# Analysis of cyber exercises approaches

© Volodymyr Mokhor[1][0000-0001-5419-9332], © Vasyl Tsurkan[2][0000-0003-1352-042X] and © Valeriia Pokrovska[2][0000-0002-1318-5521]

[1] Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine
[2] Institute of special communication and information protection National technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
v.mokhor@gmail.com, v.v.tsurkan@gmail.com, Hilariyap@gmail.com

**Abstract.** Raising awareness of the organization's employees comes down to cyber exercise. They can target both an individual employee and specialists in general. This is implemented mainly in four stages of organization of the cyber exercises. In the first stage, the purpose, scenarios, evaluating system of results for their execution are defined, and scenario-modeling environment is established. It is tested for compliance with the purpose of cyber exercises within the second stage. In the third stage, cybersecurity scenarios are being developed. The results of the execution are evaluated in the fourth stage. This is due to the relevance of the analysis of approaches to the organization of cyber exercises. In solving this problem, it was established that there was no uniform interpretation of this concept. First, such ambiguity of interpretations is associated with the direction of cyber exercises. Therefore, approaches to their organization are focused on obtaining theoretical knowledge, practical skills, and cybersecurity skills. Primarily, an incident detection and prevention approach is common. Another common approach is assessment of cybersecurity through penetration testing. The application of these approaches can be generalized and organized as a game.

**Keywords:** cybersecurity, scenario, incident, cyber exercises, cyber exercises approaches.

## 1 Introduction

An important element of promoting and maintaining cybersecurity in an organization is knowledge and awareness of existing threats types and real attacks on critical infrastructure. [1]. Cyber exercises are organized through awareness-raising programs for cybersecurity organizations. [2]. It mainly comes down to training in an interactive form and is characterized by orientation both for the individual employee and for specialists as a whole.

There are four stages in the organization of cyber exercises [1-3]. In the first stage, goals, scenarios, evaluating system of results for their execution, and the scenario-modeling environment are established. The environment is being tested for compliance with

the goals of cyber exercises in the second stage. In the third stage, established cybersecurity scenarios are being worked out, while the results of their execution are evaluated at the fourth stage [3]. Depending on the purpose of cyber exercises and the training level of organization employees, it can be organized using different approaches.

## 2 Cyber exercises approaches

Now there is no unified interpretation of the “cyber exercises”, concept for example: “cyber training”, “cyber range”. Sometimes “cyberlearning” term is used, particularly, when organizing remote cyber exercises. It is focused primarily on obtaining theoretical knowledge. Unlike “cyberlearning”, a characteristic feature of “cyber training” and “cyber range” is the focus on obtaining of practical cybersecurity skills [1-4].

Such terms as “cybersecurity exercises”, “cyber defense exercises” are often used as interchangeable, and describe cyber exercises as processes for preparing, evaluating, practicing, and improving the effectiveness of the organization to ensure cybersecurity [4]. They cover large-scale computer modeling activities, as well as tabletop exercises, for example, prepared possible scenarios card.

In military terms “drills” and “exercises” sometimes refer to similar activities, especially when it comes to training sessions [4]. The term “drills” is used to describe systematic training in the use of techniques or tools by performing exercises repeatedly. The repetitive, systematic nature of tasks as "drills" distinguishes them from other types of exercises.

A typical approach to organizing cyber exercises is characterized by the acquisition of skills and abilities to respond to cybersecurity incidents. First, they focus on both their detection and prevention of manifestation in future activities [4]. In addition, it is possible to focus on assessing cybersecurity through penetration testing. This is the basis of an approach to identifying information vulnerabilities in cyberspace [5], including the use of social engineering [6]. At the same time, the use of a game approach to organizing cyber exercises is common. Within its framework, two teams are distinguished – attackers and “victims” [2].

### 2.1 Defense Oriented Approach

The specificity of each of the known approaches to organizing cyber exercises is determined by their purpose and focus, and depends on the training level (qualifications) of the organization’s specialists. Among them, an approach that focuses on responding to cyber incidents and reducing the consequences of their manifestations stands out. Therefore, cyber exercises are carried out to practice protection methods that can be used in responding to cybersecurity incidents. Defense Oriented Approach for cyber exercises is one of the most promising approaches to cybersecurity [1, 7].

Raising the awareness of the organization’s employees is achieved through various forms of cyber exercise, in particular, progressive, specialized and individual. This allows participants to test their knowledge, ability, and cybersecurity skills. Among the common forms of cyber-training, the following ones stand out [7]:

1. Tabletop exercises – this is a scenario-based discussion that validates proactive countermeasures against simulated cyber incidents. For example: Elevation of Privilege (EoP), EoP card game helps to study possible threats to software and computer systems, Cyber Atlantic exercises conducted by ENISA, Cyber 9/12 Challenge tabletop activity to developing national security policy recommendations for cyber incident scenario. These exercises validate cybersecurity plans to identify vulnerabilities and determine how to handle them.

2. Simulation exercises – these are practical training sessions in which cyber incidents are simulated. For example: Cyber Coalition, Cyber Europe exercises conducted by ENISA. Practical activities allow participants to see the effects of cyberattacks in a controlled environment.

3. Full scale Exercises – these are challenging exercises that are designed to provide practical skills in real time. For example: Locked Shields and Baltic Shields exercises. This type of simulation is realistic, it allows you to check cybersecurity plans, security policies [8]. Their main purpose is to analyze and test methods of countering cyberattacks.

The Defense Oriented Approach is more about system administration and digital forensics. Participants of cyber exercise who seek to defend themselves against cyber incidents and their consequences should be aware that defense activities are a continuous process that can be represented by a sequence of such actions [ 7]:

1. Creation of a security policy – Involves the use of various tools to eliminate vulnerabilities. Encryption methods can be used to hide the transmitted data through channels exposed to dangerous influences. Systems with known security vulnerabilities should be kept up to date by the remediation of them. Ensuring physical security provides for reliable storage of equipment.

2. Security status monitoring – Plays a critical role in determining how effectively security policy requirements are met. This is achieved by using, for example, intrusion detection and prevention systems. They can be considered as an effective solution for monitoring unwanted traffic.

3. Testing of security measures is seen as the only way to convince the implemented means to maintain the security policy. The purpose of security measures testing is to identify all possible loopholes and weaknesses of the software system, which might result in a loss of important information.

4. Improving security assurance – achieved by considering vulnerability reports and security advisories that help keep abreast of new potential attacks. Monitoring, testing, and identifying vulnerabilities is critical to refining and tuning security policies.

Such actions are considered as the basis for the presentation “Security Wheel” (see, for example [7], Fig. 1). They should be used to ensure the security of information assets, to track them by stages of the life cycle. Due to this, it is possible to timely detect attacks and, most importantly, reduce their occurrence and, as a result, improve security configuration.

In the Defense Oriented Approach, there are at least three ways to organize exercises for cyber exercises participants [8]:

1. Obtaining requirements and services that must be provided and / or developing their own measures, means to meet them.

2. Obtaining the default settings for certain systems, programs, or services that must be provided and configured to meet security requirements.
3. Access to the installed and configured systems, programs, services whose security must be ensured. In this approach, the attacker can be seen as an instructor or an external party.

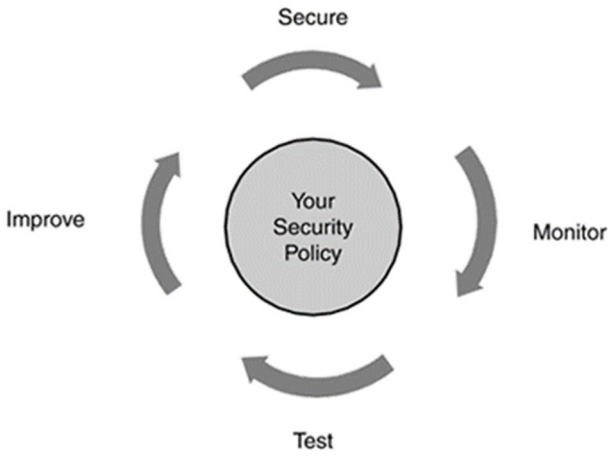


**Fig. 1.** "Security Wheel".

An example of using Defense Oriented Approach is Blue Teaming exercise. It is designed to train the team, which must ensure the security of pre-configured and secure infrastructure. Red Team real or automated (in the form of scenarios), prepares a training scenario in accordance with the set goal.

Obtaining theoretical knowledge and skills of cyber defense (cyber defence exercises, CDX) are among examples of cyber exercises. The main focus is on cybersecurity defense tasks. In particular, conducting forensic investigations and practicing security configuration skills, such as networking.

The Cyber Europe exercises focus on simulating manifestations of large-scale security incidents that could lead to a cyber crisis. The training offers opportunities for digital forensic analysis (e.g. of incidents or malware), as well as solving complex business continuity situations and overcoming cybercrises.

## 2.2 Offense Oriented Approach

Computer systems can be compromised in various ways, and countering complex and persistent attacks consists of understanding the sequence of possible malicious actions and thinking of the attacker. Exercises within the Offense Oriented Approach, namely Red Teaming, support the development of security measures and tools given the complexity of attacks. That is why this approach to organizing cyber exercises is focused on practicing proactive cyber security mechanisms. Such exercises usually simulate the protection of critical infrastructure from cyber security incidents [7, 9].

Most of the exercises in this approach to organizing cyber exercises involve operating servers and performing penetration tests on target systems. Starting with target system recognition, vulnerability detection and assessment, cyber security participants check security violations, try to use them to achieve the goal of conducting a scenario to access the target system [6, 9]. Maintaining access to the system and introducing hidden command and control systems ensures the effectiveness of cyber exercises. Testing security plan, measures, and procedures implemented by simulating attacker behavior can improve security.

Participants in cyber exercises should master the offensive model of behavior to ensure cybersecurity. It helps to better understand how to defend against cybersecurity incidents. At the same time, there is a need for a deep understanding of how to conduct attacks in order to know how to mitigate them and minimize possible losses. Therefore, the Offense Oriented Approach encourages participants to view the exercises as attackers (intruders). They will have to conduct attacks to accomplish various tasks. Simulating real attacks is reduced to performing a sequence of steps, namely (see, e.g. [9], Fig. 2):

1. Reconnaissance.
2. Weaponization (takes into account the received information during reconnaissance, creation of malicious software).
3. Delivery (detection of vulnerabilities for the threats implementation).
4. Exploitation (realization of threats due to identified vulnerabilities).
5. Privilege escalation (exploiting a bug, to gain elevated access to resources).
6. Lateral movement (when an attacker moves from a compromised device to others on this network).
7. Command and control.
8. Exfiltrate and complete (data extraction, placement backdoors).


**Fig. 2.** Red Team Actions

In Offense Oriented Approach, a system that is preconfigured for known vulnerabilities can be affected. At the same time, most of them do not necessarily have to be guided by someone during the attack.

Using Red Teaming as a cybersecurity training exercise can be an effective way to gain the decision-making skills and abilities needed to detect and counter cybersecurity incidents. Red Teaming exercises may involve the use of a set of available methods and tools, or may develop a response to unforeseen situations. Offense Oriented Approach to organize cyber exercise is extremely useful for testing infrastructure and systems, identifying security vulnerabilities, and configuration errors when learning to counter

cyberattacks. During cyber exercises, it is important to understand the possible consequences. The closest thing to cyberattack training is the format of so-called "ethical hacking", which may also be called pentesting and Red Teaming.

Examples of the "offensive" type international cyber exercises are Locked Shields, Cyber Coalition, Baltic Cyber Shield. These cyber trainings are focused on improving technical skills for response, cyber investigations, proactive response to cyber incidents in order to protect critical infrastructure.

### 2.3 War Game Approach

The approach chosen for cyber exercises should depend on their intended purpose. As a rule, they are designed to provide theoretical knowledge and practical skills to security administrators. This is realized through the use of the Defense Oriented Approach. Whereas penetration testing exercises are based on Offense Oriented Approach. However, a mixed approach, namely the War Game Approach, is advisable for a comprehensive cyber exercise.

The Mixed Approach combines the Defense Oriented Approach with the Offense Oriented Approach. Thus, its complexity is achieved when performing exercises with cyber defense. In this case, the participants of the cyber exercise are divided into two teams. The first plays the role of a defender ("victim"). The second reflects the role of attackers (intruders).

An example of cyber exercise that combines offensive and defensive approaches is the CTF competition (Capture the flag) [10]. These training exercises give participants the opportunity to feel the role of an attacker or a defender. They can test their abilities in solving cybersecurity problems. They provide for the detection of vulnerabilities, exploit implementation, data protection, forensics. Fulfillment of tasks is evaluated by the gain in the form of "flags". In particular, a file with a unique string of special characters [11]. Checking the "flags" in the system allows setting grades depending on the complexity of the tasks.

There are two main formats of CTF [11]:

1. Task-based (Jeopardy) – training is reduced to solving as many problems as possible in different areas (digital forensics, web application, cryptography, mobile Security)
2. Attack-defense – training is reduced to the protection of, for example, the network, server, confidential information and maintaining the functionality of intended services at the same time as the implementation of attacks aimed at violating services is carried out by the enemy team.

Participants in cyber exercises are involved in scenarios, and the team of attackers uses real tools of operation and penetration to attack the virtual network. The defense team monitors the state of the network and network equipment and protects the network, they can also practice counterattacks against the red team. A group of people, known as the white team, create the training environment and control the cyber training. They establish a set of rules for interaction between the red and blue teams and sometimes act as instructors to give tips to exercise participants in cyber training.

## 2.4 Cyber exercise tools

The use of tools in organizing cyber exercise is mostly reduced to such options:

1. Simulation tools – tools that allow you to conduct practical training sessions, for example [10]: online platform, cyber training range. They simulate cyber incidents, the response to which is expected in real time.
2. Tabletop tools – toolboxes that are allowed to conduct cyber exercise based on discussion, for example [12]: cards with the exercise scenario, quiz. Participants gather and discuss their role in an emergency (cybersecurity incident) and possible response options.

Both types of cyber exercise tools have their advantages and disadvantages. Full-scale modeling may involve the use of virtual network environments that allow exercise participants to monitor the manifestations of cybersecurity incidents. However, this requires a lot of resources and detailed planning. At the same time, tabletop tools should use a small period of time, taking into account the need for concentration. Because they are focused on discussions and therefore the sense of urgency and realism in modeling is lost.

If special skills are not required to prepare for the use of tabletop tools, then the use of simulation tools is due to the presence of theoretical knowledge and skills in setting them up. However, despite this, it is now common to simulate real-world situations using appropriate hardware and software. Developing realistic and scalable scenarios becomes important for effective cyber exercises. An example of such cyber exercise tools is [10]:

1. Hardware cyber range, although realistic, but large-scale, expensive and time-consuming to set up. Due to its cost, the number of exercise participants who can be trained in any of the scenarios of cyber threats is limited. In addition, it limits the total number of cyber exercise participants over a set period of time. We should also mention the wired cyber range, which is characterized by the complexity of modeling wireless tactical networks with their inherent vulnerabilities.
2. Virtual cyber range is considered as a simulation environment that provides real-time hardware and software for the implementation of cyber threats to the network infrastructure [2]. It is closely integrated with physical equipment, programs, network monitoring tools, intrusion detection and prevention systems and structural modeling "battlefield". This provides cybersecurity skills and countermeasures against cyberattacks (see, e.g. [13], Fig. 3). Simulation is about presenting a real system with an analog that is easier to manage, providing the same functionality, without reference to a specific location and equipment.

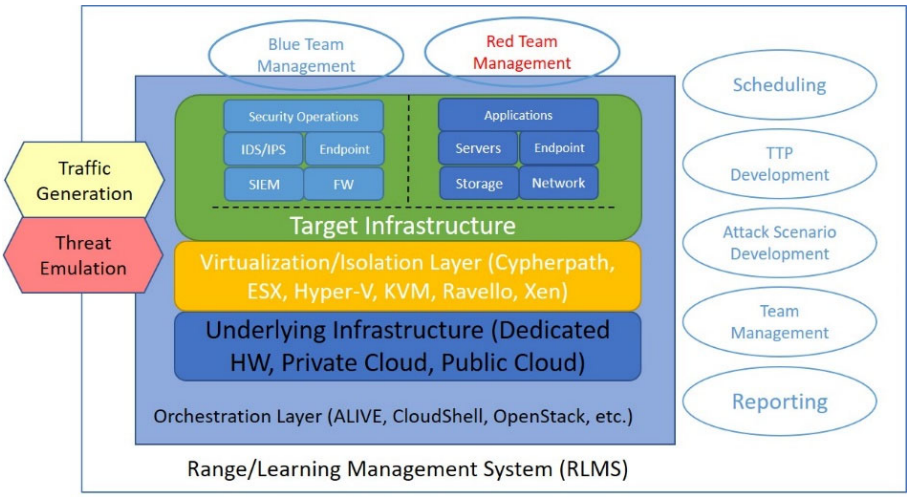


**Fig. 3.** General cyber range model

The general cyber range model of a cyber exercise site is defined by the following components [2, 13]:

1. Orchestration Layer – layer that uses input data from RLMS. It is designed to orchestrate cybersecurity tools. At the same time, it integrates the technology and service components of the cyber range.
2. Underlying Infrastructure – level of infrastructure, which determines the realism and accuracy of the cyber range. In addition, ways of generating traffic and modeling attacks are used.
3. Virtualization Layer – layer, which is defined as a firewall between the target and underlying infrastructures. Whereas the target infrastructure is considered relative to the feasibility of attacks.
4. Target Infrastructure – a simulated environment in which cyber exercise participants training. Based on the purpose of their organization, scenarios will be generated to create the target infrastructure at the orchestration level. A scenario may contain configuration-specific information, including IP address ranges, routing information, server stacks, and software.

The approaches to organizing cyber exercises are analyzed in Table 1, taking into account the peculiarities of their use and the relevant tools (see Table 1).

**Table 1.** Analysis of cyber exercises approaches

| S. No | Formulation of the approach | Features of using the approach | Tools |
|---|---|---|---|
| 1. | Defense Oriented Approach | Focuses on countering manifestations of cybersecurity incidents and preventing their consequences. Acquires cybersecurity skills and abilities. Pre-prepared scenarios are used. | cards with the exercise scenario, quiz, virtual cyber range |
| 2. | Offense Oriented Approach | Proactive cybersecurity measures are practiced. Counter-attack skills are obtained to counteract the feasibility of cyber incidents. Pre-prepared scenarios are used. | virtual cyber range, online platform |
| 3. | War Game Approach | Combined Defense Oriented Approach with Offense Oriented Approach. Assumes division of participants into teams (e.g., "victim", ttacker, mentor). There are no pre-prepared scenarios. | virtual cyber range, online platform |

## Conclusion

Thus, the organization of cyber exercises is accompanied by the use of various concepts. Each of them determines their specificity, taking into account the orientation of both the individual employee and the specialists as a whole. Such features determine the choice of approaches to the organization of cyber exercises. In particular, they can focus on individual cybersecurity tasks, for example, on incident response ("Cyber defense"), cybersecurity assessment ("Compensation Testing"), or reduction of the number of solutions to the game ("War game").

## References

1. Seker, E., Ozbenli, H.: The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). pp. 1-9, IEEE, Glasgow, Scotland, UK, (2018) https://doi.org/10.1109/CyberSecPODS.2018.8560673, last accessed 2020/18/11.
2. Yamin, M., Katt, B., Gkioulos, V.: Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. Computers & Security, vol. 88 (2020), https://doi.org/10.1016/j.cose.2019.101636, last accessed 2020/11/10.
3. Kick, J.: Cyber exercise playbook. The MITRE Corporation, Wiesbaden, Germany (2014).
4. Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P., Tovarnak, D.: Lessons learned from complex hands-on defence exercises in a cyber range, In: IEEE Frontiers in Education Conference (FIE). pp. 1-8. IEEE, Indianapolis, IN, USA, https://doi.org/10.1109/FIE.2017.8190713, last accessed 2020/11/10.
5. Matania, E., Yoffe, L., Goldstein, T.: Structuring the national cyber defence: in evolution towards a Central Cyber Authority. Journal of Cyber Policy, vol. 2, no. 1, 16-25 (2017), https://doi.org/10.1080/23738871.2017.1299193, last accessed 2020/11/10.

6. Mokhor, V. V., Tsurkan, O. V., Tsurkan, V. V., Herasymov, R. P.: Information Security Assessment of Computer Systems by Socio-engineering Approach. In: Proc. XVII International Scientific and Practical Conference Information Technologies and Security: selected papers. Vol. 2067. Aachen, Germany: CEUR WS, 2017. pp. 92-98, http://ceur-ws.org/Vol-2067/paper13.pdf.
7. Patriciu, V. V., Furtuna, A. C.: Guide for designing cyber security exercises. In: Proceedings of the 8th WSEAS International Conference on E-Activities and Information Security and Privacy, pp. 172–177. World Scientific and Engineering Academy and Society, WSEAS (2009).
8. Knüpfer, M., Bierwirth, T., Stiemert, L., Schopp, M., Seeber, S., Pöhn, D., Hillmann, P.: Cyber Taxi: A Taxonomy of Interactive Cyber Training and Education Systems. Model-driven Simulation and Training Environments for Cybersecurity, vol. 12512, 3-21 (2020), https://doi.org/10.1007/978-3-030-62433-0_1, last accessed 2021/16/01.
9. López de Jiménez R.: Pentesting on web applications using ethical – hacking. In: IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI), pp. 1-6. IEEE, San Jose, Costa Rica, https://doi.org/10.1109/CONCAPAN.2016.7942364, last accessed 2020/11/10.
10. Dewar, Robert, S.: Cybersecurity and Cyberdefense Exercises, CSS Cyber Defense Reports, Center for Security Studies (CSS), ETH Zurich, (2018), https://doi.org/10.3929/ethz-b-000314593, last accessed 2020/18/11.
11. Cowan, C., Arnold, S., Beattie, S., Wright, C., Viega, J.: Defcon Capture the Flag: Defending Vulnerable Code from Intense Attack. In: Proceedings DARPA Information Survivability Conference and Exposition. vol. 1, pp. 120-129, Washington, DC, USA, https://doi.org/10.1109/DISCEX.2003.1194878, last accessed 2020/12/18.
12. Angafor, G., Yevseyeva, I., He, Y.: Game-based learning: A review of tabletop exercises for cybersecurity incident response training. Security and Privacy 3(6), 117-131 (2020), https://doi.org/10.1002/spy2.126, last accessed 2020/23/12.
13. National Initiative for Cybersecurity Education (NICE). The Cyber Range: A Guide. Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification and Training, https://cutt.ly/8kipFaN, last accessed 2020/23/12.