MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică şi Microelectronică

Departamentul Ingineria Software şi Automatică

Şef departament:

FIODOROV Ion dr., conf.univ.

„___” _____ 2026

EFICIENȚA MEDIILOR CYBER RANGE ÎN FORMAREA COMPETENȚELOR DE SECURITATE CIBERNETICĂ

Student: **_____** **Ghijițchi Tatiana, TIA-241M**

Coordonator: **_____** **Peca Ludmila, dr., lect. univ.**

Consultant: **_____** **Cojocaru Svetlana, asist.univ.**

Chişinău, 2026

REZUMAT

În ultimii ani, extinderea rapidă a serviciilor digitale a transformat securitatea cibernetică într-un domeniu strategic, marcat de un deficit global de aproape 4,8 milioane de specialişti neocupaţi. Decalajul dintre pregătirea teoretică universitară şi competenţele practice solicitate de angajatori reprezintă una dintre cauzele principale ale acestui deficit, justificând necesitatea unor metode educaţionale inovatoare, bazate pe simulare şi practică aplicată.

Lucrarea de faţă analizează potenţialul mediilor de tip Cyber Range ca instrumente pentru dezvoltarea competenţelor practice în securitate cibernetică şi propune un model didactic aplicabil în context universitar, cu referire directă la Universitatea Tehnică a Moldovei. Metodologia îmbină analiza documentară şi comparativă cu cercetarea empirică prin chestionar aplicat studenţilor de la FCIM UTM.

Primul capitol fundamentează teoretic domeniul şi prezintă trei studii de caz internaţionale reprezentative. La Universitatea Masaryk din Cehia, platforma KYPO Cyber Range a demonstrat că feedbackul automatizat creşte rata de finalizare a sarcinilor cu 34%. Exerciţiile NATO CCDCOE din Tallinn - în special Locked Shields - au generat o rată de angajare de 78% pentru absolvenţii participanţi, faţă de 54% pentru cei fără experienţă similară. La Epitech Paris, integrarea TryHackMe pentru peste 2.500 de studenţi a produs o rată de finalizare a laboratoarelor de peste 80%, faţă de 60% în modelul tradiţional. Concluzia comună a acestor cazuri este că valoarea educaţională a mediilor Cyber Range derivă din coerenţa integrării lor într-un sistem didactic orientat spre competenţe autentice.

Al doilea capitol realizează o analiză comparativă a platformelor TryHackMe şi Hack The Box în context educaţional. TryHackMe este optimă pentru nivelul introductiv şi intermediar, prin structura ghidată şi accesibilitatea ridicată, în timp ce Hack The Box este adecvată pentru nivelul avansat, prin scenariile de tip open-ended hacking care reproduc condiţiile reale din industrie. Utilizate secvenţial, cele două platforme configurează un continuum pedagogic complementar.

Al treilea capitol analizează contextul educaţional la FCIM UTM prin două metode complementare: analiza curriculumului existent şi un chestionar aplicat unui eşantion de 91-92 de studenţi. Rezultatele indică faptul că 58,2% dintre studenţi percep formarea actuală ca dominată de teorie, iar 82,6% identifică scenariile realiste de atac-apărare ca cele mai utile activităţi practice. Niciuna dintre fişele disciplinelor analizate nu menţionează explicit platforme Cyber Range ca instrument formal de laborator.

Al patrulea capitol propune un model didactic structurat în patru etape progresive: explorare practică, conceptualizare, aplicare practică şi evaluare a competenţelor. Modelul este inspirat din principiile sistemului educaţional finlandez şi aliniat la profilurile European Cybersecurity Skills Framework definite de ENISA. Integrarea propusă presupune alocarea a 30-40% din orele de laborator pentru activităţi pe platforme Cyber Range, fără modificări structurale majore ale curriculumului existent.

ABSTRACT

In recent years, the rapid expansion of digital services has transformed cybersecurity into a strategic field, marked by a global shortage of nearly 4.8 million unfilled specialist positions. The gap between theoretical university preparation and the practical competencies demanded by employers represents one of the main causes of this shortage, justifying the need for innovative educational methods based on simulation and applied practice.

This thesis analyses the potential of Cyber Range environments as tools for developing practical cybersecurity competencies and proposes a teaching model applicable in a university context, with direct reference to the Technical University of Moldova. The methodology combines documentary and comparative analysis with empirical research through a questionnaire administered to students at FCIM UTM.

The first chapter provides the theoretical foundation of the field and presents three representative international case studies. At Masaryk University in the Czech Republic, the KYPO Cyber Range platform demonstrated that automated feedback increases task completion rates by 34%. The NATO CCDCOE exercises in Tallinn - particularly Locked Shields - generated an employment rate of 78% for participating graduates, compared to 54% for those without similar experience. At Epitech Paris, the integration of TryHackMe for over 2,500 students produced a laboratory completion rate exceeding 80%, compared to 60% in the traditional model. The common conclusion across these cases is that the educational value of Cyber Range environments derives from the coherence of their integration into a teaching system oriented toward authentic competencies.

The second chapter presents a comparative analysis of the TryHackMe and Hack The Box platforms in an educational context. TryHackMe is optimal for introductory and intermediate levels through its guided structure and high accessibility, while Hack The Box is suited for advanced levels through its open-ended hacking scenarios that replicate real-world industry conditions. Used sequentially, the two platforms form a complementary pedagogical continuum.

The third chapter analyses the educational context at FCIM UTM through two complementary methods: analysis of the existing curriculum and a questionnaire administered to a sample of 91–92 students. Results indicate that 58.2% of students perceive current training as theory-dominated, while 82.6% identify realistic attack-defence scenarios as the most useful practical activities. None of the discipline syllabi analysed explicitly mention Cyber Range platforms as a formal laboratory tool.

The fourth chapter proposes a teaching model structured in four progressive stages: practical exploration, conceptualisation, practical application, and competency assessment. The model is inspired by the principles of the Finnish educational system and aligned with the European Cybersecurity Skills Framework profiles defined by ENISA. The proposed integration involves allocating 30–40% of laboratory hours to Cyber Range platform activities, without major structural changes to the existing curriculum.

CUPRINS

ABREVIERI ȘI DEFINIȚII

ISC2 - International Information System Security Certification Consortium

ENISA - European Union Agency for Cybersecurity

ECSF - European Cybersecurity Skills Framework

CyBOK - Cyber Security Body of Knowledge

CSIS - Center for Strategic and International Studies

ITU - International Telecommunication Union

DNSC - Directoratul Național de Securitate Cibernetică

NIST - National Institute of Standards and Technology

NICE - National Initiative for Cybersecurity Education

EFTA - European Free Trade Association

USAID - United States Agency for International Development

GCI - Global Cybersecurity Index

DESI - Digital Economy and Society Index

NIS2 - Network and Information Security Directive

PNRR – Planul Național de Redresare și Reziliență

SOC - Security Operations Center

CTF - Capture The Flag

HTB - Hack The Box

LMS - Learning Management System

CISO - Chief Information Security Officer

FCIM - Facultatea Calculatoare, Informatică și Microelectronică

FET - Facultatea Electronică și Telecomunicații

Cyber Range - Mediu virtual complex care simulează infrastructuri informatice reale (rețele, servere, aplicații și servicii), utilizat pentru instruire practică, exerciții de atac–apărare și evaluarea competențelor în securitate cibernetică într-un cadru controlat.

Cybersecurity - Domeniu interdisciplinar care vizează protejarea sistemelor informatice, rețelelor, aplicațiilor și datelor împotriva atacurilor, accesului neautorizat, perturbărilor sau distrugerii, prin utilizarea de tehnologii, procese și practici de securitate.

Penetration testing / penetration tester - Proces de evaluare a securității unui sistem informatic prin simularea unor atacuri controlate, realizate de specialişti (penetration testers), cu scopul identificării vulnerabilităților exploatabile și formulării recomandărilor de remediere.

Red teaming - Metodă avansată de testare a securității care presupune simularea unor atacuri complexe, coordonate și realiste asupra unei organizații, pentru a evalua capacitatea de detectare și răspuns a echipelor defensive și a mecanismelor de securitate.

Capture the Flag (CTF) - Tip de exercițiu sau competiție practică în securitate cibernetică în care participanții rezolvă provocări tehnice pentru a identifica vulnerabilități, a extrage date sau a obține „flag-uri”, demonstrând competențe tehnice specifice.

Scaffolding (pedagogic) - Concept educațional care desemnează oferirea de suport gradual cursanților în procesul de învățare, prin ghidare, explicații și structuri intermediare, până la dobândirea autonomiei în rezolvarea sarcinilor.

Open-ended hacking - Abordare de învățare practică bazată pe explorare liberă și rezolvarea de probleme fără instrucțiuni pas cu pas, în care cursantul își dezvoltă strategiile proprii de analiză și exploatare a vulnerabilităților.

Room / rooms - Unități de învățare structurate din cadrul platformei TryHackMe, care conțin materiale teoretice, sarcini practice și exerciții interactive, organizate tematic pentru dezvoltarea progresivă a competențelor.

Dragonfly - Scenariu sau exercițiu de simulare cibernetică utilizat în instruire, conceput pentru a reproduce atacuri asupra infrastructurilor informatice și pentru a evalua reacția și competențele participanților în contexte realiste.

INTRODUCERE

Transformarea digitală accelerată a ultimului deceniu a redefinit modul în care organizaţiile publice şi private îşi desfăşoară activitatea. Dependența crescândă de infrastructuri informatice complexe, servicii cloud şi sisteme interconectate a creat un mediu în care vulnerabilitățile tehnice generează consecinţe directe şi măsurabile: întreruperi ale serviciilor esențiale, pierderi financiare semnificative şi riscuri la adresa securității naționale. În acest cadru, securitatea cibernetică a devenit o prioritate strategică, iar formarea specialiştilor capabili să răspundă eficient ameninţărilor în continuă evoluţie reprezintă o necesitate recunoscută la nivel internațional.

Datele disponibile confirmă amploarea acestei provocări. Conform ISC2 Cybersecurity Workforce Study 2024, numărul posturilor neocupate în domeniu se apropie de 4,8 milioane la nivel global, iar aproximativ 60% dintre organizații semnalează că lacunele de competențe le-au afectat concret capacitatea de protecție. Problema nu este doar cantitativă - nu lipsesc doar oameni, ci lipsesc competențe specifice, operaționale, dobândite prin practică directă, nu prin studiu teoretic.

Această realitate expune o limitare structurală a formării universitare tradiționale. Programele de studii în securitate cibernetică oferă, în general, o bază conceptuală solidă, însă componenta practică rămâne adesea insuficientă sau deconectată de cerințele reale ale industriei. Absolvenţii întâmpină dificultăţi în a gestiona situaţii dinamice, în a utiliza instrumente specializate şi în a lua decizii sub presiunea timpului - competențe care nu se formează prin prelegeri frontale sau laboratoare cu scenarii predefinite şi rezultate cunoscute dinainte.

Mediile de tip Cyber Range oferă un răspuns concret la această problemă. Prin simularea unor infrastructuri informatice reale într-un cadru controlat, aceste platforme permit studenţilor să exerseze tehnici ofensive şi defensive, să analizeze incidente simulate şi să lucreze în echipă reproducând dinamica unui centru operaţional de securitate. Experienţa internaţională demonstrează că integrarea coerentă a acestor medii în curriculum generează rezultate măsurabile: rate mai mari de angajare, progrese semnificative în competenţele tehnice şi o motivaţie crescută pentru domeniu.

Prezenta lucrare porneşte de la această premisă şi urmăreşte două obiective principale. Primul constă în analizarea potenţialului mediilor Cyber Range ca instrumente educaţionale, prin examinarea literaturii de specialitate şi a studiilor de caz internaţionale relevante. Al doilea obiectiv vizează proiectarea unui model didactic aplicabil în contextul specific al Universităţii Tehnice a Moldovei, fundamentat empiric pe analiza curriculumului existent şi pe datele colectate prin chestionar de la studenţii FCIM UTM.

Structura lucrării reflectă acest demers în patru capitole: fundamentarea teoretică şi studiile de caz internaţionale, analiza comparativă a platformelor TryHackMe şi Hack The Box, analiza contextului educaţional local şi, în final, proiectarea modelului didactic pilot bazat pe Cyber Range.

BIBLIOGRAFIE

[1] ISC2 – Cybersecurity Workforce Study 2024, https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

[2] ISC2 – Cybersecurity Workforce Study 2025, https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

[3] Țurcanu, D.; Peca, L.; Prisacaru, A.; Țurcanu, T. - Cyber security professional development within CYBERCOR. https://ibn.idsi.md/sites/default/files/imag_file/87-98_12.pdf

[4] Peca, L.; Țurcanu, D.; Melnic, R. - The relevance of e-learning resources in computer networks courses: an evaluation based on student perceptions. https://press.utm.md/index.php/jss/article/view/2024-7-4-07/07-pdf

[5] Peca, L.; Dumbraveanu, R.; Țurcanu, D. - The sustainability of e-learning in higher education. https://press.utm.md/index.php/jss/article/view/2024-7-3-07/07-pdf

[6] Peca, L. - E-learning experiences in the Computer Networks course in higher education. https://agepi.gov.md/en/intellectus/intellectus-2-2023/e-learning-experiences-computer-networks-course-higher-education

[7] Peca, L.; Dumbraveanu, R.; Țurcanu, D. - Optimizing computer network learning through sequential e-learning based on digital technology. https://press.utm.md/index.php/jss/article/view/2023-6-3-10/10-pdf

[8] Catal, C., et al. - CyBOK Knowledge Gaps Analysis, https://pmc.ncbi.nlm.nih.gov/articles/PMC9362361/

[9] ENISA - European Cybersecurity Skills Framework (ECSF), https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf

[10] ENISA - Addressing Skills Shortage and Gap Through Higher Education, https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

[11] Fortinet - Global Cybersecurity Skills Gap Report, https://www.globenewswire.com/news-release/2025/10/08/3163383/0/en/Fortinet-Annual-Report-Indicates-AI-Skillsets-Critical-to-Cybersecurity-Skills-Gap-Solution.html

[12] International Telecommunication Union (ITU). Global Cybersecurity Index 2020. 2021. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[13] Romanian Cybersecurity Strategy 2022-2027, https://dig.watch/resource/romanian-cybersecurity-strategy-2022-2027

[14] NICE Community Coordinating Council – Cyber Range Project Team. The Cyber Range: A Guide. National Institute of Standards and Technology (NIST), 2023. https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf

[15] Yamin, M. M., Katt, B., Gkioulos, V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, 2020. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture - ScienceDirect

[16] Vykopal, J., Vizvary, M., Ošlejšek, R., Čeleda, P., Tovarňák, D. Lessons learned from complex hands-on defence exercises in a cyber range. IEEE Frontiers in Education Conference (FIE), 2017. Lessons learned from complex hands-on defence exercises in a cyber range | IEEE Conference Publication | IEEE Xplore

[17] Švábenský, V., Vykopal, J., Čeleda, P., Dovjak, J. Automated Feedback for Participants of Hands-on Cybersecurity Training. Education and Information Technologies, 2023. https://link.springer.com/article/10.1007/s10639-023-12265-8

[18] TryHackMe, „About TryHackMe", Site oficial TryHackMe, 2026. https://tryhackme.com/about

[19] Hack The Box Ltd., *Hack The Box – Main website*, site oficial, 2022, https://www.hackthebox.com

[20] TryHackMe, "Learning paths.", TryHackMe | Paths

[21] Hack The Box, "Pro Labs.", https://www.hackthebox.com/hacker/pro-labs

[22] Hack The Box Academy, https://academy.hackthebox.com/

[23] Hack The Box, "Higher education.", https://www.hackthebox.com/higher-education

[24] TryHackMe, "How to best engage your students in cyber security learning.", https://tryhackme.com/resources/blog/engage-your-students-in-cyber-security

[25] Švábenský, V., Vykopal, J., Čeleda, P., Krčál, M. - *Enhancing Cybersecurity Skills by Creating Serious Games* - ITiCSE 2021, ACM Conference on Innovation and Technology in Computer Science Education. https://dl.acm.org/doi/10.1145/3430665.3456367

[26] Pernik, P. - *Improving Cyber Security: NATO and the EU* - NATO CCDCOE Policy Paper, Tallinn, 2018. https://ccdcoe.org/library/publications/improving-cyber-security-nato-and-the-eu/

[27] Brangetto, P., Veldre, M. - *Exercise Locked Shields as a Technical Cyber Defence Exercise* - NATO CCDCOE, Tallinn, 2015. https://ccdcoe.org/uploads/2018/10/Art-08-Exercise-Locked-Shields-as-a-Technical-Cyber-Defence-Exercise.pdf

[28] Schmitt, M.N. (ed.) - *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* - Cambridge University Press, 2017. https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/

[29] TryHackMe - *How to Best Engage Your Students in Cyber Security Learning: Epitech Case Study* - TryHackMe Resources Blog, 2023. https://tryhackme.com/resources/blog/engage-your-students-in-cyber-security

[30] Epitech - *Epitech Pedagogy: The Innovative Pedagogy* - Site oficial Epitech, 2024. https://www.epitech.eu/en/epitech-pedagogy/

[31] Sahlberg, P. (2015). *Finnish Lessons 2.0*. Routledge. https://doi.org/10.4324/9781315749031

[32] Kolb, D. A. (1984). *Experiential Learning: Experience as the Source of Learning and Development*. Prentice Hall. https://learningfromexperience.com

[33] Barrows, H. S. (1986). A taxonomy of problem-based learning methods. *Medical Education*, 20(6), 481–486. https://doi.org/10.1111/j.1365-2923.1986.tb01386.x

[34] OECD (2021). *Digital Education Outlook 2021: Pushing the Frontiers with Artificial Intelligence, Blockchain and Robots*. https://www.oecd.org/education/digital-education-outlook

[35] Ministerul Educației și Cercetării al Republicii Moldova (2022). https://mec.gov.md

[36] Guvernul Republicii Moldova (2023). Strategia de transformare digitală. https://gov.md

[37] European Commission (2022). *Digital Education Action Plan 2021–2027*. https://education.ec.europa.eu

[38] FCIM UTM (2025). Planul de învățământ - program master Securitate Informațională. https://fcim.utm.md/programe-de-master/securitate-informationala-masterat/

[39] Yin, R. K. (2014). *Case Study Research: Design and Methods* (5th ed.). SAGE Publications.

[40] Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). SAGE Publications.

[41] NIST / NICE (2020). *Workforce Framework for Cybersecurity (NICE Framework)*. NIST Special Publication 800-181r1.https://www.nist.gov/system/files/documents/2020/11/16/NICE%20Framework%20SP%20800-181%20November%202020.pdf

[42] Lonka, K. (2018). Growing Minds - 21st Century Competences and Digitalisation among Finnish Youth. University of Helsinki.

[43] Darling-Hammond, L., Hyler, M. E., & Gardner, M. (2017). *Effective Teacher Professional Development*. Palo Alto, CA: Learning Policy Institute