ECAI 2017 - International Conference – 9th Edition
Electronics, Computers and Artificial Intelligence
29 June -01 July, 2017, Târgoviște, ROMÂNIA

Modeling And Simulation Architecture For Training In Cyber Defence Education

Georgiana Subaşu[1], Livia Roşu[1], Ion Bădoi[1]
[1]Military Technical Academy
Bucharest, Romania
georgiana.subasu@gmail.com, rosulivia@ymail.com, ibadoi@hotmail.com

Abstract – **The diversity and complexity of cyber threats are constantly evolving. In this paper we emphasized some considerations about the imperative need of effectively using the existing solutions for training in the educational area. To overcome these issues, we propose a scalable, flexible and interoperable architecture which integrates the concept of modeling and simulation in order to provide adjustable and cost-effective method for those interested in the education and training of specialists in Cyber Security.**

Keywords – training; education; cyber security; cyber range; modeling and simulation; model; mission; exercise; cyber defence

I. INTRODUCTION

Modeling and simulation of combat actions were an important step towards the development of the combat actions response abilities related to conventional war. The training exercises carried out for the successful fulfilment of a combat mission in the traditional space are dynamic, expensive and complex by their nature and the diversity of weaponry and systems used by the attending personnel. These need the mapping of all requirements to simulation systems, by creating models dependent on the real time of mission deployment [1].

Modern military missions integrate information and communication systems to send confidential information, its storage devices, but also equipment monitored using control information systems.

The field of cyber security started to develop new dimensions together with the increase of the automation degree of the technology level and complexity of technologies used at the same time with the extension and enhancement of information threats. The quality of cyber security is given by the degree of personnel awareness and training, by the update of technological and practical security solutions used.

The literature handles the issue of building models and making simulations for educational purposes by various works, by approaching topic variations such as: Cyber awareness, Cyber resilience, Cyber security training, Cyber hygiene or Modeling and Simulation Cyber Operation [2], [3].

The necessity of training a generation of specialists in the field of cyber security is increasingly shaped from the security requirements that the working environment imposes from the specialized users and IT specialists [4]. The importance of cyber security determines the vital nature of user education.

The key elements in the realistic simulation of a mission are the dynamics of cyber attacks, constant development of infrastructure, existing vulnerabilities and the need to be aware of the possible impact. To overcome these issues we integrated a series of criteria necessary in an adjustable, flexible and interoperable architecture that can be used as a basis for training environments.

II. MODELING AND SIMULATION IN CYBER DOMAIN

Modeling and simulation provide us an ideal solution to practice, a training tool in the field of cyber security with no disturbing effects on the environment and real infrastructure.

In the case of cyber security, *modeling* is the process of creating a normalized view of the cyber security situation. The model will contain information about network infrastructure, security procedures, vulnerabilities, used services, and threats [5]. The training exercises validate the designed models. The modeling of an attack vector should approach seemingly separate elements, various characteristics and behaviors in a complex and dynamic model that meets the requirements by the new types of cyber attacks.

The purpose of training through *simulation*, as carried out based on such models, is to analyze the possible impact on confidential data, the decision-making process, but also on how the involved personnel responds in the created situation. The modeling and simulation technologies are the *"key element"* ensuring an effective management of security risks.

The paper [6] emphasizes the need of an ontological representation for the modeling of cyber assets in order to improve the Computer Network Defense. *Cyber resilience* is characterized by the ability to understand, adapt and approach the modification of network requirements for the deployment of missions.

A proposed method to train the entities for increasing the cyber resilience requires the development of possible and realistic training

978-1-5090-6458-8/17/$31.00 ©2017 IEEE

scenarios, which would approach various situations, discover functional deficiencies, but also test the response capabilities for the assessment of decision factors, training level and response possibilities [7].

The cyber defense exercises require different planning and organizational requirements, depending on the environment they are carried out in. The goals must be determined from the exercise planning step, so they will be clear in the preparation and organization stage of the exercise infrastructure [8].

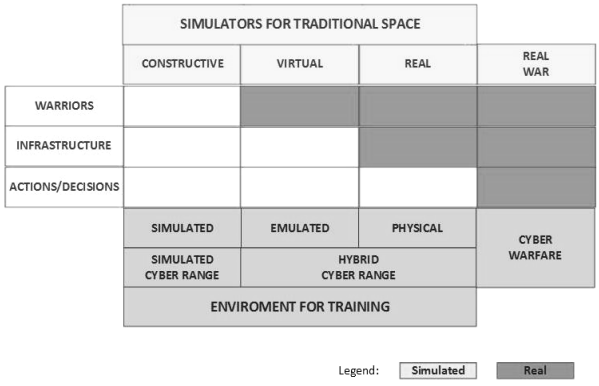
Real simulation is carried out on real systems with real people, whose equivalent in the cyber area are the cyber defense exercises (CDX), deployed in the form of security competitions in physical environment, in isolated networks attended by specialists in the field.

Virtual simulation involves real people and simulated systems [9], enabling the assessment of practical, control and cooperation capabilities of the attendants, by using simulations of the real systems. The emulation testbeds provide the possibility of training deployment by interacting with the simulated systems. An emulated environment maps the desired network topology and requires software configurations on its physical infrastructure. This may be an optimum training and research solution to increase the level of cyber education.

Constructive simulation prepared for the training in the traditional combat space is performed by using the simulated systems operated by simulated entities [9]. The trained personnel is able to insert the system entry data or to exercise the decision-making process. The results determination is not influenced by the operational capabilities of the participants. In cyberspace, simulation-style environments are similar to constructive simulation systems, and they have the role of analyzing and instructing staff on the effects of cyber attacks and appropriate defensive measures. The implementation and validation of the measures analyzed on the real networks is difficult because the simulations have the tendency to abstract the details of particular cyber attacks [10].

In Figure 1 are presented the elements of the simulation systems for the combat actions associated with the traditional space and their correspondence in the training solutions in the cyberspace.

Figure 1. Environments for training in traditional vs. cyberspace



Creating an ideal environment for training deployment in order to improve security is based on a solution combining *live*, *virtual* and *constructive* (LVC) simulation systems, which can ensure a quality training.

III. TRAINING SOLUTIONS IN CYBERSPACE

Modeling the working environment with its vulnerabilities, integration of different types and traffic and attack simulation tools are meant to emphasize the possible effects on systems under crisis situations. Also, this method trains the reaction and response manner of the attending personnel.

The simulated training environments assume significantly lower implications in the deployment of an exercise meant to increase the degree of awareness as regards the main attack techniques and the implementation of the proper security actions. In case that the exercise intends to perform a real-time simulation of a cyber conflict on a replica of the physical infrastructure, the implications are higher.

The main concern in the field of national security is the *cyber warfare*, a persistent and exponential threat to the information systems that are increasingly exposed to different types of information attacks, intrusions and disturbances. The complexity of systems, the various and specific roles, the multiple capabilities and connections require a good security management, performant resources, a personnel with advanced knowledge and a good response capability.

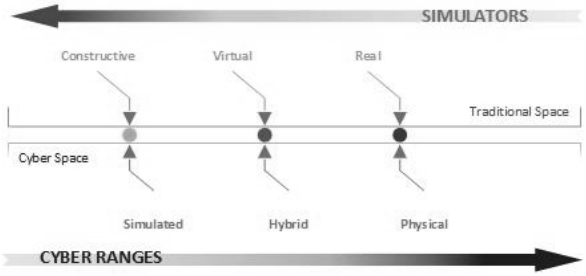
The high increase of threats in the cyberspace, together with the decrease of those in the traditional space, made the first option for the training in the traditional battlefield to be based on the *constructive simulation systems.* This type of simulation ensure planning, analysis, training, testing and periodical evaluation of personnel with minimum costs and infrastructure, as compared to the virtual or real simulation systems that involve specialized equipment, personnel and weaponry with much higher costs.

As regards the cyber security and defense, the organizations increasingly call on training environments integrating *physical systems*, where the attendants need to consider the space and time constraints, coordinate, cooperate and be competitive with other teams of professionals. These training environments also known as cyber competitions require much higher financial, human and material resources, by providing realistic pertinent training, evaluation and testing of the response capabilities.

The *real, virtual and constructive simulation systems* are integrated in hybrid solutions and represent the main option of organizations. They provide an isolated training environment where the live working conditions can be replicated by using virtual machines and real network elements, communication, etc. The real infrastructure elements increase the degree of realism and adaptability of the training environment.

In Figure 2 we can see that the constructive simulation systems are the most used training solutions in the traditional battlefield. In the case of cyberspace, we are increasingly selecting for realism, choices directed towards cyber ranges with hybrid or even physical architecture.

Figure 2. Trends in the use of training environments



Unlike the constructive simulation systems, that are on an increasing demand in the traditional combat space, the constraints of the simulated environment make the training solutions with virtual architecture a solution less demanded by organizations for the cyberspace-related training, but most suitable for the educational system. Although they provide increased scalability, flexibility and portability, they cannot comprise the complexity of an exercise from the viewpoint of realism and dynamic factors occurring in the real environment (e.g. the system behavior, disturbance of functionalities).

IV. THE NECESSITY OF CYBER RANGES IN EDUCATION

The environment, infrastructure, personnel, applications and capabilities are under the constant pressure of cyber threats. The virtual environment merges the real one and the new technologies, services and models pushing the existing concepts and regulations to their limits [11].

A Cyber Range is a realistic training environment based on network modeling and simulation, mainly meant to test and evaluate capabilities, techniques and methods of prevention, defense and counteraction of cyber attacks.

The computer networks, communication systems and their vulnerabilities interact with the physical infrastructure, the human and decision factors, making up an interoperable environment by its structure and indivisible by its necessity. The clear identification of the connections between systems and entities, functionality and property represents the main challenge.

A Cyber Range for cyber defense exercises wishes to provide a safe and realistic environment where attack and defense strategies are evaluated in real-time. This provides the users testing, evaluation and training possibilities to improve the defense capabilities and security actions.

Cyber Ranges are flexible and adaptable environments, they allow creation of exercise topology, addition of new virtual machines and real infrastructure elements during its deployment and provide the possibility to recreate training exercises with identical scenarios, configurations and models or to re-instantiate the "image" at any given time during the exercise.

Creating a Cyber Range for cyber defense exercises may be considered a true challenge if we think about the requirements of the military system. More than a consistent infrastructure, there is a need of a secured network able to create a close copy of the military communication systems with no internet access.

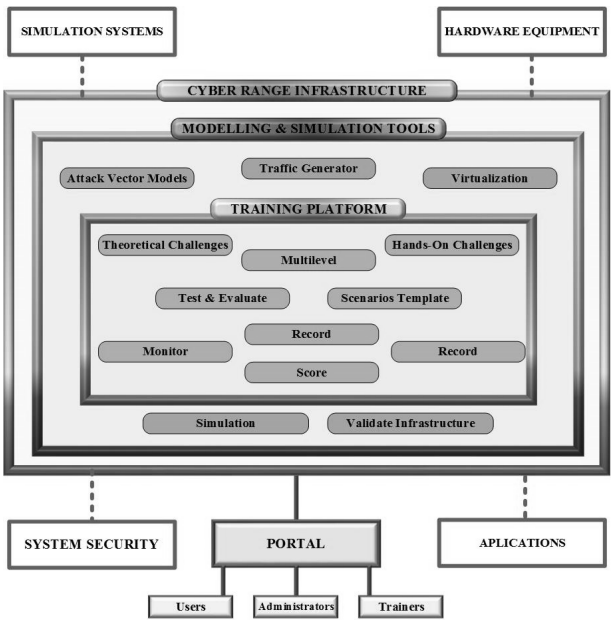
To ensure a quality pedagogical, educational and training process, Cyber Ranges integrate a collection of events that are helpful in planning, executing and analyzing the results, as it stands for a testing, development and research possibility for future generations of specialists in cyber security.

V. A PROPOSED ARCHITECTURE FOR TRAINING IN CYBER DEFENSE EDUCATION

In order to improve the degree of cyber security education we propose a flexible, scalable and interoperable architecture for a dedicated environment that meets the demands of different types of training.

The proposed architecture presented in Figure 3 allows for the rapid and automatic creation of a network topology with the necessary configurations, testing and assessment of the abilities through pre-established training exercises, monitizing and recording of the participants' performances, as well as evaluation and analysis of their actions. It has three major components that form a learning system and a safe, adaptable and easy to use training environment.

Figure 3. Training environment architecture



Cyber Infrastructure is the hardware resource for training. This component allows the attachment of additional network elements or required security

systems, software tools or applications, making it interoperable by connecting with simulation systems for conventional combat actions or other training tools.

Modeling and Simulation Tools are used to fulfill the specific requirements for the proper development of the training according to its objectives. Virtualization of infrastructure elements, legitimate and illegitimate traffic, use of attack vector and network models and their simulation enable realistic training in an isolated environment. These tools allow the validation of an infrastructure from its design stage.

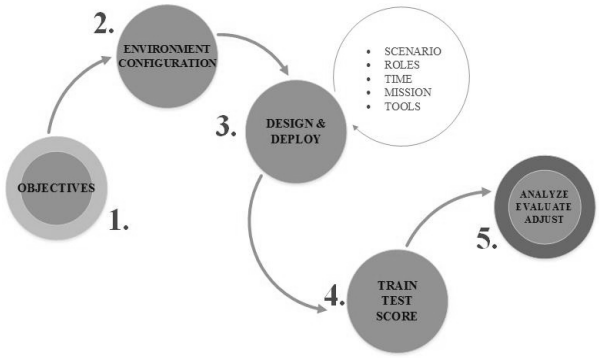
Training Platform is the main element of the architecture facilitating training with the help of theoretical or hands-on challenges organized on multiple levels using predefined or new scenarios. Also, this component provides the ability to monitor, record, report, and score the actions taken to accomplish the missions.

Access to the training system is accomplished by a portal through which all user categories (users, trainers, administrators) authenticate and get specific permissions according to their role in the exercise.

The proposed architecture aims to provide effective training by solving specialized Q&A and hands-on activities to contribute to the development of cyber education. Automating operations by integrating modeling and simulation tools enhances traffic fidelity, asset analysis, and virtualization capabilities without compromising training objectives and requirements.

Carrying out a training exercise for cyber defense using the proposed architecture implies the observance of a methodology. The workflow presented in Figure 4 combines 5 essential steps representing activities necessary for successful development of training by concretization the initial objectives.

Figure 4. Workflow diagram for training exercises



By following the workflow and using the integrated components in the proposed architecture, we can carry out attack-defense (red vs. blue), attack-attack (red on red) war games or Capture the Flag competitions.

VI. CONCLUSIONS

This paper presents an optimum architecture for education in cyber defence based on features derived from the complexity, benefits and necessity of a simulation-based training environment.

The proposed architecture can be used for a wide range of applications, as modeling & simulation capability in the cyber field, but especially for training in Cyber Defense Education.

Combining all the types of simulation into one training environment is an ideal solution for designing and developing realistic cyber battlefields, which allow the cyber warriors to train themselves.

There are several courses of future development arising from the ideas presented above. A further direction is to make a comparison between our proposed architecture and existing military or commercial training solutions.

A highest priority is represented by the constant improvement and advancement of the capabilities held by performing cyber defense exercises. The performance of interdisciplinary training exercises, on an institutional level, provides the possibility to test and develop the response capabilities in front of the new cyber threats.

REFERENCES

[1] S. Musman, A. Temin, M. Tanner, D. Fox and B. Pridemore, "Evaluating the impact of cyber attacks on missions", International Conference on Cyber Warfare and Security, Academic Conferences International Limited, 2010.

[2] T. J. Mowbray, "Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions", John Wiley & Sons, 2013.

[3] F. Schreier, "On cyberwarfare", 2015.

[4] C. Paulsen, E. McDuffie, W. Newhouse and P. Toth, "NICE: Creating a cybersecurity workforce and aware public", IEEE Security & Privacy 10.3, 2012.

[5] "Modelling & Simulation for Cyber Defence", Nato Manual.

[6] K. O'Sullivan and B. Turnbull, "The cyber simulation terrain: Towards an open source cyber effects simulation ontology", 2015.

[7] S. Hajkowicz, "Global megatrends: Seven patterns of change shaping our future", Clayton South, Victoria: CSIRO, 2015.

[8] "Cybersecurity Test and Evaluation Guidebook", 2015.

[9] "DoD Modeling and Simulation (M&S) Glossary", Department of Defence, 2011.

[10] J. Davis and S. Magrath, "A survey of cyber ranges and testbeds", Defence Science and Technology Organisation Edinburgh (Australia) Cyber and Electronic Warfare Div, 2013.

[11] "EU cyber cooperation: the digital frontline", European Network and Information Security Agency (ENISA), 2012.