Information & Security

Published since 1998

M. Turčaník
vol. 46, no. 3 (2020): 304-310
https://doi.org/10.11610/isij.4622

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

Research Article

A Cyber Range for Armed Forces Education

Michal Turčaník (✉)

Armed Forces Academy, Liptovsky Mikulas, Slovakia, http://www.aos.sk

ABSTRACT:

Cyber security is one of the prominent global challenges due to significant increase in the number of cyberattacks over the last few decades. Cybersecurity awareness and cyber security training are promoted by hyper-realistic virtual environments termed as cyber ranges. This article highlights the concept of a cyber range. Cyber range for educational purposes in the armed forces has been proposed taking into account the important parameters a cyber range should incorporate. The author takes into account the use cases, the topology and software tools of the newly created cyber range.

ARTICLE INFO:

RECEIVED: 28 JUN 2020

REVISED: 11 Sep 2020

ONLINE: 20 Sep 2020

KEYWORDS:

cyber range, education and training

Introduction

Cyber security is becoming more and more important in our world. Exposure to cyber threats is getting wider and more transverse. Cyberattacks and cyber threats are almost everywhere. Whether counting personal, bossiness or military data breaches, individual or state supported cyber thefts, system outages from hacker attacks or vulnerabilities detected to critical infrastructure, the growing numbers are staggering.

Cyber range must help cyber security professionals prepare for real-world situations and provide a secure environment for cyber security education, training and testing. It also performs research as an advanced platform for industrial control systems security.[1]

This paper is divided into five sections. The motivation for building of cyber range is described in section 1. Section 2 shall provide background information

✉ Tel.: +421960423011; E-mail: michal.turcanik@aos.sk

about cyber ranges. Section 3 will describe the use of proposed cyber range. The topology of the proposed cyber range is described in section 4. Section 5 will show selected groups of tools for cyber range to fulfil the main tasks of cyber range. Finally, we will conclude the paper and outline future work.

1. Motivation

Operational cyber environments are not suitable for building a systematic knowledge of new cyber threats and to train responses to them. Therefore, cyber ranges or testbeds are usually built to provide a realistic environment suitable for training security and operations teams. A cyber range provides a place to practice correct and timely responses to cyberattacks. The learners can practice skills such as network defence, attack detection and mitigation, penetration testing, and many others in a realistic environment. The main reasons for cyber range creation determine the goals that we will achieve.

There are two main reasons why cyber defence range for armed forces should be built. The first one is critical need of state and military entities who are seeking staff development and skills training. The gap between trained cyber specialists and open cyber positions must be filled quickly. The existing staff must improve the skills in area of cyber defence to react to current threats.

The second main reason is importance of increase of university education level in the area of cyber defence given by armed forces academy. Cyber ranges focus on educational experiences that contribute to a student's academic experience and guarantee well prepared military personnel.

2. Cyber Range

2.1 What is a Cyber Range?

A cyber range is a virtual environment used for training and exercising in cyber security related areas. In cyber range environment, military and civilian personnel are trained in using both defensive and attacking tools, tactics, and strategies. A cyber range can also serve as test bed for developing cyber technology. Cyber range may be a virtual environment, but there are some alternatives. For instance, a hybrid cyber range is a combination of real and virtual components. This kind of cyber range is especially useful for cyber training of physical systems, such as embedded or industrial systems.

2.2 Cyber Range Examples

The DETER project was started in 2004 with the main interest of support cyber security research and education. Software Emulab which is used allow to create an integrated experiment management and control environment SEER. In the environment a set of traffic generators and monitoring tools are integrated and they have the ability to run a small set of dangerous experiments in a strictly controlled environment that enables research utility and minimizes risk.[2]

National Cyber Range (NCR) is a military facility to emulate military and adversary networks for the purposes of realistic cyber vulnerability testing, supporting training and mission rehearsal exercises.[3] The U.S. Department of Defense has been funded the development since 2009 and the target personnel are governmental organizations.[3]

Michigan Cyber Range (MCR) is an unclassified private cloud. MCR is controlled by a non-profit organization. The MCR has offered several services in cyber security education, testing and research since 2012. The MCR Secure Sandbox is used to create simulation of a real-world networked environment (web servers, database server, mail servers and several types of hosts.[4]

SimSpace Cyber Range (SSCR) enables the realistic simulation which can be composed of network components, network infrastructure, tools and threats. The SSCR is running as a service hosted in public clouds, at the dedicated data centre, or installed in the customer's network infrastructure. The users could use several types of preconfigured networks which simulate a variety of different environments.[5]

EDU Range is another cloud-based solution for preparing and realization interactive cyber defence exercises. EDU Range was developed by Evergreen State College in Washington. EDU Range is an open-source software with a web frontend based on Ruby and backend deploying virtual machines and networks hosted at Amazon Web Services.[6]

The Estonian cyber range project was started in 2011. The cyber range is under military command but it is a project financed by government. The main goal of this project is to support the development of Estonian cyber defence capabilities. The cyber range covers not only military requirements, but are also allows to realize national and international initiatives.[7]

2.3 Cyber Range Architectures

The cyber ranges discussed above could be classified on basis of infrastructure as public, private or federated. From architectural point of view a cyber range could be realized by several different approaches: host-based virtualization, local network virtualization and commercial offerings. There are many specialized providers that offer dedicated cyber ranges, virtual IT labs, and other platforms that are capable of servicing cyber security needs.

Cloud-based solutions are easier to implement and they are more popular in non-military applications. Their flexibility from point of view of customer is also better. Second choice is more suitable for military use. On-premise cyber security labs provide full control over technology and all training, but it is a more costly option.

2.4 Target Audience of the Cyber Range

Target audience or users of the cyber range can be divided into several groups: students, teachers, scientists and professionals.

- Students of the military university will apply their theoretical and practical knowledge in a simulated network environment.

- Teachers will use cyber ranges as special classrooms for teaching, training and evaluation their students. They have to motivate students to learn about cyber security.
- Scientists are required to think about worst-case behaviours and rare events, and that can be challenging to model realistically. Cyber security science must deal with inherently multiparty environments, with many users and systems.
- Professionals can be from different groups such as information technology, law enforcement, police, crime investigation, cyber security, incident response team, that use cyber ranges for improving individual and team knowledge and skills.

2.5 Cyber Range Main Tasks

A state-of-the-art solution of the cyber range must be a complex one, in order to improve all the expected skills of cyber-security experts. The trained personnel have to create analytical skills in different areas. The solution should cover these tasks: identification and mitigation of the cyber threats and vulnerabilities, detection and analysis of different attack patterns and fast response and full recovery of the attacked systems.

The conditions of training must be set as much as possible to real environment during the exercise. The simulated environment of created infrastructure must use comprehension of the parts of cyber-security domains. A cybersecurity defence model must be hybrid: the training scenarios should consist of more than one critical infrastructure from command post of brigade and division level to air and Special Forces units. The cyber range must also have ability to interconnect with other cyber ranges not only military but also civilian. Future cyberattacks will be aimed not only to military but also to civilian infrastructure, such as: power grid, transportation and banks.

3. Proposed Use of Cyber Range

Created cyber range can be used for several different applications. During its design and development, these three main use cases were identified:

- cyber security education and training,
- research and development,
- cyber security exercises.

All these use cases have a similar set of requirements on the cyber range, but they vary in task-specific tools, which must be used for solving a specific problem. Prepared content and required user interactions will be also different for specific task. We must also expect various knowledge, skills, and effort level of the students, teachers, scientists and professionals.

3.1 Cyber Security Education and Training

To realize education a huge amount of study content must be created in order to support a particular educational activity (presentations, exercises, etc). The first use case covers a selected type of educational activities (challenges, competitions, capture the flag games, and cyber exercises) and must support user interactions between students and teachers in the cyber range. It is important to put minimal requirements on the students' knowledge of the cyber range infrastructure and other technical details of the hardware solution.

3.2 Research and Development

State, military and also private companies have to respond to cyberattacks and predict risks. They must use the latest generation cyber defence solutions. Without a research and development in this area, we could not anticipate future threats and predict behaviour of cyber attacker or analyse his activity in our environment (communication and computer networks, industry and critical infrastructure).

The cyber range allows research and development of new methods for detection of malicious software, threats and behaviour. Cyber range provides optional monitoring infrastructure for experiments. Proposed methods can be tested in network infrastructures of the cyber range.

3.3 Cyber Security Exercises

Cyber security exercises allow participants to apply theoretical, practical knowledge and experience in a physical environment without fear of adversely affecting the deployed systems and equipment. Cyber security exercises are also important approach beyond pure training and drill. From point of view learning of security officers, there is no big difference between a prepared event and a real incident.[8] Executions of exercises can support verification of security procedures and plans. Also security policies can be validated and checked in the simulated environment. Cyber security exercise can help with testing communication and information technology and identifying gaps in resources. Before introduction of new equipment to the service specific tests must be done in secure environment. The techniques of active learning are applied to all participants, who have to be focused on exercise activities in a fast-moving, rapidly changing environment such as cyber security.[9]

4. Cyber Range Topology

The topology of proposed cyber range will be composed from 4 rooms, which is inspired by the three-room game concept used in modelling and simulation world. First room will be used for all server infrastructures. Blue team or personnel under cyber education will have one room equipped with desktop and mobile devices which will allow together with server infrastructure create model of defended network. Read team or attackers will have a separate room equipped with all tool to realize offensive operation (details in the next section). The last room will be used by analytics and staff preparing and directing the exercise.

From this room will be possible to manage, store and analyze all events of the training or education.

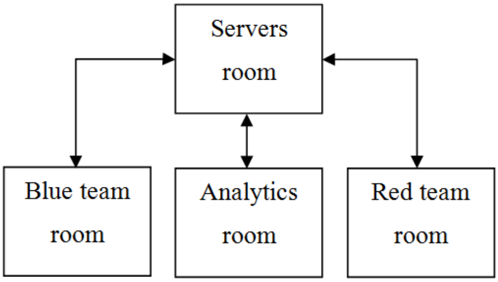

Figure 1: The Cyber Range Topology.

5. Tools Categories for Cyber Range

The importance of automation and sophisticated tools increases with increasing size and complexity of cyber ranges. The networks for cyber exercises should be built quickly and events for training which will be executed also should be described and planned precisely. After configuration of the network virtual users automatically perform the activities of real users to generate simulated network traffic. The analysis infrastructure will be used to monitor all executed events and can investigate in detail the results of those events. The cyber range to fulfil all tasks given on the base of proposed use should include following software:

- virtualization tools,
- security information and event management tools,
- analytical and forensic tools for desktop and mobile platforms,
- encryption tools,
- penetration testing tools.

6. Conclusion

Proposed cyber range can be used for supports multiple use cases (research, education and training). We would like to organize cyber exercises at university level at first and then we would like to cooperate with signal components to create cyber exercises for military units. Primary use from point of view of education will be hands-on security courses for students. They will receive realistic experience in cyber security.

Current work will focus on development of tools for the preparation and execution of cyber exercises and partial experiments. In the future cyber range can be connected to other facilities to create a more realistic cyber-physical environment. Cyber range will be a good platform for execution of sophisticated cyberattacks and provide a research environment for simulation, detection, and mitigation of cyber threats against critical infrastructure.

Acknowledgment

This research was supported by the Research and Development Program of the Slovak Republic 2015 granted by the Ministry of the Education of the Slovak Republic under No. OPVaV-2015/1.1/03-SORO VI20162019014 – Analysis and Simulation of Information and Security Threats Workplace.

References

[1] Dan Lohrmann, "Cyber Range: Who, What, When, Where, How and Why?" *Government Technology Magazine* 31, no. 2 (March 2018): 529–551.

[2] Jelena Mirkovic, Terry V. Benzel, Ted Faber, Robert Braden, John Wroclawski, and Stephen Schwab, "The DETER Project," in *IEEE International Conference on Technologies for Homeland Security* (HST '10), 2010.

[3] Bernard Ferguson, Anne Tall, and Denise Olsen, "National Cyber Range Overview," In *IEEE Military Communications Conference*, Baltimore, MD, USA, 2010, pp. 123–128.

[4] MCR, "The Michigan Cyber Range," https://www.merit.edu/cyberrange.

[5] Rossey Lee, "SimSpace Cyber Range," *ACSAC 2015 Panel: Cyber Experimentation of the Future (CEF): Catalyzing a New Generation of Experimental Cybersecurity Research*, Boston, United States, 2015.

[6] Richard Weiss, Franklyn Turbak, Jens Mache, and Michael Locasto, "Cybersecurity Education and Assessment in EDURange," *IEEE Security & Privacy* 15, no. 3 (2017): 90-95.

[7] Estonian Ministry of Defence, "Estonian Defence Force's Cyber Range," 2014.

[8] Tim Prior and Florian Roth, *CSS Study: Learning from Disaster Events and Exercises in Civil protection Organizations*, Risk and Resilience Reports (Center for Security Studies, Zurich, 2016).

[9] Lance Hoffman, Timothy Rosenberg, Ronald Dodge, and Daniel Ragsdale, "Exploring a National Cybersecurity Exercise for Universities," *IEEE Security and privacy* 3, no. 5 (2005): 27– 33.

About the Author

Michal **Turčaník** is an associate professor at the Department of Informatics at the Armed Forces Academy in Liptovsky Mikulas. He has been teaching different subjects for more than 20 years. He is a Panel Member of the STO IST organization for the Slovak republic. His scientific research is focusing on reconfigurable logic, artificial intelligence and computer networks.