https://doi.org/10.53656/str2026-3-1-com

Education in the Information Society
Образованието в информационното общество

COMPUTER-BASED TRAINING AND SIMULATIONS IN THE MULTILAYERED TRAINING MODEL FOR CYBER DEFENSE SPECIALISTS AT "VASIL LEVSKI" NATIONAL MILITARY UNIVERSITY

Yavor Dechev,
Radoslav Dimov
"Vasil Levski" National Military University (Bulgaria)

Abstract. This article examines computer-based exercises and simulations and their place in the multi-layered model of training for cyber defense specialists at the "Vasil Levski" National Military University. In their presentation, emphasis has been placed on the specifics of the training of military IT specialists. Additionally, the opportunities for cadets to participate in international exercises and projects in the field of cyber defense have been considered.

Keywords: training model; computer-based training and simulations; cybersecurity; CyberRange

Introduction

For more than 50 years, computer specialists in the Armed Forces of the Republic of Bulgaria have been trained at the military school in the city of Shumen – formerly the Higher Military Artillery School, and since 2002, the Faculty of Artillery, Air Defense, and Communication and Information Systems at the "Vasil Levski" National Military University (NMU) in Veliko Tarnovo. Over the years, the specialty "Military Cybernetics" has undergone several name changes, but its trainees have consistently received an interdisciplinary and broad-based education in the field of "Computer Science."

The main specialty in the Department of Computer Systems and Technologies is "Organization and Management of Military Formations at the Tactical Level," with a specialization in "Military Communication and Information Systems." This program falls under professional field 9.2, "Military Affairs." Cadets earn a "Bachelor's" degree after completing a five-year full-time study program, unlike civilian universities, where the duration is typically shorter. Additionally, they obtain a civilian specialty in "Computer Systems and Cybersecurity" within professional field 5.3, "Communication

and Computer Engineering," receiving the qualification of "Computer Engineer – Cybersecurity Expert."

Cadets acquire fundamental competencies, knowledge, and skills in the field of communication and information technologies. Furthermore, the training program fosters personal development, active civic engagement, social inclusion, and competitiveness in the job market. The combination of military and civilian education is achieved through the study of foundational and specialized modules, which include mandatory, elective, and optional disciplines (specialized courses), as well as the implementation of new and diverse teaching methods.

The training model at NMU is multilayered and encompasses various aspects of cadet education (Stoykov et al., 2018). It includes several types of training: theoretical engineering, practical engineering, and leadership development. The goal is to prepare future officers both as commanders and as engineering specialists. Additionally, the training program emphasizes the development of patriotic spirit and moral education, as these are two interrelated aspects of personal growth that play a crucial role in shaping moral and civic values, particularly in the context of society and the nation (Mladenova, 2019).

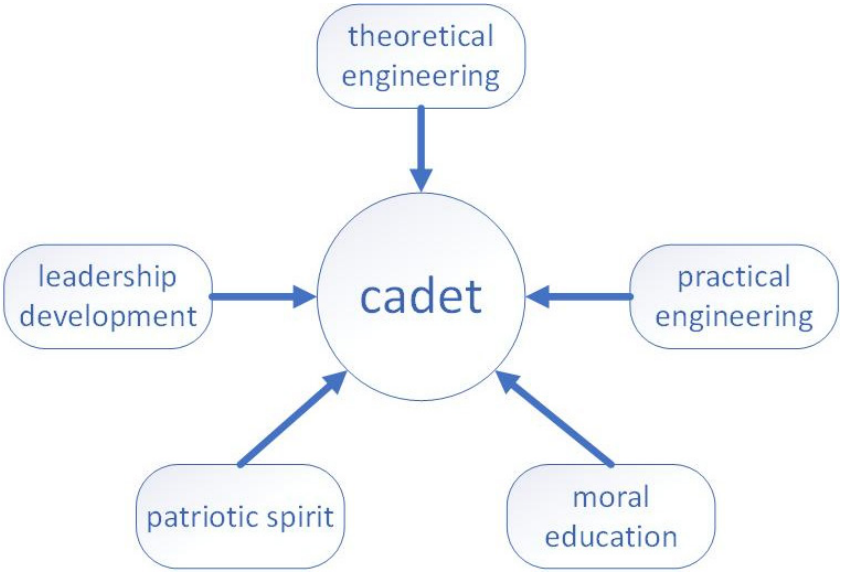


Figure 1. Training model at NMU

All training programs for cadets include two main sections: "Military Specialty" and "Civilian Specialty." The disciplines that ensure military specialization are divided into the

following modules: "Military Training," which is further categorized into basic, general, and specialized training; "National Security, Resource Management, and Fundamentals of State and Law," "Language, Leadership, and Physical Training," and "Practical Training and Internship." The disciplines under the "Civilian Specialty" section are organized into four modules: "Fundamental" and "Specialized," "Language and Physical Training," and "Practical Training."

Computer-based training and simulations are an essential component of the training model at NMU. By participating in them, future IT specialists enhance and expand their practical knowledge and skills in modern computer systems and cyber defense systems.

Computer-based training and simulations at NMU are of several types: computer-based simulations within the JCATS system, complex tactical exercises, and NATO international cyber defense exercises.

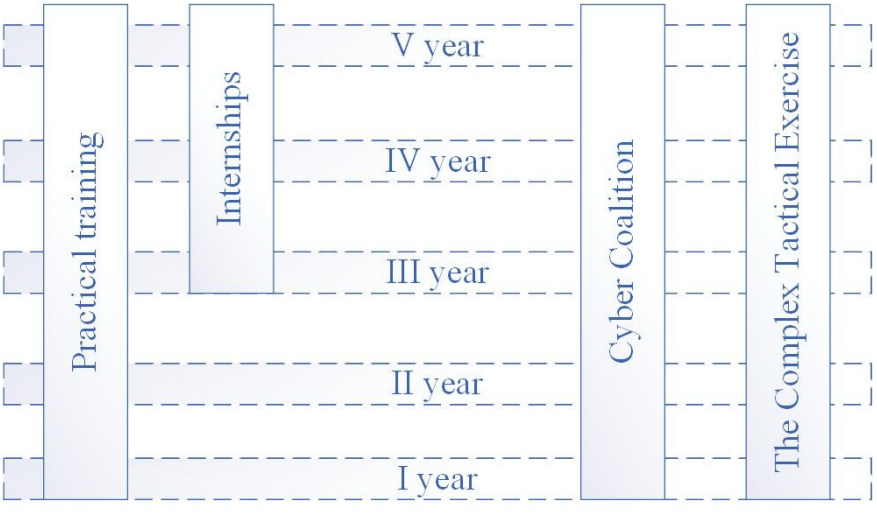


Figure 2. Types Computer-based training and simulations at NMU

Practical training in both specialties is ensured through internships, tactical exercises, and simulations.

JCATS

The Joint Conflict and Tactical Simulation (JCATS) system is used by security organizations as a tool for training, analysis, mission planning, and exercises. The system focuses on command-and-control processes. Conducting war games within this platform emphasizes the development of cadets' leadership qualities and their ability to collect, process, and analyze various types of information. One of the primary responsibilities of

an officer is decision-making in combat scenarios (solving a given problem).

JCATS has been integrated into the training model of the National Military University (NMU) since 2006 (Berchev et al. 2024). It is utilized by students from all specialties, but primarily by cadets who will later be assigned to command positions. The system is actively used during complex tactical exercises.

Complex Tactical Exercise

The Complex Tactical Exercise (CTE) aims to enhance the field training of cadets and assess their professional and leadership skills under physical and psychological stress conditions.

During the CTE, cadets perform tasks such as:

– Planning and establishing the communication and information system (CIS) and individual communication nodes (CIN);

– Providing communication and information services and ensuring their security;

– Implementing cybersecurity measures and simulating cyberattacks on the CIS;

– Performing duty and security tasks for the CIN.

Cadets from all academic years participate in the exercise. Depending on their training level, they assume either command or operational roles.

– First- and second-year cadets build the physical CIS and provide security for the designated objects.

– Third- and fourth-year cadets contribute to CIS setup and provide communication and information services.

– Fifth-year cadets are mainly assigned command positions and are responsible for planning and managing the various activities.

During the exercise, officer instructors act only as advisors.

Cyber Attacks in the CTE

Since 2023, an additional element has been included in the CTE: cyberattacks on the established CIS. Two specialized teams participate:

– Red Team: Simulates a real hacker group, using the tactics, techniques, and procedures of a designated adversary.

– Blue Team: Conducts monitoring and analysis of cyberattacks, incident response, and tests standard operating procedures.

Cyberattacks target the information system and provided services. Additionally, attacks can focus on disrupting the physical communication and power grid or damaging specific hardware components.

Military Training and Field Conditions

Throughout their time at NMU, cadets receive specialized engineering training along with education aimed at developing professional skills and resilience necessary for handling high-risk situations and operational stress. The CTE places strong emphasis on teamwork. Participation in the exercise is directly related to the cadets' future responsibilities as

commanders. They learn how to work together, plan operations, manage subordinates, and take responsibility for decisions.

Ongoing military conflicts worldwide demonstrate that computer specialists in the armed forces operate computing systems in combat zones. Personnel managing C4I (Command, Control, Communications, Computers, and Intelligence) systems, communication specialists, and UAV operators are actively engaged alongside infantry forces. Unlike civilian university students, NMU cadets conduct their practical training outside classrooms, in field conditions or buildings without established communication networks. For several days, cadets work and live-in field camps, regardless of weather conditions. Equipment is either housed in tents or placed in open terrain, making the setup and maintenance of communication networks significantly more challenging.

Cybersecurity Exercises

Since 2020, cadets specializing in Computer Systems and Cybersecurity have been actively participating in NATO's Cyber Coalition and Locked Shields cyber defense exercises – the largest annual cybersecurity training events of the Alliance.

Although these international exercises are not officially included in the cadets' curriculum, they are a crucial component of their specialized training.

One of the advantages of civilian universities is their autonomy – they have fewer restrictions and can independently work on projects. However, when it comes to international cyber exercises, military academies benefit from their centralized management. These exercises are conducted under NATO's supervision, with the Ministry of Defense of Bulgaria serving as the primary coordinator and organizing the Bulgarian national team's participation (Nikolov, 2020).

The benefits of cadet participation include (Vasilev et al., 2021):

– Military universities leverage the already established structure of these exercises, requiring minimal additional organization.

– They contribute only part of the participants without needing to provide expensive IT equipment.

– Cadets participate as part of Bulgaria's Cyber Incident Response Team (Blue Team).

During the exercises, cadets develop competencies in:

– Digital forensics

– Cyber incident response

– Malware analysis

– Threat intelligence

– Utilizing methodologies and databases for adversary tactics, techniques, and procedures analysis

– Endpoint security and monitoring

The competitive nature of Locked Shields further motivates cadets as they engage in various cyber defense and attack scenarios. Since these exercises are multinational, cadets also improve their proficiency in technical English in real-time. The exercises take

place on specialized CyberRange platforms, which provide a virtualized environment for simulating different cyber tactics, techniques, and procedures across multiple scenarios. Additionally, evaluation and feedback mechanisms play a key role for both participants and organizers. Unlike open training platforms, CyberRange infrastructures are restricted to exercise participants only, ensuring that IT specialists outside the program cannot access them for personal skill development.

Participating in international exercises also introduces future officers to opportunities for further professional qualification courses in NATO member states. Once they join the Bulgarian Armed Forces, they can attend these advanced courses worldwide, allowing them to enhance their cyber defense expertise for free while advancing their careers as officers.

The Bulgarian Ministry of Defense recognizes the success of cadets in NATO-organized exercises and competitions. In response, it invests in technical equipment and software to continuously upgrade the Cyber Operations Center at the Faculty of Artillery, Air Defense, and Communication and Information Systems (CIS). The expansion of this center enhances NMU's capabilities, positioning it as a leading institution for training cyber defense specialists at a global level.

Internships and Military Training

Military internships take place at the final stage of cadet training, within military units responsible for IT infrastructure and cyber defense of the Bulgarian Armed Forces. By the time cadets begin their internship, they have completed theoretical training in core subjects, equipping them with knowledge as IT engineers. The main objective of the internship is to develop practical skills for various roles, including command, staff, engineering, and technical positions. Cadets gain hands-on experience with military computing and communication systems, some of which are not covered in their academic coursework due to their classified nature. During the internship, cadets work with real-world military hardware and IT infrastructure, further enhancing their technical expertise. The internship spans the last three semesters, with each phase taking place at a different military unit. This approach provides cadets with firsthand experience of various formations and the specific tasks performed by military IT specialists.

Additionally, the internship includes exposure to administrative duties, preparing cadets for the management responsibilities they will assume as future officers.

In the short term, the Department of Computer Systems and Technologies aims to integrate cadet participation in the maintenance of the CyberRange platform at the Defense Institute "Prof. Tsvetan Lazarov" as part of their military internship.

Conclusion

In conclusion, several key aspects of the application of computer-based training exercises and simulations in the education model of IT specialists at NMU can be highlighted.

The overall training process is structured into two main directions:

1. Acquiring and reinforcing specialized knowledge and skills – Cadets work with real military equipment, allowing them to complement their theoretical training with practical experience.

2. Leadership development – One of the primary objectives of military education is to train future commanders for the Bulgarian Armed Forces. Unlike practical training in civilian universities, military exercises and simulations expose cadets to physical and psychological challenges, preparing them for the demands of real-world military operations.

REFERENCES

Berchev, D., & Petkov, S. (2024). Integrating simulation systems in cadet training: Challenges and opportunities. In *Second national scientific and practical conference "Digital transformation of education – problems and solutions"*. ISBN 978-954-712-928-3.

Mladenova, R. (2019). *Influence of the military environment and leadership training on the development of the individual resilience of trainees at a higher military education institution* (Doctoral dissertation, Nikola Vaptsarov Naval Academy).

Nikolov, B. (2020). A concept for establishing a security operations and training centre at the Bulgarian Naval Academy. *Information & Security: An International Journal, 46*(1), 27 – 35.

Stoykov, S., Dimitrova, S., & Marinov, R. (2018). Scientific management of resource knowledge in the teaching system of security and defense. In *ENTerprise REsearch InNOVAtion Conference (2018)*.

Vasilev, P., Stoyanov, N., & Tsonev, T. (2021). Approach to developing innovative cybersecurity training programs. In: *International Conference on Advanced Research and Technology for Defence*.

✉ **Dr. Yavor Dechev**
ORCID iD: 0000-0003-1881-8727
WoS Researcher ID: AAB-3524-2021
Vasil Levski National Military University
Artillery, Air Defence and CIS Faculty
Shumen, Bulgaria
E-mail: yazdechev@nvu.bg

✉ **Radostin Dimov**
Scopus ID: 59243008700
Vasil Levski National Military University
Artillery, Air Defence and CIS Faculty
Shumen, Bulgaria E-mail: rsdimov95@gmail.com