European Research Studies Journal
Volume XXIX, Issue 2, 2026

pp. 606-615

Cyber Threats to Public Administration as a Challenge to the Security of EU Countries

Submitted 18/04/26, 1st revision 08/05/26, 2nd revision 20/05/26, accepted 29/06/26

Tomasz Grudniewski[1], Zbigniew Ciekanowski[2], Jarosław Wołejszo[3], Sławomir Mazur[4], Andrzej Soboń[5], Valeriy Kuznetsov[6]

Abstract:

Purpose: *The aim of this article is to identify the scale, structure and significance of cyber threats targeting the public administration of European Union member states in the context of national security and institutional resilience.*
Design/Methodology/Approach: *A qualitative approach was adopted in this study, comprising a review of the relevant literature, an analysis of European Union legal acts and strategic documents (in particular the NIS2 Directive), and a secondary analysis of statistical data from reports by the European Union Agency for Cybersecurity (ENISA). The research question was formulated as follows: how do cyber threats directed against public administration affect the security and stability of the functioning of European Union member states? The research hypothesis posits that cyber threats to public administration – due to their scale, nature and link to hybrid threats – constitute a significant destabilising factor for the security of EU Member States, making the public administration sector a critical element of the national security system.*
Findings: *The research findings indicate that public administration is among the most frequently targeted sectors in EU Member States. Cyber threats, such as DDoS attacks, data breaches and ransomware, lead to disruptions to the continuity of operations of public institutions, data loss and a decline in public trust. At the same time, these incidents are increasingly part of the logic of hybrid threats, also affecting the political and social dimensions of state functioning.*
Practical Implications: *The findings point to the need to strengthen cybersecurity management systems in public administration, including the implementation of a risk-based approach, the development of incident response capabilities and the improvement of information security management systems (ISMS). The effective implementation of EU regulations and increased*

[1]*John Paul II University in Biała Podlaska, Poland, ORCID: 0000-0003-3394-8992 e-mail: gisbourne2@gmail.com;*
[2]*The same as in 1, ORCID: 0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl;*
[3]*President Stanisław Wojciechowski University of Kalisz, Poland, ORCID: 0000-0002-7216-3496, e-mail: j.wolejszo@uniwersytetkaliski.edu.pl;*
[4]*Andrzej Frycz Modrzewski University, Kraków, Poland, ORCID: 0000-0002-5056-2280 e-mail: smazur@orange.pl;*
[5]*War Studies University, Poland, ORCID: 0000-0003-2540-2252, e-mail: andrzej.sobon@wp.pl;*
[6]*Railway Research Institute, ORCID: 0000-0003-4165-1056, e-mail: vkuznetsov@ikolej.pl;*

investment in organisational, technological and skills-based resources are also of key importance.
Originality/Value: *The article contributes to the academic discourse by providing a comprehensive, systemic approach to the issue of cyber threats in public administration, highlighting their significance not only from a technical perspective but also as a key element of national security and systemic resilience within the European Union.*

Keywords: *Cybersecurity, public administration, national security, European Union, incident.*

JEL Codes: *H56, F52, H83.*

Raper type: *Research article.*

1. Introduction

The ongoing digitalisation of administrative processes in European Union member states has significantly increased the efficiency of public institutions and citizens' access to public services. At the same time, however, the digital transformation has led to an increase in public administration's dependence on ICT systems, making it particularly vulnerable to threats in cyberspace. Cyberattacks targeting public administration are no longer purely technical in nature; increasingly, they have organisational, social and political consequences, directly affecting the security of EU Member States.

In recent years, public administration has become one of the main targets of cyberattacks in Europe. This is confirmed by analyses carried out by the European Union Agency for Cybersecurity (ENISA), according to which the public sector – including central and local government – is among the most frequently attacked areas of state infrastructure (ENISA, 2025).

Of particular significance are incidents that compromise the availability of public services, the integrity of data and the confidentiality of information processed by state institutions, which may lead to disruptions in the continuity of administrative operations, a loss of public trust and a weakening of the state's capacity for crisis response.

The significance of cyber threats to public administration has also been formally emphasised at the regulatory level of the European Union. The NIS2 Directive (Directive (EU) 2022/2555) classifies public administration as a high-criticality sector, imposing an obligation on Member States to implement comprehensive cyber risk management measures and incident response systems. This indicates that the

cybersecurity of public administration is perceived not merely as a technical issue, but as an element of internal security and national resilience.

The aim of this article is to analyse cyber threats to public administration as one of the key challenges to the security of European Union member states. The research question formulated in this paper is as follows: how do cyber threats targeting public administration affect the stability and security of EU member states? The hypothesis posits that the scale and nature of cyber-attacks against public administration mean that this sector has become a critical element of the state security system, and its vulnerability to cyber incidents may lead to cascading effects in other areas of state functioning.

The article employs research methods, in particular a review of the relevant literature, an analysis of strategic documents and EU legal acts, and a secondary analysis of statistical data contained in ENISA reports. This approach enables a comprehensive examination of the issue of cyber threats to public administration, both from an empirical and a systemic perspective, with regard to the security of European Union member states.

2. Characteristics of Cyber Threats to Public Administration in European Union Member States

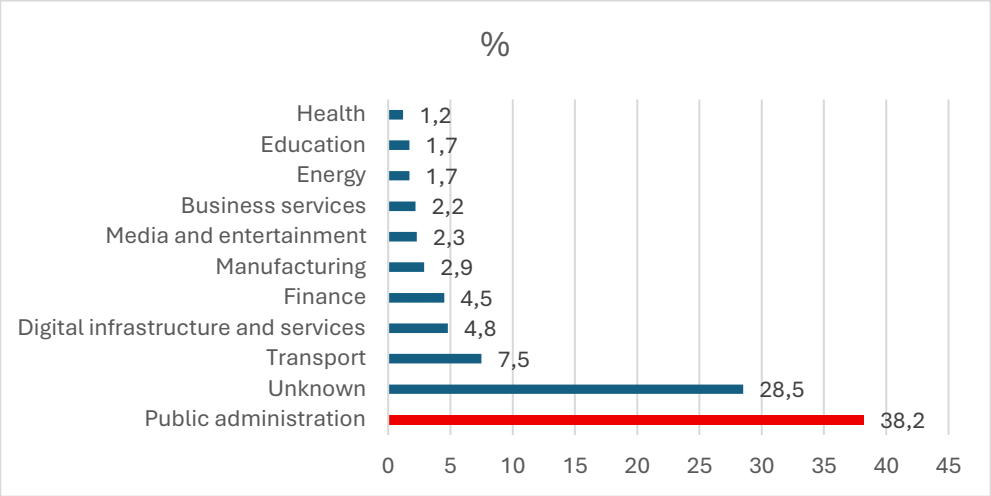
Public administration in the European Union is one of the most crucial components of the state apparatus, comprising institutions that carry out public tasks involving highly sensitive information and organisational processes. The rapid development of information and communication technologies and the increasing digitalisation of administrative processes mean that these institutions are becoming attractive targets for cybercrime, cyberattacks and other threats in cyberspace (Li and Liu, 2021).

According to the latest report by the European Union Agency for Cybersecurity (ENISA), the public administration sector in the European Union was the most frequently targeted sector in 2024 in terms of the number of cyber incidents, accounting for over 38 per cent of all reported incidents of this type (ENISA, 2025).

These figures cannot be overlooked in an analysis of national security, as cyber incidents targeting public administration can lead to disruptions in the provision of key public services, the loss of confidential information and breaches of the integrity of state systems. The chart below shows recorded incidents broken down by sector.

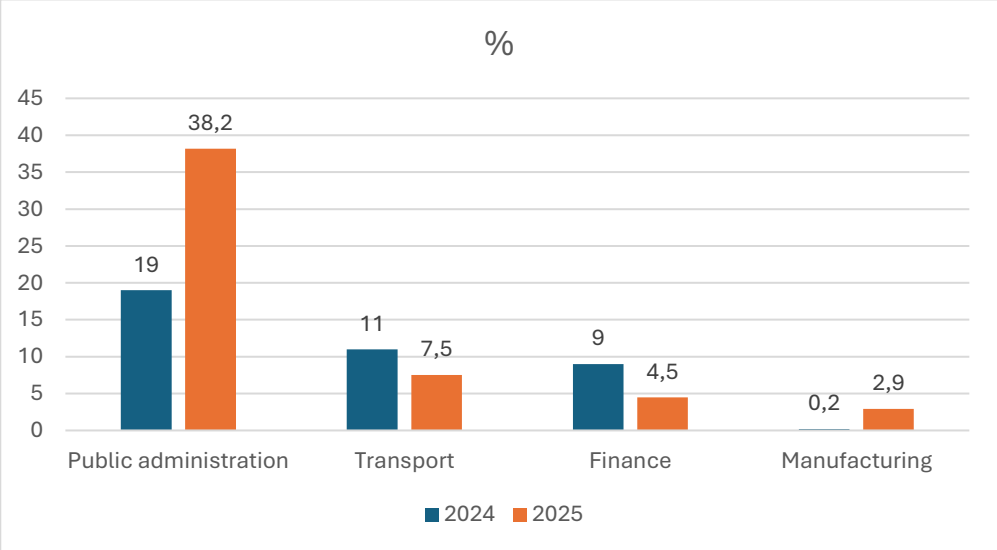
Although public administration, transport, and the financial sector had already been identified as the most frequently targeted sectors in EU Member States during the previous reporting period, a significant increase in incidents targeting public administration was recorded. A key factor behind this increase was the higher proportion of DDoS attacks against this sector carried out by hackers. The chart below compares the most frequently targeted sectors with the previous year.

Figure 1. *Recorded incidents broken down by sector.*



Source: *ENISA Threat Landscape 2025, p. 16.*

Figure 2. *Comparison of recorded incidents in the most vulnerable sectors in 2024 and 2025.*



Source: *ENISA Threat Landscape 2025, p. 17.*

As in the previous year, the public administration sector remains the most frequent target of attacks, accounting for 38% of all incidents. A marked increase in attacks has been recorded, primarily due to DDoS attacks by hackers.

The highest number of incidents concerns public administration in France (27%), Italy (26.3%) and Germany (16.2%), followed by Spain (15.3%) and Poland (15.1%) (ENISA, 2025).

The nature of cyber threats against public administration institutions is varied, and a review of the literature points to several dominant categories of attacks. Among these, Distributed Denial of Service (DDoS) attacks play a particularly significant role; in 2024, according to data from the EU agency, they accounted for the largest share of incidents targeting public administration (ENISA, 2025).

DDoS attacks involve overloading network infrastructure or application services, leading to the temporary shutdown of administrative systems. Research indicates that their scale and frequency have increased in recent years, partly due to the growing availability of tools that facilitate their execution (Nuraeni, Nugraha, and Aminanto, 2025).

The second significant type of threat is data breaches, which involve unauthorised access to IT systems and the leakage or theft of information. Literature reviews emphasise that such breaches often result from security vulnerabilities, poor access control management or outdated IT infrastructure (Brzostek, 2023).

In the context of public administration, these breaches may result in the disclosure of citizens' personal data or information of a strategic nature, which has direct implications for national security.

Furthermore, some of the literature highlights the growing significance of ransomware attacks as a systemic threat. These attacks involve encrypting an organisation's IT resources and demanding a ransom in exchange for their decryption. Ransomware, whilst less common than DDoS attacks or data breaches, often has more severe consequences for the functioning of public institutions, including the paralysis of administrative processes and the need to restore systems following an incident (Nuraeni, Nugraha, and Aminanto, 2025).

The academic literature also emphasises that public administration may be the target of cyber-attacks of a political and ideological nature, carried out by hacktivist groups or state actors who use cyberspace to exert influence or cause destabilisation (Li and Liu, 2021). Such actions not only compromise the integrity of administrative systems but may also affect citizens' perceptions of the effectiveness of state institutions, which in turn has implications for the functioning of the state as a whole.

An analysis of cyber threats to public administration in European Union member states shows that both the technical aspects of attacks (DDoS, ransomware, data breaches) and non-technical motivations (political, hybrid) constitute significant risk factors that must be taken into account in ensuring national security.

These challenges require a broad research perspective and effective defence strategies that take into account both technological and organisational aspects.

3. Cyber Threats to Public Administration and the Stability of the Functioning of European Union Member States

Cyber threats targeting the public administration of European Union member states should be analysed not only in terms of technical incidents but, above all, as a phenomenon that affects the stability of a state's functioning and its ability to carry out fundamental public tasks (Ciekanowski *et al.,* 2024).

This is because public administration plays a key role in the internal security system, being responsible for the continuity of decision-making processes, the delivery of public services and the protection of citizens' interests. Disruptions to its operations caused by cyberattacks can lead to cascading effects on other sectors of the state.

One of the most significant consequences of cyber threats to public administration is the disruption of business continuity within state institutions. DDoS attacks, although often short-lived, cause periodic unavailability of administrative portals, public register systems or citizen service platforms.

The literature on the subject emphasises that even temporary disruptions to access to public services can reduce administrative efficiency and weaken public trust in the state (Bada and Nurse, 2020). From a systemic perspective, this phenomenon should be regarded as a threat to state resilience (Szleszyński and Dudziak-Gajowiak, 2023).

Incidents involving data security breaches have far more serious consequences for state stability. The loss or leakage of data processed by public administration – in particular, personal data, financial information, or sensitive data – can lead to long-term consequences, such as an increased risk of crime, identity theft, or a weakening of the protection of the state's strategic interests. Research indicates that public administration is particularly vulnerable to such incidents due to the complexity of IT systems and insufficient cybersecurity maturity in some EU Member States (Tikk and Kerttunen, 2020).

Cyber threats to public administration also affect national security by generating organisational and financial costs. Ransomware attacks, although relatively less frequent, lead to the paralysis of administrative systems, the need to restore IT infrastructure, and the temporary suspension of public services. The literature emphasises that the consequences of such incidents extend beyond the economic dimension and include a weakening of the state's ability to respond to crises and manage emergencies (Cavelty and Wenger, 2020).

Furthermore, the security of information and IT systems in public administration directly impacts the long-term stability of the state's functioning. Research into information security management within public administration bodies has revealed numerous organisational problems, such as the lack of *an* appropriate Information *Security Management System* (ISMS), shortcomings in risk analysis, and inadequate

audits and controls, which increase the risk of serious breaches and weaken the organisation's resilience to cyber incidents (Szczepaniuk *et al.,* 2020).

Another significant aspect of the impact of cyber threats on the stability of EU Member States is their political and social dimension. Cyberattacks targeting public administration are increasingly part of hybrid operations, in which technical measures are combined with information and psychological influence.

Hacktivist groups and actors linked to third countries use cyberspace to undermine the authority of public institutions, reinforce disinformation narratives and escalate social tensions (Rid, 2020; Klimburg, 2017). In this context, cyber threats to public administration are becoming tools of strategic influence rather than merely technical problems.

From the perspective of EU member states' security, the link between cyberattacks on public administration and current geopolitical events is particularly worrying. Analyses indicate that an increase in the intensity of attacks often correlates with political decisions by member states, such as participation in international operations, military support or economic sanctions. This phenomenon confirms the view that cyberspace has become a fully fledged arena of international competition, in which public administration is one of the main targets of influence (Fujs and Bernik, 2020).

Cyber threats to public administration have a direct and indirect impact on the stability of the functioning of European Union member states (Ciekanowski *et al.,* 2023, p. 783). These include disruptions to the continuity of public institutions' operations, threats to data protection, increased costs of state functioning, and political and social impacts that form part of the logic of hybrid threats. Consequently, the issue of cybersecurity in public administration should be treated as an integral part of national security, rather than solely as a technical or administrative matter.

4. Public Administration as a Critical Component of the Cybersecurity System in EU Member States

Public administration in the Member States of the European Union plays a dual role within the cybersecurity system: on the one hand, it is one of the most frequently targeted sectors; on the other, it forms the foundation of a state's ability to maintain operational continuity, enforce the law and deliver public services in the face of disruptions.

From a systemic perspective, this means that cyber incidents within public administration can act as 'risk amplifiers', compounding the impact on public trust, the state's regulatory and service functions, and crisis coordination. From an EU perspective, public administration is also a high-criticality sector under the NIS2 legal framework, which formalises the obligation to enhance cybersecurity resilience and maturity in public institutions (Directive (EU) 2022/2555, 2022).

The results of ENISA's analyses indicate that public administration remains a target of particular 'visibility' and vulnerability. In its sectoral report on public administration, ENISA highlighted the predominance of incidents affecting availability (in particular DDoS attacks), alongside the significance of data breach and ransomware incidents, which – although fewer in number – have a greater impact on business continuity and the reputation of institutions (ENISA, 2025).

These findings should be considered alongside the assessment of sectoral maturity: NIS360 identifies public administration as a sector burdened by a 'criticality–maturity' gap (high criticality coupled with relatively low maturity), which translates into a need for systemic measures rather than merely ad hoc ones (ENISA, 2025).

In this context, it is of key importance to implement cyber risk management mechanisms within public administration, which NIS2 defines as a set of organisational and technical measures, including, amongst others, incident response, business continuity and crisis management, supply chain security, network and system security, as well as policies and procedures for assessing the effectiveness of security measures (Directive (EU) 2022/2555, 2022).

From the perspective of national security practice, three areas are particularly important:

- institutionalising management's responsibility for cybersecurity,
- building detection and response capabilities (detection–response–recovery),
- mitigating systemic risks arising from dependence on ICT service providers and cloud solutions.

The systemic dimension is reinforced by EU initiatives focused on solidarity and response capabilities. The Cyber Solidarity Act – adopted as a regulation – establishes mechanisms to support the detection of, preparedness for and response to incidents within the EU, as well as the development of capabilities, which is also significant for public administration as a sector highly exposed to incidents (Regulation (EU) 2025/38, 2025).

In practice, this means shifting the focus from purely reactive measures to a resilience-oriented approach that encompasses shared resources, cross-border cooperation, exercises, and the strengthening of staff competencies. At the same time, in light of the growing role of geopolitically motivated incidents, public administration cybersecurity should be treated as an element of national security and state resilience, rather than merely an IT issue (ENISA, 2025).

From the perspective of EU Member States, public administration is therefore a critical component of the cybersecurity system for three reasons. Firstly, the scale and

nature of the threats indicate sustained pressure on public services, and service disruptions and data breaches may pose internal security risks.

Secondly, the NIS2 requirements necessitate a shift towards risk-based cybersecurity management and management accountability, which transforms the governance model of public institutions.

Thirdly, EU solidarity tools (including the Cyber Solidarity Act) strengthen response and coordination capabilities, which may limit the cascading effect of incidents within the public administration, provided this is supported by investment in maturity, staff and inter-institutional cooperation.

5. Conclusion

The analysis confirms that cyber threats targeting public administration are among the key challenges to the security of European Union member states. The scale and nature of cyber incidents, encompassing both attacks on the availability of public services and breaches of data confidentiality and integrity, indicate that public administration is currently one of the most vulnerable sectors of state functioning. At the same time, its role in carrying out public tasks means that the consequences of cyber-attacks extend beyond the technical dimension, affecting institutional stability, public trust and states' capacity for crisis response.

The research findings unequivocally confirm the hypothesis that the public administration's vulnerability to cyber threats can lead to cascading effects within the state's security system. Disruptions to the continuity of public institutions' operations, the loss of citizens' data or the temporary unavailability of key information systems may undermine the state's operational capabilities and its credibility as the guarantor of security and public order. In this context, cyberspace is becoming a significant arena for competition and influence, forming part of the logic of hybrid threats.

Another key finding of the analysis is the growing importance of the European Union's regulatory and institutional frameworks in public administration cybersecurity. The NIS2 Directive and initiatives such as the Cyber Solidarity Act point to the EU's commitment to systematically strengthening the resilience of the public sector through risk management, enhancing organisational maturity and developing incident response capabilities.

However, the effectiveness of these measures will depend on the consistent implementation of regulations at national level and on substantial investment in the human, organisational and technological resources of public administration.

Cybersecurity in public administration should be treated as an integral part of the national security of European Union Member States. It requires a holistic approach that combines legal, organisational and technical solutions with the development of a

security culture within public institutions. Further research in this area should focus on assessing the effectiveness of the regulations being implemented, comparing Member States, and analysing the public administration's capacity to function in the face of growing threats in cyberspace.

References:

Bada, M., Nurse, J.R.C. 2019. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises. Information and Computer Security, 28(3), pp. 393-410.

Brzostek, A. 2023. Cybersecurity in public administration – legal aspects, Zeszyty Prawnicze, 23.3/2023, pp. 95-108.

Cavelty, M.D., Wenger, A. 2020. Cyber security meets security politics: Complex technology, fragmented politics, and networked science, Contemporary Security Policy, 41(1), pp. 5-32.

Ciekanowski, Z., Gruchelski, G., Nowicka, J., Żurawski, S., Pauliuchuk, Y. 2023. Cyberspace as a Source of New Threats to the Security of the European Union. European Research Studies Journal, Volume XXVI, Issue 3, pp. 782-797.

Ciekanowski, Z., Nowicka, J., Czternastek, M., Żurawski, S., Mikosik, P. 2024. How Cybersecurity Shapes Effective Organisational Management. European Research Studies Journal, Volume XXVII, Issue 2, pp. 454-464.

ENISA Threat Landscape 2025.

ENISA Sectoral Threat Landscape. Public Administration, 2025.

Klimburg, A. 2017. The Darkening Web: The War for Cyberspace, New York: Penguin Press.

Li, Y., Liu, Q. 2021. A comprehensive review study of cyber-attacks and cybersecurity: Emerging trends and recent developments. Energy Reports, 7, pp. 8176-8186.

Nuraeni, A., Nugraha, Y., Aminanto, M.E. 2025. Revisiting Cyber Threats in Government Sectors: A Systematic Review of Attacks, Challenges, and Policy-Level Defences. International Journal of Advances in Data and Info, 6(2), pp. 447-459.

Rid, T. 2020. Active Measures: The Secret History of Disinformation and Political Warfare, Vol. 64, No. 1, Centre for the Study of Intelligence.

Szleszyński, A, Dudziak-Gajowiak, D. 2023. Resilience of public administration bodies to cyberattacks, Scientific Journal of the Military University of Land Forces, 209(3), pp. 182-205.

Szczepaniuk, E., Szczepaniuk, H., Rokicki, T., Klepacki, B. 2020. Information security assessment in public administration. Computers & Security, Volume 90.

Tikk, E., Kerttunen, M. 2020. Routledge Handbook of International Cybersecurity. Routledge.