Romania and the European Union

Introduction

Beyond its technical dimensions, cybersecurity is currently redefined as a multidimensional pillar of national and European strategic stability (Apachiței, 2021), requiring a shift from reactive to proactive defense approaches. To ensure data and system integrity, cybersecurity governance deploys a cohesive set of institutional standards and regulatory policies (Mijwil et al., 2023: 3). In global competition, cyber-attacks now serve as pivotal tools for economic sabotage and espionage (Bouhafs, 2025: 2). This shift creates opportunities, but also major risks related to data security and digital infrastructure vulnerability. Recent assessments indicate limited cybersecurity readiness across core NIST functions, highlighting systemic vulnerabilities in digital governance (Hossain et al., 2025: 2).

On a global scale, digitization has become a fundamental tool for improving and modernizing public administration and strengthening the relationship between the state and society. At the same time, increasing dependence on digital infrastructures amplifies cyber risks, especially those affecting the confidentiality and integrity of public information. The efficiency of digital public services is closely linked to public trust in data protection systems (Schneider, 2025: 1-3).

The European Union (EU), for its part, faces the challenge of balancing technological innovation and data protection. Farrand and Carrapico examine how the discourse on *digital sovereignty* has become central to European policy, marking a shift from regulatory capitalism—based on extensive collaboration with the private sector — to regulatory mercantilism, aimed at reducing dependence on external technology providers. The authors show that the Union aims to reassert its control over digital infrastructures and cyberspace as an expression of citizen protection and strategic autonomy (Farrand & Carrapico, 2022: 435–437). The EU has developed a coherent regulatory framework that includes the NIS 2 Directive, the General Data Protection Regulation (GDPR), and the European Union Cybersecurity Act, which provide uniform protection for critical infrastructure and personal data. At the same time, a report by the European Court of Auditors draws attention to the fact that legislative fragmentation and insufficient coordination between Member States limit the effectiveness of common cybersecurity policies. The lack of consistent operational cooperation between national and European agencies affects the implementation of security standards at the level of public administrations (European Court of Auditors, 2019: 5–6). NIS2 represents the EU's primary regulatory instrument for fortifying cybersecurity standards across Member States (Kianpour et al., 2025: 167).

The Romanian state is aligning itself with this European direction by creating a complex strategic framework, represented by the National Cybersecurity Strategy 2022-2027, supported by specialized institutions - Romanian National Computer Security Incident Response Team CERT-RO2, National Cybersecurity Coordination Center (CNCS), Special Telecommunications Service (STS), and Authority for the Digitization of Romania (ADR).

At a theoretical level, recent studies in the specialized literature emphasize that digitization, while bringing democratic benefits, can trigger systemic vulnerabilities when cybersecurity is not viewed as a fundamental dimension of governance. Govindraj

2 The National Cyber Security Directorate (DNSC) is the legal successor of the National Cyber Security Incident Response Team (CERT-RO), having taken over its activities, attributions, and staff since 2021.

demonstrates that digital governance and cybersecurity are inseparable concepts: attacks on public infrastructure can influence not only the functionality of the administration, but also public perception of the legitimacy of institutions, gradually weakening citizens' trust in the state (Govindraj, 2024). Based on these aspects, this paper aims to analyze the relationship between cybersecurity and institutional trust in digital governance. The main question guiding the study is the following: to what extent does cybersecurity, in the context of digital governance, help strengthen the trust and accountability of the state or, on the contrary, produce new forms of vulnerability and institutional exclusion?

To answer this question, the research is based on a comparative perspective between Romania and other European Union member states, focusing on digital infrastructure, institutional response capacity, regulations, and public perception of data protection. The ultimate goal of the study is to demonstrate that cybersecurity is not just a technological component, but a fundamental prerequisite for democratic accountability and the legitimacy of the digital state.

2. Theoretical and conceptual framework

2.1. The interdependence of digital governance, cybersecurity, and trust

Digitalization can be understood as a fundamental element of modern administration, supporting both institutional resilience and public safety (Mureșan, 2025: 256–257). Schneider points out that, in the context of digital governance, cybersecurity is *a basic pillar of good governance* because it ensures the confidentiality, accessibility, and reliability of digital services provided to citizens (Schneider, 2025: 2).

Institutional trust refers to the extent to which community members perceive public authorities as competent, open, and willing to protect their needs and confidential data. In his paper, Saqib Saeed shows that the use of digital public services is directly influenced by the level of trust citizens have in the security and confidentiality of information provided by government institutions. (Saeed, 2023: p. 2–3). Institutional trust increasingly depends on the state's ability to manage personal data and ensure digital infrastructure integrity. The author proposes a user-centered privacy perspective, which requires citizen involvement in the design of security tools in order to increase the level of acceptance and use of electronic services (Saeed, 2023: 5–6). Therefore, trust becomes a key element essential for the smooth running of digital governance, based on the balance between efficiency and security. Schneider demonstrates that successful digital governance models integrate adaptive digital protection strategies with public-private collaboration tools, using innovative technologies such as artificial intelligence and distributed ledgers to reduce risk and strengthen public trust. (Schneider, 2025: 5) At the same time, Mureșan emphasizes the idea that advanced administrations are required to develop integrated digital resilience, combining regulation, professional training, and interinstitutional cooperation to strengthen the protection of public infrastructures (Mureșan, 2025: 257).

At the European level, Petersons observes that policies on digital governance – including the GDPR, the Digital Markets Act, and the Digital Services Act – aim to balance technological progress with data security and fundamental rights. Cybersecurity is therefore becoming a cross-cutting element of all European digital governance rules (Petersons, 2025: 2–4). In modern literature, the concept of trust-by-design has gained relevance, highlighting the fact that citizens' trust in digital services must be strengthened from the system design stage. Saeed suggests a model in which data protection and security are user-centered design elements, rather than after-the-fact control functions (Saeed, 2023: 6–7).

2.2. Digital sovereignty and democratic legitimacy

Democratic accountability in the context of digitalization refers to the ability of institutions to manage digital technologies in a transparent, ethical, and inclusive manner, while maintaining public control over decision-making processes. As highlighted by Hulkó et al. (2025: 1–2), the process of digitalization redefines state responsibilities, as areas such as data protection, regulation, and digital infrastructure are increasingly closely linked to the protection of citizens' fundamental rights. Therefore, protecting cyberspace is not only a matter of security, but also an act of strengthening democracy and civic control over technology.

Cyber protection can no longer be separated from the democratic legitimacy of institutions. Farrand and Carrapico demonstrate that, in the era of digital sovereignty, securing infrastructure and information is not just a technological priority, but rather a condition for the political and financial independence of European states (Farrand & Carrapico, 2022: 436–437).

Similarly, Hulkó argues that losing control over digital infrastructures can compromise not only national security, but also society's perception of the state's ability to defend it, thus affecting democratic trust (Hulkó et al., 2025: p. 3). Consequently, legitimacy in digital governance stems from the state's ability to maintain a balance between effectiveness, data protection, and civic engagement, making cybersecurity a constituent element of democratic engagement.

- **Methodology**
  - **European models and analysis criteria**

This study takes a comparative approach to highlight how different European Union member states deal with the relationship between cybersecurity and institutional trust in digital governance. According to Petersons, the mechanism for developing digital policies in the EU is represented by a variety of national models which, although converging towards the same standards (GDPR, Network and Information Security Directive 2 **-** NIS2, Cybersecurity Act), differ in terms of their degree of implementation and institutional coherence (Petersons, 2025: 3–5). In this context, Estonia is analyzed as a model of comprehensive digital transformation; Germany, as an example of institutionalized regulation; and the Netherlands, as the initiator of public-private partnerships in critical infrastructure protection (European Court of Auditors, 2019: 6–7).

a. Structure of the analysis and data sources

The analysis is structured around: 1. Digital infrastructure and its protection – the level to which public systems are protected by standards, audits, and critical incident response protocols (Mureșan, 2025: 258); 2. Institutional response capacity – the presence of integrated tools for cooperation between institutions and immediate response to cyber threats (Schneider, 2025: 4); 3. Legislative framework and national policies – consistency between national legal norms and European directives on data security, communications infrastructure security, and digital governance (Petersons, 2025: 4–5); 4. Public perception and level of trust – how society assesses the security of digital public services and the level of openness of institutions. Saqib Saeed highlights that end-user perception is fundamental to the success of any e-government strategy, as trust is a direct result of perceived security (Saeed, 2023: 6).

The research is based on a comparative assessment of national cybersecurity strategies, public reports from National Cyber Security Directorate (DNSC), National Cybersecurity Coordination Center **(**CNCS), Special Telecommunications Service (STS), and Authority for the Digitalization of Romania (ADR), as well as official European

Union documents (NIS2 Directives, GDPR, EU Cybersecurity Act). Furthermore, assessments and studies carried out by European Union Agency for Cybersecurity – ENISA (2023), Organization for Economic Co-operation and Development (OECD), and the European Court of Auditors were consulted, providing a unified perspective on the performance of Member States in implementing the European digital security framework (European Court of Auditors, 2019: 5–8). The methodological perspective fits into a qualitative-descriptive model, aiming to examine policy content and recognize institutional patterns rather than statistically measure performance. The study has inherent limitations due to the absence of uniform public data on security incidents and the degree of public trust. However, by combining institutional and theoretical perspectives, the research contributes to a better understanding of how cybersecurity determines legitimacy and democratic accountability. Mureșan believes that, in a context of accelerated digital transformation, the ability of public authorities to prevent and manage digital risks is a fundamental benchmark of institutional legitimacy and governance efficiency. (Mureșan, 2025: 259).

4. European context and reference policies

Over the last 10 years, the European Union has consolidated an extensive regulatory framework designed to ensure the protection of critical digital infrastructure, the security of personal data, and the cyber resilience of Member States. According to Petersons, this development reflects the shift from market-oriented digital governance to rights- and security-oriented governance, in which citizen protection becomes fundamental. Petersons points out that the impact of the GDPR has gone beyond the borders of the EU, influencing data protection legislation in many other regions of the world (Petersons, 2025: 2–4). However, according to the European Court of Auditors' assessment, the success of these provisions depends on the level of cooperation between national and European agencies, which often remains insufficient (European Court of Auditors, 2019: 5–6).

4.1. National models: Estonia, Germany, and the Netherlands

In her analysis, Mureșan demonstrates that the success of the Estonian model stems from a correlation between secure technological infrastructure (the X-Road system), digital education, and an institutional culture supported by trust and openness (Mureșan, 2025: 258). According to the European Court of Auditors, this mechanism is achievable thanks to close collaboration between public institutions and the private sector, as well as precise legislation on data privacy (European Court of Auditors, 2019: 7). Petersons highlights that this model illustrates the principle of national responsibility for digital security, with the BSI acting as the pivotal authority for implementing NIS standards and collaborating with European agencies (Petersons, 2025: 4–5). Farrand and Carrapico state that Germany is one of the first countries to include digital sovereignty in its national security plan, allocating resources to its own cloud infrastructures and information centers to reduce dependence on external actors (Farrand & Carrapico, 2022: 437). According to the European Court of Auditors report, this approach is particularly effective in the field of critical infrastructure (transport, energy, communications), where private sector participation allows for rapid identification of threats and a coordinated response (European Court of Auditors, 2019: 8). Table 1 illustrates that trust, institutional coordination, and cooperation among stakeholders are important for the effectiveness of digital services. Estonia, Germany, and the Netherlands exemplify three different models of digital governance and cybersecurity, based on digital identity, centralization, and public-private partnerships.

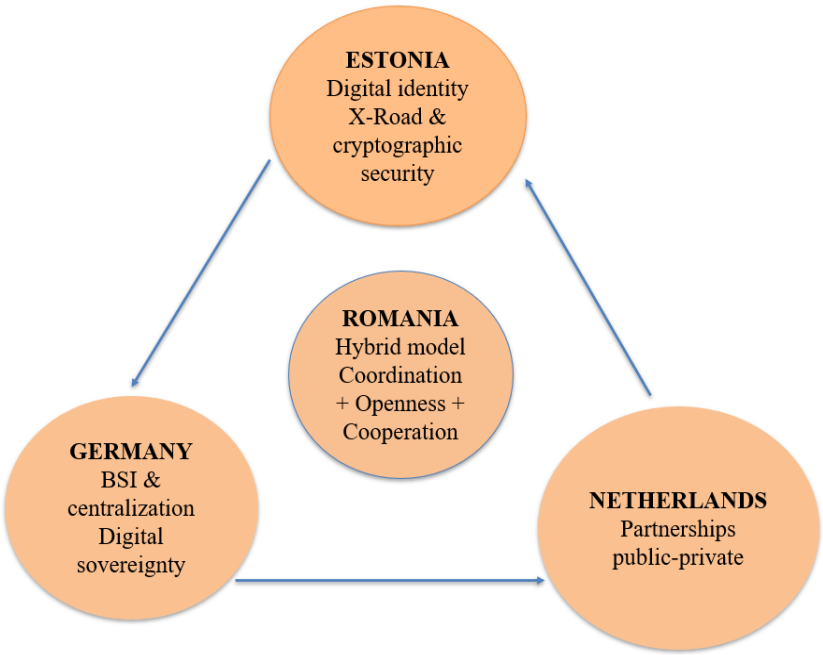
Table 1. Digital governance and cybersecurity models: Estonia, Germany, Netherlands

Country	Model type	Key security feature	The Role of Trust	Relevance for Romania
Estonia	Unique Digital Identity + X-Road	Cryptographic Security and Digital Literacy	An institutional culture based on openness	Interoperability and integrated digital services
Germany	Centralization via BSI + digital sovereignty	National Pivot Authority + NIS Standards	Clear national responsibility	Institutional coordination
Netherlands	Public–private partnerships	Protection of Critical Infrastructure	Transparency and data sharing	Cooperation with the private sector

Source: Author's own work

Figure 1 illustrates how Romania can evolve by integrating European influences, such as Estonia's transparent organizational architectures or the public-private partnerships characteristic of Germany and the Netherlands. This model emphasizes that institutional trust is built through both technological resilience and proactive cybersecurity strategies.

Figure 1. European digital governance models relevant for Romania



Source: Author's own work

5. Analysis of the situation in Romania

5.1. Institutional framework and national objectives

Romania has made considerable improvements in developing its institutional and regulatory framework for cybersecurity, particularly since joining the European Union. The National Cybersecurity Plan 2022–2027 sets out the main national objectives in this area, focusing on the defense of critical infrastructure, interinstitutional administration, and increasing technological resilience. Mureșan notes that these goals clearly align with European directives, but their implementation is often hampered by coordination deficiencies and limited human resources (Mureșan, 2025: 258–259).

The national framework relies on a network of institutions with complementary competences, including the DNSC for managing incidents, the STS for secure communications, the CNCS for policy coordination, and the ADR for implementing digital public services. Table 2 illustrates the complementary and clear distribution of roles among key institutions in cybersecurity, ranging from operational response to strategic coordination and the implementation of secure digital services, emphasizing the importance of collaboration for a resilient digital ecosystem.

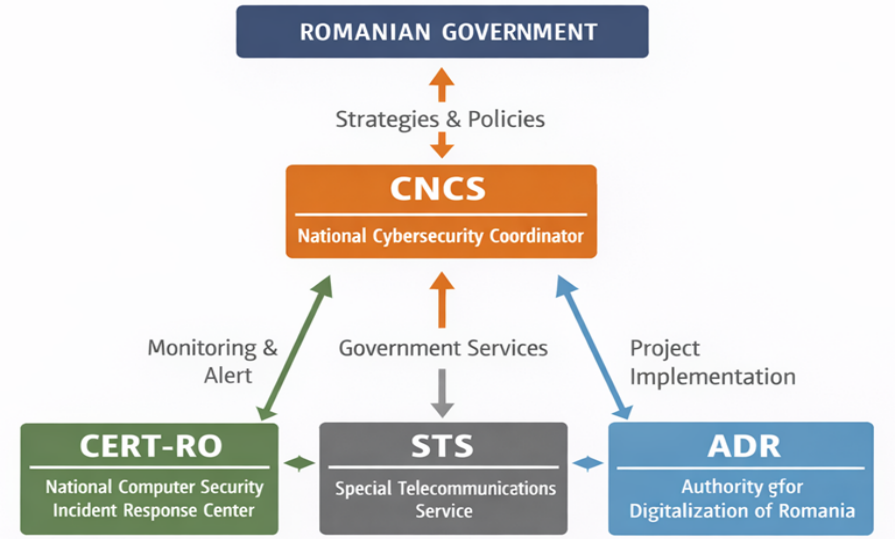
Table 2. The matrix of cyber risks and protection mechanisms in the digital transformation process

Institution	Lead role	Role in the national cybersecurity architecture
DNSC	Cyber Incident Management;	Detection, analysis, and operational response to attacks;
STS	Secure government communications;	Protecting critical transmission infrastructure;
CNCS	Strategic coordination;	Development and harmonization of security policies;
ADR	Public digitization;	Implementation of secure digital services;

Source: Author's own work

Limited inter-institutional coordination and overlapping responsibilities remain major impediments to effective digital governance (Petersons, 2025: 4–5). Farrand and Carrapico argue that European states, including Romania, should strengthen their digital independence through domestic funding and regional partnerships, as excessive dependence on external technologies can undermine national security and responsiveness (Farrand & Carrapico, 2022: 436). Figure 2 outlines the strategic and legislative framework for cyber resilience in the public sector, emphasizing institutional coordination.

Figure 2. The strategic and legislative framework for ensuring cyber resilience in the public sector



Source: Author's own work

The failure to prioritize digital modernization has kept many institutions stuck in the traditional bureaucratic model, while others have developed isolated digital solutions. As noted by Mărcuț (2021), the lack of coherent digital modernization has led to institutional fragmentation and the absence of an integrated governance framework.

5.2. Emerging threats and structural vulnerabilities

According to CERT-RO reports and European research, the most significant threats to Romania's public digital infrastructure are ransomware attacks, widespread DDoS attacks, data loss, and cyber espionage campaigns. Schneider clarifies the idea that ransomware attacks target institutions that manage large databases and critical infrastructure, exploiting human vulnerabilities and the lack of system upgrades (Schneider, 2025: 4–5). In Romania, such events have compromised medical facilities, local institutions, and administrative platforms in recent years. The same idea is supported by Saeed, who illustrates that the perception of insecurity in the digital environment leads to decreased civic participation and reluctance to use online services (Saeed, 2023: 6). Cyber espionage campaigns and phishing attacks are also on the rise, according to the European Court of Auditors. The lack of interoperability between systems and the use of outdated infrastructure increase the vulnerability of Romanian institutions to state or private actors interested in strategic data (European Court of Auditors, 2019: 7–8).

5.3. Challenges in digital governance and human resources

One of the most frequently mentioned difficulties in the literature is the lack of integrated cyber security governance. Mureșan highlights the fact that the institutions involved in protecting digital infrastructures in Romania sometimes operate in parallel, without a common data transfer platform and without standardized response procedures (Mureșan, 2025: 259). Petersons validates this view, arguing that decision-making fragmentation is a widespread European problem, but in countries with limited resources,

such as Romania, its consequences are much more visible (Petersons, 2025: 5). Qualified human resources are a critical element. Civil servants' digital skills are necessary for the effective use of technological tools and for the modernization of public institutions (ANFP, 2026: 2). In this context, Target 185 of the National Recovery and Resilience Plan aims to train 30,000 civil servants by mid-2026; by 30 September 2025, 27,859 participants had obtained certification (ANFP, 2026: 12).

The digitization of public administration must take into account not only services for the public but also the streamlining of internal workflows and the development of staff digital skills, so that digital tools can generate real efficiency (AmCham Romania, 2021: 5–6). Schneider demonstrates that effective implementation of cybersecurity requires human resources to receive ongoing training so that they can proactively recognize threats and respond effectively to incidents, which is often lacking in Eastern European administrations (Schneider, 2025: 3–4). Hulkó adds that the lack of specialized skills is exacerbated by competition with the private sector, which offers more attractive salaries, leading to the departure of IT specialists from the public sector (Hulkó, 2025: 3).

The insufficient digitization of human resources processes remains a significant challenge, as many departments still rely on manual procedures and paper documents. This slows down operations and reduces institutional efficiency (Rovner & Moore et al., 2024). Petersons believes that the lack of interoperability is a systemic risk, as it hinders the transfer of information in real time between authorities and weakens the effectiveness of the response in the event of an incident (Petersons, 2025: 6). Institutional culture is another vulnerable aspect. In many state institutions, awareness of cyber threats remains superficial. Similarly, Saeed notes that citizens' trust in public institutions is conditioned by the way in which they communicate and manage incidents, and that a lack of transparency can quickly erode the relationship between citizens and the administration (Saeed, 2023: 7–8).

5.4. The digital legitimacy of the Romanian state

Citizen trust is the foundation of any effective digital governance. When beneficiaries understand that their data is not being adequately protected, trust in digital services and, implicitly, in state institutions erodes. Hulkó argues that cyber vulnerabilities should be understood not only as technical problems, but also as forms of democratic weakness, because they call into question the state's ability to guarantee fundamental rights in the digital environment (Hulkó, 2025: 4). Therefore, the case of the Romanian state highlights the delicate balance between the ambition for digital modernization and the imperative to strengthen cyber protection mechanisms. In the absence of a security-oriented institutional culture and without continuous investment in human and technological resources, digitization can become a source of vulnerability rather than progress. However, by highlighting European examples and through stronger collaboration between state institutions, the Romanian state can turn cyber security into a real pillar of democratic trust and the legitimacy of digital governance.

6. Cybersecurity and public trust

Mureșan highlights the fact that the protection of personal data has become a central pillar of trust in the exercise of democratic governance, and that cybersecurity is what transforms this trust into institutional capital (Mureșan, 2025: 257–258). Saeed emphasizes that the adoption of electronic public services depends on citizens' trust in e-government channels and on the perceived usability of security and privacy mechanisms

(Saeed, 2023: 5). Digital trust depends on consistent security policies, transparency, and effective incident response.

Schneider (2025) shows that transparent communication of security measures strengthens public confidence in digital governance. In Romania, the lack of a consolidated institutional culture of confidentiality fuels a fragile perception of security. Mureșan notes that, for many citizens, cybersecurity is associated more with a technical risk than with a civic right, which limits the degree of digital participation (Mureșan, 2025: 259). This perception is also reflected in the reluctance to use public online platforms, a phenomenon which, in the absence of a communication strategy, may slow down the process of administrative modernization. Petersons shows that, in the European context, trust in digital governance depends on the combination of three factors: a unified regulatory framework (such as the GDPR), secure infrastructure, and effective public communication (Petersons, 2025: 2–4).

Security incidents have significant social and political consequences, undermining the relationship between citizens and the state. Farrand and Carrapico propose a complementary perspective: cyber vulnerabilities in state institutions can be interpreted as forms of democratic failure, as they reveal the authorities' inability to defend the digital sovereignty of citizens (Farrand & Carrapico, 2022: 435–453). At the same time, the European Court of Auditors points out that inadequate management of security incidents can have a domino effect, undermining confidence not only at national level but also across the European Union (European Court of Auditors, 2019: 6–7).

7. Public policy recommendations

Digital transformation in Romanian public administration cannot be separated from strengthening cybersecurity. As Mureșan emphasizes, digitalization that is not supported by a solid cybersecurity framework risk becoming a source of institutional vulnerability rather than a genuine form of modernization (Mureșan, 2025: 257–258). In order for digitization to become a means of democratic trust, the Romanian state needs to adopt systemic public policies that are coherent and harmonized with European practices. The first step is to strengthen coordination between the main actors — CNCS, DNSC, STS, and ADR. Farrand and Carrapico demonstrate that the success of the German (through Federal Office for Information Security - BSI) and Dutch models stems from the functioning of central institutions with regulatory and response powers, not just guidance (Farrand & Carrapico, 2022: 437). It would be advisable for the Romanian state to integrate the functions of strategy, monitoring, and response into a coherent national entity with a well-defined mandate and direct decision-making powers.

When it comes to cybersecurity, it cannot be separated from technological infrastructure. According to Schneider, outdated IT systems are the main risk factor in the functioning of digitized public administrations. (Schneider, 2025: 4). Romania must prioritize investments in a controlled transition to EU-certified cloud infrastructures, modernization of public computer networks, and the introduction of common encryption and identity verification standards. In addition to the technological component, the ongoing training of public officials is essential. Recommendations in this regard include developing a National Digital Literacy Program for the Public Sector, with modules on digital/cyber hygiene, response in case of a breach, identifying social engineering attacks, and ethics and responsibility in personal data management. Table 3 details the cybersecurity governance architecture, linking strategic planning with operational response through targeted training modules.

Table 3. The Architecture of Cybersecurity Governance: Linking Strategic Planning with Operational Response

Nr.	Training module	Main content	Objective
1.	Digital/Cyber Hygiene	Best practices for using IT systems	Incident Prevention
2.	Response in the event of a breach	Reporting and Rapid Response Procedures	Mitigating the impact
3.	Identifying social engineering attacks	Recognizing Phishing and Digital Manipulation	Increased vigilance
4.	Ethics and Professional Responsibility	Personal Data Protection and Legal Compliance	Compliance with GDPR regulations

Source: Author's own work

This initiative could be implemented through a partnership between ADR, universities, and ENISA, based on the model of the European Cybersecurity Skills Academy program. It is imperative that the Romanian state take a proactive stance in implementing the European regulatory framework – not just procedural compliance, but rather active participation in defining EU policies. Hulkó emphasizes that digital sovereignty does not imply withdrawal from international cooperation, but rather the ability to contribute fairly to the formulation of global norms (Hulkó, 2025: 4). Therefore, the Romanian state should accelerate the transposition of the NIS2 Directive and the future eIDAS 2.0 Regulation, incorporate European Union certification standards, and actively engage in cross-border interoperability initiatives, such as the European Digital Identity Wallet. Petersons notes that active involvement in digital governance at the European level is not only a technical issue, but rather a form of democratic accountability of public authorities, who have a duty to protect citizens in cyberspace as well (Petersons, 2025: 5–6).

Conclusions and Recommendations

Digitalization represents a structural transformation of the relationship between citizens and the state, with cybersecurity at its core. Citizen trust is a prerequisite for digital governance, while cybersecurity ensures the protection of this relationship.

In Romania, although specific strategies and institutions such as DNSC, STS, and ADR have been established, implementation is often hindered by fragmented inter-institutional coordination and limited human and financial resources. Structural vulnerabilities, such as the lack of interoperability between IT systems and an organizational culture in which information security is understood solely as a technical task, increase the risks associated with cyberattacks. Therefore, it is necessary to strengthen the institutional framework by establishing a single national coordination body to eliminate overlapping responsibilities and centralize real-time risk assessment. The proposals call for essential investments in EU-certified cloud infrastructure and the implementation of a national program for ongoing digital literacy training for public

servants, aimed at fostering a culture of cybersecurity hygiene and proactive threat identification.

Aligning with European standards such as the NIS2 Directive and GDPR will enable Romania to transform cybersecurity into a pillar of digital sovereignty and democratic trust.

References:

Agenția Națională a Funcționarilor Publici. (2026, March 23). *Cadrul de competențe digitale generale pentru funcționarii publici*. ANFP. Disponibil la: https://www.anfp.gov.ro/media/n1pf5hp5/cadru-competente-digitale-tsi-2024-concurs-national.pdf

AmCham România. (2021). *Transformarea digitală la nivelul administrației publice locale*. București: AmCham.

Apachiței, I. D. (2021). Dimensiunea cibernetică a securității naționale în raport de dreptul european. *Analele Științifice ale Universității „Alexandru Ioan Cuza" din Iași, Științe Juridice*, 67(1), 217–238. https://doi.org/10.47743/jss-2021-67-1-16

Bouhafs, H. (2025). Cybersecurity in the digital era: Between digital transformation and protection challenges. *Law and World*, 11(3), 117–131. https://doi.org/10.36475/11.3.8

Durach, F., Mărcuț, M., Puchiu, R., & Ștefan, V. (2021). *De la digitalizare la transformare digitală în România* (Policy Brief nr. 9). Institutul European din România.

European Court of Auditors. (2019). *Challenges to effective EU cybersecurity policy* (Special Report No. 24). Luxembourg: Publications Office of the European Union.

European Union Agency for Cybersecurity. (2023). *Building effective governance frameworks for the implementation of national cybersecurity strategies*. Heraklion: ENISA.

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and 'taking back control': From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, 31(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Govindraj, C. V. (2024). Digital governance and cybersecurity: Challenges in the age of e-governance. *ShodhKosh: Journal of Visual and Performing Arts*, 5(1), 4328–4332. https://doi.org/10.29121/shodhkosh.v5.i1.2024.442

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. *Urban Governance*, 5(1), 1–19. https://doi.org/10.1016/j.ugj.2024.11.002

Hulkó, G., Kálmán, J., & Lapsánszky, A. (2025). The politics of digital sovereignty and the European Union's legislation: Navigating crises. *Frontiers in Political Science*, 7, 1548562. https://doi.org/10.3389/fpos.2025.1548562

Kianpour, M., Davis, P. A. E., & Windekilde, I. M. (2025). Digital sovereignty in practice: Analyzing the EU's NIS2 directive. *International Journal of Information Security*, 24, 167. https://doi.org/10.1007/s10207-025-01090-4

Mijwil, M. M., Filali, Y., Aljanabi, M., Bounabi, M., & Al-Shahwani, H. (2023). The purpose of cybersecurity governance in the digital transformation of public

services and protecting the digital environment. *Mesopotamian Journal of Cybersecurity*, 2023, 1–6. https://doi.org/10.58496/MJCS/2023/001

Mureșan, D. (2025). Cybersecurity and digital transformation: The foundation of trust in public administration. *RAIS Conference Proceedings*, 256–259. https://doi.org/10.5281/zenodo.17073110

Petersons, E. (2025). The role of the European Union in shaping digital governance: Policies, challenges, and future prospects. *SSRN Scholarly Paper*. https://dx.doi.org/10.2139/ssrn.5145970

Rovner & Moore SRL, Public Research SRL, Transparency International Romania, & Deloitte Consultanță SRL. (2024). *Analiza nevoilor de competențe și instruire pentru resurse umane în administrația publică*. București: Agenția Națională a Funcționarilor Publici.

Saeed, S. (2023). Digital transformation in governmental public service provision and usable security perception in Saudi Arabia. *Information*, 16(247), 1–23.

Schneider, G. B. C. (2025). The importance of cybersecurity in digital government implementations. *Revista Científica Cognitionis*, 8(1), 1–23. https://doi.org/10.38087/2595.8801.585

Article Info

Received: April 25 2026
Accepted: June 20 2026

How to cite this article:

Grosu, D. M. (2026). Cybersecurity and institutional trust in digital governance: lessons from Romania and the European Union. *Revista de Științe Politice. Revue des Sciences Politiques,* no. 90, pp. 188-200.