USING CYBER RANGES IN CYBERSECURITY TRAINING AS AN ACTION PLAN IN THE FACE OF HYBRID THREATS

Major General Stayko PROKOPIEV

Commandant of the Rakovski National Defence College, Sofia, Bulgaria

Associate Professor Dr. Veselina ALEKSANDROVA

Rakovski National Defence College, Sofia, Bulgaria

Dr. Elitsa PAVLOVA

University of National and World Economy, Sofia, Bulgaria

Dr. Violeta VASILEVA

Future Innovation Labs, Sofia, Bulgaria

DOI: 10.55535/RMT.2025.3.19

Cyber ranges are key tools for developing effective strategies and tactics to protect against hybrid threats, which combine traditional military methods with cyberattacks. In this scientific paper, the authors examine the significance of using cyber ranges in cybersecurity training, analysing their architecture, main principles of design and implementation, and their lifecycle. The question of how these platforms can be used to enhance strategic resilience and national defence through simulating various scenarios and vulnerabilities is explored. Specific recommendations for integrating cyber ranges into action plans against hybrid threats are also provided. The employment of cyber ranges for the preparation of personnel, organizations, and consequently states can increase their readiness and capability to respond to complex and multifaceted hybrid threats, ensuring better protection of their critical infrastructures and information systems. This approach not only supports strategic resilience and strengthens national defence but also creates a foundation for international cooperation and knowledge exchange in the field of cybersecurity.

Keywords: hybrid threats; cyber range; cybersecurity; strategic resilience;

INTRODUCTION

In recent years, we have witnessed a rapid development of information technologies and cyberspace, which, as a global phenomenon, has changed the characteristics of the behaviour of individual societies and individual citizens in particular. The Internet, as a global network affecting all spheres of public life, is becoming not only the largest repository of information, but also the place where a significant potential of critical infrastructure and services at the state and corporate levels is concentrated. The global network is becoming an increasingly significant factor for national security and defence. All this leads to new challenges and hybrid threats in cyberspace, which are characterized by high dynamics, complexity and unpredictability. The development of offensive capabilities for conducting large-scale cyber operations by terrorist and extremist organizations, as well as by individual state entities, as a tool for achieving destructive and inhumane objectives against society and citizens, is one of the main reasons for rethinking the role of cyberspace as an element of hybrid threats and a fifth domain of conflicts and interaction.

The increase in risks and threats in the geopolitical and strategic security environment, as well as in cyberspace, creates conditions for increasing the vulnerabilities of military communications and information systems for command and control. There is a need for effective and timely implementation of protection measures for own systems as well as for the development of cyber defence capabilities compatible with those of NATO member states. Cyber security requires resources, such as material, human, financial and technological ones.

At the NATO Summit in Warsaw in 2016, cybersecurity was identified as one of the main priorities of the organization. Priority areas were also identified, such as building the Alliance's collective capabilities, including cyber defence in the planning process, and increasing member states' investments in this area. It is because, for many years, armed struggle and war have been waged in four physical domains that objectively exist – on land, in the air, in the maritime space, and in space. After the Warsaw meeting, the fifth domain – cyberspace – is defined (Grigorov, 2016).

In the transition to network-centric capabilities, high-tech systems for command and control of troops, intelligence, targeting and control of intelligent weapons, the dependence of our systems is actually becoming very high. For example, if cyber operations lead to the inoperability of the global positioning system (GPS), all missile systems that are guided and controlled by GPS will not be able to function. Cyber operations can lead to catastrophic consequences if, during a military operation, the armed forces have not taken appropriate measures to protect their own command, control, guidance and attack systems. That is why NATO has identified cyberspace as the fifth domain, important for defence.

It is necessary to develop policies and guidance documents for the Armed Forces cyber defence in accordance with the consideration of cyberspace as the fifth domain. It is related to strategic sustainability, national defence and the need to actively counter hybrid threats, cyber attacks and hybrid wars.

For this purpose, the opportunities of our membership in NATO and the EU can be used to participate in joint initiatives to build common capacity and capabilities; to share information on cyber incidents and mutual assistance with state institutions and international organizations in a coordinated manner; to cooperate with the business and academic community; to achieve expert capacity in cybersecurity and to increase preparation through periodic training and participation in cyber exercises with cyber polygons.

CYBER RANGE ARCHITECTURE

The cyber range architecture includes a work platform, a user interface, scenarios, projects and infrastructure, and teams. The user interface forms a realistic cyberspace consisting of real devices and virtual machines. Registration in the platform covers the functions of the instructor and participant profile elements, respectively.

The platform consists of a set of technologies used as a foundation on which applications, processes, and services can be developed. The platform contains the main elements that provide automated processes such as creating virtual machines, simulating network traffic, installing software packages, mass creating network user accounts, monitoring the state of the workspace, and visualizing information for instructors and participants. The elements can be developed or implemented using, customizing, and configuring open-source solutions. However, they must comply with standards to ensure their interoperability and reuse.

The main elements of the cyber range platform are related to:

1. *Tracking*. The platform must be able to track the status of the workspace elements, extracting information related to the status of services, processes, applications and software updates; creating and deleting users (including user rights and sessions) and files; firewalls; intrusion detection systems; network traffic data.

2. *Registry*. The registry manages the platform database, which maintains participant records according to data obtained from tracking and those submitted by the *"Instructor"*.
3. *Feedback and reports*. Feedback and reports visualize data on the evolution of cyber attacks occurring in a given exercise; changes in the results of the teams participating in a given course; team score; workspace elements. Visualization of training data is key to improving the effectiveness of exercises.
4. *Automation*. The element includes mechanisms that automate the workspace functions for generating network traffic, virtual user accounts that perform virtual actions, and automated cyberattacks. Generating network traffic enhances the realism of the platform. Network traffic generators should simulate traffic of various protocols (e.g. HTTP – HyperText Transfer Protocol, SMTP – Simple Mail Transfer Protocol, POP – Post Office Protocol, FTP – File Transfer Protocol, ICMP – Internet Control Message Protocol) and provide means for specifying the source, destination, duration, and amount of generated traffic.
5. *User interface*. The space is created in an automated manner based on the scenario selected by the instructor and downloaded from the scenario repository. The workspace elements are interconnected with the platform elements and include virtual or physical computers, mobile devices, network devices, servers, services, integrated technologies, wireless networks etc.

User Interfaces

The user interfaces for instructors and participants provide various capabilities, which are shown in *table 1.*

Table 1: Cyber range instructor and participant user interface capabilities (authors' design)

Functionality / UI element	**Instructors**	**Participants**
Dashboard	View sessions, participant status, exercise results	Personal progress, upcoming tasks, current level
Scenarios and missions	Create, configure and manage scenarios	Access scenarios, execute missions, report results

Functionality / UI element	Instructors	Participants
Real-time monitoring	Tracking of participants' actions and network traffic in the simulated environment	Visualization of their own actions and their consequences on the system
Analysis and reports	Generation of individual and group reports, assessment of skills	Access to personal report and recommendations for improvement
Communication module	Built-in chat, ability to send instructions and feedback	Built-in chat for questions, team collaboration
Gamification	Setting criteria for points and achievements	Accumulation of points, achievements, comparison with other participants
Integration with external systems	Adding real cyber threats and actual attacks for training	Accumulation of points, achievements, comparison with other participants
Role and access management	Defining access levels and roles	Access only to training missions and own results
Interactive labs	Setting up virtual environments for different scenarios	Practical exercises in a secure simulation environment
Feedback and assessment	Direct feedback, individual comments	Possibility of self-assessment and receiving personalized recommendations

Scenarios

Scenarios are created by combining tasks, conditions, goals, and learning materials that are stored in a repository. Scenario elements include: virtual machines and network devices used as templates during workspace creation; scripts for creating and deploying the workspace; configuration files for platform elements. A scenario defines the steps that participants must follow to complete the exercise. Each step includes sub-goals, a set of conditions, and learning elements. Attributes are set that describe the details of the scenario, including name, description, difficulty level, and complexity.

Teams

Teamwork helps to evaluate attack scenarios in real-world conditions (Yamin, 2020). The red and blue teams are common to all cyber polygons. The red team carries out the attack on users' computers using viruses, malware, and more, designed by the white team. The green team is responsible for simulating wired or wireless connections between users and their computers or smartphones to the network infrastructure. The blue team members take on either the role of defenders of the system, protecting it from cyberattacks, or the role of investigators of a cyberattack and its consequences. The white team creates cyberattack scenarios in order to track the success or failure of the blue team. The yellow team reports situational awareness by reproducing innocent users compromising the security of the network. Some cyber polygons use a grey and purple team. The grey represents normal traffic and service requests to be supported, and the purple is a collaboration between the red and blue teams responsible for protective techniques.

During the exercise, the instructor gives advice related to the learning content and receives information from the tracking elements, checks whether the learners have managed to perform the appropriate actions within the allotted time, and evaluates them.

BASIC PRINCIPLES FOR SELECTING AND IMPLEMENTING CYBER RANGE

The design and implementation of cyber ranges should be guided by several core principles to ensure maximum educational value and replicate the operational dimensions of cybersecurity challenges (Hart et al., 2020).

❖ ***Accuracy and Realism***

Training environments are essential for developing skills that are directly transferable to operational contexts. Cyber ranges should accurately replicate network topologies, system configurations, services and applications with realistic performance characteristics and constraints, typical user activities and business processes within which to detect security-related events. Similarly, adversary behaviour should reflect documented tactics, techniques and procedures of real-threat actors. Realistic representation of the impacts of both successful attacks and defensive measures helps trainees understand events relevant to their decisions – business impacts, service disruptions that may arise from security incidents or mitigation actions. Technical accuracy ensures that skills acquired during training can be directly applied to real-world scenarios.

❖ ***Scalability and Flexibility***

The dynamic nature of cybersecurity requires learning environments that can adapt to a variety of needs. Cyber range must work with varying numbers of participants, from individual training to large-scale team exercises involving dozens or hundreds of participants. Learning platforms must support scenarios of varying complexity, from focused skill-building exercises to comprehensive incident response simulations. The environment must be configurable to represent different business sectors, organizational structures, and technical architectures.

❖ ***Insulation and Security***

Proper containment is essential for both security and educational purposes. Complete *network separation* ensures that malicious activities in the learning environment cannot affect production systems. *Data isolation* means that learning environments should use synthetic or properly sanitized datasets. Learning environments should replicate the characteristics of production data without exposing sensitive information. *Robust authentication and authorization mechanisms* are needed to restrict access to appropriate learning scenarios and system components based on learner roles and permissions. Another important part is *logging and monitoring systems* that track all activities in the learning environment. Mechanisms to *prevent unauthorized extraction* of tools, techniques, or scenarios from the learning environment help protect intellectual property and prevent potential misuse of learning materials.

❖ ***Reproducibility and Standardization***

Consistent learning experiences require systematic approaches.

RECOMMENDATIONS FOR INTEGRATING CYBER RANGE INTO HYBRID THREAT RESPONSE PLANS

Hybrid threats pose complex and multifaceted challenges that require coordinated and adaptive response strategies. In the context of modern strategic resilience and national defence, cyberspace plays an increasingly important role as an arena for conflicts and attacks. One of the effective methods for preparing for and responding to these threats is the use of cyber ranges – virtual environments that simulate real-world conditions and scenarios. Specific recommendations for integrating cyber ranges into hybrid threat response plans include the following:

Development of Realistic Scenarios. The first step towards successfully integrating cyber ranges is the development of realistic scenarios that reflect potential hybrid threats. These scenarios should include combinations of physical, informational and psychological attacks, as well as interactions between different actors (government, private sector, civil society). It is important that the scenarios should be updated regularly to reflect new trends and tactics of adversaries.

Training and Simulations. Cyber ranges provide a unique opportunity to conduct training and simulations that prepare personnel for real-world situations. These exercises may include incident detection and response training, crisis management, and inter-agency coordination. Training should be systematic and periodic to ensure ongoing readiness and skill development.

Cooperation and Coordination. Effective countermeasures against hybrid threats require close cooperation between various stakeholders. Cyber ranges can serve as platforms for joint exercises and information exchange between government institutions, private companies, and international partners. This cooperation not only improves interoperability, but also builds trust and mutual understanding between participants.

Technological Readiness and Infrastructure. The successful integration of cyber ranges requires the availability of an appropriate technological infrastructure. It includes high-performance computer systems, simulation software, and data analysis tools. In addition, reliable communication channels and secure networks must be provided to ensure information security and continuity of operations.

Monitoring and Evaluation. The integration of cyber ranges into hybrid threat response plans should be subject to ongoing monitoring and evaluation. It includes analysing the results of simulations, identifying weaknesses and gaps, and implementing corrective measures. Regular review and updating of procedures and policies ensure their effectiveness and adaptability to changing conditions.

THE MAIN CHALLENGES IN DESIGNING AND IMPLEMENTING A CYBER RANGE

The main challenges in designing and implementing a cyber range are related to the high costs of preparation, high requirements for testing, building a learning strategy and evaluation. The preparation phase requires many resources, specialized personnel, as well as a long period of time. According to a study on the evaluation of cyber defence exercises using a visual analysis process, a cyber range should be a safe, legal and isolated environment from external networks and the Internet (Ošlejšek, 2018). For this reason, special attention needs to be paid to the installation of applications and tools, the construction of network services, the provision of controlled access to the Internet, as well as the involvement of specialized personnel to test and make optimizations and adjustments. Another challenge facing educational cyber ranges is that they must be based on good teaching practices including learning objectives, participant characteristics etc. Cybersecurity training requires the formation of an interactive and multi-layered learning environment. Exercise scenarios must meet the needs and experience level of the learners. The integration of emerging technologies such as artificial intelligence and digital twins is transforming traditional approaches, while standardization efforts continue to develop worldwide.

CONCLUSIONS

In conclusion, it can be summarized that integrating cyber ranges into hybrid threat response plans is a key element for enhancing national and international security. By developing realistic scenarios, conducting training and simulations, promoting cooperation, providing the necessary technological infrastructure, and continuous monitoring and evaluation, the ability to prevent and respond to complex threats can be significantly improved. Effective cyber ranges require modular, scalable architectures with high-quality simulations and adherence to established pedagogical frameworks and comprehensive evaluation mechanisms.

Cyber ranges represent a powerful tool that can help organizations and states address the challenges in the face of hybrid threats to achieve strategic resilience and national defence.

ACKNOWLEDGEMENTS

This publication was financed by the Ministry of Education and Science in implementation of the National Scientific Program – Security and Defence that is funded by Ministry of Education and Science of the Republic of Bulgaria in implementation of National Strategy for the Development of Scientific Research 2017-2030 and was adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

BIBLIOGRAPHY:

1. Grigorov, M. I. (2 December 2016). *Petiyat domeyn i zaplahite v kiberprostranstvoto*, https://armymedia.bg/2016/12/02/петият-домейн-и-заплахите-в-киберпрос/, retrieved on 10 September 2025.
2. Ošlejšek, R. J. (2018). *Evaluation of Cyber Defense Exercises Using Visual Analytics Process.* EEE Frontiers in Education Conference (pp. 1-9). doi:https://doi.org/10.1109/FIE.2018.8659299.

3. Hart, S., Margheri, A., Paci, F., Sassone, V. (2020). *Riskio: A Serious Game for Cyber Security Awareness and Education.* Computers & Security, 95, 101827. doi:https://doi.org/10.1016/j.cose.2020.
4. Yamin, M. M. (2020). *Cyber ranges and security testbeds: Scenarios, functions, tools and architecture*, 101636. Computers & Security (88).