Information & Security

Elitsa Pavlova
vol. 50, no. 2 (2021): 149-159
https://doi.org/10.11610/isij.5006

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Implementation of Federated Cyber Ranges in Bulgarian Universities: Challenges, Requirements, and Opportunities

Elitsa Pavlova

University of National and World Economy, Sofia, Bulgaria
http://www.unwe.bg

ABSTRACT:

Cyber education has been one of the global challenges in recent years. Attacks are becoming more sophisticated, and it is increasingly difficult to provide a safe working environment. Hyper-realistic virtual environments called cyber ranges help increase the level of cybersecurity training. Access to multi-domain exercises is needed to make full use of their capabilities, combine information technology networks and other appropriate infrastructure. A systematic review of the modern cyber ranges used for teaching and research purposes in higher education institutions has been made. This study aims to analyse cyber range characteristics, functionalities, and requirements for their implementation and integration in accordance with the EU regulations. The results will be used in the development of a conceptual model for a cybersecurity training laboratory at the University of National and World Economy, Sofia, Bulgaria. Its inclusion in the teaching and research process is a relevant, important, and promising area for the future of higher educaiton in cybersecurity.

ARTICLE INFO:

RECEIVED: 08 June 2021
REVISED: 03 SEP 2021
ONLINE: 16 SEP 2021

KEYWORDS:

cyber range, functionalities, classification, training, education, university, Bulgaria

Tel.: +359 889 89 67 27; E-mail: epavlova@unwe.bg

Introduction

Digital transformation is becoming an important element in strategies and plans for the development and improvement of higher education. The application of new approaches in education, new ways of exchanging information, and group work must improve and transform all processes and services in higher education institutions. Educational institutions around the world are losing millions, recovering from incidents caused by cyberattacks, and the demand for cybersecurity experts is increasing. Cyber Ranges (CR) can fill this gap by combining hands-on experience with educational courses and cybersecurity competitions.

According to the National Institute of Standards and Technology (NIST), CRs are defined as interactive systems, tools, and applications. They provide a secure environment for gaining hands-on experience and work individually or with other cyber ranges, supporting certain network services. However, not every CR is open or intended to be used by every category of users: institutions; security specialists; military agencies and CNO; operational security centers (SOCs); teachers; students; researchers; event organisers.

Many universities around the world are investing in cyber education. "It's this virtual environment where you can practice skills and simulate attacks safely," said Rebecca Michael, executive director of cyberspace in Ohio, University of Cincinnati.

The advantage of having a range at a university such as the Virginia Cyber Range at Virginia Technical University is that the university takes care of the hardware, installation, management, and configuration. Whether it is simulations, competitions, or labs, cyber ranges visualise what students are learning in theory, and this is essential for cyber education. Once basic skills are acquired, students can use simulations, not only focusing on intrusive systems but also ready to defend themselves against such attacks. X-Force Command, based in Cambridge, Massachusetts, offers educational opportunities for both high school and university students. CEO Christopher Krumi says the site hosted a competition in which more than 250 students from five universities took part.

Cyber ranges are one way for colleges and universities to develop their cyber education programs. The Cincinnati Cyber Range has brought together many departments to form a more comprehensive program. The School of Information Technology, the Department of Computer Science, and the Department of Political Science participate together in cyberspace.

There is still no developed network of cyber ranges in Bulgaria that can be actively used for the various educational needs and degrees in higher education. There is only one cybersecurity laboratory at Varna Technical University, and the largest digital technology education center SoftUni has Software Engineering Labs.

Methods

A detailed review of the literature is made, and the CRs used in higher education for research, training and exercises were examined. They have different capa-

bilities and infrastructure, and their integration leads to scalability and reliability. Analysis of the architecture of the cyber range shows a separation of test and simulation environments.

Interviews were conducted with system and network administrators from several universities in Bulgaria, and good practices and procedures for working in the process of digital transformation were discussed. An analysis of cyber education in Bulgaria and the opportunities for development and implementation of CRs in various bachelor's, master's, doctoral, and research programs.

Functionalities and Classification

The European Union Agency for Network and Information Security (ENISA) reports that the number of cybersecurity exercises used in universities has increased in the last year.[1]

CR functionalities are available to their users and administrators. Depending on their purpose, some of them may be considered desirable or mandatory. A careful assessment of the integration and compatibility challenges that may arise is needed. Cyber ranges are operation-oriented, and their performance depends on certain parameters, such as size, infrastructure, scenario, simulation environment, access, automation, and performance. They range from single stand-alone bands in an organization to Internet replication bands that are accessible from around the world and used by private, public organizations, students, researchers, and more. They can be classified based on their usage, infrastructure, cloud platform usage, teams, and test environment.

The cases of use depend on the technical parameters, such as computing power, memory and disk capacity, network characteristics and topology, available operating systems, applications, physical environment, etc. Conducting competitions, training or exercises in cybersecurity requires multiple interconnected cyber ranges. Users of these interconnected CRs can benefit from reduced costs and the availability of targeted, realistic event content.[2] The development and operation of a CR require significant resources in terms of funding, skilled people, and working hours. CR aggregation means the interaction of two or more CRs, which may have different network topologies and uses. This has two main advantages: the ability to create complex scenarios and the ability to create a single market where multiple providers can publish their services.

CRs use environments that contain both physical and virtual components and can be used to present realistic learning scenarios. Chandra [3] suggests the efficiency to be increased through the use of container technology. Carnegie Mellon University [4] is developing open-source software tools to create secure and realistic cyber simulations. According to a study by Beveridge, bringing realism to cybersecurity education is extremely important.[5] A review of existing definitions identifies two ways to define cyber ranges: a simulation environment and a platform. A simulation environment focuses on ICT and is defined as a static mode because it usually refers to a simulation environment that is designed to meet specific uses and requirements. A platform is defined as a

group of technologies that are used as the basis of other applications, processes, or technologies. This view of the CR is more dynamic because there are different functionalities in the use of the simulation environment. A cyber exercise is a planned event during which an organisation simulates cyberattacks and information security incidents.

The European Cyber Security Organisation, ECSO, defines CR as follows:[6] A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, mobile and physical systems, applications, and infrastructures, including the simulation of attacks, users and their activities, and of any other Internet, public or third-party services which the simulated environment may depend upon. A CR includes a combination of core technologies for the realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific CR use cases.

According to the study "Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture,"[7] Figure 1 shows the architecture of the cyber range. It includes scenario, monitoring, training, management, merging, environment. The script combines the type and purpose of the exercise, the plotline, and the environment in which it takes place. The choice of teams depends on the scenario. Management includes resources, scope, and role. All areas of cyber band architecture are consistent and interconnected.

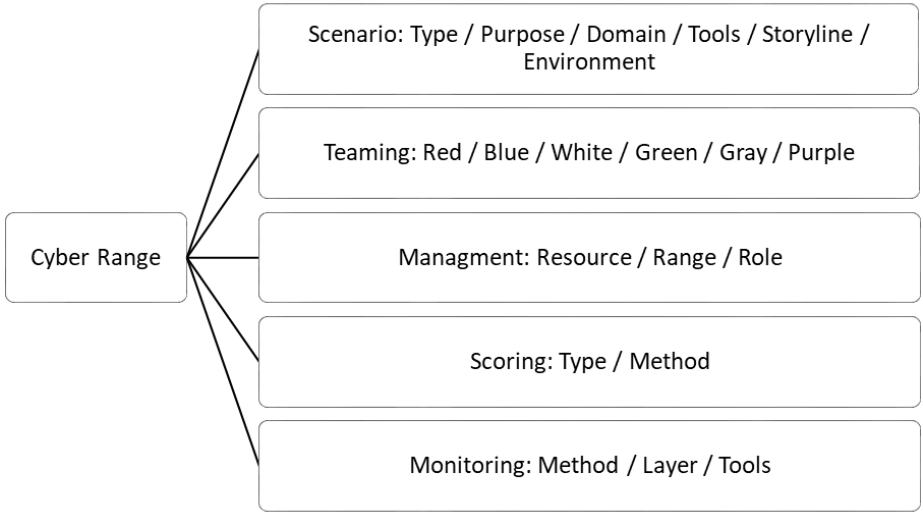

Figure 1: Cyber range architecture. Source: Cyber ranges and security testbeds: Scenarios, functions, tools, and architecture.

Cyber ranges are mainly used for research, training and exercises. Research requires environments that are fully controlled but at the same time complex to develop and test a new tool or to design new methods of attack. The training serves the practice and education of cybersecurity - specialized courses and certificates. Cyber exercises include various competitions for attack and defence.

Cyber ranges can be classified based on their infrastructure – public, private or federal. The federal infrastructure includes cyber bands such as NCR, CRATE, NATO, Raytheon and DoD, while the IBM scope belongs to the private infrastructure. CISCO, Baltimore, and Virginia's cyber ranges are both public and private infrastructure groups. Interestingly, the Michigan Cyber Range and the Florida Cyber Range belong to all classifications.

Some universities are deploying a virtual private network (VPN), while others rely on the Virtual Clone Network (VCN). VCN includes risk management, real-time cyber incident hypothesis testing and provides scalability and reliability. VPN is configuration-dependent and works well for file sharing, access to blocked websites, bypassing filtered content, and online anonymity. The study shows that all cyber bands which use cloud platforms have VPN, with the exception of the University of Delaware, which has VPN but doesn't have cloud infrastructure.

Teamwork helps to assess attack scenarios in real conditions.[8] Red and blue teams are common to all cyber ranges. The red team attacks users' computers using viruses, malware, and more designed by the white team. Green is responsible for simulating wired or wireless connections between users with their computers or smartphones to the network infrastructure. The blue team manages the security of the network infrastructure and is the target audience of the exercise. The white team creates cyber-attack scenarios to track the success or failure of the blue team. The yellow team takes into account situational awareness by reproducing innocent users who compromise the security of the network. Some cyber ranges use a grey and a purple team. The grey team represents normal requests for traffic and services to be maintained, and the purple team is a collaboration between the red and blue teams responsible for security techniques.

Another way to classify CRs is based on the test environment in the form of virtual machines and a sandbox. Although both methods provide isolation, they have different software, files, and operating systems. Virtual machines provide complete isolation, while sandboxes have flexibility. CRs often use both virtual and physical infrastructure to offer a safe and realistic environment for learning and testing cyber skills. The Davis and Magrat [9] study shows the available opportunities for building and managing cyber bands for monitoring and analysis training scenarios. Researchers categorize CRs as simulation using software models of real cases, as overlay if using real production equipment, and as emulation in case of running real applications of individual equipment.

The main use is training, says the report "Thinking about Cybersecurity," and then there is research and development. "Cyber experts must be highly qualified, able to recognize and respond to complex situations, assess risks and vulnerabilities, deal with insecurity, solve problems, have security thinking."[10]

Examples of the Use of Cyber Ranges in Higher Education

Universities and academic organizations are working hard to build or join cyber ranges in order to expand curricula and attract students. The Cyber Range in Michigan is an example of this, providing cybersecurity training and research in an unclassified private cloud operated by the Merit network. It offers cybersecurity classes and exercises and enables the development and testing of Merit customers and members around the world.

The project of the Federation of Cyberspaces aims to build cyberspace throughout the EU. It involves eleven EU Member States, the European Space Agency, and the European Defence Agency. Another initiative is the CyberSec4Europe project, which focuses on the management of the European cybersecurity network. The ECHO project, launched by the European Commission, has the vision of creating and managing a network of competence in the field of cybersecurity.

Building a CR depends on the approach to design features such as flexibility, scalability, isolation, interoperability, efficiency, service-based access, and risk assessment. Examples are KYPO CR Platform, TELECOM Nancy, RISE CR, Airbus CyberRange, RI CODE, Virginia CR.

KYPO CR Platform was developed by Masaryk University and is based on modern technologies such as containers, infrastructure, and open-source software. The cloud-based approach allows you to start with just one test server and then increase it. The hardware can be used more efficiently, and the cyber band platform can host as many different types of content as the cloud can handle. An open approach to content encourages learning sharing. Creating and editing is done using standard tools such as Ansible and Packer. The data is stored in file formats such as JSON and YAML in a Git repository.

The TELECOM Nancy platform (University of Lorraine, France) allows the construction, implementation, and experimentation of realistic and complex IT infrastructures for simulation and analysis of various attack and defense scenarios. It is open to cooperation and provides support for both training and research. It uses HNS (Hybrid Network Simulation) servers developed by DIATEAM. The solution is hybrid, as virtualised topologies can be easily interconnected with other physical network platforms.

RISE CR (Research Institute, Stockholm, Sweden) aims to provide hands-on training and exercises in cybersecurity; environment for modern applied research; a forum for participation and organization of international competitions in ethical hacking and certification of cybersecurity.

Airbus CyberRange is a multifunctional cyber simulation platform accessible via a web interface and does not require the installation of additional software.

It is used by critical organizations (CNI, governments, and the military) and maintains partnerships with universities and research centers in connection with specializations in cybersecurity, bachelor's and master's programs. It offers several types of content: topologies, virtual machines, containers, attacks, traffic generators, and scenarios.

The CODE research institute (University of the Bundeswehr Munich, Germany) uses a CR based on an open, modular platform and architecture. It includes four virtual network infrastructures with scenarios and 80 individual exercises from 9 different areas. The university provides a learning environment for the so-called CNO (Computer Network Operation) or CERT skills of Master Cyber Security students. The goal is to practice virtualized cyberattacks that present the real world in an environment completely isolated from other networks. The cyber band is separate from the rest of the infrastructure. Students, trainers, and administrators can connect through Microsoft terminal servers.

Cyberbit Range is the most widely used hyper-realistic platform among higher education institutions. It is used both for a practical cyber lab and for training and education of cybersecurity professionals by simulating real networks, security tools, and malicious traffic. Allows customization of every aspect of a training session, including the development of new scenarios and training programs.

Virginia CR is based on the cloud and provides a wide variety of security exercises in an isolated virtual environment.[11] It provides user-specific content as well as platform-based access to the platform. Learners gain a solid foundation in cybersecurity through a variety of technical or theoretical courses.

Security Challenges

In the study Cyber Ranges and Test Beds for Education, Training and Research, an analysis of the cyber ranges used in higher education was made.[12]

Cyber ranges have different capabilities and infrastructure, and their integration leads to scalability and reliability. Simulation training can help with data analysis as well as decision-making processes. The real simulation is performed in the form of cyber exercises in the physical environment of isolated networks. Virtual simulation deals with practical evaluation and control by simulating real systems. CRs allow remote access for students, researchers, etc., and automation checks the configuration of all devices and ensures the security of the infrastructure. Productivity is an important component. CRs can work with multiple high-traffic websites simultaneously. Load balancing depends on the size, number of platforms and tools it supports.

Table 1 on Cyber Ranges' features shows that the largest percentage of CR systems are used for research (R), training (T) and exercise (E). Masaryk University, Naval Postgraduate School and the Florida Cyber Range are also using them for education (ED), the last one being used also for operations (O) and testing (TE). The Florida Cyber Range provides advanced training and testing solutions

for academic, government and industry organizations through exercises, competitions (C), operations and research. Educational materials, including curricular resources, labs and hands-on exercises are provided to support educational use.

The security challenges are grouped into the following categories: Web (W), Cryptography (C), Forensics (F), Exploitation (E), Steganography (S), DDoS (DD), APT (AP), Ransomware (R), SQL Injection (SI), Malware Analysis (MA), Reverse Engineering (RE), Risk Management (RM), Information Security Economics (ISE), Cyber Management (CM), Cyber Policy (CP).

Courses include: Digital Forensics (DF), Software Security (SS), Digital Forensics (DF), Network Security (NS), Web Security (WS), Operational Technology Security (OS), Hardware Security (HS), Cloud Security (CS), Configuration management (CM).

This shows that cyber ranges are used successfully for training in bachelor's and master's programs, public administration, business, and for a diverse portfolio of goals related to cyber education.

Most cyber ranges provide on-premise and remote access. Table 1 shows that Virginia Cyber Range offers a variety of courses and exercises covering different levels of training.[13] Some of them are: advanced packaging tool and port scanning; social engineering; anatomy of an attack; attack phases, threats, and attack vectors; basics of computer networking. In broken authentication and in-depth SQLi lesson, students use the cyber range: Cyber Basics (2018) environment to learn how to manually execute SQL injections to retrieve personally identifiable information, discover account credentials, and modify shopping carts. In course "Cracking Authentications," students use the Cyber Range: Kali Linux and Vulnerable Windows 7 environment to crack authentications using Hydra, Hashcat, John the Ripper and online tools. Students will be immersed in the addictive cryptographic cracking arena that is essential to becoming an ethical hacker. During this lab exercise Defending Against Public WiFi Hacker Attacks, students gain experience and knowledge in network administration, ports, protocols, IP addresses, port scanning, and firewalling. The university has a laboratory that introduces students to various self-assessment tools that help organizations assess how effectively they are implementing the NIST cybersecurity framework.

The Michigan Cyber Range includes experience in cybersecurity education based on the National Institute of Standards and Technology and the guidelines of the National Cybersecurity Education Initiative. The 8570 compliant courses are offered through four out of the five recognized certification providers in partnership with Cyber World Institute. Merit Network is the only non-profit in North America able to offer EC Council, ISC2, CompTIA and ISACA. Courses are available live online, in person, and private on-site.

Table 1. Table 1. Cyber Ranges' features
Source: based on "Cyber Ranges and TestBeds for Education, Training and Research"

Operator	Objective	Security Challenges	Courses
De Montfort University	R, T, E	W, E, AP	DF, SS, IC
Royal Military Academy	R, T, E, ED	W, F, DD, AP	DF, NS, WS
Masaryk University	R, T, E, ED, C	W, F, E, SI, MA	DF, NS
Austrian Institute of Technology	R, T, E	W, F, E, DD, AP, R, MA	NS, WS, OS
Naval Postgraduate School	T, E, ED	W, C, E, DD, SI, MA, RE	SS, NS, WS
Norwegian University of Science and Technology	R, T, E	W, C, F, E, S, DD, AP, R, SI, MA, RE, RM, ISE, CM, CP	DF, HS, SS, NS, CS, WS, CM
Virginia Tech	R, T, E	W, C, F, E, S, SI, RE	DF, SS, NS, WS
Università degli Studi di Milano	R, T, E	W, F, SI, MA, RB	DF, WS
JAMK University of Applied Sciences	R, T, E	W, C, F, E, S, DD, AP, R, SI, MA, RE	DF, HS, SS, NS, CS, WS
Florida Cyber Range	R, O, TE, C, ED	W, C, SI, E, DD	DF, HS, SS, NS, CS, WS, CM
Michigan Cyber Range	ED, R, T, E, C	W, CP, E, DD, CM	HS, SS, NS, CS, WS, OS, CM
Georgia Cyber Range	ED, R, T, E	W, F, E, S, SI, CM	HS, SS, NS, CS, WS, CM

Conclusions

This report considers the CRs and their federation as an important part of cyber education at the university. Modern CRs must have features such as simulated smart grids, virtual cyber work centers, wireless sensor networks, real-time intrusion detection systems, new authentication and confidentiality mechanisms, automatically configurable systems, smart, mobile, and integrated technologies. The addition of these features will help to identify vulnerabilities in different systems and will enable researchers to develop innovative safeguards. Augmented Reality must be included as an influential technology creating a new

interactive experience for learners. 5G/6G networks will transform services using mobile and wireless network infrastructures. Lovas' study highlights the benefits of container technology[14] to achieve scalability and portability.

There is still no developed network of cyber ranges in Bulgaria that can be actively used for the various educational needs and degrees in higher education. They must be built in such a way that they can be used for research purposes within EU projects. Another important aspect is the ability of CR to generate measurable data in a semi-automated manner with limited human intervention. They should include a portable version for demonstration purposes and be easily deployed as a modern training tool in various cybersecurity events. Training focused on preventing, detecting and mitigating cyber attacks involving complex networks and hybrid infrastructures is crucial. This imposes a trend to move from traditional cyber bands to digital twins, which will become dominant for the reproduction of critical infrastructures.

The analysis shows that the cyber ranges used in higher education are focused on realistic scenarios to help users gain focused learning with experience. Based on the federation of cyber ranges, programs for digital identity management, access to critical resources, organizational security and cybersecurity in higher education institutions can be developed. Cyber education is extremely important, relevant and promising area, as the human factor is the weakest link in the security of any organization. The results will be used in the development of a conceptual model for a cybersecurity training laboratory at University of National and World Economy.

Acknowledgements

This publication is supported by the University of National and World Economy's research grant UNWE NID NI 24/2021. My sincere gratitude also to my supervisor, Associate Professor Georgi Penchev, for providing guidance and feedback throughout this project.

References

[1] ENISA Europa, "Good Practice Guide on Training Methodologies," Report/Study, November 12, 2014, https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies.

[2] ECSO (European Cyber Security Organisation), 2021, https://ecs-org.eu/publications.

[3] Yogesh Chandra and Pallaw Kumar Mishra, "Design of Cyber Warfare Testbed," in *Software Engineering*, edited by M. N. Hoda, Naresh Chauhan, S.M.K. Quadri, and Praveen Ranjan Srivastava (Singapore: Springer, 2019), 249-256, https://doi.org/10.1007/978-981-10-8848-3_24.

[4] Dustin Updyke, Geoffrey Dobson, Thomas Podnar, Luke Osterritter, Benjamin Earl, and Adam Cerini, "GHOSTS in the Machine: A Framework for Cyber-Warfare Exercise

NPC Simulation," Technical Report, AD1068374, 2018, https://apps.dtic.mil/sti/citations/AD1068374.

[5] Robert Beveridge, "Effectiveness of Increasing Realism Into Cybersecurity Training," *International Journal of Cyber Research and Education (IJCRE)* 2, no.1 (2020), 4, https://doi.org/10.4018/IJCRE.2020010104.

[6] ECSO, *Understanding Cyber Ranges: From Hype to Reality*, White Paper, 2020.

[7] Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos, "Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture," *Computers & Security* 88 (January, 2020): 101636, doi:10.1016/j.cose.2019.101636.

[8] Ibid.

[9] Jon Davis and Shane Magrath, "A Survey of Cyber Ranges and Testbeds," Report, ADA594524, 2013, https://apps.dtic.mil/sti/citations/ADA594524.

[10] Melissa Dark "Thinking about Cybersecurity," *IEEE Security & Privacy* 13, no. 1 (Jan.-Feb. 2015): 61 - 65, https://doi.org/10.1109/MSP.2015.17.

[11] Virginia Cyber Range, 2021, https://www.virginiacyberrange.org.

[12] Nestoras Chouliaras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag, "Cyber Ranges and TestBeds for Education, Training, and Research," *Applied Sciences* 11, no. 4 (2021): 1809, https://doi.org/10.3390/app11041809.

[13] Virginia Cyber Range.

[14] Róbert Lovas, Péter Kardos, András Zénó Gyöngyösi, and Zsolt Bottyán, "Weather Model Fine-Tuning with Software Container-Based Simulation Platform," *Quarterly Journal of the Hungarian Meteorological Service* 123, no. 2 (April - June, 2019): 165–181, https://doi.org/10.28974/idojaras.2019.2.3.

About the Author

Elitsa **Pavlova** is a doctoral student at the University of National and World Economy at the Department of National and Regional Security. The topic she is working on is "Development and Implementation of a Model for Digitalization Management of Higher Education Institutions in Bulgaria. Security Aspects." She graduated with a master's degree from the same department in 2006 and a master's degree in engineering at the Technical University in Sofia in 1999. She works as a network administrator in the Department of Information Technology at UNWE. https://orcid.org/0000-0002-2210-7904