RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
August 7-8, 2025
DOI:10.5281/zenodo.17073110

Cybersecurity and Digital Transformation: The Foundation of Trust in Public Administration

Doina Mureșan

Associate Researcher, Legal Research Institute "Acad. Andrei Rădulescu" of the Romanian Academy,
Doctoral Professor, "Dimitrie Cantemir" Christian University, Bucharest, Romania,
Doctoral Supervisor, "Alexandru cel Bun" Military Academy, Chisinau, Republic of Moldova
dmuresan1404@gmail.com

Abstract: The digital transformation of public administration generates major opportunities for efficiency, transparency, and proximity to citizens. However, this process is accompanied by increased exposure to cyber risks, which can affect not only IT infrastructures but also public trust in state institutions. This paper analyzes the interdependence between digitalization and cybersecurity, highlighting the role of strategic management in data protection and ensuring the continuity of public services. Through an integrated approach – which combines the European and national legislative frameworks, security technologies, inter-institutional cooperation, and human resource training – public administration can build digital resilience and strengthen citizens' trust. The conclusions emphasize that cybersecurity is not a secondary element of digitalization, but the foundation on which it rests.

Keywords: digitalization, cybersecurity, public administration, governance, trust

Introduction

Public administration is evolving rapidly under the pressure of the need for efficiency, transparency, and rapid response to citizens' demands, becoming increasingly dependent on digitalization. In this context, the convergence between administrative governance and digital transformation requires public institutions to develop robust cybersecurity capabilities.

At the European level, the NIS 2 Directive (EU 2022/2555) provides a coherent legal framework that requires public administrations to raise the standard of protection against cyber threats, through strict measures regarding risk management, constant training of employees and periodic vulnerability assessment. In Romania, the national cybersecurity strategy for the period 2022–2027, adopted by Government Decision no. 1321/2021, is the cornerstone of national digital security policies, accompanied by a concrete action plan for implementation. Also, the process of transposing the NIS2 Directive into national legislation is actively underway; GEO 155/2024 was adopted in December 2024 and entered into force in January 2025, while reporting and registration norms are expected during 2025.

These developments stem from the strategic need to protect critical infrastructures, citizens' data and online public services. In this context, cybersecurity management is no longer an isolated technical field, but a central vector of state responsibility. Institutional maturity is now assessed by the capacity of each authority to integrate governance, legislation, professional training and inter-institutional cooperation into a coherent digital resilience architecture.

Digital transformation of public administration: opportunities and vulnerabilities

The process of digitizing public administration represents one of the most significant reforms of contemporary governance. The use of digital technologies in the provision of public services has the potential to improve decision-making transparency, streamline administrative processes and bring institutions closer to citizens. In Romania, initiatives such as the National Platform *Ghișeul.ro*, the interoperability system of basic registers or the expansion of electronic signature are relevant examples of progress towards a citizen-oriented digital administration. Let's determine what the opportunities for digitizing public administration are, in a real way.

Thus, the *digital transformation of public administration* offers significant premises for strengthening governance and modernizing the relationship between the state and the citizen. Among the main benefits are accessibility, efficiency, transparency and stimulating innovation - all contributing to the creation of a more flexible and accountable administration. *Accessibility and inclusion* are the developments that are achieved by introducing digital platforms so that citizens can interact with public institutions quickly, remotely and without being constrained by geographical or bureaucratic barriers. Access to online services reduces the gaps between urban and rural areas and facilitates the participation of vulnerable groups in administrative life. Thus, digitalization becomes a tool for social inclusion and democratization of access to public services.

Administrative efficiency results from the digitalization of internal processes, which significantly reduce operational costs and request processing time. The automation of repetitive procedures frees up human and financial resources, which can be redirected to activities with higher added value. At the same time, the simplification of administrative circuits increases the capacity of institutions to promptly respond to citizens' needs and to better manage crisis situations. Another strategic advantage of digitalization is the possibility of monitoring and evaluating the performance of public services in real time. The publication of open data, access to information and the traceability of processes contribute to the accountability of institutions and the strengthening of citizens' trust. Digital governance is thus defined by a more balanced relationship between the state and society, based on dialogue and mutual control. Digitalization also has the immediate effect of *developing interconnected ecosystems*, in which public institutions can cooperate efficiently and share data securely. The interoperability of information systems is an essential condition for reducing redundancies and for basing public policies on concrete data. In addition, the integration of emerging technologies, such as artificial intelligence or big data analysis, supports the decision-making process and stimulates innovation in public management.

But if digitalization promises efficiency and modernization, it also brings a set of risks and limitations that cannot be ignored. The vulnerabilities of digital transformation affect not only technological infrastructures, but also the ability of the administration to maintain its credibility and stability in front of citizens.

A first vulnerability is *exposure to cyber risks*. As public services migrate online, institutions become prime targets for cyber attacks. Threats such as ransomware, phishing or unauthorized access to databases can paralyze administrative activity and compromise sensitive citizen data. A major security incident has the potential to quickly erode public trust and call into question the entire digitalization strategy. One identified risk *is the fragmentation of IT infrastructures* resulting from the existence of heterogeneous, often outdated, information systems that do not communicate effectively with each other. The lack of interoperability creates bottlenecks and vulnerabilities, generating difficulties in data exchange and in implementing integrated public policies. At the same time, the use of outdated technologies increases exposure to attacks and limits the adoption of innovative solutions.

It is true that the success of digitalization depends on *human resources,* and the lack of digital skills remains a major problem. Public administration employees are not always prepared to manage complex systems or recognize cyberattack attempts. At the same time, citizens who do not have sufficient digital knowledge risk being excluded from the process of accessing public services, which contradicts the principle of inclusion. From a data security perspective, the dependence on external providers such as cloud solutions or commercial platforms to support its digital infrastructure raises questions about data security, digital sovereignty and the state’s ability to fully control information flows. In the absence of clear regulations and solid governance, the risk of transferring vulnerabilities to third parties becomes significant.

We believe that digital transformation represents a double challenge: on the one hand, it promises a more open and efficient administration; on the other hand, it brings threats that can compromise the very essence of public governance. The answer does not lie in limiting digitalization, but in integrating cybersecurity as an inseparable part of the process. Only by carefully balancing innovation and protection can public administration provide modern services while maintaining the safety and trust of citizens.

We support the statements with some real examples from the Romanian public administration: the cyberattack on the Chamber of Deputies in January 2024, following which hackers accessed the institution's database and stole over 300 electronic documents, including personal information of parliamentarians (Cornea & Cârlugea, 2024). The stolen information was later published on the dark web, and the attackers demanded a ransom in cryptocurrency to delete the data. Another example is the ransomware attack on hospitals in Romania (February 2024), in which several hospitals in Romania were affected by a cyberattack that encrypted files on the institutions' servers, blocking access to data essential for medical activity. The attack took place between February 12-15, 2024 and was coordinated at the national level, affecting several hospital units simultaneously and increasing computer fraud in 2024 by 40.2% compared to the previous year, in line with global and European Union trends, according to the annual report of the National Directorate for Cyber Security (DNSC, 2024). At the same time, malware attacks recorded a significant increase of 286.8% (DNSC, 2024). These statistics highlight the vulnerability of public administration to cyber threats and the need to strengthen security measures.

These examples support the significant risks to which public institutions in Romania are exposed in the context of accelerated digitalization. The identified vulnerabilities highlight the need to implement robust cybersecurity measures and effective governance to protect data and critical infrastructures.

Cybersecurity management as a foundation for public trust

In the context of accelerated digitalization, cybersecurity can no longer be seen as just a technical component, but as a central strategic element of public governance. Citizens' trust in public administration directly depends on the capacity of institutions to protect digital infrastructures and sensitive data, as well as on the way they manage cyber risks and incidents. In this regard, the Romanian public administration operates within a complex European and national legislative framework. At the European level, the NIS2 Directive (EU 2022/2555) imposes high cybersecurity standards for public and private entities providing essential services, including state institutions. The implementation of NIS2 involves the development of security strategies, risk assessment, incident notification and staff training.

At the national level, the National Cyber Security Strategy 2022–2027 (2021) and associated legislation (GEO 155/2024) establish clear rules for the protection of critical infrastructures and citizens' data. This includes reporting procedures, periodic audits and prevention measures integrated into the decision-making process. By complying with these regulations, public institutions can demonstrate accountability and transparency, thus strengthening public trust. An effective management of cybersecurity involves the creation of dedicated structures within each public institution, making both management and employees accountable. The organization can include specialized security departments, incident coordination offices and rapid response teams (internal CERTs or collaborations with CERT-RO).

Security plans and policies must be integrated into daily administrative processes, so that incident prevention and response are part of the organizational culture. Only through accountability and involvement at all levels can service continuity and sensitive data protection be ensured. Effective cybersecurity also requires investments in modern technologies: intrusion detection and prevention systems (IDS/IPS), encryption, regular

backups and continuous monitoring solutions (SIEM). Infrastructures must be designed to minimize vulnerabilities and allow for rapid recovery in the event of an incident. In addition, interoperability between the systems of different public institutions facilitates cooperation and the rapid exchange of information on security incidents, preventing the spread of attacks and reducing response time. If we approach it from the perspective of human resources and organizational culture, employees represent the first and most important shield of cybersecurity. Continuous training in the field of information security, risk awareness and attack simulations (phishing, malware, etc.) contributes to reducing human errors. Also, promoting a security-oriented organizational culture - in which employees understand that data protection is an integral part of their responsibility - is essential for the success of cybersecurity policies.

We appreciate that the digital resilience of public administration cannot be achieved in isolation. Sharing information on cyber threats and incidents between institutions, collaboration with CERT-RO and with European bodies (ENISA, EU security agencies) are key tools for prevention and rapid response. This cooperation allows for the standardization of procedures, the creation of common response protocols and the strengthening of the capacity of institutions to manage complex attacks. In addition, it demonstrates to the public that institutions are proactive and coordinated, thus strengthening trust in the state's ability to protect data and digital services.

Cybersecurity, seen as a pillar of trust, is built through transparent policies, secure infrastructures, trained personnel and inter-institutional cooperation, and effective cybersecurity management transforms digitalization from a potential risk into a strategic advantage. Thus, cybersecurity becomes not just a technical tool, but an essential pillar of modern governance and the relationship of trust between the state and society. To transform cybersecurity into a pillar of public trust, the administration must integrate digital protection into all its processes. This requires that security be part of the design of services and procedures, not just an element added later. Standardizing risk and cyber incident management processes thus becomes an essential condition for the coherent functioning of public institutions.

Moreover, investments in infrastructure and technology remain a priority. Modernizing IT systems, eliminating vulnerabilities and implementing monitoring, encryption and backup solutions allow the protection of critical data and ensure interoperability between institutions. In parallel, human resources must be strengthened through continuous training programs, the development of digital skills and the creation of an organizational culture oriented towards security and responsibility. Employees thus become the first shield against cyber threats, and their active involvement reduces the risk of errors and incidents. We appreciate that other key elements of a resilient administration are governance and inter-institutional cooperation. The creation of dedicated coordination and incident response structures, collaboration with CERT-RO, ENISA and other European bodies for the exchange of good practices and common protocols allow for a rapid and efficient reaction to cyber attacks.

Last but not least, transparency and communication with citizens are fundamental to building trust. Informing the public about the security measures implemented, how personal data is protected and developing inclusive policies increase citizens' sense of security and promote the acceptance of digital services. Therefore, a coherent strategy, combining technological infrastructure, human resources, governance and transparent communication, allows public administration to transform cybersecurity from a challenge into a strategic advantage, strengthening both the efficiency of digitalization and the relationship of trust with society.

Metode și instrumente de cercetare

The methodology used in the study is based on an integrated approach, which combines theoretical and conceptual analysis with empirical evaluation of documents and institutional good practices. The choice of this approach was determined by the interdisciplinary nature of the topic, located at the intersection of administrative sciences, information technology and the field of national security.

A first research method used was documentary analysis, which involved consulting relevant national and European legislation on cybersecurity and digitalization of public administration. This stage allowed for the outline of the legal and institutional framework in which the process of digital transformation of administration is carried out. Strategies and programmatic documents issued by governments and international organizations (European Commission, OECD, UN) were also analyzed, in order to capture the directions of action and standards promoted at a global level.

In order to highlight the strengths and vulnerabilities of the Romanian framework, the comparative method was applied. It aimed to study the experiences of European states recognized for the advanced degree of digitalization and security of public administration, such as Estonia, Denmark or Finland. The comparison of institutional models and technological solutions allowed the identification of good practices and lessons applicable in the national context, while also providing a basis for formulating recommendations adapted to local realities.

Since the research topic is not reduced to a simple inventory of data, but also involves understanding perceptions and the socio-institutional context, the qualitative analysis method was used. This involved a careful examination of scientific articles, technical reports and official documentation, in order to capture the dominant trends, emerging challenges and possible risks in terms of cybersecurity. At the same time, public discourses and institutional policy documents were analyzed to reveal how the authorities approach the relationship between digitalization and citizen trust. The tools that supported the research process included: international scientific databases (Google Scholar, Springer, Scopus), for identifying and analyzing relevant academic literature; institutional reports and official statistics (Eurostat, European Commission, Romanian Digital Authority, CERT-RO), useful for understanding the current state of digitalization and the level of security; and case studies on the implementation of secure e-government projects, which facilitated understanding the practical applicability of theoretical concepts.

Finally, all the information collected was subjected to a synthetic analysis, aimed at integrating multiple perspectives into a coherent vision. By correlating the regulatory framework, international experiences and national particularities, it was possible to highlight the direct relationship between cybersecurity and the degree of trust of citizens in digital public administration. This stage allowed the formulation of pertinent conclusions and directions of action that would contribute to strengthening the digital transformation process.

Results and discussions

The application of research methods and tools allowed to outline a complex picture of the relationship between cybersecurity and digital transformation in public administration. The results obtained highlight the fact that the digitalization of public services represents a major strategic objective for Romania and the European Union, but the success of this process directly depends on the level of security of IT infrastructures and the trust of citizens in their use.

Regarding the current level of digitalization and cybersecurity, the documentary analysis showed that Romania has made important steps in aligning the legislative framework with European standards (GDPR, NIS2, National Cyber Security Strategy). However, the degree of implementation of digital solutions at the institutional level remains uneven, with significant differences between central institutions and local administration. At the same time,

the CERT-RO and Eurostat reports indicate a low level of use of digital public services by citizens, mainly due to the perception of lack of security and limited trust in the protection of personal data.

Comparative studies of international practices and lessons learned have highlighted that countries such as Estonia or Finland have built their digitalization success on a robust cyber infrastructure and coherent security policies. In these cases, citizens' trust has been strengthened through institutional transparency, interoperability of IT systems and digital education campaigns. These good practices suggest that cybersecurity should not be treated as a secondary stage, but as a fundamental premise of any digitalization initiative.

From the perspective of citizens' perception and trust, qualitative analysis of public and institutional discourse reveals a discrepancy between official messages on digital transformation and citizens' actual perception. While authorities promote the benefits of digitalization, the level of distrust remains high due to reported security incidents and the lack of clear accountability mechanisms. This aspect confirms the hypothesis that cybersecurity is crucial for the success of digital transformation and that public trust is built through direct and constant experiences of safe use of online services.

The research results show that there is an interdependent relationship between security and digitalization: without a solid cyber protection framework, the digital transformation process risks being fragile and generating resistance from citizens. At the same time, the lack of coherent digitalization makes it difficult to implement effective security measures, as disparate and outdated systems represent a major risk. Therefore, public administration must approach these two dimensions as complementary parts of the same process, aimed at increasing efficiency and strengthening social trust.

In conclusion, cybersecurity and digital transformation are inseparable elements of the process of modernizing public administration. Only through a coherent integration of cybersecurity measures into digitalization strategies can a framework of trust and stability be ensured for citizens. Strengthening this foundation not only optimizes the functioning of institutions, but also contributes decisively to increasing the transparency, efficiency and legitimacy of administrative acts. The digitalization of public administration is not complete without cybersecurity. People will have the confidence to use online services only if they know that their data is protected and that the systems operate without risks. Therefore, security and technology must go hand in hand to build a modern, efficient, and citizen-friendly administration.

References

Cornea, O., & Cârlugea, S. (2024, February 4). Atacul informatic de la Camera Deputaților, raportat cu întârziere. *Europa Liberă România.* https://romania.europalibera.org/a/atac-informatic-camera-deputatilor-institutii/32799931.html

European Commission. (n.d.). *NIS2 Directive: securing network and information systems.* https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. *Official Journal of the European Union*, L 333, 80–152. http://data.europa.eu/eli/dir/2022/2555/oj

Government of Romania. (2021). Decision No. 1321 of 30 December 2021 on the approval of the National Cybersecurity Strategy and Action Plan for 2022-2027 of Romania. *Official Gazette of Romania*, No. 2, January 3, 2022. https://legislatie.just.ro/Public/DetaliiDocumentAfis/250128

National Directorate for Cyber Security (DNSC). (2024). *Annual Activity Report 2024, approved by HCSAT no. 77/30.06.2025*. https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024

NIS2 Directive. (n.d.). *Key Cybersecurity Challenges For The Public Administration Sector.* https://nis2directive.eu/public-administration/