Information & Security

V. Slavchev
vol. 50, no. 2 (2021): 161-168
https://doi.org/10.11610/isij.5007

Published since 1998 ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Using Cyber Ranges in Cybersecurity Management Educational Programmes

Veselin Slavchev

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

ABSTRACT:

The demand for better-trained cybersecurity specialists is growing globally, triggering interest in advanced technology solutions supporting education and training. The analysis of cyber ranges used at various European universities, presented in this article, aims to determine the most appropriate cyber range for the needs of the Master's program in Cybersecurity Management of the University of National and World Economy in Sofia, Bulgaria.

ARTICLE INFO:

RECEIVED: 17 JUNE 2021
REVISED: 08 SEP 2021
ONLINE: 16 SEP 2021

KEYWORDS:

cyber range platform, education, training, cyber security, information security management

Introduction

The purpose of this study is to select and define a cyber range platform for the needs of a cybersecurity management educational programme at the University of National and World Economy. According to predictions from Cybersecurity Ventures, an estimated 3.5 million cybersecurity jobs will be available and eventually unfilled by 2021. While global cybercrime damages are predicted to reach $6 trillion annually by 2021,[1] 61% of companies find most of the cybersecurity applicants unqualified.[2] There is a solution to the problems with a chronic shortage of well-trained cybersecurity professionals. The use of cyber ranges to train cybersecurity professionals is an innovative approach that shortens learning time relative to traditional teaching methods. Comparative analysis (benchmarking) has been performed to select the most appropriate

✉ Tel.: +359988785099; E-mail: veselin.slavchev@unwe.bg

cyber-scope platform for the needs of a Master's program in Cybersecurity management.

The main objectives and research areas in which knowledge enhancement and validation will be sought are:

- the most important aspects of cybersecurity management, as well as the methods, means, and procedures for ensuring cybersecurity;
- management systems, information and communication systems related to the security and protection of critical information infrastructure;
- design of secure information systems in cyberspace;
- management of IT projects in the public and private sectors;
- acquiring scientific skills in the preparation of complex analyses, which from a formal point of view will help to explore the systems of rules (semantic field) for the manifestation of a complex structure of laws and regulations related to cybersecurity;
- acquiring skills in optimizing the internal organizational processes in the different units of organizations dealing with security at the national and private levels;
- acquiring capabilities and knowledge in handling information of different types and complexities, as well as protecting information sensitive to organisations.

Cyber ranges are interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet-level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing. A cyber range may include actual hardware and software or may be a combination of physical and virtual components. Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic but also replicates network services such as webpages, browsers, and email as needed by the customer. Students can use cyber ranges to apply knowledge in a simulated network environment, develop cyber skills, work as teams to solve cyber problems, and prepare for cyber credentialing examinations. Educators can use cyber ranges as a classroom aide or an instructor assessing students virtually.[3]

Globally, the use of isolated environments for training, exercising, competitions, cybersecurity research is increasing. More and more universities are trying to compensate for the lack of cybersecurity experts through the use of advanced technologies.

The use of Cyber Range Platforms in the Republic of Bulgaria is a novelty. By the time of writing this paper, we were able to identify only one Cyber Range Platform working at the Black Sea Security Academy at Varna Free University, "Chernorizets Hrabar." It supports 15 scenarios and three levels of complexity, designed for students, experts, and law enforcement officers. The training will

be provided by leading Israeli specialists, and those who have completed the course will receive a joint certificate from the Black Sea Security Academy and the Israeli Center for Innovation and Cybersecurity, the university announced. "The Cyber Range simulator is a necessary component in cybersecurity training, without which specialists in this field cannot be formed. This simulator trains employees from government and law enforcement agencies of leading countries, experts responsible for security in the financial sector, and critical infrastructures.[4] This cyber range platform is designed primarily for cybersecurity technicians with no managerial functions.

Methods

Qualitative comparative analysis is used in this study. The source of the study is the database created by the European Union Agency for Cybersecurity, ENISA.[5] Leading European universities and academic organisations using cyber ranges for student learning are selected for the purposes of the analysis. The universities are chosen based on the availability of accessible information on cyber ranges application in an academic environment.

Comparative analysis in the business economy, also referred to as Benchmarking, is a process of comparing manufacturing or administrative processes and achievements to industry bests and best practices from other companies. Metrics typically measured are quality, time, and cost.

Comparative analysis requires management personnel to identify the best companies in their industry or any other industry where a similar process exists and to compare the results and actions of those studied to their own actions and results to learn how well the targets perform and, more importantly, how they achieve it.

The main characteristics that are considered important in the conducted research are the academic disciplines in the master's program in cybersecurity at UNWE are described in Table 1 as follows:

- Fundamentals of cybersecurity,
- Industrial Control Systems / SCADA,
- Cryptography in cybersecurity,
- Legal aspects of cybersecurity,
- EU theory and practice in the field of cybersecurity,
- Anti-crisis management in cybersecurity,
- Protection of critical infrastructure,
- Fundamentals of intelligence in cybersecurity,
- Innovation in cybersecurity,
- Good practices in cybersecurity,
- Cyber secure Internet,
- Penetration testing,
- Information protection in crises,

- Artificial intelligence in cybersecurity.

The possible options for deploying and using cyber ranges are:

- as part of the Master's programmes in Management Studies;
- outsourcing to external companies;
- joint deployment and cybersecurity trainings.

Virtualization allows:

- cost reduction;
- flexibility in training;
- opportunities to test diverse scenarios.

Simulations can be based on:

- ready-made scenarios from other cyber ranges;
- own scenarios.

Alternative ways can be applied for creating simulations and scenarios:

- using scripts;
- using specialized software.

The following universities were selected for the purposes of the conducted study: JAMK University of Applied Sciences, AIT Austrian Institute of Technology, Royal Military Academy, Masaryk University. The cyber ranges used at these universities are JYVSECTEC, cyberrange.at, CyLab, and KYPO, respectively.

Table 1 shows that, in terms of *Fundamentals of cybersecurity* all of the listed cyber ranges are eligible for training of students.

As to the *Industrial control systems / SCADA* discipline, only CyLab does not offer the possibility of more comprehensive simulation.

All four cyber ranges studied offer a functionality for Cryptography training.

Training using cyber ranges is not applicable to to the *Legal aspects of cybersecurity* and *EU theory and practice in the field of cybersecurity* disciplines and it is not offered by any cyber range.

Anti-crisis management in cybersecurity can be used as an educational program in all four cyber ranges. Disaster recovery and cybersecurity incident responses represent a basic functionality for all cyber ranges.

Protection of critical infrastructure is related to the use of ICS / SCADA and, for that reason, CyLab cannot be fully utilized. All other cyber ranges offer training related to the protection of critical infrastructures.

All cyber ranges allow installing additional software for cyber intelligence. All four cyber ranges have the same capabilities, according to this indicator.

Cyber range training is not suitable for the *Innovation in cybersecurity* discipline. It is not offered by any cyber range.

The use of different types of virtualization allows training in the application of *Good practices in cybersecurity.*

Table 1. Training capacity of cyber ranges used by universities.

Cyber range University	JYVSECTEC JAMK	cyberrange.at AIT	CyLab RMA	Kypo MU
Fundamentals of cybersecurity	y	y	Y	Y
Industrial Control Systems / SCADA	y	y	N/A	y
Cryptography in cybersecurity	y	y	y	y
Legal aspects of cybersecurity	N/A	N/A	N/A	N/A
EU theory and practice in the field of cybersecurity	N/A	N/A	N/A	N/A
Anti-crisis management in cybersecurity	y	y	y	y
Protection of critical infrastructure	y	y	partial	y
Fundamentals of intelligence in cybersecurity	y	y	y	y
Innovation in cybersecurity	N/A	N/A	N/A	N/A
Good practices in cybersecurity	N/A	N/A	N/A	N/A
Cybersecurity in Internet	y	y	y	y
Penetration testing	y	y	y	y
Information protection in crises	y	y	y	y
Artificial intelligence in cybersecurity	N/A	N/A	N/A	N/A

Cybersecurity in Internet and penetration testing includes many components such as network security, ransomware attacks, phishing, spear phishing, DDoS, APT, social engineering and is suitable for training from all studied cyber ranges.

All studied cyber ranges also provide training opportunities for the *Information protection in crises* discipline.

Artificial intelligence in cybersecurity – none of the listed cyber ranges offer training opportunities in the field of artificial intelligence.

In addition to training students in the Master's program in Cybersecurity management at UNWE, the cyber range should be available for use by external companies. In order to meet this criterion, the study also collected information about the possibilities for remote access to the cyber range. Table 2 notes the capabilities of different cyber ranges for remote access. All of the cyber ranges studied offer remote access capability.

To reduce costs, increase scalability and flexibility in the offered educational services, it is important that the utilized cyber range supports virtualization technologies. Table 2 shows that all four studied cyber ranges are based on virtualization technologies.

Table 2. Characteristics of cyber range.

Cyber range	JYVSECTEC	cyberrange.at	CyLab	Kypo
University	JAMK	AIT	RMA	MU
Remote access	1	1	1	1
Virtualization	1	1	1	1
Open source	0.5	0.5	0.5	1
Scoring system	1	0	0	1

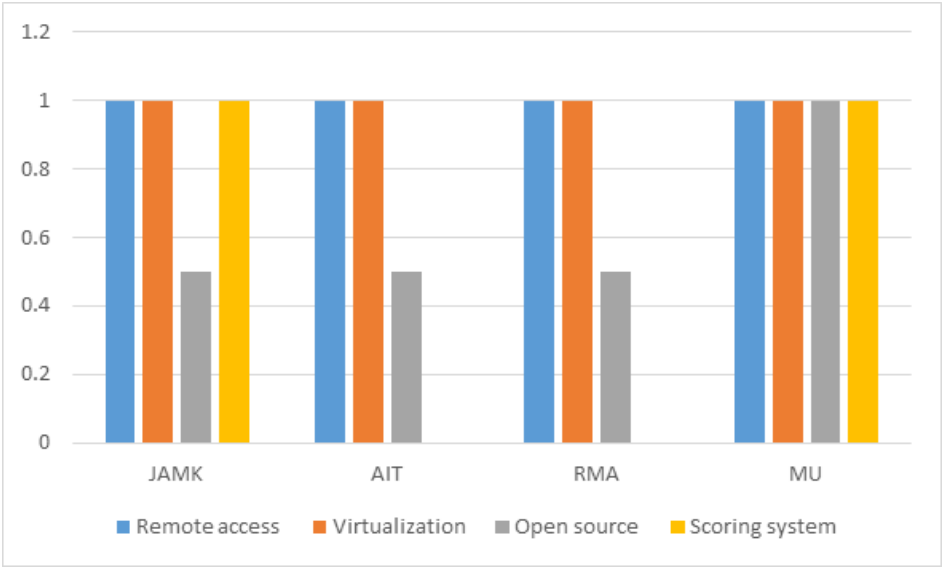

Figure 1: Characteristics of cyber range.

Open source was chosen as a benchmark because of the ability to check code for vulnerabilities, modify it, and add new functionality to existing code. Kypo cyber range is a fully open-source platform, which distinguishes it from its alternatives.

Half of the surveyed platforms have a system for evaluating the conducted trainings. Scoring systems are different and difficult to compare. Scoring systems facilitate the learning process and track student development.

What CRP functionalities should be available for the purposes of a cybersecurity management education program?

Cybersecurity management specialists have managerial functions, and their responsibilities are related to the management of people, processes, events.

There is a need to create different scenarios simulating the recovery of information and communication infrastructure after catastrophic events. The CRP must be able to simulate processes such as creating and restoring backup copies, detecting a risk event, limiting the damage in the event of a risk event, terminating the risk event and restoring the full functionality of the system.

Results

The study shows that the differences between the selected cyber ranges for the selected parameters are small and negligible. There are significant differences between cyber ranges in parameters that are not subject of this study.

Conclusions

Based on the analysis of the characteristics of the studied cyber ranges, Kypo can be selected as the most suitable for the requirements of the UNWE. The selected cyber ranges have exactly the same characteristics on all observed parameters, with the exception of CyLab, which does not have training capabilities related to ICS/SCADA and critical infrastructure protection. Cyber range platform Kypo is flexible, scalable, allows customization and creating scenarios. The widespread use of open-source technologies allows recruiting specialists from external companies.

Good practices in the use of cyber scopes are:

- Conducting trainings and exercises in a realistic environment with no risk of damaging communications and information equipment.
- Simulation of real users, which is a built-in functionality in the cyber range. Simulated user activities increase the level of realism in training and education. Human Actor-Like Orchestration (HALO) feature that can quickly simulate human activity, letting you deliver training that keeps your team on their toes.
- Selection of the right content. The cyber range should offer a large range of pre-built scenarios. The ability of a particular training program to generate scenarios based on specification is extremely important for the beneficial use of cyber ranges.
- Easy to use. The cyber range should allow the use of the platform without involvement of highly qualified specialists.

It is recommended that all the best practices listed above be included in future a cyber range projects in accordance with the of the UNWE Master's programs in Cybersecurity.

Acknowledgements

This publication is supported by the University of National and World Economy's research grant UNWE NID NI 24/2021.

References

1 Marcus Chung, "Signs your cyber security is doomed to fail," *Computer Fraud & Security* 2020, no. 3 (2020): 10–13.

2 William Crumpler and James A. Lewis, *Cybersecurity Workforce Gap* (Washington, DC, USA: Center for Strategic and International Studies (CSIS), 2019).

3 National Institute of Standards and Technology (NIST), "Cyber Ranges," 2018, https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf.

4 "The only Cyber Range on the Balkans comes to Varna," *Kmeta .bg*, 2020, in Bulgarian, https://kmeta.bg/edinstveniyat-na-balkanite-kibersimulator-cyber-range-idva-vuv-varna/.

5 European Union Agency for Cybersecurity (ENISA), "Cybersecurity education: Education courses," 2021, https://www.enisa.europa.eu/topics/cybersecurity-education/education-map/education-courses.

About the Author

Veselin Slavchev is a doctoral student at the University of National and World Economy (UBWE), Department of National and Regional Security. The topic he is working on is "Increasing cybersecurity in a university environment." He graduated with a Master's in Management information systems from Sofia University "St. Kliment Ochridski." He works as a senior expert in the Department of Human resources at UNWE.