DESIGN AND IMPLEMENTATION OF VIRTUAL LABORATORIES FOR CYBERSECURITY EDUCATION IN HIGHER EDUCATION INSTITUTIONS

Khusenov Murodjon Zokhirovich

Associate Professor, Department of Artificial Intelligence and Information Security, Bukhara State University, Bukhara, Uzbekistan

E-mail: m.z.xusenov@buxdu.uz ORCID: 0000-0002-1533-3102

Abstract. The persistent global shortage of cybersecurity professionals and the inherently practice-oriented nature of the discipline make hands-on laboratory training an indispensable component of cybersecurity education. Traditional physical laboratories, however, impose high capital and maintenance costs, limited accessibility and weak scalability, which is particularly restrictive for regional higher education institutions. This article substantiates an architectural and pedagogical framework for the design and institutional implementation of virtual laboratories for cybersecurity education. The study relies on a comparative analysis of deployment models reported in the international literature — on-premises virtualization, private and public cloud environments, and dedicated cyber range platforms — and on design-based research methodology. As a result, a five-layer reference architecture of a university virtual cybersecurity laboratory is proposed, comprising infrastructure, virtualization and orchestration, scenario, pedagogical integration, and governance layers, together with a three-phase implementation roadmap. The discussion addresses cost–realism trade-offs, scaffolding requirements for novice learners and instructor preparation. The framework is oriented towards the conditions of higher education institutions of Uzbekistan implementing the national digital transformation and cybersecurity agenda.

Keywords: *cybersecurity education; virtual laboratory; cyber range; virtualization; cloud computing; hands-on learning; higher education*

1. Introduction

The demand for qualified cybersecurity specialists continues to outpace supply: according to the ISC2 Cybersecurity Workforce Study, the global workforce gap was estimated at approximately 4.8 million specialists in 2024 [1]. At the same time, cybersecurity is a fundamentally applied discipline. The international curricular guidelines CSEC2017, developed by the Joint Task Force of ACM, IEEE-CS, AIS SIGSEC and IFIP WG 11.8, consistently emphasize that knowledge areas such as data, software, system and connection security must be mastered through application and practice rather than through lectures alone [2].

Conventional physical computer laboratories satisfy this requirement only partially. Recent comparative research notes that on-premises laboratory facilities frequently suffer from high maintenance costs, limited accessibility and hardware constraints that reduce scalability and efficacy, while legacy teaching methods are increasingly seen as insufficient for preparing students to face real-world cybersecurity threats [3]. An additional, security-specific constraint is that many core exercises — malware behaviour analysis, network attacks, privilege escalation, incident response drills — cannot be safely executed on production university networks and therefore require strictly isolated, easily resettable environments.

Virtual laboratories (VLabs) have emerged as a response to these constraints. A virtual cybersecurity laboratory is understood here as a software-defined environment of interconnected virtual machines, containers and emulated network devices in which learners perform offensive, defensive and forensic exercises under controlled isolation. Empirical evidence supports their pedagogical value: a survey conducted among learners and educators of cybersecurity distance courses found that both groups perceived virtual laboratories as engaging, interactive and effective in improving the understanding of cybersecurity concepts, with a positive impact on active learning and problem-solving [4]. A systematic literature review of online cybersecurity teaching in universities likewise identifies virtual laboratories, simulations and gamification

among the key instruments that provide hands-on experience, enhance motivation and facilitate active learning [5].

The literature further distinguishes between guided virtual laboratories, which lead the learner through predefined tasks, and cyber ranges, which reproduce larger, more realistic infrastructures for open-ended exercises and team-based attack–defence scenarios [6]. Experience reports indicate that cyber ranges can be productively used at different levels of education, from schoolchildren to university students and professionals, although technically demanding challenges may discourage participants without prior background [7]. Mature platforms supporting such training include the open-source KYPO Cyber Range Platform developed at Masaryk University [8], as well as integrated environments built on network emulators such as GNS3 and EVE-NG that improve the scalability of networking and cybersecurity laboratories [9].

For the Republic of Uzbekistan the problem is of particular relevance. The national strategy “Digital Uzbekistan — 2030” provides for the wide introduction of digital technologies in education and the development of digital skills [10], and the Law of the Republic of Uzbekistan “On Cybersecurity” (No. LRU-764, 2022) institutionalizes requirements for the protection of information systems and, implicitly, for the training of personnel capable of ensuring it [11]. Regional universities, including Bukhara State University, must therefore build practice-oriented cybersecurity training under significant resource constraints. The aim of this study is to substantiate the architecture and the implementation methodology of a virtual laboratory environment for cybersecurity education in a regional higher education institution. The objectives are: (i) to perform a comparative analysis of deployment models for virtual cybersecurity laboratories; (ii) to develop a layered reference architecture aligned with curricular requirements; (iii) to elaborate a phased implementation roadmap.

2. Materials and Methods

The source base of the study comprises peer-reviewed journal articles, conference papers, preprints and technical documentation published in 2017–2026 and indexed in IEEE Xplore, SpringerLink, MDPI, Frontiers and arXiv, supplemented by the documentation of established laboratory and cyber range platforms. Publications were selected if they (a) addressed virtual laboratories, cloud laboratories or cyber ranges in higher cybersecurity education and (b) contained either empirical evaluation data or substantiated architectural solutions.

Three complementary methods were applied. First, a comparative analysis of deployment models was carried out along six criteria: capital and operating cost; scalability; realism (fidelity) of scenarios; accessibility for learners; administrative overhead; and safety of isolation. Second, design-based research methodology was used to synthesize a layered reference architecture that generalizes solutions identified in the literature and adapts them to the constraints of a regional university. Third, the mapping method was used to align laboratory modules with the CSEC2017 knowledge areas [2] and with the work roles of the NICE Workforce Framework for Cybersecurity (NIST SP 800-181) [12], which ensures the curricular validity of the proposed environment.

The study is analytical and design-oriented in character: the effectiveness indicators referred to in Section 3 are drawn from the cited published studies rather than from the author's own field experiment. The experimental verification of the proposed architecture in the educational process of Bukhara State University constitutes a separate stage of the research and is discussed as a direction of further work.

3. Results

3.1. Comparative analysis of deployment models. The analysis of the literature allows four basic deployment models of virtual cybersecurity laboratories to be distinguished: on-premises desktop virtualization, private cloud (server) virtualization,

public cloud laboratories, and dedicated cyber range platforms. The comparative study of on-premises VirtualBox-based laboratories and cloud laboratories hosted on AWS EC2 demonstrates that cloud environments reduce infrastructure costs, provide near-ubiquitous remote access and scale elastically, at the price of recurring usage fees, dependence on connectivity and additional data governance obligations [3]. On-premises laboratories preserve full control and one-time investment but are limited by hardware capacity and administrative burden [3]. Cyber ranges occupy the upper end of the realism spectrum: unlike guided laboratories that train "on rails", they support open scenarios, red–blue team exercises and realistic infrastructures, which industry analyses consider increasingly necessary as guided laboratories show their limitations [6]; the corresponding price is the highest demand for resources and specialist staff [6, 7]. The results of the comparison are summarized in Table 1.

Table 1. Comparative characteristics of deployment models for virtual cybersecurity laboratories

Deployment model	Typical technologies	Strengths	Constraints
On-premises desktop virtualization	VirtualBox, VMware Workstation on laboratory PCs	Full control; no recurring fees; operation without external connectivity	Hardware limits; high maintenance; weak remote access [3]
Private cloud / server virtualization	Proxmox VE, VMware ESXi; GNS3, EVE-NG emulation	Centralized administration; snapshots and fast reset; campus-wide access	Up-front server investment; administrator expertise required [9]
Public cloud laboratory	AWS EC2, academic cloud programmes	Elastic scalability; pay-as-you-go; access from anywhere	Recurring cost; connectivity dependence; data governance [3]
Dedicated cyber range	KYPO CRP, U.S. Cyber Range and similar platforms	High-fidelity scenarios; attack–defence team exercises; built-in analytics	Highest cost and complexity; specialist staff [6–8]

3.2. Reference architecture of a university virtual cybersecurity laboratory. Generalizing the analysed solutions, a five-layer reference architecture is proposed. The infrastructure layer comprises the physical compute, storage and network resources, which may be located on campus, in a national or commercial cloud, or combined in a hybrid scheme depending on the institution's budget profile identified in subsection 3.1. The virtualization and orchestration layer provides hypervisor- and container-based provisioning of laboratory topologies, snapshot-based reset of exercises, template management and, critically, network isolation of laboratory segments from the production university network. The scenario layer contains the didactic content proper: libraries of intentionally vulnerable virtual machines, preconfigured attack–defence topologies, log and traffic datasets for forensic exercises, and machine-readable scenario descriptions that make exercises reproducible and shareable between institutions.

The pedagogical integration layer connects the technical environment with the educational process: integration with the learning management system, electronic laboratory manuals, automated verification of task completion (including flag-based checking), and learning analytics that expose progress and typical errors to the instructor. Finally, the governance layer defines role-based access control, acceptable use and ethics rules, legal compliance with national cybersecurity legislation [11], and procedures guaranteeing that offensive tooling remains confined to the isolated environment. Mapping the scenario layer onto CSEC2017 [2] and NICE work roles [12] yields a module structure covering network security, operating system security, web application security and penetration testing, digital forensics, and incident response, which together support the principal practice-oriented courses of a cybersecurity-related curriculum.

3.3. Implementation roadmap. For a regional university, a three-phase roadmap is substantiated. Phase 1 (pilot, one semester): deployment of an open-source private-cloud stack (e.g., Proxmox VE with GNS3/EVE-NG and a basic set of vulnerable machine templates) for a single course such as network security, with manual

assessment. Phase 2 (institutionalization, one to two academic years): extension to the cluster of security-related courses, integration with the LMS, introduction of automated flag-based assessment, allocation of a laboratory engineer and a methodologist, and approval of governance regulations. Phase 3 (federation): selective use of public cloud resources for peak loads and advanced scenarios, participation in inter-university exercises and national competitions, and sharing of scenario libraries with partner institutions, which distributes development costs across the academic community.

4. Discussion

The proposed framework is consistent with the empirical evidence accumulated in the literature. The expectation that the virtual laboratory will increase engagement and active learning is grounded in survey results showing positive perceptions of VLabs by both learners and educators in cybersecurity courses [4] and in the systematic review that places virtual laboratories among the central instruments of effective online cybersecurity education [5]. The layered separation of scenario content from infrastructure follows the logic of mature platforms such as KYPO [8] and addresses the scalability concerns documented for integrated emulation-based laboratories [9].

At the same time, the analysis warns against two simplifications. First, the choice between on-premises, cloud and range-based deployment is not binary: cost evidence [3] and the realism argument [6] jointly favour a hybrid model in which routine exercises run on institutional infrastructure, elastic cloud capacity is rented for advanced or peak-load scenarios, and full-scale range events are reserved for capstone activities. Second, realism without scaffolding can be counterproductive: experience with cyber ranges shows that overly technical challenges may reduce the intention of unprepared participants to continue studying cybersecurity [7]. The scenario layer must therefore implement graduated difficulty, hint systems and preparatory briefings, and instructors require targeted professional development before high-fidelity exercises are introduced.

The limitations of the study follow from its design: the framework is substantiated analytically, and its effectiveness claims are at present transferred from the cited external studies. The next stage of the research is a quasi-experimental verification in the educational process of Bukhara State University, with pre- and post-measurement of practical skill indicators in experimental and control groups. In the national context, the implementation of such laboratories operationalizes the objectives of the “Digital Uzbekistan — 2030” strategy [10] and creates the institutional capacity required by the cybersecurity legislation of the Republic of Uzbekistan [11].

5. Conclusion

Hands-on training is a constitutive element of cybersecurity education, and virtual laboratories are currently the most realistic way to provide it at scale under the resource constraints of regional universities. The comparative analysis performed in this study shows that deployment models differ systematically in cost, scalability, realism and administrative burden, and that a hybrid combination of institutional virtualization, cloud capacity and periodic cyber range events offers the most balanced profile. The proposed five-layer reference architecture — infrastructure, virtualization and orchestration, scenarios, pedagogical integration, and governance — links technical design directly to curricular requirements through CSEC2017 and the NICE Framework, while the three-phase roadmap makes implementation tractable for institutions starting from a low base. Further research will be devoted to the experimental evaluation of the framework in real courses and to the development of a shared national library of laboratory scenarios for the universities of Uzbekistan.

References

1. ISC2. Cybersecurity Workforce Study 2024. ISC2, 2024. [Online]. Available: https://www.isc2.org/research

2. Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. ACM / IEEE-CS / AIS SIGSEC / IFIP WG 11.8, 2017. DOI: 10.1145/3184594.
3. Optimizing Cybersecurity Education: A Comparative Study of On-Premises and Cloud-Based Lab Environments Using AWS EC2 // Computers (MDPI). 2025. Vol. 14, No. 8, Art. 297. [Online]. Available: https://www.mdpi.com/2073-431x/14/8/297
4. Kebande V. R. The Impact of Virtual Laboratories on Active Learning and Engagement in Cybersecurity Distance Education // arXiv preprint arXiv:2404.04952. 2024. [Online]. Available: https://arxiv.org/abs/2404.04952
5. How universities teach cybersecurity courses online: a systematic literature review // Frontiers in Computer Science. 2024. Vol. 6, Art. 1499490. DOI: 10.3389/fcomp.2024.1499490.
6. Infosec Institute. How are virtual labs and cyber range simulations different? 2020. [Online]. Available: https://www.infosecinstitute.com/resources/cyber-range/how-virtual-labs-and-cyber-range-simulations-are-different/
7. Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education // Technology, Knowledge and Learning. 2025. DOI: 10.1007/s10758-025-09840-y.
8. Vykopal J., Oslejsek R., Celeda P., Vizvary M., Tovarnak D. KYPO Cyber Range: Design and Use Cases // Proceedings of the 12th International Conference on Software Technologies (ICSOFT). 2017.
9. Integrated Virtual Laboratory for Networking, Cybersecurity, and Automation Education with Enhanced Scalability // Frontiers in Education. 2026. Art. 1708228. DOI: 10.3389/feduc.2026.1708228.
10. Decree of the President of the Republic of Uzbekistan No. UP-6079 “On Approval of the Strategy ‘Digital Uzbekistan — 2030’ and Measures for Its Effective Implementation”. October 5, 2020.

11. Law of the Republic of Uzbekistan No. LRU-764 “On Cybersecurity”. April 15, 2022.
12. Petersen R., Santos D., Smith M. C., Wetzel K. A., Witte G. Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181 Rev. 1. Gaithersburg: NIST, 2020.