Journal of Engineering Science *Vol. XXXII, no. 2 (2025), pp. 87 - 98*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

https://doi.org/10.52326/jes.utm.2025.32(2).08
UDC 331.108.4:159.9:004.056.5(478)

CYBER SECURITY PROFESSIONAL DEVELOPMENT WITHIN CYBERCOR

Dinu Țurcanu, ORCID: 0000-0001-5540-4246,
Ludmila Peca *, ORCID: 0000-0002-4394-2933,
Adrian Prisacaru, ORCID: 0000-0001-7809-0868,
Tatiana Țurcanu, ORCID: 0000-0002-8972-8262

Technical University of Moldova, 168, Stefan cel Mare Blvd., Chisinau, Republic of Moldova
* Corresponding author: Ludmila Peca, *ludmila.peca@isa.utm.md*

Received: 04. 12. 2025
Accepted: 05. 17. 2025

Abstract. One of the main development challenges facing the Republic of Moldova is its vulnerability to state security threats and risks. In the context of the objectives for developing the digital economy and digitalizing public services, measures to counter cyber threats and risks become imperative. Law No. 48/2023 on cyber security stipulates the implementation of requirements, measures, and mechanisms to ensure a sufficiently high level of security for networks and information systems in the Republic of Moldova, capable of guaranteeing the protection of the vital interests of individuals and legal entities, society, and the state, as well as the national interests of the Republic of Moldova. In this regard, the human resources' preparation level plays a primary role and is a priority. Developing cybersecurity skills among staff is an indispensable part of the process of ensuring the cybersecurity of systems and information resources. The creation of the National Institute for Cybersecurity Innovation CYBERCOR aims ultimately to ensure the necessary level of cybersecurity competencies among personnel, strengthening the security of networks and information systems. The appropriate professional development of public authority staff at any level and employees of other legal entities, public or private, will enable the prevention and counteraction of cyber threats and risks.

Keywords: *cybersecurity, personal development, training programs, professional development, cybersecurity training exercises.*

Rezumat. Una dintre principalele provocări de dezvoltare cu care se confruntă Republica Moldova este vulnerabilitatea sa la amenințări și riscuri la adresa securității statului. În contextul obiectivelor de dezvoltare a economiei digitale și digitalizării serviciilor publice, măsurile de contracarare a amenințărilor și riscurilor cibernetice devin imperios necesare. Legea nr. 48/2023 privind securitatea cibernetică prevede implementarea cerințelor, măsurilor și mecanismelor necesare pentru a asigura un nivel suficient de ridicat de securitate a rețelelor și sistemelor informatice din Republica Moldova, capabil să garanteze protecția intereselor vitale ale persoanelor fizice și juridice, ale societății și ale statului, precum și a intereselor naționale ale Republicii Moldova. În acest sens, nivelul de pregătire a resurselor umane joacă un rol esențial și reprezintă o prioritate. Dezvoltarea competențelor în domeniul

securității cibernetice în rândul personalului este o componentă indispensabilă a procesului de asigurare a securității sistemelor și resurselor informaționale. Crearea Institutului Național de Inovații în Securitatea Cibernetică CYBERCOR are ca obiectiv final asigurarea nivelului necesar de competențe în domeniul securității cibernetice în rândul personalului, consolidând securitatea rețelelor și a sistemelor informatice. Formarea profesională adecvată a angajaților autorităților publice, indiferent de nivel, precum și a salariaților altor entități juridice, publice sau private, va permite prevenirea și contracararea amenințărilor și riscurilor cibernetice.

Cuvinte-cheie: securitate cibernetică, dezvoltare personală, programe de formare, dezvoltare profesională, exerciții de instruire în domeniul securității cibernetice.

1. Introduction

In a global context dominated by rapid digitalization, the Republic of Moldova is rapidly developing its information and communication technology (ICT) sector, significantly contributing to economic growth and providing a solid foundation for IT innovation and outsourcing. The launch of Moldova's Digital Transformation Strategy 2023–2030 reflects the country's ambition to build a robust digital economy and strengthen cybersecurity culture [1]. However, in this process, cyber threats have become a major challenge, putting pressure on the digital security of both public and private infrastructures. The COVID-19 crisis highlighted the vulnerability of essential digital services to cyberattacks, emphasizing the need for a robust cybersecurity culture at all levels of society.

The ICT sector has grown rapidly due to high market demand, dynamic competition, and coordinated support from all involved stakeholders. Contributing approximately 7% to the national GDP and generating annual revenues of around 15 billion MDL (approximately 900 million USD), the ICT sector has become a key pillar of the Moldovan economy. Between 2015 and 2020, information technology (IT) became the primary growth driver, surpassing telecommunications, with a 3.6% contribution to GDP in 2020, compared to only 0.8% in 2013, when IT was first prioritized as a national policy focus.

This growth has been supported by competitive costs, advantageous location, and the availability of skilled professionals in Moldova, as well as by fiscal incentives offered to residents of the Virtual Moldova IT Park. International and national reports on digitalization (such as the UN DESA e-Government Index, the Networked Readiness Index, and reports from ANRCETI) reflect progress in internet access, IT device usage, and the implementation of e-government platforms.

However, ICT development and digital transformation have contributed to a substantial growth in cyber risks. The acceleration of digitalization has attracted numerous cyber threats, further amplified by the pandemic, which highlighted the vulnerability of digital services and the economy to these constantly evolving risks.

For example, the assessment report [2] conducted by the International Telecommunication Union (ITU) provides an overview of cyber threats in the Republic of Moldova. Like other countries, Moldova is affected by various types of cyberattacks that target government entities, the private sector, and the general population. Although authorities monitor cyber threats related to government entities, achieving a holistic understanding of cyberattacks at the national level remains challenging This issue is also highlighted in the *Moldova Cybersecurity Governance Assessment* developed by DCAF, which outlines persistent challenges in institutional coordination, clarity of roles, and the visibility of cyber risks at the

national level [3]. Common types of cybersecurity incidents include online scams, phishing (including smishing and vishing), ransomware, web defacement, and denial of service attacks.

Since 2015, Moldova has faced attacks such as DDOS, phishing, brute force attacks on government information systems, and hijacking of official websites. The private sector is equally exposed, with small and medium-sized enterprises (SMEs) representing approximately 98.6% of all businesses in the country as of 2019 [4]. These SMEs are particularly vulnerable due to their limited capacity to implement robust cybersecurity measures. According to ODIMM data, fewer than 17% of SMEs have effectively integrated digital technologies into their operations, revealing both a significant untapped potential and an urgent need to adopt standardized cybersecurity protocols [5].

According to the 2020 Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU), the Republic of Moldova ranks 33rd in Europe and 63rd globally. The GCI serves as a benchmark for evaluating national commitment to cybersecurity across five key domains: legal, technical, organizational, capacity development, and cooperative measures.

2. Materials and methods

The methodological approach adopted for cybersecurity capacity development at CYBERCOR integrates theory with applied practice, combining formal instruction with hands-on simulations. A key element is the E-Academy platform, available through CYBERCOR's internal learning environment, which enables realistic training environments by simulating corporate networks and attack scenarios. These simulations are aligned with international frameworks such as ISO/IEC 27001 and ISO/IEC 31000, and cover all phases of cyber incident response—protection, detection, reaction, and recovery.

Additionally, the curriculum design process involves collaboration with industry partners (e.g., Cisco, Fortinet, Palo Alto), allowing the integration of certified training programs. Practical content includes structured exercises in computer networks and network security, developed by academic staff, and used across bachelor and master's levels. Training outcomes are monitored through performance assessments, SIEM tools, and feedback systems, ensuring the practical relevance and adaptability of content to current threats.

All methodological components aim to support the development of both individual skills and organizational readiness in the cybersecurity field.

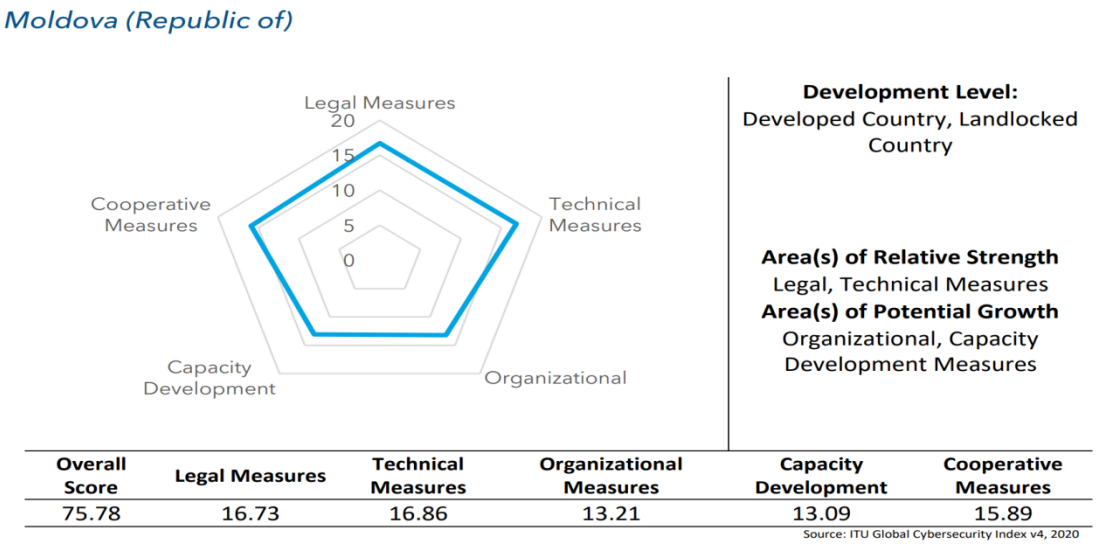
3. Results and discussions

According to the 2020 Global Cybersecurity Index (GCI) published by ITU, the Republic of Moldova demonstrates varied performance across the assessed cybersecurity domains. In terms of legal measures, Moldova obtained a score of 16.73, reflecting a well-developed legal framework for cybersecurity. Technical measures also registered a strong performance, with a score of 16.86, indicating the presence of robust digital protection tools and infrastructure.

In contrast, organizational measures scored 13.21, suggesting that improvements are needed in the strategic planning and governance of cybersecurity at the institutional level. Capacity development scored 13.09, highlighting the urgent need to expand training, education, and workforce development programs in cybersecurity. For cooperative measures, Moldova scored 15.89, reflecting active participation in international partnerships and collaborative initiatives.

Overall, Moldova achieved a GCI score of 75.78, ranking 33rd in Europe and 63rd globally. These results underscore the country's strengths in legal and technical dimensions

while also revealing areas for further development - particularly in organizational maturity and capacity building. Figure 1 presents Moldova's scores across the five core areas of cybersecurity, as assessed in the 2020 GCI.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
75.78	16.73	16.86	13.21	13.09	15.89

Source: ITU Global Cybersecurity Index v4, 2020

Figure 1. Moldova's scores across evaluation domains as reflected in the 2020 Global Cybersecurity Index (GCI) report [6].

According to the ITU's assessment report aimed at supporting the establishment of a national Computer Incident Response Team (CIRT-MD), the slight decline in Moldova's performance in 2020 compared to previous years was primarily attributed to changes in the GCI methodology and question weighting. Nevertheless, Moldova has made steady progress since 2015, particularly in adopting national policies and cooperation agreements designed to enhance the protection of critical information infrastructure.

In response to these challenges, the National Institute for Cybersecurity Innovation – CYBERCOR – was established to serve as a key driver for national cybersecurity progress. The institute plays a fundamental role in professional development, acting as a platform for advanced training, capacity building, and the consolidation of a national network of cybersecurity specialists.

4. The role of CYBERCOR in professional development

The primary objective of the Institute for Innovation in Cybersecurity CYBERCOR is to enhance cybersecurity competencies, contributing to the formation of a network of specialists equipped to address today's information security challenges. CYBERCOR's mission is to provide advanced training and support the development of organizational capabilities through a combination of educational programs and applied exercises that ensure comprehensive, up-to-date training for personnel involved in protecting digital infrastructures.

CYBERCOR is dedicated to fostering professional development in information security, aiming to build competencies at all levels of society, from technical staff to decision-makers. It offers both analytical and implementation services for security systems, as well as specialized training designed to strengthen organizational resilience against cyber incidents.

A fundamental objective of CYBERCOR is to train specialists to secure a high standard of theoretical and practical readiness in the protection of informational assets. These training sessions are designed to help organizations develop monitoring, management, and incident

resilience capacities. Following training, organizations are expected to autonomously identify and eliminate the primary causes of attacks and implement effective corrective measures to prevent future incidents. The training also encompasses processes for acquiring, developing, and maintaining ICT systems, ensuring data confidentiality, integrity, and availability in line with organizational protection standards.

CYBERCOR offers a variety of programs and workshops that adhere to international standards, such as the ISO 2700X and 3100X families, relevant for information security and risk management. These workshops are essential for the efficient management of organizational continuity and for improving information security standards. During these sessions, essential recommendations are provided that organizations should implement to ensure strong cybersecurity governance and to develop robust risk assessment and management processes.

CYBERCOR promotes the establishment of a robust IT governance system that ensures effective cyber risk management at the organizational level. This includes developing a clear information security policy and strategy as an integral part of the company's overall development strategy. Key objectives of this governance system include:

1. **Implementing an IT governance structure**. Ensures efficient management of IT and cybersecurity risks through a governance system focused on analyzing and mitigating cyber risks.
2. **Information security policy and strategy**. As part of the organization's overarching strategy, the security policy should define objectives and necessary measures for information protection.
3. **Determining an acceptable risk level**. Each organization should establish a risk tolerance level, integrating it into the risk strategy and providing regular reports on risks across processes and applications.
4. **Information security audits.** IT governance and security processes should undergo regular audits as per a set plan to identify vulnerabilities and evaluate compliance with security standards.
5. **Introducing the role of information security officer**. Creating a dedicated information security role with well-defined responsibilities and boundaries supports centralized and effective security management.
6. **Monitoring and evaluating security measures**. Involves assessing the effectiveness of implemented measures and regularly reviewing security policies through penetration testing and other practical evaluations.
7. **Education and awareness programs**. Raising employee awareness of the importance of information security is essential for reducing risks associated with the improper use of systems.
8. **Security incident management**. Organizing processes for prompt and effective responses to security incidents at the organizational level and assigning responsibilities for information security.
9. **Long-term acquisition and development plan**. Establishing a security systems acquisition and development plan for 1, 3, and 5-year periods ensures strategic security planning.
10. **Business continuity and disaster recovery plans**. Organizing a continuity and post-incident recovery plan is crucial for maintaining operational continuity in case of disasters.

11. Incident impact analysis and implementation of intervention plans. Involves assessing the impact of incidents and planning quick interventions, including periodic testing of systems and crisis communication plans.

12. National and international cooperation. CYBERCOR aims to ensure effective cooperation at both national and international levels, disseminating relevant information, alerts, and international best practices to organizations in critical sectors.

Moldova's national commitment to cybersecurity is also reflected in the National Security Strategy adopted in December 2023. This document places cybersecurity among the country's top strategic priorities and calls for stronger institutional resilience and broader cooperation across all sectors [7]. At the organizational level, applying concrete measures helps build the capacity to prevent and respond effectively to cyber threats, while also ensuring continuity of operations. In this broader context, aligning Moldova's legislation with European Union standards is a necessary step, especially given the country's current status as an EU candidate.

A critical step in aligning Moldova's cybersecurity framework with European standards is the transposition of the NIS2 Directive, the Directive (EU) 2022/2555 of the European Parliament and of the Council, which sets out measures for a high common level of cybersecurity across the Union. This process also involves amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, while repealing the earlier Directive (EU) 2016/1148 [8]. The implementation of NIS2 is a national priority and plays a key role in strengthening Moldova's cyber defense capabilities. It supports both institutional alignment with EU standards and the development of a more robust and coordinated cybersecurity ecosystem in the country [9,10].

5. Initiatives and training activities

The National Institute for Cybersecurity Innovation plays a crucial role in professional development by organizing specialized courses and workshops in cybersecurity. Through the simulation platform „E-Academy", CYBERCOR provides participants with an integrated experience that combines theory with applied practice, enabling them to strengthen their skills in a realistic environment. This platform is designed for both professionals and individuals responsible for security within small and medium-sized companies, where practical training opportunities have previously been limited due to resource constraints.

Key focus areas of the cybersecurity training platform

1. Realistic simulation of cyber threats. The „E-Academy" platform offers participants a virtual environment that faithfully replicates a corporate network. It is equipped with a full range of security tools and devices (firewalls, routers, IPS/IDS, and SIEM products) that enable complex simulations, including sophisticated attacks like ransomware and malware. All activities are recorded for later analysis and performance assessment. This customizable environment allows participants to learn how to detect, investigate, and respond effectively to current cyber threats.

2. Network versatility. The adaptability of the platform allows for simulations of diverse configurations tailored to the needs and profile of each participating organization. A variety of attack scenarios, including simulations of complex threats such as trojans, exploits, and DDoS attacks, helps trainees identify specific vulnerabilities and better understand the need for investments in cybersecurity.

3. **Diversity of simulated threats**. A key feature of „E-Academy" is its ability to simulate a wide range of attacks tailored to different types of organizations. This includes both common and advanced threats, reflecting the complexity of modern cyber threats and preparing participants to handle incidents that could disrupt a company's operational continuity.

4. **Adaptable curriculum**. The platform offers specialized courses, such as Fileless Attack, Ransomware and Encryption, and Corporate Espionage. Each course is structured to cover all phases of the incident response cycle, including protection, detection, reaction, and recovery. In addition to simulation-based courses, CYBERCOR's curriculum incorporates practical resources developed by local academic staff, including collections of solved exercises designed to support hands-on learning in core areas such as computer networks [13] and network security [14]. These materials are widely used in undergraduate and master's programs, helping students consolidate their technical understanding through real-world examples.

5. **Advanced learning, analysis, and feedback tools.** The platform includes a complex set of tools for vulnerability scanning and SIEM exercises, providing real-time feedback to participants. Instructors can monitor participants' progress, offering personalized guidance and discussing results in detail during evaluation sessions. Additionally, participants can revisit specific stages through video recordings to analyze decisions made and improve their response strategies.

To address the cybersecurity skills gap, CYBERCOR collaborates with external partners such as Cisco, Fortinet, and Palo Alto. These partnerships support the continuous development of training programs, ensuring that the content and technologies used remain aligned with international best practices. This approach also reflects broader trends identified in recent reports, such as Fortinet's global overview of workforce challenges in cybersecurity [11], as well as ENISA's recommendations for advancing cybersecurity education and skills across the European Union [12]. Additionally, these collaborations enable the provision of internationally recognized courses and certifications, preparing participants to meet the increasingly rigorous demands of the cybersecurity field.

Figure 2. Simulation of the „Dragonfly" Cyber Attack (exercise).

The „E-Academy" platform includes advanced simulations of persistent and sophisticated attacks, such as „Dragonfly". This type of advanced persistent cyber threat is

known for targeting critical infrastructure, including government entities, essential sectors like energy, water, aviation, and industrial manufacturing. Attacks in the "Dragonfly" family focus on compromising industrial control systems, with the ultimate goal of gaining unauthorized access to organizational networks and disrupting their operations.

During the simulation, participants are trained to detect suspicious activities associated with attacks like „Dragonfly", investigate targeted components and vulnerabilities, and implement response measures.

The simulation covers complex attack scenarios, including network exploitation techniques and unauthorized access to control systems, reflecting the disruptive potential of such attacks on the operation of critical infrastructures. This model provides trainees with practical experience in identifying, analyzing, and mitigating threats that impact sectors essential to national security.

The „E-Academy" platform is designed to meet the specific needs of trainees and the cybersecurity market in the Republic of Moldova. The objective of CYBERCOR and the „E-Academy" platform is to contribute to the preparedness of Moldovan IT specialists by promoting a solid understanding of security incidents and attacks, as well as an effective response capability.

Through the realistic and immersive learning environment of „E-Academy", the platform offers trainees not only technical knowledge but also essential practical skills, such as configuring security systems and understanding the risks associated with improperly implemented measures. This enables organizations to develop long-term security strategies, multi-year security plans, and prioritized investments in systems and dedicated personnel. These skills are crucial for preparing companies to withstand cyberattacks and protect critical infrastructure effectively.

To ensure high-quality and continuously updated cybersecurity skills, the platform also functions as a research and development laboratory. This center enables the team to develop and validate new cybersecurity tools and techniques, test security architectures, and analyze malware for a better understanding of attack mechanisms.

CYBERCOR provides continuous and solid cybersecurity education to partner organizations, ensuring a practical and adaptable approach to current threats. CYBERCOR's training approach is also grounded in modern e-learning methodologies, combining theoretical instruction with interactive, digital environments that support independent learning and experimentation. Previous research has emphasized the value of e-learning in developing ICT skills and its role in shaping effective engineering education strategies [15,16].

The National Institute for Cybersecurity Innovation, established at the Technical University of Moldova supported through the Future Technologies Project (FTA), sponsored by USAID and the Government of Sweden, was created in response to the shortage of specialized cybersecurity personnel, both nationally and internationally. In Moldova, cybersecurity is an underpromoted field and is rarely addressed within the traditional education system (secondary, high school, and university), lacking sufficient integration into the curriculum.

The founding of the Institute aims not only to train a new generation of cybersecurity professionals but also to increase awareness and integrate this essential field into youth education.

6. Objectives and actions of the National Institute for Cybersecurity Innovation

Founded to address the shortage of cybersecurity specialists, CYBERCOR at the Technical University of Moldova aims to accomplish the following objectives and measurable actions in its first year of operation:

1. **Research and studies**
   - Conduct studies on methods for ensuring the cybersecurity of networks and digital services, with a focus on preventing attacks and enhancing the cyber resilience of information systems.
   - Develop software resources to protect data managed within cyber infrastructures.
   - Implement and test advanced security architectures and protocols.
2. **Professional development and continuous training**
   - Support theoretical and practical training for students, master's candidates, doctoral students, and professors, stimulating creativity and innovation in cybersecurity.
   - Organize cyber exercises and simulations within the Academy to prepare specialists for realistic cyberattack scenarios.
   - Offer training and workshops for IT personnel in the public and private sectors to strengthen national cyber defense capabilities.
3. **Partnerships and cooperation**
   - Collaborate with public institutions to develop cybersecurity skills in line with the state's plan for enhancing public sector personnel.
   - Participate in working groups to develop cybersecurity curricula at all educational levels.
4. **Dissemination and publicity**
   - Disseminate academic results and research to increase interest in cybersecurity and expand the market.
   - Publish scientific articles, patent technical innovations, and participate in national and international conferences.
5. **Technical support and infrastructure**
   - Provide technical and informational support for conducting cybersecurity workshops and training sessions.
   - Establish a specialized lab equipped with cutting-edge technologies and tools provided by global leaders in cybersecurity solutions (Cisco Systems, BitDefender, Palo Alto, MicroFocus, Fortinet, etc.).

In addition to building technical capacity, CYBERCOR places emphasis on cultivating a sense of mission and shared purpose among trainees and educators. This perspective aligns with modern approaches to leadership and organizational development, which highlight the importance of understanding "why" behind every professional action [17]. Hosted from the Technical University of Moldova, with support from the Information Technology and Cybersecurity Service (STISC), the Electronic Governance Agency (AGE) and the Cybersecurity Agency (ASC), CYBERCOR will contribute to strengthening national security infrastructure and support the government's digital transformation processes.

The National Institute for Cybersecurity Innovation offers multi-dimensional education in cybersecurity, including undergraduate and master's programs at the Technical University of Moldova, as well as executive education tailored to professionals and managers in the field. CYBERCOR is also actively involved in training teachers in schools and high schools,

disseminating best practices in cybersecurity among students, and contributing to the modernization of the school curriculum in cybersecurity.

7. Strategic development directions of CYBERCOR

The National Institute for Cybersecurity Innovation CYBERCOR aims to unify and coordinate cybersecurity initiatives within the Technical University of Moldova, consolidating a strategic action plan to advance this essential field. The new entity welcomes collaboration with international partners and top cybersecurity solution providers, fostering a high-quality educational environment that aligns with market needs.

In its first year of operation, CYBERCOR plans to implement the following measurable actions:

1. **Faculty training**. Training and certifying at least 20 faculty members from the FCIM and FET faculties through advanced programs provided by industry leaders, supported by Pearson VUE Testing Center.
2. **Student Training**. Including cybersecurity courses for 200 students annually within the undergraduate and master's programs at FCIM and FET. Developing micro-master programs in cybersecurity.
3. **Enhancing teaching capacity**. Integrating at least five industry trainers to improve the quality of the academic teaching process alongside university faculty.
4. **Providing practical training**. Offering internships for students at STISC, AGE, and private cybersecurity companies, ensuring hands-on training.
5. **Organizing competitions and events**. Hosting at least two national competitions in cybersecurity, with a minimum of 100 student participants. Organizing a roundtable with at least 50 participants from the public and private sectors to discuss current cybersecurity challenges and the role of academia.
6. **Training for educational institution staff**. Collaborating with the General Directorate of Education, Youth, and Sports in Chișinău to provide training for school directors on online safety, reaching an audience of at least 100 participants.
7. **Training public sector employees**. Organizing cybersecurity training for at least 600 public sector employees, subject to the approval of mandatory retraining through government decision.
8. **Inviting international trainers**. Collaborating with international trainers, especially from Romania, to enhance education quality and overcome potential language barriers.
9. **Establishing educational partnerships**. Forming at least three partnerships with leading cybersecurity providers to implement authorized courses and utilize software resources and educational tools in the training process.

The National Institute for Cybersecurity Innovation „CYBERCOR” is committed to developing a qualified workforce and strengthening national capabilities in cybersecurity, thereby supporting digital transformation and the resilience of critical infrastructures in the Republic of Moldova.

8. Conclusions

The results of the GCI reveal Moldova's partial progress in strengthening digital resilience. While the legal and technical measures are relatively strong, the organizational dimension and capacity development remain underdeveloped. In response to this need, the CYBERCOR Institute was created to strengthen national capacities through advanced training. Through partnerships with industry leaders and simulation-based learning, CYBERCOR

contributes to the consolidation of a skilled cybersecurity workforce. The human-centered approach supports the development of practical abilities and institutional readiness to respond to cyber threats, thus contributing to improving the overall national cybersecurity posture. Continued investment in such structured professional development initiatives is essential to ensure Moldova's resilience against emerging cyber threats.

A version of these results was initially presented at the International Conference on Electronics, Communications and Computing (ECCO 2024), held on 17–18 October 2024 in Chișinău.

Conflicts of interest. The authors declare no conflicts of interest.

References

1. Government of the Republic of Moldova. Announcement regarding the initiation of the development of the Digital Transformation Strategy of the Republic of Moldova for the years 2023–2030 [in Romanian] 2023. Available online: https://particip.gov.md/ru/document/stages/anunt-privind-initierea-elaborarii-strategiei-de-transformare-digitala-a-republicii-moldova-pentru-anii-20232030-stdm-2030/9355. (accessed on 22 January 2025).
2. International Telecommunication Union (ITU). Assessment Report of Moldova National Computer Incident Response Team (CIRT-MD) 2022. Available online: https://moldova.un.org/sites/default/files/2023-01/CIRT-Assessment-Moldova-final.pdf. (accessed on 9 February 2025)
3. Geneva Centre for Security Sector Governance (DCAF). Moldova Cybersecurity Governance Assessment 2019. Available online: https://www.dcaf.ch/sites/default/files/publications/documents/MoldovaCybersecurity GovernanceAssessment.pdf (accessed on 21 May 2025).
4. National Bureau of Statistics of the Republic of Moldova. Total number of enterprises and the share of SMEs in Moldova [in Romanian] 2023. Available online: https://statistica.gov.md/newsview.php?l=ro&idc=168&id=6716. (accessed on 2 February 2025).
5. Organization for the Development of Small and Medium Enterprises (ODIMM). Digitalization of SMEs in the Republic of Moldova [in Romanian] 2023. Available online: https://www.odimm.md/ro/digitalizarea. (accessed on 19 February 2025)
6. International Telecommunication Union (ITU). Global Cybersecurity Index (GCI) Report 2021. Available online: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed on 12 January 2025).
7. Parliament of the Republic of Moldova. Decision No. HP391/2023 of 15.12.2023 on the approval of the National Security Strategy of the Republic of Moldova [in Romanian] Published in: Official Monitor No. 17–19, 17 January 2024. Available online: https://presedinte.md/app/webroot/uploaded/Proiect%20SSN_2023.pdf.
8. European Commission. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *Official Journal of the European Union*, 27 December 2022. Available online: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (accessed on 21 May 2025).
9. Dinu Țurcanu, Natalia Spinu, Serghei Popovici, Tatiana Țurcanu. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020.*In: Journal of Social Sciences*, Vol. IV, no. 1 (2021), pp. 74 – 83.
10. Peca, L.; Țurcanu, D. Reducing cyber risk through a human–centred approach. *Journal of Engineering Science,* 2025, 32(1), pp.18–31.
11. FORTINET. *Cybersecurity Skills Gap Report 2024*. Available online: https://www.fortinet.com/resources/reports/cybersecurity-skills-gap. (accessed on 5 January 2025).
12. ENISA. Cybersecurity Skills Development in the EU: An Overview. European Union Agency for Cybersecurity, 2023. Available online: https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu (accessed on 13 April 2025).
13. Peca, L.; Țurcanu, D. *Computer networks: Practical examples solved to be introduced in computer networks.* ; Tehnica-UTM, Chisinau, RM, 2022, 188 p.
14. Peca, L.; Țurcanu, D. Network security*: Practical examples solved to be introduced in network security*. Tehnica-UTM, Chisinau, RM, 2023, 243 p.

15. Dumbraveanu, R.; Peca, L. E-learning in Developing ICT Skills of Future Engineers. In: *1st International Online Scientific Conference ICT in Life*, August 2022, Osijek, Croația. 2022, pp. 86-95.
16. Peca, L. The power of eLearning from promises to practices applied in engineering. *Journal of Social Sciences* 2023, 6(1), pp. 69-80.
17. Sinek, S.; Mead, D.; Docker, P. *Find your why: A practical guide for discovering purpose for you and your team*. Portfolio, New York, SUA, 2017, 242 p.

Citation: Țurcanu, D.; Peca, L.; Prisacaru, A.; Țurcanu, T. Cyber security professional development within CYBERCOR. *Journal of Engineering Science*. 2025, XXXII (2), pp. 87-98. https://doi.org/10.52326/jes.utm.2025.32(2).08.

Submission of manuscripts: jes@meridian.utm.md