CHALLENGES OF ARTIFICIAL INTELLIGENCE IMPLEMENTATION IN CYBERSECURITY OF SMES FROM THE REPUBLIC OF MOLDOVA IN THE CONTEXT OF ACCELERATED DIGITALISATION

CZU: 004.8:[004.056:334.72.012.63/.64](478)
DOI: https://doi.org/10.53486/tids2026.36

LUCIA GUJUMAN
Associate Professor, Academy of Economic Studies of Moldova
e-mail: gujuman.lucia@ase.md
ORCID ID: 0000-0001-7940-4291

EMILIA GOGU
Associate Professor, Academy of Economic Studies of Bucarest
e-mail: emilia.gogu@csie.ase.ro
ORCID ID: 0000-0002-7333-7128

ZINOVIA TOACĂ
Associate Professor, Academy of Economic Studies of Moldova
e-mail: toaca@ase.md
ORCID ID: 000-0002-8304-1961

VITALIE URSACHI
Academy of Economic Studies of Moldova
e-mail: ursachi.vitalie@ase.md
ORCID ID: 0009-0008-9206-1324

Abstract. The accelerated digital transformation of small and medium-sized enterprises (SMEs) generates new cybersecurity vulnerabilities, while artificial intelligence (AI) offers advanced tools for threat detection and prevention. This study examines the challenges of AI adoption in cybersecurity for SMEs in the Republic of Moldova, employing a mixed methodology combining scientific literature analysis, national statistical data analysis, and comparison with the European regulatory framework. Results indicate that Moldovan SMEs are predominantly exposed to phishing attacks (60–70%), ransomware (50–60%), and account compromise (45–60%), with a low level of cybersecurity maturity and significant deficits in competencies and resources for AI-based solution adoption. The study proposes an implementation framework adapted to the local context, aligned with NIS2 Directive (EU 2022/2555), the AI Act (EU 2024/1689), and GDPR (EU 2016/679) requirements. The authors' contribution consists in adapting the NIST framework augmented with AI to the specificities of Moldovan SMEs and formulating recommendations for strengthening cybersecurity resilience.

Keywords: *artificial intelligence; cybersecurity; SMEs; Republic of Moldova; NIS2; AI Act; digitalization.*

JEL Classification: O33; L86; K24; M15; D81

INTRODUCTION

Small and medium-sized enterprises (SMEs) constitute the backbone of the Republic of Moldova's economy, representing 99.2% of all registered enterprises and providing over 65% of the national workforce.(Biroul Național de Statistică al Republicii Moldova, 2025) In the context of the national accelerated digitalization program, reflected in the Digital Transformation Strategy of the Republic of Moldova 2023–2030, approved by the Government of the Republic of Moldova in

September 2023, SMEs have registered an increasing dependence on IT infrastructure and digital services.(Carayannis et al., 2024)

This positive development, however, is accompanied by a proportional increase in exposure to cyber threats. According to the World Economic Forum Global Cybersecurity Outlook 2026 (WEF, 2026), over 77% of organizations are already using artificial intelligence (AI) to detect threats and automate response to cybersecurity incidents. However, AI adoption in SMEs remains significantly lower than in large corporations, due to specific economic, technological and organizational barriers.

The Republic of Moldova faces a double challenge: on the one hand, accelerating digitalization in the context of the European integration process (Law No. 315/2022 on the National Development Strategy "European Moldova 2030"), and on the other hand, the need to align with the European regulatory framework in the field of cybersecurity and artificial intelligence, including the NIS2 Directive (EU 2022/2555), the Artificial Intelligence Regulation (AI Act, EU Regulation 2024/1689) and the General Data Protection Regulation (GDPR, EU 2016/679).

The main objective of this paper is to analyze the challenges of implementing AI in cybersecurity for SMEs in the Republic of Moldova and to propose an implementation framework adapted to the local context, in correlation with the applicable European regulations. The study aims to fill a gap identified in the specialized literature: the absence of AI adoption models in cybersecurity specifically adapted for SMEs in EU associated states with limited institutional capacity.

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY – GLOBAL TRENDS

The use of artificial intelligence in cybersecurity has seen exponential growth in recent years, reflecting both the sophistication of cyber threats and the technical advancement of machine learning algorithms. According to the World Economic Forum Global Cybersecurity Outlook 2026(World Economic Forum, 2026), over 77% of organizations globally are using AI for anomaly detection, incident response automation, and user behavioral analysis.

Research in the literature confirms the effectiveness of AI-based solutions in reducing the time to detect cyber incidents. The Cost of a Data Breach Report 2024 published by IBM Security demonstrates that organizations that use AI and automation in cybersecurity identify and contain security breaches 98 days faster than those that do not use such technologies, generating average savings of $2.22 million per incident (IBM, 2024a).

The Data Breach Investigations Report 2025 shows that credential misuse (22%), vulnerability exploitation (20%), and phishing (16%) are the main vectors through which attackers gained initial access to the breaches analyzed, excluding those caused by errors or internal misuse (Verizon, 2025). For SMBs, these findings highlight the importance of taking concrete steps: protecting accounts, regularly updating systems, and training employees to recognize phishing attempts.

The study published by Rombaldo Junior, Becker and Johnson (2023) in arXiv – entitled “Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity” – conducts a systematic review of the literature on cybersecurity in SMEs for the period 2017–2023. The authors analyze 77 relevant studies, identifying 44 unique themes, and conclude that SMEs face difficulties in ensuring cybersecurity, related to insufficient risk awareness, limited knowledge and restricted financial resources.(Rombaldo Junior Carlos and Johnson Shane, 2023)

A recent contribution is the study by Awan et al. (Awan *et al.*, 2026), published in the journal Scientific Reports, which proposes a cybersecurity framework for SMEs in the field of software development. It combines generative artificial intelligence practices with artificial neural networks

(ANN) and interpretive structural modeling (ISM) to identify threats and organize risk reduction measures. The results suggest the potential of this approach, but its evaluation in other enterprises and in the long term requires further research.

BARRIERS TO AI ADOPTION BY SMES

The study published in PLOS ONE (2025) by Rasdi and Baki – "Navigating the AI landscape in SMEs: Overcoming internal challenges and external obstacles for effective integration" – collects primary data through in-depth interviews with representatives of six SMEs from different sectors and identifies major internal obstacles, including resistance to change, fear of job loss and restricted resources, alongside external obstacles such as the dynamic technological landscape and strict regulatory requirements (Mohd Rasdi and Umar Baki, 2025).

Research published in the Journal of Ethics and Emerging Technologies (2026) – "The Role of Information Security in Responsible AI for Digital SMEs: A Systematic Review of Frameworks, Challenges, and Best Practices" – highlights that, although existing studies focus predominantly on technical and public policy solutions, the human factor remains under-represented in the specialized literature, despite its critical role in cybersecurity (Quainoo and Ahad, 2026). The authors emphasize that financial limitations and skills shortages are the main obstacles to the implementation of responsible AI in digital SMEs.

EUROPEAN REGULATORY FRAMEWORK – NIS2, AI ACT AND GDPR

The European Union has developed in recent years a complex and coherent regulatory framework for cybersecurity and the responsible use of artificial intelligence, with direct implications for SMEs in the Member States and associated countries.

Directive (EU) 2022/2555 (NIS2), adopted on 14 December 2022, set 17 October 2024 as the deadline for Member States to transpose its provisions into national law. It significantly expands the scope of cybersecurity obligations across 18 critical sectors, including energy, transport, healthcare, digital infrastructure and public administration. As a general rule, these obligations apply to medium-sized and large entities in the covered sectors, although certain smaller entities are also included. Article 20 requires management bodies to approve and oversee cybersecurity risk-management measures and provides for their accountability for infringements. Article 16 establishes EU-CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises (European Parliament and Council of the European Union, 2022). On 20 January 2026, the European Commission proposed targeted amendments to NIS2 to increase legal clarity and simplify compliance. According to the Commission, the proposed changes would ease compliance for 28,700 companies, including 6,200 micro and small-sized enterprises (European Commission, 2026a).

The Artificial Intelligence Act (AI Act), Regulation (EU) 2024/1689 of 13 June 2024, entered into force on 1 August 2024. It sets common rules for AI in the European Union, with requirements that vary according to how a system is used and the risks it poses. For SMEs adopting AI-based cybersecurity tools, an important distinction concerns the classification of high-risk systems. Annex III covers AI used as a safety component in certain critical infrastructure, but recital 55 specifies that components used solely for cybersecurity do not qualify as safety components in this context. A cybersecurity tool is therefore not automatically considered high-risk: its classification depends on its intended use and the relevant legal criteria(European Parliament and Council of the European Union, 2024). The rules take effect in stages. Following the AI Omnibus amendments in 2026, most provisions became applicable on 2 August 2026. The requirements for high-risk systems listed in

Annex III apply from 2 December 2027, while those for high-risk systems embedded in regulated products covered by Annex I apply from 2 August 2028 (European Commission, 2026b).

The interaction between the AI Act and NIS2 is particularly relevant: essential and important entities developing or using AI systems must comply with both the cybersecurity requirements imposed by NIS2 and the specific risk management framework provided for by the AI Act. The overlap is particularly pronounced with regard to incident reporting obligations and supply chain governance (Graux *et al.*, 2025). The European Union Agency for Cybersecurity (ENISA) provides detailed technical guidance for the implementation of Implementing Regulation (EU) 2024/2690, supporting digital infrastructure entities in complying with the requirements of NIS2 (ENISA, 2025).

THE SPECIFIC CONTEXT OF THE REPUBLIC OF MOLDOVA

The Republic of Moldova is advancing its digital transformation through the Digital Transformation Strategy for 2023–2030, developed with UNDP support. At the time of the strategy's approval in 2023, UNDP reported that 44% of public services for entrepreneurs and 34% of those for citizens were available online (UNDP, 2023). Earlier evidence also points to a developed digital infrastructure: an article published on the UNDP website in 2021 reported 4G coverage across 98% of the country's territory, based on 2020 data, and described the ICT sector's contribution to national GDP as approximately 7% (Botezatu Serghei, 2021). These figures provide historical context for Moldova's digital transformation rather than a measure of its current level of digitalisation.

Despite progress in digitalisation, Moldova still needs to strengthen its national cybersecurity capabilities. The ITU Global Cybersecurity Index 2024 places the country in Tier 3 ("Establishing"), indicating that its cybersecurity framework is still developing(ITU, 2024). An important step was the adoption of Law No. 48/2023 on cybersecurity, drafted with support from Estonia and aligned with EU standards (Runde, Kieff and Bryja, 2024; 2024). Institutional development also included the establishment of the Cybersecurity Agency under Government Decision No. 1028/2023 and the National Institute for Cybersecurity Innovation "Cybercor" at the Technical University of Moldova under Government Decision No. 671/2023. These institutions support national cybersecurity governance and the development of specialised skills, respectively (Government of the Republic of Moldova, 2023a; 2023b).

The SME Policy Index: Eastern Partner Countries 2024 identifies challenges affecting the development and digital transformation of SMEs in the Republic of Moldova, including difficulties in accessing finance and gaps in digital skills. The report also recognises progress in strengthening the institutional and regulatory framework, while highlighting the need for further reforms and more targeted support for SME digitalization (OECD., 2024). In 2024, the Ministry of Economic Development and Digitalization developed and published the White Paper on Artificial Intelligence and Data Governance. The document sets out a strategic vision for the responsible use of AI and data to support innovation and economic development. Although it is not a formal policy document, it provides guidance for future national policies, emphasising skills development, resilient infrastructure, responsible AI adoption and alignment with EU standards (MDED, 2024).

RESEARCH METHODOLOGY

This research adopts a mixed-methods approach, which combines qualitative and quantitative dimensions, allowing for a comprehensive analysis of the phenomenon studied from both a theoretical and an applied perspective. This approach is considered appropriate for studies that involve both the

analysis of macroeconomic and technological trends and the assessment of specific institutional contexts (Creswell and Plano Clark, n.d.).

The methodology includes the following main components:

• Systematic analysis of scientific literature indexed in Scopus and Web of Science databases, with a focus on publications from 2020–2026, on the use of AI in SME cybersecurity, adoption barriers and implementation frameworks;

• Analysis of relevant European regulatory documents: NIS2 Directive (EU 2022/2555), AI Act Regulation (EU 2024/1689), GDPR (EU 2016/679) and Cyber Resilience Act (CRA, 2024);

• Statistical analysis of secondary data on the structure of SMEs and the level of digitalization in the Republic of Moldova, using official sources: National Bureau of Statistics (NBS, 2025), Ministry of Economy and Digitalization (MED, 2023, 2024), UNDP Moldova (2023, 2024);

• Analysis of empirical data on the typology and prevalence of cyberattacks on SMEs, based on international reports Verizon DBIR (2025), IBM Security (2024) and ENISA Threat Landscape (2024);

• Comparative analysis between the European Union and the Republic of Moldova on cyber maturity, AI adoption and regulatory framework;

• Original conceptual approach for developing an adapted framework for implementing AI in the cybersecurity of SMEs in the Republic of Moldova, based on the NIST Cybersecurity Framework standard (NIST, 2024) and augmented with AI components.

Methodological limitations include the absence of primary data collected directly from SMEs in the Republic of Moldova due to access and availability constraints, which also constitutes a direction for future research. The data used are representative at the macro trend level, not at the individual organization level.

CYBER THREAT PROFILE OF SMES

Analysis of available data reveals that SMEs in the Republic of Moldova and comparable regions are exposed to a wide range of cyber threats, with different prevalences depending on the sector and level of digital maturity. Table 1 presents the distribution of the main types of attacks, correlated with international data:

Table 1. Distribution of types of cyberattacks in SMEs

Attack type	Estimated share (%)	Main reference source
Phishing and social engineering	60–70	Verizon DBIR (2025); ENISA (2024)
Ransomware	50–60	IBM Security (2024); WEF (2026)
Credential Compromise	45–60	Verizon DBIR (2025)
Exploitation of technical vulnerabilities	30–45	ENISA Threat Landscape (2024)
Supply chain attacks	20–35	WEF (2026); ENISA (2024)
Insider threats	15–25	IBM Security (2024)

Source: *Prepared by the authors based on Verizon DBIR (2025), IBM Security (2024), ENISA (2024), WEF (2026)*

Phishing remains one of the main initial access vectors in data breaches, although the 2025 Verizon Data Breach Investigations Report places it behind credential abuse and vulnerability exploitation. The report also finds that approximately 60% of the breaches analysed involved a human

element, highlighting the continuing importance of employee awareness and secure working practices (Verizon, 2025). These findings suggest that an AI-supported cybersecurity framework for SMEs should combine technical protection with regular staff training.

Ransomware is a particular concern for smaller organisations. In the Verizon dataset, it was involved in 88% of breaches affecting small and medium-sized businesses, compared with 39% of breaches affecting large organisations (Verizon, 2025). The financial consequences of data breaches are also substantial: IBM's Cost of a Data Breach Report 2024 estimates an average global cost of USD 4.88 million across the organisations studied (IBM, 2024a). This figure covers data breaches generally, rather than ransomware incidents or SMEs alone, and provides broader context for the economic importance of cybersecurity.

Implementing AI solutions in cybersecurity offers measurable advantages, extensively documented in the literature. The main benefits identified are:

- AI in cybersecurity: artificial intelligence and machine learning can help organisations analyse cyber threats, but attackers can also use these technologies to develop more sophisticated attacks. Understanding both sides of this development can guide the design of cybersecurity measures in Industry 4.0 environments (De Azambuja et al., 2023).
- Faster identification and containment of breaches: AI and automation can support security teams in identifying and containing data breaches more quickly. IBM's 2024 report found that organisations using these technologies extensively identified and contained breaches an average of 98 days faster than those that did not use them (IBM, 2024b).
- Lower breach costs: AI and automation can help organisations reduce the financial impact of data breaches. IBM's 2024 report found that organisations using these technologies extensively had average breach costs USD 1.88 million lower than those that did not use them (IBM, 2024b).

THE CHALLENGES OF ADOPTING AI IN SMES IN THE REPUBLIC OF MOLDOVA

Although artificial intelligence offers important opportunities for strengthening cybersecurity, its use in SMEs is still limited, including in the Republic of Moldova. The analysis of the specialized literature and available data allowed the identification of six main categories of challenges that hinder the adoption of these solutions:

Table 2. Barriers to AI adoption in SME cybersecurity

Category	Specific Challenges	Relevance for Moldova
Financial	High licensing and implementation costs; ROI difficult to quantify in the short term	High – limited access to financing
Technical	Depreciated IT infrastructure; lack of interoperability; insufficient volume of data to train AI models	High – heterogeneous infrastructure
Human Resources	Shortage of AI and cybersecurity specialists; organizational resistance to change	Very high – brain drain
Regulatory	The complexity of compliance with NIS2, AI Act and GDPR; auditability and transparency requirements	Environment – national legislation in alignment
Organizational	Absence of a security culture; lack of integrated security strategy	High – low level of maturity
Financial	Risks regarding the protection of personal data processed by AI systems; GDPR requirements	Average – GDPR framework partially implemented

Source: *Authors' compilation based on Management Review Quarterly (2024), Rasdi & Baki (2025), ENISA (2024), and OECD/EBRD (2024).*

The lack of advanced digital skills is a challenge for the digital transformation of SMEs in the Republic of Moldova. The OECD/EBRD report (OECD and European Bank for Reconstruction and Development, 2023) highlights the persistent nature of the deficit of advanced ICT skills and the need to strengthen digital readiness in small enterprises. In the context of the present research, these findings suggest that the availability of the necessary skills may also limit the adoption of AI solutions for cybersecurity.

The complexity of the European regulatory framework represents an additional challenge for SMEs falling within the scope of these acts. The study carried out at the request of the European Parliament(Graux *et al.*, 2025) highlights overlaps and difficulties in correlating the AI Act with other European digital regulations. For enterprises with limited resources, identifying applicable obligations and organizing the compliance process may require additional effort. In the case of SMEs from the Republic of Moldova, the relevance of the requirements of NIS2, AI Act, GDPR and CRA should be analyzed according to the activities carried out and the relations with the European Union market.

PROFILE OF SMES IN THE REPUBLIC OF MOLDOVA

SMEs occupy an important place in the economy of the Republic of Moldova, both in terms of their number and their contribution to job creation. In 2023, they constituted 99.2% of all reporting enterprises and had 65.3% of their average number of employees. Most SMEs were active in trade (33.1%), followed by professional, scientific and technical activities (9.2%), agriculture, forestry and fishing (8.9%) and manufacturing (7.9%). Enterprises in the field of information and communications represented 5.9% of all SMEs (Biroul Național de Statistică al Republicii Moldova, 2025).

The level of cyber maturity of Moldovan SMEs is generally low, characterized by:

- ✓ Mixed IT infrastructures, combined with depreciated equipment and outdated applications;
- ✓ Formal cybersecurity policies absent or insufficiently implemented in most organizations;
- ✓ Budget dedicated to cybersecurity below 2% of total IT spending;
- ✓ Generalist IT staff without specialization in cybersecurity or artificial intelligence;
- ✓ Lack of tested disaster recovery and business continuity plans.

In the case of industrial SMEs, the use of operational technology (OT) equipment and IoT devices requires increased attention to cybersecurity. Their integration into networks can introduce additional vulnerabilities, especially when existing systems have limited protection mechanisms. Therefore, security measures need to be adapted to the specificities of the equipment and production processes (ENISA, 2018).

In the financial services sector, stricter regulatory requirements do not eliminate cyber risks, as access to financial resources and sensitive data can attract attackers. In traditional trade and agriculture, digitalization must be accompanied by the development of protective capabilities. Businesses with limited digital resources and skills may face difficulties in preventing and managing cyber incidents.

AI implementation framework in cybersecurity proposed for SMEs

The analysis of the specialized literature, European regulations and the particularities of SMEs in the Republic of Moldova formed the basis for the development of a framework for implementing AI in cybersecurity, called AI-NIST-SME-MD Framework. The proposed framework is based on the five functions of the NIST Cybersecurity Framework, version 1.1 (National Institute of Standards and

Technology, 2018), and integrates artificial intelligence components adapted to the needs and resources of these enterprises:

Table 3. AI-NIST-SME-MD Framework for Implementing AI in Cybersecurity

NIST Function	Proposed AI Component	Recommended Tooling R	Related Requirement
Identification	Automated risk assessment with ML algorithms; IT asset mapping	Vulnerability scanners cu ML; Asset management tools	NIS2 Art. 21; AI Act Art. 9
Protection	Adaptive behavior-based controls; advanced authentication (MFA + biometrics)	Zero Trust Architecture; AI-enhanced IAM	GDPR Art. 32; NIS2 Art. 21
Detection	IDS/IPS with ML; behavioral analysis (UEBA); real-time anomaly detection	SIEM cu ML; NDR tools	NIS2 Art. 23; AI Act Art. 15
Response	SOAR automation; automatic alert triage; automatic isolation of compromised systems	SOAR platforms; AI-driven playbooks	NIS2 Art. 23; AI Act Art. 13
Recovery	Planuri de continuitate generate și testate cu IA; analiză post-incident automata	BCP/DRP tools; AI forensics	NIS2 Art. 21(f); ISO 22301

Source: *Original contribution by the authors, adapted from NIST CSF (2018), NIS2 (EU 2022/2555) and AI Act (EU 2024/1689)*

The author's contribution consists in adapting the NIST framework to the needs and possibilities of SMEs in the Republic of Moldova. The model takes into account the limited financial resources, the diversity of the IT infrastructure and the lack of personnel with specialized skills, as well as the relevant European requirements, including NIS2 and the AI Act, to the extent that they are applicable. The modular structure allows for the gradual introduction of the proposed measures and their expansion as the enterprise develops its capabilities and has additional resources.

The use of AI in SME cybersecurity involves both capitalizing on its benefits and examining the applicable legal requirements. Solutions for anomaly detection, user authentication and network monitoring are not automatically classified as high-risk systems. The classification depends on the purpose of use and the conditions set out in the AI Act. For systems falling into this category, the regulation establishes requirements regarding risk management, transparency, human oversight, accuracy, robustness and cybersecurity (European Parliament and Council of the European Union, 2024).

Within the proposed model, these principles are considered benchmarks for the responsible use of AI. Their application aims to support the understanding of the generated results, the intervention of personnel when necessary and the monitoring of risks during use. For SMEs in the Republic of Moldova, legal obligations should be analyzed depending on the activity of the enterprise and the scope of the regulation.

For SMEs to which these requirements apply, documenting compliance and organising human supervision may require additional effort. Meeting the obligations requires time, technical skills and legal knowledge, resources that may be limited in small enterprises. In this context, practical guides, staff training and support measures tailored to the needs of SMEs can facilitate the responsible use of AI and compliance with legal requirements. The AI Act provides for support measures for these enterprises and takes into account their needs in the development of implementation guidelines (European Parliament and Council of the European Union, 2024).

CONCLUSIONS AND RECOMMENDATIONS

The analysis highlights the potential of artificial intelligence to support SMEs' cybersecurity by detecting threats, automating incident response activities, and using available resources more efficiently. However, realizing these benefits depends on the readiness of enterprises and the integration of AI solutions into existing processes. For SMEs in the Republic of Moldova, limited financial resources, lack of specialized skills, and the need to modernize IT infrastructure can make this process difficult.

The study's findings indicate the need for a gradual approach, in which digitalization is accompanied by the development of cyber protection capabilities. Staff training, risk assessment, and access to technical support are important directions for the responsible use of AI. At the same time, European requirements must be analyzed according to the activity of each enterprise and the scope of relevant regulations.

The AI-NIST-SME-MD framework proposed in the paper aims to provide SMEs with a benchmark for the gradual integration of AI into cybersecurity. Its modular structure allows for the selection of measures based on the identified risks, available resources and the level of preparedness of the enterprise. The application of the framework can support the strengthening of protection and the organization of the compliance process, and its practical usefulness is to be assessed through testing in SMEs in the Republic of Moldova.

- Based on the results of the analysis, the following recommendations are proposed to support SMEs in the Republic of Moldova in the adoption and responsible use of AI in cybersecurity:
- Develop a financial support program for SMEs, facilitating investments in cybersecurity, including the adoption of AI solutions appropriate to their needs. The funding could combine national resources with European opportunities, subject to the eligibility conditions of the relevant programs.
- Strengthening assistance services for SMEs in the field of cybersecurity, through a specialized structure or by developing the capacities of existing institutions. These services could include technical consultancy, risk assessment and staff training.
- Develop a practical guide on the requirements of NIS2 and AI Act relevant to SMEs, explaining the conditions of applicability and the necessary measures for compliance. The guide could be developed with the involvement of competent institutions and specialists in the field.
- Examine the opportunity of tax incentives for investments in cybersecurity, including for AI solutions, based on an assessment of the costs and benefits for businesses.
- Develop university and continuing professional training programs in cybersecurity and AI, by strengthening the collaboration between universities, businesses and public institutions. The focus should be on the practical skills needed to implement and use these solutions.

REFERENCES

Awan, M., Alam, A., Khan, R.A., Alwageed, H.S., Ayouni, S. and Almagrabi, A.O., 2026. A generative AI-driven cybersecurity framework for small and medium enterprises software development: an ANN-ISM approach. *Scientific Reports*, 16(1), p.9813. https://doi.org/10.1038/s41598-026-37614-8.

Biroul Național de Statistică al Republicii Moldova, 2025. *Activitatea întreprinderilor mici și mijlocii în anul 2024*. Biroul Național de Statistică al Republicii Moldova. Available at: https://statistica.gov.md/ro/activitatea-intreprinderilor-mici-si-mijlocii-in-anul-2024-9557_61902.html.

Botezatu Serghei, 2021. *Digital Transformation of Moldova: there is no way back*. United Nations Development Programme. Available at: https://www.undp.org/moldova/blog/digital-transformation-moldova-there-no-way-back

Carayannis, E.G., Dumitrescu, R., Falkowski, T. and Zota, N.-R., 2024. Empowering SMEs "Harnessing the Potential of Gen AI for Resilience and Competitiveness". *IEEE Transactions on Engineering Management*, 71, pp.14754–14774. https://doi.org/10.1109/TEM.2024.3456820.

Creswell, J.W. and Plano Clark, V.L., n.d. *Designing and Conducting Mixed Methods Research*. 3rd edn. Thousand Oaks, CA: SAGE Publications.

De Azambuja, A.J.G., Plesker, C., Schützer, K., Anderl, R., Schleich, B. and Almeida, V.R., 2023. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*, 12(8), p.1920. https://doi.org/10.3390/electronics12081920.

ENISA, 2018. *Good Practices for Security of Internet of Things in the Context of Smart Manufacturing*. European Union Agency for Network and Information Security. Available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot.

ENISA, 2025. *Technical implementation guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures*. Institution. Available at: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

European Commission, 2026a. *Commission strengthens EU cybersecurity resilience and capabilities*. European Commission. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-strengthens-eu-cybersecurity-resilience-and-capabilities.

European Commission, 2026b. *Timeline for the Implementation of the EU AI Act, 2026*. AI Act Service Desk. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act.

European Parliament and Council of the 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

European Parliament and Council of the European Union, 2024. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

Government of the Republic of Moldova, 2023a. *Hotărârea Guvernului nr. 671 din 13 septembrie 2023 privind dezvoltarea profesională în domeniul securității cibernetice*. Available at: https://www.legis.md/cautare/getResults?doc_id=139187&lang=ro.

Government of the Republic of Moldova, 2023b. *Hotărârea Guvernului nr. 1028 din 21 decembrie 2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică*. Available at: https://www.legis.md/cautare/getResults?doc_id=140895&lang=ro.

Graux, H., Garstka, K., Murali, N. and Cave, J., 2025. *Interplay between the AI Act and the EU digital legislative framework*. [PE 778.575] European Parliament. Available at: https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU%282025%29778575.

IBM, 2024a. *Cost of a Data Breach Report 2024*. IBM. Available at: https://emea.ingrammicro.com/getmedia/6ed5227f-ce0a-445e-98a2-8a2c195df484/IBM-Cost-of-a-Data-Breach-Report-2024.pdf.

IBM, 2024b. *Cost of a Data Breach Report 2024*. IBM. Available at: https://emea.ingrammicro.com/getmedia/6ed5227f-ce0a-445e-98a2-8a2c195df484/IBM-Cost-of-a-Data-Breach-Report-2024.pdf.

ITU, 2024. *Global Cybersecurity Index 2024*. International Telecommunication Union. Available at: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

MDED, 2024. *[POLICY PAPER] Cartea Albă privind Inteligența Artificială și Guvernanța Datelor – primul document cadru de politici al MDED*. Ministerul Dezvoltării Economice și Digitalizării. Available at: https://mded.gov.md/ .

Mohd Rasdi, R. and Umar Baki, N., 2025. Navigating the AI landscape in SMEs: Overcoming internal challenges and external obstacles for effective integration. *PLOS One*, 20(5), p.e0323249. https://doi.org/10.1371/journal.pone.0323249.

National Institute of Standards and Technology, 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.6.

OECD., EBRD., 2024. *SME Policy Index: Eastern Partner Countries 2024*. OECD Publishing. Available at: https://www.oecd.org/en/publications/sme-policy-index-eastern-partner-countries-2024_3197420e-en/full-report.html.

OECD and European Bank for Reconstruction and Development, 2023. *SME Policy Index: Eastern Partner Countries 2024: Building Resilience in Challenging Times*. SME Policy Index. OECD Publishing. https://doi.org/10.1787/3197420e-en.

Quainoo, C.R. and Ahad, M.A.R., 2026. The Role of Information Security in Responsible AI for Digital SMEs: A Systematic Review of Frameworks, Challenges, and Best Practices. *Journal of Ethics and Emerging Technologies*, 36(1), pp.1–29. https://doi.org/10.55613/jeet.v36i1.193.

Rombaldo Junior Carlos, B.I. and Johnson Shane, 2023. *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity*. Available at: https://arxiv.org/abs/2309.17186.

Runde, D.F., Kieff, L. and Bryja, T., 2024. *Strengthening Moldova's Cyber Landscape*. Center for Strategic and International Studies.

UNDP, 2023. *A 100% digital state: The strategy for digital transformation of the Republic of Moldova for 2023-2030, approved by the Executive*. United Nations Development Programme. Available at: https://www.undp.org/moldova/press-releases/100-digital-state-strategy-digital-transformation-republic-moldova-2023-2030-approved-executive .

Verizon, 2025. *2025 Data Breach Investigations Report*. Verizon. Available at: https://www.verizon.com/business/resources/Tc25/reports/2025-dbir-data-breach-investigations-report.pdf.

World Economic Forum, 2026. *Global Cybersecurity Outlook 2026*. World Economic Forum. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2026/ [Accessed 30 September 2026].