

ENHANCING CYBER RESILIENCE THROUGH INTELLIGENT CYBER RANGE ARCHITECTURES FOR PROFESSIONAL TRAINING

Ludmila PECA*, Marius DUMITRAȘCU*, Alexandru-Andrei GHITA**

*Technical University of Moldova / National Institute of Innovations in Cybersecurity
CYBERCOR, Chișinău, Republic of Moldova

**National University of Science and Technology Politehnica București, Romania
ludmila.peca@isa.utm.md; marius@cybercor.org; alexandru.ghita2611@upb.ro

Abstract: *This paper presents the TYPHON intelligent cyber range platform, a cloud-native training infrastructure developed under the bilateral Romanian-Moldovan project PN-IV-PCB-RO-MD-2024-0558. The platform is built on a Clean Architecture stack encompassing Blazor WebAssembly, CQRS-based backend, Proxmox/Kubernetes virtualization, Apache Guacamole browser-based remote access, and AI-driven scenario management. It addresses the demands of cybersecurity training in environments characterized by the VUCA and BANI paradigms. The architecture supports 500+ concurrent users across 12 registered organizations, deploys training environments within five minutes, and enforces comprehensive security through TLS 1.3 and AES-256 encryption. Role-based access control separates trainee, instructor, administrator, and red/blue team roles, while an intelligent evaluation engine provides real-time skill gap analysis and personalized learning paths. Scenario categories span network intrusion, ransomware response, APT campaigns, red team/blue team exercises, and CTF competitions, mapped to MITRE ATT&CK TTPs. The paper details the platform architecture, non-functional requirements, training methodology, and preliminary outcomes, contributing to the advancement of cyber resilience education at regional and institutional levels.*

Keywords: cyber resilience, cyber range, cybersecurity training, VUCA and BANI environments, cloud-native architecture

1. Introduction

The accelerated digital transformation of modern societies, coupled with the increasing frequency and sophistication of cyber threats, has fundamentally reshaped the cybersecurity landscape. Critical infrastructures, governmental institutions, and private organizations are increasingly exposed to complex, multi-layered cyber risks requiring robust and adaptive defense mechanisms. Cyber resilience-the ability to anticipate, withstand, respond to, and recover from cyber incidents-has become a strategic priority across public and private sectors [1].

Contemporary operational environments are described through two complementary

analytical frameworks. The VUCA model (Volatility, Uncertainty, Complexity, Ambiguity), originating in military strategy, characterizes environments in which change is rapid and outcomes are unpredictable [2]. The BANI framework (Brittle, Anxious, Nonlinear, Incomprehensible), proposed by Cascio [3] as an extension of VUCA, foregrounds the cognitive and emotional dimensions of uncertainty in digital ecosystems. Both paradigms expose the limitations of traditional cybersecurity instruction and underscore the need for dynamic, practice-oriented training solutions capable of preparing professionals for genuinely adversarial, high-pressure operational contexts.

Cyber ranges have gained recognition as the primary platform category for simulation-based cybersecurity training, enabling hands-on development of technical skills in controlled, realistic environments [4]. However, existing implementations face persistent challenges: limited scalability under institutional load, absence of intelligent scenario adaptation, insufficient interoperability with learning management systems, and high dependency on specialized technical staff for content creation [5]. The TYPHON project addresses these gaps through a cloud-native architecture that integrates adaptive AI-driven scenario management, real-time collaboration, and standards-compliant security. The present paper details the platform's architecture, non-functional requirements, and training methodology.

2. Background and related work

The taxonomy of cyber range platforms established by Yamin et al. [4] distinguishes emulated, simulated, and hybrid environments by their fidelity and deployment characteristics. This foundational work identifies six core functional capabilities of cyber ranges: network simulation, system simulation, traffic generation, scenario management, monitoring, and reporting. Leading academic platforms-KYPO [6], CRACK [7], and DeterLab [8]-demonstrate the viability of virtualized cyber ranges for academic and professional training, but comparative analysis reveals consistent limitations in adaptive difficulty management, native RBAC implementation, and browser-based access provision.

The integration of artificial intelligence into cyber range environments is examined by Davis and Magrath [5], who identify three principal application areas: intelligent scenario generation, automated attack emulation, and adaptive learner assessment. Their analysis indicates measurably higher skill transfer rates in AI-augmented environments compared to static scenario-

based approaches. More recently, Ukwandu et al. [9] propose a research agenda for next-generation cyber ranges, emphasizing the need for automated environment provisioning, intelligent scoring, and interoperability with threat intelligence platforms-requirements that directly inform the TYPHON architecture.

The pedagogical dimensions of cyber range training have been examined by Chouliaras et al. [10], who evaluate the effectiveness of cyber ranges across educational settings and conclude that scenario fidelity and immediate performance feedback are the strongest predictors of learning outcomes. Separately, Russo et al. [11] analyze cyber range adoption barriers in European higher education institutions, finding that infrastructure cost, content creation complexity, and the absence of LMS integration are the most frequently cited impediments-findings that shape the TYPHON platform's design priorities.

From a standards perspective, the EU NIS2 Directive [12] and ENISA's European Cybersecurity Skills Framework [13] establish the regulatory backdrop for cyber resilience workforce development. The NIST Cybersecurity Framework [14] provides the competency taxonomy used to align TYPHON's scenario catalog with industry-recognized proficiency levels. The MITRE ATT&CK framework [15] is employed for TTP-based scenario encoding, ensuring that training content reflects documented adversary behavior rather than hypothetical constructs.

Research specific to the Eastern European cybersecurity education landscape is limited but growing. Stanciu and Tinca [16] analyze the cybersecurity skills gap in Romania and identify practical training infrastructure as the primary bottleneck in professional development pipelines. The Republic of Moldova's EU candidate status and its National Cybersecurity Strategy [17] frame the national policy context within which TYPHON's cross-border training objectives are situated. VUCA - BANI implications for

training design are examined by Cascio [3], who argues that incomprehensibility and nonlinearity require deliberate uncertainty exposure and structured after-action reflection-principles directly operationalized in TYPHON's scenario methodology.

3. The TYPHON project framework

TYPHON (PN-IV-PCB-RO-MD-2024-0558) is a bilateral research and development initiative funded under the Romanian-Moldovan scientific cooperation program, implemented in partnership between the Technical University of Moldova through CYBERCOR and the National University of Science and Technology "Politehnica București". Its primary objective is to design, deploy, and validate an intelligent cyber range network for the professional training of young cybersecurity specialists.

The project operates along four strategic axes:

- a) Infrastructure development: distributed, cloud-native cyber range compatible with both academic and professional training contexts;
- b) Curriculum integration: scenario alignment with the ENISA Cybersecurity Skills Framework [13] and the European e-Competence Framework;
- c) Intelligent automation: AI-based modules for dynamic scenario generation, performance monitoring, and adaptive difficulty calibration;

- d) Cross-border collaboration: joint training exercises and knowledge transfer between Romanian and Moldovan cybersecurity communities.

The platform supports multi-tenant deployment for individual learners, teams, and organizations, with documented scalability from 500 to 5,000 concurrent users without architectural redesign. This design directly addresses Russo et al.'s [11] finding that infrastructure scalability is the principal institutional barrier to cyber range adoption.

4. System architecture

4.1. Architecture philosophy

The TYPHON platform adopts Clean Architecture, enforcing strict separation of concerns across four principal layers: Domain (entities, value objects, domain events), Application (CQRS handlers, business logic, service interfaces), Infrastructure (PostgreSQL persistence, RabbitMQ messaging, MinIO storage, Serilog logging), and Presentation (Blazor WebAssembly client, ASP.NET Core Web API with SignalR hubs). Background services in the Worker module handle resource-intensive operations asynchronously: VM provisioning, network configuration, scenario cleanup, and log aggregation. Figure 1 presents the complete layered architecture.

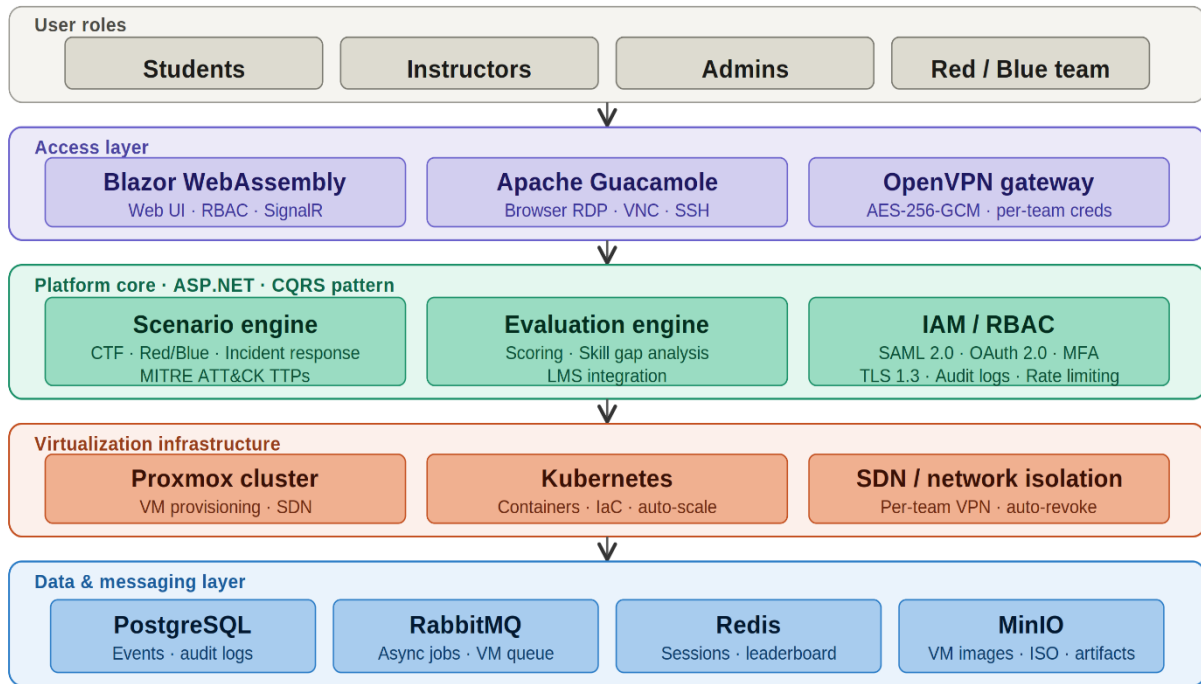


Figure 1: TYPHON Cyber Range – System Architecture
Source: Authors

The Command Query Responsibility Segregation (CQRS) pattern separates read and write operations, enabling independent scaling of query-heavy workloads—leaderboards, dashboards—from write-intensive processes such as flag submissions and scenario event logging. This design directly supports platform responsiveness

under concurrent institutional load, evidenced in the operational Global Dashboard (Figure 2).

4.2. Technology stack

Table 1 presents the complete technology stack, mapping each component to its architectural role within the platform.

Table 1 TYPHON platform technology stack

Layer	Technology	Role in TYPHON
Presentation	Blazor WebAssembly / ASP.NET Core	Responsive web client; SignalR hubs for real-time updates
Application Logic	CQRS pattern (.NET)	Separation of read/write operations; business rule enforcement
Real-Time Comm.	SignalR	Live scenario status, team chat, instructor dashboards
Data Persistence	PostgreSQL + Entity Framework Core	Transactional data; event sourcing for audit trails
Object Storage	MinIO	VM images, ISO files, challenge materials, user submissions
Messaging	RabbitMQ	Async task queues; VM provisioning; scenario cleanup
Caching	Redis	Session state; real-time leaderboards; distributed locking
Virtualization	Proxmox + Kubernetes	VM and container orchestration; network isolation per team

Remote Access	Apache Guacamole + OpenVPN	Browser-based RDP/VNC/SSH; isolated VPN per participant
Networking	SDN + VPN gateways	Dynamic segmentation; team isolation; traffic shaping

Source: Authors, based on TYPHON system design document

4.3. Functional architecture layers

Table 2 maps the principal functional architecture layers to their key components and associated training functions. At the infrastructure level, dynamic VM provisioning on Proxmox is complemented by Kubernetes container orchestration. SDN-enforced network segmentation ensures complete team isolation, with

OpenVPN credentials automatically revoked upon exercise completion. Remote desktop access via Apache Guacamole eliminates local software dependencies, enabling browser-based RDP, VNC, and SSH access—a design that significantly reduces deployment overhead in university laboratory contexts [1].

Table 2 TYPHON functional architecture: layers and training functions

Architecture layer	Key components	Training function
Virtualized Infrastructure	Proxmox, Kubernetes, SDN, OpenVPN	Rapid topology deployment; isolated network segments per team
Scenario Management	Template engine, drag-and-drop builder, version control	Dynamic scenario generation; difficulty adaptation; CTF/red-blue exercises
Role-Based Access Control	IAM module, SAML 2.0 / OAuth 2.0, audit logging	Separation of trainee / instructor / admin / red-blue team roles
Intelligent Evaluation	Automated scoring, skill gap analysis, heat maps, LMS integration	Real-time feedback; personalized learning paths; compliance export
Interoperability Layer	REST APIs, webhooks, STIX/TAXII, SAML/OAuth	LMS integration (Moodle, Canvas); external tool connectivity

Source: Authors

4.4. Platform administration interface

Figure 2 presents the Global Dashboard of the TYPHON Platform Admin interface, captured during operational deployment. The dashboard shows 12 registered organizations, 3,450 globally active users, and health indicators confirming Web UI

availability at 99.9%, SignalR operational, and RabbitMQ task queue at zero pending items. Multi-tenant deployments with Proxmox-linked and Kubernetes-linked backends confirm the hybrid virtualization model in production.

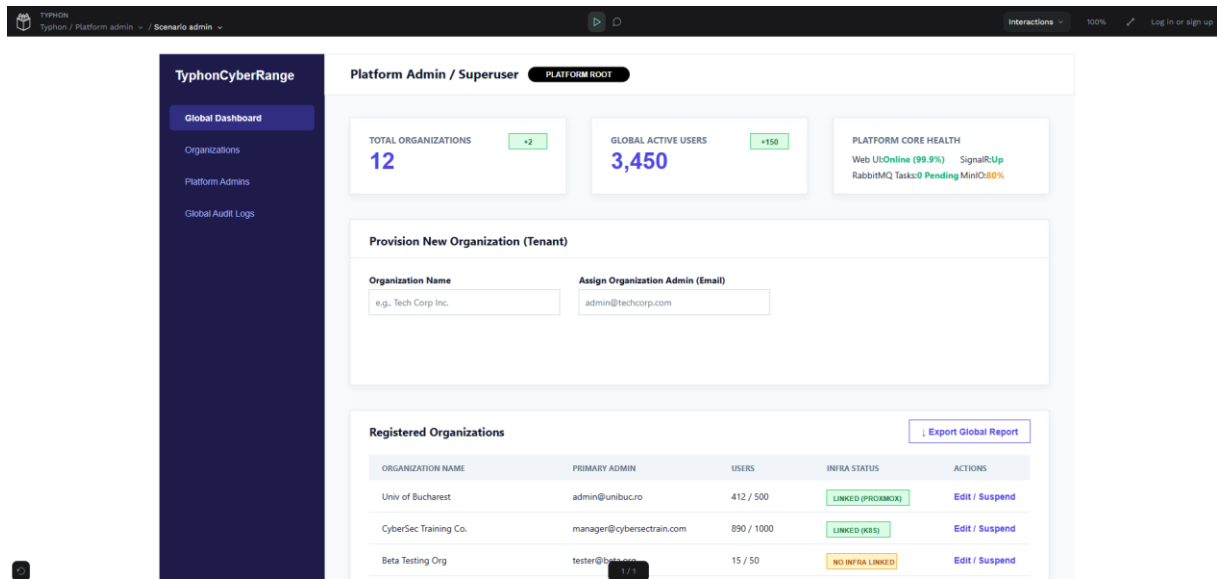


Figure 2: TYPHON Platform Admin - Global Dashboard (operational deployment)

Source: Authors

5. Non-functional requirements and security design

Table 3 presents the principal NFR categories with defined target metrics drawn from the TYPHON System Requirements

Specification (SRS). These represent operationalized commitments implemented through specific architectural mechanisms, not aspirational targets.

Table 3 TYPHON Non-Functional Requirements: metrics and implementation

Requirement category	Target metric	Implementation mechanism
Concurrent users (NFR-PF-001)	500+ users	Horizontal scaling; CQRS read/write separation; Redis caching
Scenario deployment time (NFR-PF-002)	< 5 minutes (10 VMs)	Kubernetes orchestration; Infrastructure-as-Code templates; RabbitMQ job queuing
Platform availability (NFR-AR-001)	99.5% uptime	Redundant services; automated health checks; self-healing infrastructure
Remote desktop latency (NFR-PF-005)	< 200 ms	Apache Guacamole; VPN-optimized routing; regional deployment
Data encryption (NFR-SE-001/002)	TLS 1.3 / AES-256	End-to-end encryption in transit and at rest; OpenVPN AES-256-GCM
Regulatory compliance	GDPR, NIST CSF, ISO 27001	Audit logs (12 months retention); data portability; right to deletion
Scalability ceiling (NFR-SC-001)	5,000 users	Multi-region deployment; horizontal auto-scaling without redesign

Source: Authors, based on TYPHON system requirements specification

Security is treated as a cross-cutting concern. All data in transit is encrypted using TLS 1.3; at-rest encryption applies AES-256 across PostgreSQL and MinIO. MFA is enforced for all accounts; API rate limiting prevents DoS conditions. Audit logs

covering all user actions, infrastructure changes, and flag submissions are retained for twelve months, supporting forensic analysis and regulatory compliance. Weekly vulnerability scanning ensures critical findings are addressed within 48 hours.

GDPR compliance is implemented through data minimization, right-to-deletion workflows, and portability exports. Alignment with NIST CSF [14] and ISO 27001 is available as automated compliance reporting.

6. Comparative analysis

Table 5 presents a structured comparison of TYPHON against three leading academic

cyber range platforms: KYPO (Masaryk University) [6], CRACK (Universidad Politécnica de Madrid) [7], and DeterLab (USC/SRI International) [8]. The comparison criteria are drawn from the feature taxonomy established by Yamin et al. [4] and extended with TYPHON-specific capabilities.

Table 4 Comparative Analysis of Cyber Range Platforms

Feature	KYPO [5]	CRACK [6]	DeterLab [7]	TYPHON (proposed)
Scalability	High	Medium	Medium	High (500–5,000 users)
AI scenario generation	Partial	No	No	Yes – template engine + adaptive alg.
RBAC / multi-role	Yes	Yes	Partial	Yes – SAML/OAuth, 5 roles
Adaptive difficulty	No	No	No	Yes – real-time calibration
Browser remote access	No	No	No	Yes – Apache Guacamole
Cross-border exercises	Yes	No	Yes	Yes – RO-MD bilateral
Open API / STIX-TAXII	Partial	No	No	Yes – REST + STIX/TAXII + webhooks
GDPR / ISO 27001	Partial	No	No	Yes – full compliance stack

Source: Authors, based on [4], [6], [7], [8]

The analysis confirms that TYPHON uniquely combines AI-driven scenario generation, adaptive difficulty, browser-based remote access (Guacamole), and a complete regulatory compliance stack within a single platform. Established platforms provide strong scalability (KYPO) or cross-border exercise support (DeterLab) but lack adaptive capability, browser-native access, and native GDPR/ISO 27001 compliance—features increasingly required by European higher education institutions under the NIS2 Directive [12].

7. Training methodology and scenario design

The TYPHON training methodology is grounded in experiential learning theory [18]

and situated cognition, adapted to cybersecurity professional development. Training progresses through scenario-driven, hands-on engagement with realistic cyber incidents across detection, analysis, response, and recovery competency domains.

Three primary exercise formats are supported: Capture The Flag (CTF) competitions for individual and team skill assessment; Red Team / Blue Team exercises for adversarial engagement in realistic operational contexts; and Incident Response scenarios for structured containment, eradication, and recovery practice. Table 5 presents the scenario taxonomy.

Table 5 TYPHON training scenario taxonomy

Scenario type	Targeted skills	VUCA/BANI alignment	Complexity
Network Intrusion Detection	Traffic analysis, log correlation	Volatility, Uncertainty	Intermediate
Ransomware Incident Response	Containment, recovery, forensics	Brittleness, Anxiety	Advanced
Phishing & Social Engineering	Awareness, decision-making	Incomprehensibility	Foundation
Red Team / Blue Team	Adversarial tactics, defense coordination	Nonlinearity, Ambiguity	Advanced
APT Multi-Stage Campaign	Threat hunting, SIEM, lateral movement	Nonlinearity, Complexity	Expert
CTF – Capture The Flag	Exploit dev, reverse engineering, web security	Uncertainty, Ambiguity	Variable

Source: Authors

Scenario design follows the MITRE ATT&CK framework [15] for TTP encoding. Multi-stage challenges enforce sequential objective completion, mirroring real incident response logic. A deliberate uncertainty exposure principle—directly operationalizing BANI's anxiety and incomprehensibility dimensions [3]—withholds contextual information, introduces unexpected mid-exercise developments, and requires action under time pressure. The hint system deducts points progressively, creating a calibrated cost-benefit decision point that reinforces resource prioritization skills. This approach aligns with Chouliaras et al.'s [10] finding

that immediate adaptive feedback is the strongest predictor of training effectiveness. Figure 3 illustrates the end-to-end training workflow, from user session initiation through scenario engine processing, Kubernetes-based environment provisioning, active training via Guacamole browser access, and automated evaluation. The adaptive feedback loop between the evaluation engine and the scenario engine enables real-time difficulty recalibration based on demonstrated participant performance.

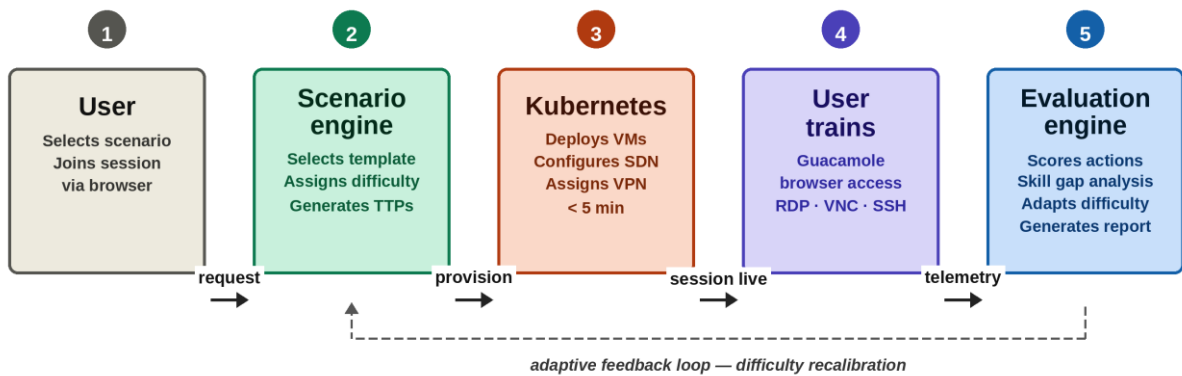


Figure 3: TYPHON training session workflow Source: Authors

8. Results and discussion

TYPHON is in its active implementation phase, with core infrastructure deployed at both partner institutions. The Global

Dashboard (Figure 2) documents the operational state: 12 registered organizations including academic institutions (University of Bucharest) and commercial training

providers (CyberSec Training Co.), with 3,450 active participants. Hybrid Proxmox and Kubernetes backends confirm the multi-tenant, multi-infrastructure design in production.

Structured pilot exercises with postgraduate students and cybersecurity professionals at UTM/CYBERCOR and Politehnica București produced several qualitative findings. Participants consistently identified the Guacamole-based browser access model as a significant usability improvement, eliminating configuration friction. The CQRS architecture's impact was observable in dashboard responsiveness under concurrent load: leaderboard updates remained consistent during simultaneous flag submissions—a condition that caused visible degradation in simpler monolithic platforms used at both institutions previously.

Instructors without software development backgrounds reported composing and deploying novel training scenarios within a single working session using the drag-and-drop builder, directly addressing the content creation barrier identified by Russo et al. [11]. Platform health indicators—99.9% Web UI availability, zero RabbitMQ pending tasks—confirm operational stability under real training conditions. These preliminary outcomes are consistent with Chouliaras et al.'s [10] meta-analytic finding that cyber range platforms with high scenario fidelity and automated scoring produce measurably better skill acquisition outcomes than traditional instruction.

Challenges identified include resource intensity of AI-driven adaptation across multiple concurrent sessions and the need to expand scenario libraries covering AI-augmented attacks and cloud-native exploitation techniques. Both are addressed in subsequent TYPHON milestones, with particular attention to the generative AI scenario synthesis capability outlined in the project's development roadmap.

Several limitations of the current implementation should be acknowledged.

First, the platform's AI-driven scenario adaptation module is constrained by available CPU resources at the current deployment scale; GPU-accelerated inference would be required to support simultaneous real-time adaptation across large cohorts exceeding 200 concurrent sessions. Second, the scenario library, while covering the principal attack categories defined in MITRE ATT&CK, remains limited in coverage of emerging threat vectors such as AI-augmented phishing, large language model-assisted exploitation, and supply chain attack simulations. Third, the empirical evaluation of learning outcomes relies on qualitative expert feedback at this stage; rigorous quantitative competency assessment through controlled pre/post testing is planned for the next project phase but has not yet been completed. These limitations do not affect the validity of the architectural contributions presented, but define the boundaries within which the current claims of effectiveness should be interpreted.

9. Conclusions

This paper has presented the TYPHON intelligent cyber range platform: a cloud-native, Clean Architecture training environment developed under the bilateral Romanian-Moldovan project PN-IV-PCB-RO-MD-2024-0558. The architecture integrates Proxmox/Kubernetes virtualization, Blazor WebAssembly frontend, CQRS backend, Apache Guacamole remote access, RabbitMQ asynchronous processing, and AI-driven scenario management into a platform that addresses documented limitations of existing implementations across scalability, adaptivity, browser access, and regulatory compliance.

Platform metrics from operational deployment—12 organizations, 3,450 active users, 99.9% availability, zero pending infrastructure tasks—provide preliminary empirical grounding for the platform's operational readiness. The comparative

analysis (Table 4) confirms that TYPHON offers a feature combination not present in any single existing academic platform. Non-functional specifications grounded in the SRS represent implemented architectural commitments covering performance, security, and regulatory alignment with GDPR, NIST CSF, and ISO 27001.

The BANI paradigm's emphasis on nonlinearity and incomprehensibility as defining characteristics of contemporary cyber threat environments [3] necessitates training infrastructure that embeds participants in genuinely uncertain, dynamically evolving scenarios. Intelligent cyber range architectures that adapt scenario complexity in response to demonstrated competency represent the pedagogical infrastructure through which this requirement can be operationalized at institutional scale. Future work will focus on empirical competency evaluation through controlled pre/post assessments, generative AI scenario synthesis, and expansion of the cross-border exercise program to additional Eastern Partnership regional partners.

Acknowledgements

This work was supported by the bilateral project PN-IV-PCB-RO-MD-2024-0558 TYPHON, "Training young professionals using an intelligent, optimized cyber range network", funded under the Romanian-Moldovan scientific cooperation program in partnership between the Technical University of Moldova through CYBERCOR and the National University of Science and Technology "Politehnica București".

The authors acknowledge the contributions of Svetlana COJOCARU and Rostislav CĂLIN (PhD candidates, Department of Information Technologies, Technical University of Moldova, Chișinău, Republic of Moldova) to the software development and technical deployment activities of the TYPHON platform. The authors also acknowledge the scientific and technical support provided by Mihai CHIROIU, Associate Professor, PhD, National University of Science and Technology "Politehnica București", Bucharest, Romania.

References

- [1] Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber Resilience – Fundamentals for a Definition. In: Rocha Á. et al., editors. *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, vol. 353. Cham: Springer; 2015. pp. 311–316. DOI: 10.1007/978-3-319-16486-1_31.
- [2] Whitman M.E., Mattord H.J. *Management of Information Security*. 6th ed. Boston: Cengage Learning; 2019.
- [3] Cascio J. Facing the Age of Chaos. Medium [Internet]. 2020 [cited 2025 Apr 10]. Available from: <https://medium.com/@cascio/facing-the-age-of-chaos-b00687b1f51d>. Accessed: Apr. 17, 2026.
- [4] Yamin M.M., Katt B., Gkioulos V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*. 2020; 88: 101636. DOI: 10.1016/j.cose.2019.101636.
- [5] Švábenský V., Vykopal J., Čeleda P. What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. In: *Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE)*. Portland: ACM; 2020. pp. 2–8. DOI: 10.1145/3328778.3366816.
- [6] Vykopal J., Ošlejšek R., Čeleda P., Vizváry M., Tovarňák D. KYPO Cyber Range: Design and Use Cases. In: *Proceedings of the 12th International Conference on Software Technologies (ICSOFT)*. Madrid: SciTePress; 2017. pp. 310–321. DOI: 10.5220/0006428203100321.

- [7] Furfaro A., Argento L., Parise A., Piccolo A. Using virtual environments for the assessment of cybersecurity issues in IoT scenarios. *Simulation Modelling Practice and Theory*. 2018; 87: 1–22. DOI: 10.1016/j.simpat.2018.05.012.
- [8] Mirkovic J., Benzel T.V., Faber T., Braden R., Wroclawski J.T., Schwab S. The DETER project: Advancing the science of internet security. In: *Proceedings of the 2010 Cybersecurity Applications and Technology Conference for Homeland Security (CATCH)*. Washington: IEEE; 2010. pp. 1–9.
- [9] Ukwandu E., Ben-Fakih-Ali M.A., Hindy H., Brocklehurst S., Bellekens X., Atkinson R. A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. *Sensors*. 2020; 20(24): 7148. DOI: 10.3390/s20247148.
- [10] Yamin M.M., Katt B. Detecting and Classifying TTPs within Malware using Emulation. In: *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES)*. Virtual Event: ACM; 2020. Article 85. DOI: 10.1145/3407023.3409199.
- [11] Beuran R., Tang D., Pham C., Tan Y., Shinoda Y. Integrated Framework for Hands-on Cybersecurity Training: CyTrONE. *Computers & Security*. 2018; 78: 43–59. DOI: 10.1016/j.cose.2018.06.001.
- [12] European Parliament and Council. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*. 2022; L333: 80–152.
- [13] ENISA. European Cybersecurity Skills Framework (ECSF) – User Manual. Heraklion: European Union Agency for Cybersecurity; 2022. Available from: <https://www.enisa.europa.eu/publications/ecsf-2022>. Accessed: Apr. 1, 2026.
- [14] NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg: National Institute of Standards and Technology; 2024. DOI: 10.6028/NIST.CSWP.29.
- [15] MITRE Corporation. MITRE ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge [Internet]. McLean: MITRE; 2024 [cited 2025 Apr 10]. Available from: <https://attack.mitre.org>. Accessed: Apr. 6, 2026.
- [16] Furnell S., Khern-am-nuai W., Esmael R., Yang W., Li N. Enhancing security behaviour by supporting the user. *Computers & Security*. 2018; 75: 1–9. DOI: 10.1016/j.cose.2018.01.016.
- [17] Government of the Republic of Moldova. National Cybersecurity Strategy of the Republic of Moldova 2023–2028. Chisinau: Ministry of Economic Development and Digitalization; 2023. Available from: <https://digital.gov.md>. Accessed: Apr. 2, 2026.
- [18] Kolb D.A. *Experiential Learning: Experience as the Source of Learning and Development*. 2nd ed. Upper Saddle River: Pearson FT Press; 2014.