POSTMODERN EDUCATION AND TECHNOLOGICAL DEVELOPMENT. CYBER RANGE AS A TOOL FOR DEVELOPING CYBER SECURITY SKILLS

Ella Ciupercă, Alexandru Stanciu, Carmen Elena Cîrnu

National Institute for Research and Development in Informatics (ROMANIA)

Abstract

Education systems have undergone profound transformations in response to changes in both the workplace and society. In the context of a permanent diversification of the challenges facing education in a world where the pace of change is more accelerating than ever, technology-facilitated learning has become an important part of the education/training system for both educational institutions and for companies that want to train their staff. Technology-facilitated learning systems are increasingly present in the lives of corporations and in the education system because they offer what the study of different disciplines in a traditional way fails - constantly and permanent connection with the needs of the labor market in accordance with the latest technological developments. Cybersecurity is an example that has become even more important after the migration of many activities in the digital space because of the SARS COV 2 pandemic. In the field of automated command and control systems, there is an important need for cybersecurity competencies as such equipment manages the proper functioning of many critical infrastructures.

Deterioration of critical infrastructure because of cyber-attacks can have a significant impact on national security, the economy, and the livelihoods and security of all citizens. Learning instruments like cyber range can play an extremely important role in developing the ability to defend against threats in cyberspace. By means of cyber polygons, the manifestation of these attacks can be studied in conditions of minimizing the costs involved in security simulations and tests. Because they are controlled virtual environments, the results of simulations and performance tests can be recorded, analyzed, and reproduced to prevent further failures and errors, and thus cyber range can contribute to increasing the agility and responsiveness of IT security solutions. They can be developed and installed both at the government level and in business organizations and research centers to solve complex problems and test new ideas. In this paper, we will comparatively analyze the main dimensions and functionalities of training in cybersecurity through cyber-range solutions, having as a premise the importance of understanding the indestructible dyad competencies of ensuring cybersecurity - ability to ensure national security.

Keywords: Education systems, e-learning, cybersecurity, cyber polygons.

1 INTRODUCTION

Educational technology refers to the use of tools, technologies, processes, procedures, resources and strategies to improve learning experiences in a variety of ways, such as formal learning, informal learning, non-formal learning, lifelong learning, on-demand learning or on-the-job learning. Although technology is finally integrated into education, its use for teaching and learning remains a challenge.

By integrating technology into education, educators aim to generate pedagogical changes and address fundamental issues that affect students. Therefore, technology can be considered both a tool and a catalyst for change. Today, the technologies used to improve and facilitate learning can be found everywhere. Leaving aside other contextual factors - such as unequal access to technological innovations - we can say that technology is part of education when it is used for both teaching and learning. Once incorporated into schools, the main purpose of technology is to change the way teachers and students gather, access, analyze, present and transmit information [1].

The concept of cybersecurity is closely linked to how an organization assesses and manages operational risks. The risk is often correlated with vulnerabilities that may exist, for example those related to the business environment, IT infrastructure, automation and control systems, but also physical assets that may be under the direct control of a previously mentioned system.

The overall process of implementing cybersecurity controls is meant to reduce business risk. However, if an organization does not properly plan its exposure and risk tolerance, then the overall effectiveness

of these controls is much lower than initially expected. The development of cybersecurity in terms of security policies, administrative procedures, business processes and technological solutions aims to target certain identified risk areas and reduce the impact on an organization if a cyber event is aimed at one of its assets. If an organization fails to identify risk areas, then it may not be able to properly select, implement and measure security controls to reduce these risks.

Cyber-attacks are designed to be as difficult to detect as possible and use unknown vulnerabilities that cannot be protected. Examples as Stuxnet and Flame are well known, both attacks being carried out over long periods of time without being detected, although payload URLs of these were designed for different purposes: Stuxnet was designed to induce irreversible damage to the centrifuges for enriched uranium, and Flame was designed to collect security information that would allow subsequent cyber-attacks.

From the previous examples it is obvious that cybersecurity activities require both human skills and advanced technological solutions. Therefore, organizations need tools that facilitate the automatic detection of anomalies, graphs for monitoring system parameters, but also qualified human resources equipped with high cybersecurity competencies.

2 CONTEXTS OF THE LEARNING PROCESS AND THE NEED TO USE EDUCATIONAL TECHNOLOGIES

The industrial age has initiated a series of innovations, but many changes have been introduced by the current information society. Schools have faced various challenges in redefining their goals, taking into account the differences in social status, race, age and sex of the students concerned, time and space considerations, but also constraints related to available resources, according to the analysis conducted in [2]. According to this study, society, as such, recognizes the special importance of education as quality education can be the most powerful tool available for relaunching economic growth, improving competitiveness and promoting social inclusion.

Research in the field suggests that countries that are concerned with ensuring the highest possible level of education for the population manage to grow and develop economically, while countries that have a low level of performance of the education system face economic stagnation. A higher skilled workforce can get correspondingly higher salaries. Countries with a large number of professionals, especially in science, engineering and mathematics, tend to compete successfully in the global economy. It is recognized that the level of education has a strong impact on both the social and political spheres, including the level of health and economic well-being.

Promoting the culture of innovation remains another long-term trend, and here it plays a key role and reflects the role of the educator in encouraging innovation, creativity and entrepreneurial thinking.

In [3], Mayer proposed some principles of multimedia learning that can also be used to guide the selection of technology for educational use:

- Adequacy principle: technology should promote the general and specific objectives of the class; the technology should be appropriate to the desired level, including vocabulary level, the difficulty of concepts, methods of development, appeal to interests; the technology should be basic or additional to the curriculum; the principle of authenticity; technology must provide accurate, up-to-date and reliable information.
- Cost principle: replacements and trade-offs of alternative solutions must be considered.
- The principle of interest: technology should attract the interest of students; it should stimulate curiosity or satisfy the student's need to know; technology should have the power to motivate, encourage creativity and imaginative response among users.
- The principle of organization and balance: technology must be well organized and well balanced in content; the purpose of the material must be clearly stated or perceived; there should be a logical, clear organization in accordance with the principles of learning, such as reinforcement, transfer and application in materials.

In order to be able to make a comprehensive comparison of the two forms of learning, it is necessary to go through the main differences between the processes of the two forms of learning (Table 1), comparing several essential aspects between them.

Table 1. Differences between traditional learning and e-learning processes [4]

The traditional learning process	*The e-learning process*
The presentation is made face to face.	Uses multimedia as a type of communication.
The instructor follows all the students.	Using online technology.
The instructor was physically in the classroom.	Changing knowledge between students and with the instructor.
Distribution of time in short time intervals among a large number of students.	More free time considering the location and when connecting.
The instructor focuses on gaining "Knowledge."	The instructor focuses on acquiring "doing" skills.

3 METHODOLOGY

3.1 The characteristics and architecture of the modern cybernetic polygon

As cybersecurity concerns are on the rise, cyber polygons have an important role to play in the fight against cybercrime, as well as in developing cybersecurity defense capabilities. They can be developed and installed both at the government level and by business organizations and research centers to solve complex problems and test new ideas. They are also used for real-time evaluation of the performance of various security solutions.

The cyber polygon provides the environment for teams of professionals to work together in several areas of security, to improve their skills and to develop methods of defense against various attacks. The range of competencies can cover areas such as penetration testing, defense of communication networks, strengthening of critical infrastructures and methods of response to attacks. By means of cyber polygons, the manifestation of these attacks can be studied in the conditions of minimizing the costs involved in security simulations and tests. Because they are controlled virtual environments, the results of simulations and performance tests can be recorded, analyzed, and reproduced to prevent further failures and errors. Thus, they contribute to increasing the agility and responsiveness of IT security solutions.

It is necessary to develop support platforms for exercises that have a set of technical means to simulate various types of critical infrastructure. These means include the ability to visualize the challenges and responses that manifest on the simulated cyber-physical battlefields (CPB). Also, they should use various technical elements to express the physical properties of cyber-physical systems and the damage that can be caused by a cyber-attack on them. The platforms should be sufficiently extensible to represent different elements of critical infrastructure on the same platform and to allow cross-domain integration of different infrastructure sectors.

Cybersecurity virtual labs are a solution currently used to improve efficiency in cybersecurity training as well as response time in cybersecurity exercises. Online virtual security labs use real-world scenario simulations to provide a practical user experience. This type of laboratory-based virtual security training is proving superior to traditional methods such as on-site classrooms, training videos, and other less effective training methods.

There are several benefits to online cybersecurity labs that can be considered:

- Are cheaper because the virtual labs run online, there is no need to organize physical classrooms, coordinate instructor and employee programs, and there are no installation costs for local hardware and software, such as expenses incurred by trainers'/trainees' travel.
- Offer a tangible and practical experience. There is no better way to learn than through the experience of a simulated attack. Students can learn how to react to a threat, develop processes for eliminating threats, and how to interact with a cyber polygon.
- Are safe and secure. Because simulations run on remote servers, virtual environments are easily reusable and separate from the real network.
- Always up-to-date in terms of knowledge about threats, as the cybersecurity training service provider deals with training, with the maintenance of educational content.
- Are scalable. Adding more students to an online class is much easier than expanding a physical class.

- Provide instant feedback. The instructors have constant direct contact with the participants through online messages and chat and video conferencing applications.

3.2 Comparative analysis of cyber range solutions suitable to be used in the educational process

We have previously demonstrated the usefulness of using cyber polygons in the educational process from many points of view. Next, we perform a comparative analysis of suitable solutions to be used in the educational process of building cybersecurity competencies for ICS infrastructures' operators.

First, we build the analysis grid by identifying a series of functional criteria from the perspective of which all technological products were compared. The identified criteria reflect aspects and functionalities that we considered relevant from the perspective of the project purpose and the existing solutions in the market. As the criteria do not require YES / NO answers, but involve some details from which to result the estimated degree of compliance of the solution, we gave a score that allows a better visual representation of the information, so that graphic display elements can reflect the appreciated conformity of each analyzed solution.

The criteria were applied to the analyzed products and services, identifying a series of conformities or non-conformities in the educational process. Such solutions allow on-site education but also e-learning simulations. There are situations in which the conformity of the products to the functional criteria is partial, which will be reflected in the following compliance table.

Although some analyzed solutions do not offer explicit functionalities of ICS cybernetic polygon, they were included in the study being of interest, as already mentioned, from the perspective of the identified criteria and the diversity of technological solutions in the global free market.

An analysis was made on the technologies available globally, as follows:

- Cyberbit Range, a generic cyber polygon solution commercially offered by CyberBit, which can operate in the cloud or on-premises (https://www.cyberbit.com/solutions/cyber-range/);
- NI LabView, a generic modeling and simulation solution for ICS type technologies, offered commercially by the company National Instruments (https://www.ni.com/ro-ro/shop/labview.html);
- CaSTLE (Cyber Security Training and Learning Environment), a generic cyber polygon solution offered as a service by the Austrian Institute of Technology (https://cyberrange.at/);
- Raytheon CODE (Cyber Operations, Development and Evaluation) Center, a generic cyber polygon solution, offered commercially as a service by Raytheon (https://www.raytheon.com/cyber/capabilities/range);
- Silensec Cyber Range, a generic cyber polygon solution, offered under a free or commercial license by the Silensec Group company, which can operate in the cloud or on-premises (https://cyberranges.com);
- Dragos Platform, a cyber polygon solution, commercially offered by Dragos (https://dragos.com/platform/);
- Virtual Cloud Arena, commercially offered by CyberGym (https://www. cybergym.com/virtual-arena/).

The analysis was performed considering the following aspects of the virtual polygons considered relevant by us from the project perspective:

- Flexible architecture: consists of the possibility to define and use different technological architectures containing different technological elements. Modifying a defined architecture leads to the creation of a new architecture without overwriting or modifying the source architecture in all projects.
- Architecture segmentation: consists of the possibility to segment a virtually modeled ICS system into functional segments such as functional modules, technological level (e.g., ICS equipment, rules, commands), electronic communications level (e.g., data network, equipment, rules, commands), data presentation level (e.g., HMI, management applications, etc.), cybersecurity level (e.g., firewalls, security sensors, etc.), management level (e.g., virtual modeled system management, logos, user management), level of scenarios (e.g., various scenarios that allow the simulation of situations that may occur in the real ICS system).

- High fidelity: consists of the possibility to facilitate the detailed replication of the virtual modeled ICS system. Replication will go as far as the functionality of the equipment contained.
- Reuse of objects: consists of the possibility to reuse existing technological elements in several projects/simulations, maintaining the technological and functional characteristics. Modifying the functional and technological characteristics of an object leads to the creation of a new object without overwriting or modifying the source object in all projects.
- Standardization: consists of the possibility to ensure the interoperability between the technologically compatible virtual equipment and/or of the data. The system will allow the addition of new technological standards or electronic communications and data exchange.
- Modeled scenarios: consists of the possibility to create, modify and apply in the virtual environment of the cyber polygon, cyber-attack scenarios on some target ICS systems. Scenarios can be modified and saved, and modifying one scenario leads to the creation of another, without overwriting or modifying the source scenario in all projects. The cyber-attacks contained in the scenarios will replicate the characteristics of the cyber-attacks carried out in similar real conditions.
- Real-time simulation: consists of facilitating the observation in real-time, in the simulated environment according to the applied scenario, of the changes that occur in or on the target ICS system.
- ICS cybersecurity: consists of the inclusion of functionalities dedicated to modeling and simulation of scenarios specific to the cybersecurity of industrial control systems. The functionalities can be customized in simple or complex scenarios that include types of cyber-attacks against ICS systems.

4 RESULTS

We further present the table of conformity of technological solutions related to the relevant functional criteria, coring each of our criteria for the chosen cyber range solution, where 1 is the lowest score and 5 is the highest.

Table 2. Comparative analysis of cyber range solutions

	Cyberbit Range	***NI Labview***	***CaSTLE***	***Raytheon CODE***	***Silensec CR***	***Dragos Platform***	***Virtual Cloud Arena***
Flexible architecture	5	5	5	5	5	3	5
Architecture segmentation	5	5	5	5	5	3	5
High fidelity	5	5	5	5	5	3	5
Reuse of objects	5	5	5	5	5	5	5
Standardization	5	5	5	5	5	5	5
Modeled scenarios	5	3	5	5	5	4	5
Real-time simulation	5	5	5	5	5	3	5
ICS cybersecurity	5	3	5	3	5	4	5
Total score	35	31	35	33	35	29	35

As can be seen, four of the technological solutions analyzed fully meet the functional criteria considered relevant for the process of developing cybersecurity skills: *Cyberbit Range, CaSTLE, Silensec CR,* and *Virtual Cloud Arena*. Also, the Raytheon CODE solution is very close to meeting the relevant criteria and has a higher score than the National Instruments LabView solution. While LabView is not a dedicated cybersecurity solution, instead of meeting all other criteria, the CODE solution is a cyber-polygon for ICT infrastructures and networks, currently having lower functionality and limited scenarios for ICS infrastructures, being less efficient from the national security point of view, in spite of its high score is.

In nowadays context, when cyber-attacks are multiplying at an unprecedented rate, a national strategy on cybersecurity education is necessary and cyber ranges should be an important part of the process. The purpose of a cybersecurity exercise is to assess national preparedness for cyber threats and to improve the cyber defense capacity of national combatants [5]. A current trend in current cybersecurity

exercises is to place much more emphasis on scenarios where critical infrastructure needs to be protected. Deterioration of critical infrastructure through cyber-attacks can have a significant impact on national security, the economy and the livelihoods and security of citizens. It is therefore important to develop a comprehensive national strategy to address cybersecurity issues. This effort should be accompanied by the testing and continuous improvement of the strategy in national exercises based on the use of simulated cyber-physical battlefields around national critical infrastructure installations.

There are increasing cases of critical infrastructure simulations specifically designed for security attack exercises [5]. They have many different characteristics, but they also tend to have the common philosophy of realistically emulating the real environment and emphasizing the visualization of the physical world, controlled by digital systems in cyberspace.

5 CONCLUSIONS

Critical infrastructures, vital structures for the proper functioning of society and for ensuring national security, need well-trained staff in the field of cybersecurity. Still, due to the enormous risks that their training at the workplace would entail, the only viable solution for their education are cyber training polygons.

The changes in the workplace and society, which are driven by various challenges, have induced profound transformation to the education systems. Technology-facilitated learning systems are increasingly present in the education system because they offer new opportunities regarding the study of different disciplines when traditional systems are not adequate or even possible. We have studied the cybersecurity aspects of critical infrastructure protection, for which cyber polygons are used, and have an essential role to play in the fight against cybercrime and in developing cybersecurity defense capabilities. They can be developed and installed at the government level and by business organizations and research centers in order to solve complex problems and test new ideas. They are also used for real-time evaluation of the performance of various security solutions.

In this context, we have assessed the differences between a few cyber range solutions suitable to be used in the educational process in order to ensure cybersecurity competencies of human resource in critical infrastructures.

ACKNOWLEDGEMENTS

This work was supported by the PN 102 “Cybernetic polygon for industrial control systems - ROCYRAN” project.

REFERENCES

[1] J. Waddell and S. Vartuli, “Moving from traditional teacher education to a field-based urban teacher education program: One program’s story of reform.,” *Professional Educator*, vol. 39, no. 2, 2015.

[2] G. Natividad, R. Mayes, J.-I. Choi, and J. M. Spector, “Balancing stable educational goals with changing educational technologies: challenges and opportunities,” *e-mentor*, vol. 2015, no. 1 (58), pp. 83–94, Feb. 2015.

[3] R. E. Mayer, *Multimedia Learning*. Cambridge: Cambridge University Press, 2009.

[4] R.M. Tawafak, A.A. Sideiri, G.M. Alfarsi, M.N. Al-Nuaimi, S.I. Malik and J. Jabbar, “E-learning Vs. Traditional Learning for Learners Satisfaction,” *International Journal of Advanced Science and Technology*, vol. 29, no. 3, pp. 388–397, Jan. 2020.

[5] J. Kim, K. Kim, and M. Jang, “Cyber-Physical Battlefield Platform for Large-Scale Cybersecurity Exercises,” in *2019 11th International Conference on Cyber Conflict (CyCon)*, 2019, pp. 1–19.