Methodological Aspects of Integrating and Mathematically Modeling a Cyber Range as an Innovative IT Solution for Cybersecurity Education in Higher Education Institutions

Roman Yaroviy[1], Olena Skliarenko[1], Serhii Yahodzinskyi[1], Yanina Kolodinska[1], Oleksandr Nikolaievskyi[1] and Hanna Tereshchuk[6]

[1]*Private Higher Educational Establishment "European University", Akademika Vernadskoho Blvd. 16V, 03115 Kyiv, Ukraine*

[6]*Taras Shevchenko National University of Kyiv, Volodymyrska Str. 60, 01033 Kyiv, Ukraine*

roman.yaroviy@e-u.edu.ua, olena.skliarenko@e-u.edu.ua, serhii.yahodzinskyi@e-u.edu.ua, yanina.kolodinska@gmail.com, a.nikolaievskyi@gmail.com, ganna.tereschuk@knu.ua

Keywords: Cyber Range, Cybersecurity Education, Cyber Defense, Information Technology, Stochastic Mathematical Model, Modeling, Performance Indicators, Optimization.

Abstract: The increasing complexity of cyber threats necessitates scalable and practice-oriented approaches to cybersecurity education. This paper presents the design and evaluation of a virtual cyber range integrated into bachelor's and master's cybersecurity programs at a Ukrainian university. The proposed platform is based on a multi-layer virtualized architecture that incorporates Red, Blue, and White team environments, enabling offensive, defensive, and administrative training within a unified infrastructure. The study combines competency-based curriculum mapping with Capture the Flag (CTF) exercises and pre-/post-training assessment. Experimental results demonstrate statistically significant learning improvements, with an average Learning Gain Index (LGI) above 0.6, confirming the effectiveness of the proposed approach in developing incident response, penetration testing, and secure system configuration skills. In addition to the architectural and educational contributions, the paper introduces a stochastic discrete-time dynamic model with Markov-modulated random coefficients to evaluate cyber range effectiveness under uncertainty. The model enables quantitative assessment of long-term performance, risk levels, and resource management strategies, accounting for variability in attack intensity, system reliability, and user behavior. The proposed model is formulated independently of a specific cyber range implementation, enabling its application to a broad class of cybersecurity training and simulation platforms. The results confirm that cyber range integration strengthens competency development and aligns with international practices in cybersecurity education.

1 INTRODUCTION

During the training of students majoring in F5 "Cybersecurity and Information Protection", a crucial stage is the acquisition of practical skills in the field of information security event monitoring and the implementation of protective measures under real-world conditions, where an organization's information system is subjected to an attack.

One of the most effective ways to ensure high-quality practical training is the implementation of a cyber range into the educational process.

Cyber ranges are widely recognized as effective platforms for realistic cyber training and experimentation.

Several mature cyber range platforms are already deployed worldwide, including governmental, academic, and commercial solutions [1].

These platforms offer comprehensive attack simulations, including: phishing, DDoS, malware deployment, attacks on network infrastructure, data confidentiality breaches [2], and more.

Modern cybersecurity systems increasingly rely on adaptive and data-driven approaches for detecting anomalies and cyber attacks. Clustering-based methods and expert systems are widely used for identifying abnormal patterns and supporting decision-making processes [3].

It is worth noting that a cyber range is an expensive and fully-featured system [4] that requires significant financial investment. For educational

institutions, especially those with limited budgets, such a solution may have a long return on investment period.

Therefore, the development of an internal cyber range based on open-source virtualization technologies requires coordinated technical, methodological, and organizational efforts.

A cyber range offers real opportunities for students, cadets, IT and cybersecurity professionals to practice on "training targets" - to acquire hands-on experience without the risk of causing actual harm to a real enterprise. At the same time, a typical enterprise network infrastructure (servers, workstations, network devices, corporate software, security tools, etc.) is reproduced in a virtual environment. This standard set of components enables the modeling of a corporate network.

2 RESEARCH METHODOLOGY

The study employed a mixed-methods approach combining comparative analysis of academic sources, case studies of cyber range deployment, empirical observation of student performance, survey-based self-assessment, competency-service mapping, and quantitative statistical evaluation of learning outcomes.

The empirical data were collected from system logs, user activity records, and assessment results generated within the cyber range environment. The study involved 48 students.

All data were anonymized and processed in accordance with institutional ethical guidelines.

2.1 Analysis of Cyber Range Deployment Principles

Based on market needs analysis, expectations of primary stakeholders, and the study of global experience (e.g., Cyber Range, NATO CCDCOE, IBM X-Force Command Center), it has been determined that a multi-layered architecture is the optimal approach for designing a modern cyber range. This approach ensures scalability, flexibility, and multi-purpose use of the infrastructure - for education, security system testing, R&D, and software certification.

At the top layer of the architecture, the user web portal provides unified access to platform services, while the underlying functional layer supports integrated training, cyber exercises, competitive simulations, vulnerability research, and experimental studies of emerging technologies (Fig. 1).

All functionality is deployed on top of a virtualization platform, which is physically hosted in a local infrastructure (data center). Interactions between layers are carried out via a service bus and orchestration layer, which enables dynamic replacement of individual components (e.g., changing the sector-specific training environment - from financial to energy, transport, etc.) [5].

The cyber range infrastructure flexibly redistributes computing resources between segments as needed, and a high-performance data transmission network connected to secure, special-purpose networks allow for remote lab access. A backup and recovery system ensures the highest degree of fault tolerance of the complex.

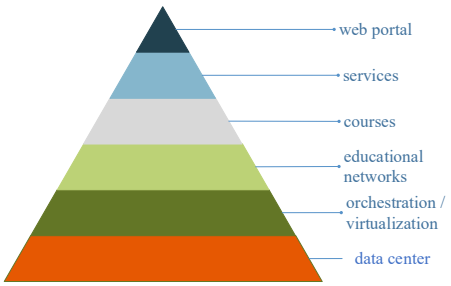

Figure 1: Multi-layered cyber range architecture.

The conceptual diagram of the “Cyber Range” virtual lab (Fig. 2) illustrates the structural design of a virtual training environment for cybersecurity. The scheme includes the Red Team segment (offensive side) and Blue Team segment (defensive side), a training target network, a cyber range control center, a core network interconnecting all components, and remote access tools. Each segment is isolated from the others using VLAN/routing but connected via a common network core to manage traffic flow [6]. All elements are labeled (in Ukrainian in the original) and linked to reflect the logical interaction of cyber range components.

The cyber range architecture (Fig. 2) consists of interconnected, isolated segments managed via a central Network Core and VLAN switching. The Red Team provides offensive capabilities using virtual machines equipped with penetration testing tools to simulate external threats, while the Blue Team utilizes traffic inspection and incident response systems to detect and mitigate simulated attacks in real time.

The primary target for these exercises is the Training Network Environment, which emulates realistic enterprise infrastructures - including DMZs and vulnerable internal services - enabling full attack lifecycle simulation [7]. Such architectures are widely

used for modeling attacks on industrial and mixed IT/OT environments and for evaluating layered defense strategies under realistic conditions [8]. The entire ecosystem is overseen by the Cyber Range Control Center (White Team), which handles virtualization orchestration, scenario deployment, and resource allocation. Finally, secure distributed participation is facilitated through a robust VPN Gateway, a model commonly adopted in cyber range architectures to enable secure collaboration without exposing internal resources to external networks [9].

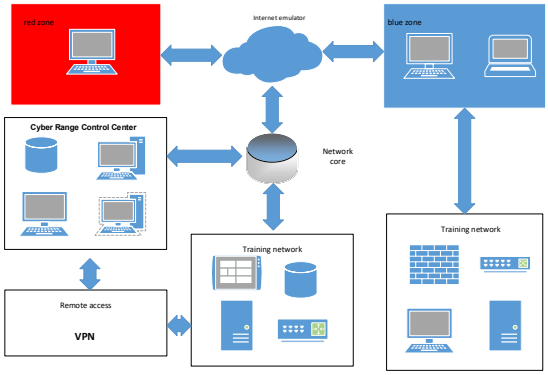

Figure 2: Cyber range virtual lab: conceptual scheme (cyber range laboratory - tecnalia).

2.2 Functional and Technical Integration of the Cyber Range

The cyber range represents an integrated hardware-software environment designed to support cybersecurity training, experimentation, and applied research through repeatable and controlled attack-defense scenarios [10], [11]. From a technical perspective, the platform relies on isolated execution environments, scalable resource management, and advanced monitoring and protection tools, including IDS/IPS, firewalls, and SIEM systems, implemented on top of virtualization infrastructures. Such architecture ensures realistic, reproducible, and secure experimentation conditions required for cybersecurity education [12] and system evaluation [9].

Functionally, the cyber range enables a wide spectrum of activities, including penetration testing, code analysis, vulnerability assessment, and security evaluation of both traditional IT systems and industrial infrastructures (SCADA/ICS). The separation of Red Team (offensive) and Blue Team (defensive) environments allows for structured simulation of cyber incidents and coordinated response scenarios.

By providing a controlled and configurable environment, the cyber range facilitates validation of cybersecurity tools, development of incident response strategies, and assessment of defense mechanisms against modern threats, including social engineering and phishing as dominant initial attack vectors [13]. The platform aligns with established frameworks such as MITRE ATT&CK and supports systematic analysis of attack vectors and defensive capabilities.

Importantly, the described functional and technical characteristics define the observable system parameters used in the proposed stochastic model, including resource utilization, incident response efficiency, and system resilience. This establishes a direct link between the cyber range infrastructure and the analytical evaluation framework introduced in this study.

2.3 Analysis of Cyber Range Integration into Cybersecurity Specialist Training

For students majoring in F5 “Cybersecurity and Information Protection”, the implementation of a cyber range enables the development of a wide range of general (GC) and professional (PC) competencies defined in the educational program. Through hands-on practice in a safe, simulated environment, students can apply acquired knowledge and gain critical professional skills [7].

The cyber range facilitates the development of key cybersecurity competencies, including technical, analytical, and collaborative skills, through realistic attack-defense simulations and tool-based exercises. The acquired competencies correspond to defined learning outcomes and internationally recognized training frameworks [14].

The cyber range was integrated into cybersecurity curricula as a practical training platform supporting hands-on skill development and competency assessment. The proposed educational model combines theoretical instruction with scenario-based simulations, enabling students to apply cybersecurity concepts in controlled yet realistic environments.

Practical exercises, including Red Team and Blue Team scenarios, contributed to the development of both technical and transversal competencies, such as incident analysis, teamwork, coordination, and critical thinking. These activities are aligned with program learning outcomes and support the achievement of key competencies in cybersecurity education (Table 1).

Table 1: Key performance indicators.

Indicator	Description
Success Rate (%)	Percentage of students who completed key tasks or earned certificates
Average Score	Mean score across training tasks, CTF events, and simulations
Attempt Count	Average number of attempts needed to complete a task successfully
Time to Completion	Average time spent completing tasks (as an efficiency indicator)
Pre-/Post-Test Score	Knowledge and skill level before and after cyber range training
Individual Ranking	Participant ranking based on their performance in training
Engagement Index	Percentage of students who completed all mandatory scenarios/blocks

Table 2: Assessment format: pre-/post-test comparison.

Group	Pre-test (avg)	Post-test (avg)	Δ (Gain)	% of Completed Cases	Avg. CTF Score
Bachelor (3rd year)	62%	84%	+22%	86%	78 points
Master (1st year)	74%	91%	+17%	93%	85 points

Knowledge Gain Analysis.

Knowledge gain Δ ≥15% is considered a significant improvement (Table 2).

Learning Gain Index (*LGI*):

$$LGI = \frac{(Post - Pre)}{(100 - Pre)}. \quad (1)$$

$LGI > 0.6$ indicates a high level of training effectiveness.

Statistical significance ($p < 0.05$) confirms a measurable impact of cyber range training. The difference between the initial and final results was statistically significant (t-test, $p < 0.05$, Cohen's d=0.8), indicating a large effect size.

The 95% confidence interval for the mean effectiveness index at the final stage was [0.78; 0.84].

Low attempt count with high success suggests confident mastery of skills.

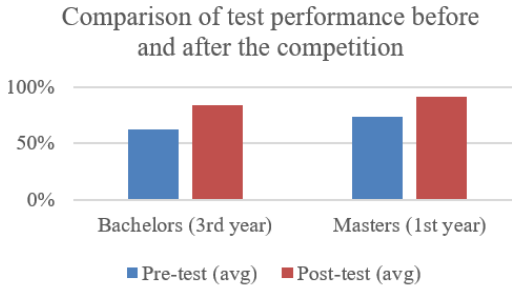

Figure 3: Comparative student test results chart.

Integrating the cyber range into bachelor's and master's programs in cybersecurity significantly enhances practical learning outcomes (Fig. 3). It develops essential competencies, fosters interdisciplinary education, and contributes to research-oriented training. The cyber range serves as a "real challenge arena with cutting-edge technology and professional growth opportunities," preparing competitive, well-rounded cybersecurity experts equipped to operate in modern cyber environments.

2.4 Construction of a Stochastic Model for Evaluating the Functioning of a Cyber Range

Unlike platform-specific evaluation approaches, the proposed stochastic discrete-time model is formulated in a generic form and is not limited to a particular cyber range implementation. The parameters of the model are derived from the functional and technical characteristics described in Section 2.2. The model can be applied to a wide class of cyber training and simulation environments, including academic cyber ranges, corporate SOC training platforms, and cyber-physical testbeds, where system performance is influenced by uncertainty in attack intensity, resource availability, and human factors.

Stochastic modeling makes it possible to describe systems whose operation depends on random factors. Instead of fixed parameters, random variables are used (normal, uniform, exponential, etc.). Similar approaches to modeling cybersecurity processes under uncertainty have been widely studied, supporting the relevance of combining probabilistic and data-driven methods in cyber range evaluation. This approach allows for accounting for unpredictability in the functioning of the cyber range (new types of attacks, human errors, equipment failures). A generalized integral assessment makes it possible to determine efficiency over a period of time as well as to build probabilistic scenarios [15], [16].

Let us consider the stages of constructing a stochastic discrete-time dynamic model with

Markov-modulated random coefficients to assess the effectiveness of a cyber polygon under conditions of uncertainty.

Step 1. Define the system input parameters. Let's introduce variables and notation for the system model:

- $k \in Z \geq 0$ - discrete time index (simulation step);
- $E_k \in R$ - aggregated effectiveness index of the cyber range at step k (can be a scalar or a vector of indicators);
- $U_k \geq 0$ - intensity of incoming events/attacks at step k;
- $R_k > 0$ - available resources (computational /network) at step k;
- α_k, β_k, γ_k - finite-state Markov random coefficients: α_k - response efficiency coefficient, β_k - coefficient (probability) of successful attack mitigation, γ_k - fault tolerance coefficient.

Step 2. Let's construct the dynamics of the performance state (a system of nonlinear difference equations). The system dynamics are represented by a nonlinear stochastic difference equation:

$$E_{k+1} = E_k + \alpha_k \frac{U_k \beta_k}{R_k(1+\gamma_k)} - \delta_k(E_k, U_k, R_k) + \eta_k \quad (2)$$

where: δ_k (.) - a deterministic or stochastic decay/saturation term (e.g., δ_k (E_k) or a saturation function S_k (E_k).

η_k, - a process noise term (e.g., $\eta_k \sim N(0, \sigma_\eta^2)$).

In vector form (if E_k is multidimensional):

$$E_{k+1} = f(E_k, U_k, \theta_k) + \eta_k, \quad (3)$$

with θ_k (α_k, β_k, γ_k).

Step 3. Introducing random coefficients. Since the functioning of the cyber range depends on random factors (human factor, unpredictable cyber threats), they can be modeled as random variables.

Markov Modeling of the Coefficients. Each coefficient evolves as a finite-state Markov chain. For instance, suppose α_k has n_α states $\{a_1, \ldots, a_{n\alpha}\}$, β_k has n_β states $\{b_1, \ldots, b_n\}$, and γ_k has n_γ states $\{g_1, \ldots, g_{n\gamma}\}$.

The corresponding transition matrices are defined as:

$$P_\alpha = \begin{pmatrix} p_{11}^{(\alpha)} & \cdots & p_{1n_\alpha}^{(\alpha)} \\ \vdots & \ddots & \vdots \\ p_{n_\alpha 1}^{(\alpha)} & \cdots & p_{n_\alpha n_\alpha}^{(\alpha)} \end{pmatrix}, \quad P_\beta = \begin{pmatrix} p_{11}^{(\beta)} & \cdots & p_{1n_\beta}^{(\beta)} \\ \vdots & \ddots & \vdots \\ p_{n_\beta 1}^{(\beta)} & \cdots & p_{n_\beta n_\beta}^{(\beta)} \end{pmatrix},$$

$$P_\gamma = \begin{pmatrix} p_{11}^{(\gamma)} & \cdots & p_{1n_\gamma}^{(\gamma)} \\ \vdots & \ddots & \vdots \\ p_{n_\gamma 1}^{(\gamma)} & \cdots & p_{n_\gamma n_\gamma}^{(\gamma)} \end{pmatrix}, \quad (4)$$

where in each row $\sum_j p_{i,j}^{(.)}$.

The model structure is independent of specific cyber range architectures and toolsets, as its state variables and stochastic coefficients can be adapted to different operational contexts. By appropriate parameterization, the model supports evaluation of diverse scenarios, ranging from small-scale educational cyber ranges to large distributed training infrastructures, thereby enabling comparative analysis and benchmarking across platforms.

Based on the proposed model, optimization problems for cyber range management can be formulated. Similar integrated decision-support approaches for managing information protection systems are widely used, where analytical models support decision-making under uncertainty. For example, the allocation of limited resources R_k may be optimized to maximize the expected effectiveness $E[E_k]$ under budget constraints, or to minimize the probability of exceeding predefined risk thresholds. Potential approaches include stochastic programming, dynamic programming methods, and policies based on partially observable Markov decision processes, when system states are partially hidden. Such approaches are consistent with modern decision-support methodologies for information protection management and support the applicability of the proposed model. Thus, the proposed mathematical model makes it possible to evaluate the effectiveness of the cyber range, where α, β, γ are random coefficients that account for efficiency, success, and fault tolerance.

Here is a brief step-by-step modeling algorithm (practical implementation of the given model).

1) Initialization. Set the initial value E_0 and select initial states for α_0, β_0, γ_0.
2) Iteration (for $k = 0, \ldots, K-1$):
   a) Generate new states α_{k+1}, β_{k+1}, γ_{k+1} according to their respective transition matrices P_α, P_β, P_γ.
   b) Specify or update U_k, R_k (deterministically or as stochastic processes).
   c) Compute E_{k+1} using the nonlinear difference equation.
   d) Optionally, generate the observation y_{k+1} using the measurement model.
3) Repetition. Repeat steps 1-2 for a large number of realizations and compute ensemble statistics (mean $E[E_k]$, variance $Var(E_k)$ quantiles, and the probability of risk threshold violation $P(E_k < E_{crit})$.

2.5 Model Implementation in a Virtualized Cyber Range Environment

To demonstrate the practical applicability of the proposed stochastic model, a pilot implementation was carried out within a virtualized cyber range environment deployed on a hybrid infrastructure based on Proxmox VE and VMware. The experimental setup simulated a university-level cybersecurity training scenario involving 48 students (32 bachelor's and 16 master's level participants) over a 6-week training period.

The cyber range environment consisted of three main segments: a Red Team environment with penetration testing tools (Kali Linux, Metasploit), a Blue Team environment equipped with monitoring and defense systems (SIEM, IDS/IPS), and a virtual enterprise network containing vulnerable services and simulated business processes. The infrastructure included 36 virtual machines distributed across 3 physical servers, with dynamic resource allocation based on workload intensity.

For model parameterization, the following key indicators were collected: task completion rate, average response time to incidents, number of successful attack mitigations, system resource utilization (CPU, RAM), and user activity logs. The aggregated effectiveness index was normalized in the range [0,1], where higher values correspond to improved training performance.

The stochastic coefficients of the model were calibrated using observed data. This calibration ensures consistency between the theoretical model and real-world system behavior. Specifically, the response efficiency coefficient (α) varied within the interval [0.6; 0.85], the attack mitigation probability (β) within [0.5; 0.8], and the fault tolerance coefficient (γ) within [0.7; 0.9], depending on system load and user behavior. The transition of these coefficients was modeled as a three-state Markov chain (low, medium, high performance states), with empirically estimated transition probabilities.

Simulation experiments were conducted for 1000 realizations over 50 discrete time steps. The results showed that the expected effectiveness index increased from 0.58 at the initial stage to 0.81 at the final stage of training, confirming a positive learning dynamic. This indicates that the model adequately reflects the process of competency development in a dynamic learning environment. The variance decreased over time, indicating stabilization of student performance and system behavior. The probability of critical performance degradation (effectiveness < 0.5) was reduced from 0.22 to 0.07 after training adaptation.

A comparative analysis of infrastructure configurations demonstrated that environments with higher resource elasticity (Proxmox-based dynamic allocation) exhibited up to 12% higher effectiveness growth compared to static configurations. This confirms the sensitivity of the model to virtualization parameters and supports its use for evaluating infrastructure impact on learning outcomes.

The obtained results validate the applicability of the proposed model for analyzing cyber range performance under uncertainty and demonstrate its potential for optimizing both educational processes and technical infrastructure configurations.

3 CONCLUSIONS

This study demonstrates that the integration of a virtual cyber range into bachelor's and master's cybersecurity programs significantly enhances practice-oriented learning and professional readiness. The proposed multi-layer cyber range architecture supports diverse educational formats, including guided training, autonomous exercises, Red/Blue team scenarios, CTF competitions, and system testing, providing a realistic and controllable environment for skill development.

The applied research methodology-combining curriculum analysis, competency-service mapping, empirical training data, and statistical evaluation - proved effective for assessing educational outcomes. Pre-/post-test analysis and performance indicators confirmed substantial learning gains, particularly in incident response, vulnerability assessment, security monitoring, and risk analysis. Team-based and gamified scenarios showed the highest educational impact, contributing to both technical competencies and collaboration skills essential for SOC and incident response roles.

The competency-cyber range service matrix validated that the platform directly supports most learning outcomes defined in cybersecurity curricula, while also enabling interdisciplinary integration across system administration, programming, cryptography, and digital forensics. The proposed approach is consistent with international cyber defense training practices adopted by NATO CCDCOE, SANS, and IBM X-Force Command, confirming its relevance and scalability [17], [18].

A key scientific contribution is the proposed stochastic discrete-time dynamic model with Markov-modulated coefficients, which provides a

generic and extensible framework for evaluating the effectiveness of cyber ranges and related cybersecurity training platforms under uncertainty. The model supports long-term performance assessment, risk estimation, and resource optimization, bridging educational experimentation with formal analytical frameworks.

Overall, the results confirm that cyber ranges represent an effective, scalable, and analytically grounded solution for modern cybersecurity education and applied research. Thus, the proposed model is not only theoretically grounded but also empirically validated based on real-world educational data, confirming its applicability for evaluating and optimizing cybersecurity training environments.

REFERENCES

[1] "Cyber training center," State Center for Cyber Protection, [Online]. Available: https://scpc.gov.ua/uk/cyber-trainer/.

[2] M. Gering, Y. Medianyk, A. Sapeha, S. Trendov, K. Karpov, H. Skaskiv, D. Kachan and E. Siemens, "Botnet Simulation and Observation Framework for AI-Driven Virtual Personas," Proceedings of International Conference on Applied Innovation in IT, vol. 13, issue 5, pp. 75–82, 2025, [Online]. Available: https://doi.org/10.25673/122810.

[3] A. J. Ajeel and J. Kh-Madhloom, "AI-Based Intrusion Detection for Smart Grid Security," Proceedings of International Conference on Applied Innovation in IT, vol. 13, issue 5, pp. 41–47, 2025, [Online]. Available: https://doi.org/10.25673/122806.

[4] V. Kampourakis, V. Gkioulos, and S. Katsikas, "A step-by-step definition of a reference architecture for cyber ranges," J. Inf. Secur. Appl., vol. 88, art. no. 103917, 2025, [Online]. Available: https://doi.org/10.1016/j.jisa.2024.103917.

[5] D. Arnold, J. Ford, and J. Saniie, "Architecture of an efficient environment management platform for experiential cybersecurity education," Information, vol. 16, no. 7, art. no. 604, 2025, [Online]. Available: https://doi.org/10.3390/info16070604.

[6] J. V. Bistene, A. F. P. dos Santos, C. E. das Chagas, and R. M. Salles, "Modeling network traffic generators for cyber ranges: A systematic literature review," J. Netw. Syst. Manage., vol. 33, no. 2, 2025, [Online]. Available: https://doi.org/10.1007/s10922-025-09901-8.

[7] L. Arsenovych, O. Nikolaievsky, O. Skliarenko, L. Lytvynenko, and I. Kydriavskyi, "Organization of training with the use of digital technologies for ensuring cybersecurity in the educational space," WSEAS Trans. Comput. Res., vol. 12, pp. 524-536, 2024, [Online]. Available: https://doi.org/10.37394/232018.2024.12.51.

[8] J. Christopher, "The 2024 state of ICS/OT cybersecurity: Our past and our future," SANS Institute, Oct. 16, 2024, [Online]. Available: https://www.sans.org/blog/the-2024-state-of-ics-ot-cybersecurity-our-past-and-our-future/.

[9] V. L. Buriachok, V. B. Tolubko, V. O. Khoroshko, and S. V. Toliupa, Information and Cybersecurity: The Socio-Technical Aspect, Kyiv: DUT, 2015, 288 p.

[10] J. M. Castillo, M. Parenthoen, and N. Louveton, "A theoretical model for enhancing cyber crisis training in cyber ranges: Bridging cognitive load, situational awareness, and immersion," Cogn. Technol. Work, 2025, [Online]. Available: https://doi.org/10.1007/s10111-025-00844-3.

[11] I. Lateş, C. Boja, and A. Zamfiroiu, "Multi-technology infrastructure for advanced training and testing in cyber range systems," Stud. Inform. Control, vol. 34, no. 3, pp. 17-28, 2025, [Online]. Available: https://doi.org/10.24846/v34i3y202502.

[12] E. S. Alomari, M. B. M. Alkorani and K. Alieyan, "Securing the Post-Quantum Internet: A Comparative Study of Quantum-Resistant Protocols and Migration Strategies," Proceedings of International Conference on Applied Innovation in IT, vol. 13, issue 5, pp. 29–40, 2025, [Online]. Available: https://doi.org/10.25673/122804.

[13] M. Albaladejo-González, P. Nespoli, F. Gómez Mármol, and J. A. Ruipérez-Valiente, "A multimodal and adaptive gamified system to improve cybersecurity competence training," Cluster Computing, vol. 28, no. 9, 2025, [Online]. Available: https://doi.org/10.1007/s10586-025-05264-6.

[14] W. Lazarov, T. Schafeitel-Tähtinen, J. Squillace, Z. Martinasek, A. Coufalikova, M. Helenius, et al., "Lessons learned from using cyber range to teach cybersecurity at different levels of education," Technol. Knowl. Learn., 2025, [Online]. Available: https://doi.org/10.1007/s10758-025-09840-y.

[15] V. Lakhno, H. Mohylnyi, V. Donchenko, O. Smahina, and M. Pyroh, "A model developed for teaching an adaptive system of recognising cyberattacks among non-uniform queries in information systems," Eastern-European J. Enterp. Technol., vol. 4, no. 9(82), p. 27, 2016, [Online]. Available: https://doi.org/10.15587/1729-4061.2016.73315.

[16] V. A. Lakhno, D. Y. Kasatkin, O. V. Skliarenko, and Y. O. Kolodinska, "Modeling and optimization of discrete evolutionary systems of information security management in a random environment," in Machine Learning and Autonomous Systems, Singapore: Springer, 2022, pp. 9-22, [Online]. Available: https://doi.org/10.1007/978-981-16-7996-4_2.

[17] J. Diakoumakos, E. Chaskos, N. Kolokotronis, and G. Lepouras, "Cyber-security gamification in federation of cyber ranges: Design, implementation, and evaluation," Int. J. Inf. Secur., vol. 24, no. 1, 2025, [Online]. Available: https://doi.org/10.1007/s10207-024-00974-1.

[18] L. O. Nweke, U. F. Okebanama, and G. U. Mba, "Enhancing entrepreneurial skills through experiential learning in IoT, AI, and cybersecurity," Discov. Educ., vol. 4, no. 1, 2025, [Online]. Available: https://doi.org/10.1007/s44217-025-00573-9.

[19] T. Schafeitel-Tähtinen and W. Lazarov, "Teaching and learning cybersecurity using capture the flag: Effectiveness comparison between university students in Finland and Czechia," Comput. Appl. Eng. Educ., vol. 33, no. 5, 2025, [Online]. Available: https://doi.org/10.1002/cae.70082.