Journal of Theoretical and Applied Information Technology
15th Msy 2026. Vol.104. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFECTIVENESS OF THE USE OF CLOUD PLATFORMS AND NETWORK SIMULATORS IN HIGHER MILITARY EDUCATION IN CBRN TRAINING

PETRO DZIUBA[1], SERHII BURBELA[2], LESIA BALAHUR[3], SERGII STEPANOV[4]

PhD in Pedagogical Sciences, Associate Professor, Department of General Military Disciplines, Faculty of State Border Security, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine
[2]PhD, Department of General Military Disciplines, Faculty of State Border Security, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine
[3]PhD in Pedagogical Sciences, Associate Professor, Department of General Military Disciplines, Faculty of State Border Security, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine
[4]PhD in Pedagogical Sciences, Deputy Head of the Department of General Military Disciplines, Faculty of State Border Security, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Ukraine
E-mail: [1]petrodz.stateborderguard.ua@gmail.com; [2]serhiiburbelasecurity@gmail.com; [3]lesia_balahur125@gmail.com; [4]sergiistepanov1982@gmail.com

ABSTRACT

The article addresses the knowledge gap caused by the absence of an integrated quantitative framework for assessing how cloud platforms and network simulators affect CBRN training in higher military education. Existing studies describe virtual simulation, specialized modelling software for radioactive material spill scenarios and institutional mechanisms for medical and biological emergency response, but they do not provide a unified comparative model that combines technical readiness, pedagogical integration, organizational adaptability, security resilience and communication interoperability. The need for this study is determined by the growing role of digitally supported CBRN training and by the requirement to evaluate not only the availability of technologies, but also their measurable contribution to practical training outcomes. The aim of the study is to develop and test a Cloud Efficiency Index (CEI) for assessing the effectiveness of cloud platforms and network simulators in the CBRN training of students of higher military educational institutions. The research employed Delphi-AHP weighting, cluster analysis, correlation and regression analysis, bootstrap modelling (n = 500), and visualization in Python, Power BI and Tableau. The study compared Ukraine, Italy, Germany and Austria and identified three digital integration models: highly consolidated, balanced and buildable. The main new knowledge created by the study is the CEI-based Digital Readiness Matrix, which links digital maturity with practical training effectiveness and allows cross-country comparison of CBRN training systems. The results showed that Italy (CEI = 0.81) and Germany (CEI = 0.78) have reached a high level of digital maturity, Austria (CEI = 0.69) demonstrates a balanced model, and Ukraine (CEI = 0.54) remains at the stage of building digital infrastructure. Correlation and regression analysis confirmed a positive relationship between digital readiness and practical training effectiveness (r = 0.77; R2 = 0.68). The scientific contribution consists in transforming fragmented literature on simulation-based CBRN training into a measurable model for evaluating digital transformation, security resilience and resilient infrastructure in military education.
Keywords: *Digital Transformation; Cloud Platforms; Network Simulators; Higher Military Education; CBRN Threats; Cloud Efficiency Index (CEI); Security Resilience; Resilient Infrastructure.*

1. INTRODUCTION

In the 21st century, digital technologies are becoming the basis for the transformation of the military education system and officer training. The use of cloud platforms, network simulators, and virtual training equipment is changing not only technical approaches to training, but also the very paradigm of responding to CBRN threats. Modern information technology (IT) tools provide interactive

modelling of combat and emergency situations for building professional competencies of future officers without risk to life and health [1; 2]. However, as evidenced by studies by Ukrainian and international authors [3; 4], the pace of implementation of digital solutions in HMEIs remains uneven. Along with technological achievements, issues of standardization, cybersecurity, and integration of simulation systems into a single educational and training circuit arise. Despite a significant number of studies on the digitalization of the educational process, there are still significant gaps in the field of military education related to the lack of a single methodological model for assessing the effectiveness of digital technologies, the lack of comparative studies between different countries, as well as insufficient attention to the issues of interoperability, data protection, and pedagogical adaptation of simulation systems. The studies [6; 7; 8] noted that digital simulations contribute to better assimilation of theoretical material, the development of practical skills, and the development of situational awareness during CBRN training. The researchers [9; 10] emphasize that the combination of VR technologies, artificial intelligence (AI), and the concept of security-informed safety analysis provides a higher level of cadet engagement, increases the effectiveness of training, and contributes to the cyber resilience of the educational environment. The motivation for the study is the need to develop a holistic, comprehensive model that allows assessing the level of digital integration in military education, taking into account technical, pedagogical, and organizational factors. This approach is designed to eliminate existing methodological gaps, create a basis for comparison between different educational systems, and contribute to the harmonization of digital training standards in the field of CBRN protection.

Previous studies show that specialized software can support the simulation of liquid radioactive material spills for educational purposes [5], while institutional platforms can structure interaction between actors involved in medical and biological emergency response [6]. However, these studies do not solve the methodological problem of how to compare the digital maturity of different military education systems by a single set of measurable technical, pedagogical, organizational and security indicators. This gap defines the need for a model that connects cloud-based and simulation-based CBRN training with observable outcome measures rather than only describing the availability of digital tools.

The topic of this study is delimited to the use of cloud platforms and network simulators in the CBRN training of students of higher military educational institutions. The study covers four national cases - Ukraine, Italy, Germany and Austria - and focuses on technical readiness, pedagogical integration, organizational adaptability, security and technical resilience, and communication interaction. It does not cover combat effectiveness in real CBRN operations, medical treatment protocols, classified military infrastructures, procurement procedures, or the internal architecture of particular proprietary simulation systems. The analysis assumes that open institutional information, expert assessment and normalized indicators are sufficient for comparative modelling, while the results remain limited by the number of countries, the expert sample size and the availability of comparable institutional data.

After the literature critique, the problem statement is formulated as follows: current CBRN training research describes digital tools, VR environments, specialized simulation software and crisis-response platforms, but lacks an integrated index that can quantify the effectiveness of cloud and simulation technologies in higher military education. The research question is: how can the effectiveness of cloud platforms and network simulators in CBRN training be measured across different military education systems, and which components of digital readiness are most strongly associated with practical training outcomes?

The aim of the study is to develop and test the author's model for assessing the effectiveness of using cloud platforms and network simulators in preparing students of higher military educational institutions for actions in conditions of radiation, chemical and biological threats. The outcome measures establishing the novelty of the study are the Cloud Efficiency Index (CEI), the five-component Digital Readiness Matrix, the classification of national digital integration models, the correlation between CEI and the share of simulator-based practical training, and the relationship between CEI and the success rate of CBRN training scenarios.

So, the relevance of the research is to substantiate the effectiveness of cloud and simulation technologies in CBRN training of military students and determining the optimal directions of their integration into the national defence education system.

The stated aim is operationalized through measurable outcomes: CEI values, component scores for TG, PI, OA, ST and CI, cluster

membership of each country, correlation coefficients between CEI and practical training indicators, and regression-based estimation of the relationship between digital readiness and scenario performance.

To aim was achieved through the fulfilment of the following research objectives:

1. Analyse academic publications, regulatory legal acts, and standards that define the requirements for digital training of personnel in the field of CBRN protection.

2. Develop the author's Digital Readiness Matrix to assess the level of implementation of simulation technologies in HMEIs.

3. Conduct a comparative analysis of the results of the use of cloud platforms in four countries (Ukraine, Italy, Germany, Austria), determining the CEI.

4. Identify correlations between the level of digital readiness of institutions, the volume of practical training and the quality of CBRN training.

The academic novelty lies in the creation of a comparative Digital Readiness Matrix for CBRN Training and in the integration of Delphi-AHP weighting, CEI calculation, clustering, regression and bootstrap verification into one assessment logic. In contrast to previous studies focused on separate VR, simulation or emergency-response tools, the proposed model produces new knowledge about how digital transformation, security resilience and resilient infrastructure jointly explain differences in CBRN training effectiveness.

The academic hypothesis of the study is that the integration of cloud platforms and network simulators into the training system for applicants to HMEIs ensures an increase in the efficiency of the educational process and the readiness of officer personnel to act in the face of threats. This is achieved through a combination of an adaptive digital environment, dynamic scenario modelling, and analytical monitoring of learning outcomes.

2. LITERATURE REVIEW

The current academic literature focuses on the digitalization of military training systems, particularly in the field of responding to CBRN threats. Most researchers agree that the introduction of cloud platforms, network simulators, and VR technologies is shaping a new paradigm of military education, in which the training process combines combat simulation, analytical tools, and interactive risk management. The researchers [10] showed that the use of Internet of things (IoT) platforms and real-time performance monitoring provides a comprehensive assessment of combat readiness during training. The authors [11] developed a model of a decision support system for missions to avoid and counter CBRN threats, which combines cognitive and technological aspects of analysis. Similarly, the scientists [12] proposed a machine learning (ML) framework that allows for risk identification and optimization of unit actions in real time.

Italian researchers [13] and Lamberti et al. [19] focus on the use of virtual and mixed reality for training CBRN operators. They demonstrate that VR platforms enhance the realism of training and provide flexible customization of scenarios depending on the level of threat. The authors [14] and [15] complement this concept by emphasizing multisensory interaction and psychophysiological feedback in the training process. German researchers [16] consider the infrastructure aspect of digital training by developing resilient communication networks for distributed sensor systems in CBRN scenarios. This study emphasizes the role of information reliability and integration of multisensor systems within military training. Similarly, the authors [17] propose the use of satellite technologies for the detection, monitoring, and modelling of CBRN threats, which demonstrates the growth of interdisciplinarity in military sciences.

The studies [18] are also indicative. They created a computer model of simulation of damage by nerve agents to practice medical response during CBRN incidents. In turn, the authors [20] presented the results of the work of the Countering Weapons of Mass Destruction Office (CWMD), where the analysis of sensor data is used to improve CBRN threat detection systems. Comparative analysis shows a significant difference between countries in the level of development of simulation platforms and digital military ecosystems. In Ukraine, cloud solutions in HMEIs are only being formed, which is confirmed by the study [2]. In Italy, VR/AR technologies are actively used in CBRN training to create virtual combat ranges [13]; [19]. In Germany and Austria, the emphasis is on networked simulators, sensor systems, and telemetric monitoring of critical infrastructure [16]; [17]. Such fragmentation of approaches makes it difficult to form a single model of digital military education that can ensure technological compatibility, secure data exchange, and unified criteria for evaluating learning outcomes.

So, the analysis of academic literature shows that current studies focuses on three main areas:

1) the development of simulation systems and VR platforms for safe training;

2) the creation of intelligent network solutions for CBRN protection;

3) the development of a digital infrastructure for interaction and data exchange.

At the same time, there is a lack of generalized models that would integrate the technical, pedagogical, and organizational parameters of digital training for CBRN threats. This study attempts to fill this gap by proposing the author's Digital Readiness Matrix to assess the effectiveness of implementing cloud and simulation technologies in military education in Ukraine, Italy, Germany, and Austria. Therefore, the results of this study are relevant not only for Ukraine, Italy, Germany, and Austria, but may also be useful for other states that are actively implementing digital solutions in military training – in particular Poland, France, the Czech Republic, Romania, the Baltic States, as well as the USA, Canada, Japan, and South Korea, where issues of cyber resilience, standardization of simulation systems, and interaction between defence agencies are gaining strategic importance. Such an expanded perspective makes the proposed model universal for different regions – Europe, North America and Asia, contributing to the creation of a global ecosystem of digital military education based on common principles of security, interoperability, and technological compatibility.

3. PROPOSED METHODOLOGY

3.1. Research design

The study was carried out in 2024–2025 based on a comparative analysis of military specialist training systems in four countries – Ukraine, Italy, Germany, and Austria, which represent different models of digital integration and simulation training in the field of CBRN protection. Ukraine was chosen as a base country, where the digital transformation of military education is at a stage of intensive development. Italy is a leader in the use of VR/AR technologies in CBRN training. Germany is distinguished by a high level of deployment of network simulators and joint training centres, and Austria demonstrates innovative models of sensor networks and civil-military interaction in the face of CBRN threats.

The methodology combines three interrelated levels of analysis:

1. Analytical and systemic – study of regulatory legal acts, standards, and academic publications on digital training of personnel in the field of CBRN protection;

2.Comparative analysis and modelling – construction of the author's Digital Readiness Matrix based on the selection of key efficiency parameters;

3. Index and analytical – calculation of the CEI and statistical analysis of the relationships between digital readiness indicators, the volume of practical training, and the quality of training.

3.2. Author's Digital Readiness Matrix

The level of implementation of cloud and simulation technologies in the CBRN training of cadets was comprehensively assessed by developing the author's digital readiness matrix. Its structure includes five key components that combine technical, pedagogical, managerial, and security parameters of the digital transformation of military education. Table 1 shows the author's Digital Readiness Matrix for the use of cloud platforms and network simulators in CBRN training of cadets, which include detection, decontamination, modelling the spread of contamination, and coordination of unit response in a digital environment.

Table 1: Author's Digital Readiness Matrix for the use of cloud platforms and network simulators in CBRN training of cadets

Component	Designation	Assessment content	Measurement method	Interpretation
Technical readiness	TG	Level of cloud services deployment, simulator stability, network bandwidth	IT infrastructure audit, latency testing, uptime analysis	Reflects the technological maturity of the learning environment
Pedagogical integration	PI	Part of training modules containing VR/AR elements, network simulations and cloud workshops	Content analysis of curricula, questionnaire surveys of teachers and students	Characterizes the depth of digital implementation in the learning process
Organizational adaptability	OA	Flexibility of management solutions, availability of digital strategy, human resource readiness	Interviews with administration, analysis of regulatory documents of higher educational institutions	Determines the institution's ability to systemic digital change

Security and technical resilience	ST	Level of cyber protection, availability of backup and disaster recovery policies	Expert verification of compliance with ISO/IEC 27001, 23247, MIL-STD 3020 standards	Assess technological security and data protection
Communication interaction	CI	Degree of integration of network simulators into common international training environments	Indicators of participation in joint training, interoperability of LMS systems	Reflects the ability to international digital cooperation

Source: developed by the authors based on [27]; [28]; [30]; [32]; [35].

The ST (Security and Technical Stability) indicator reflects the level of security and technical stability of the digital infrastructure of an educational institution. It includes criteria such as the user access and control policies, action logging and incident monitoring, compliance with international information security standards (ISO/IEC 27001, 23247), the use of multi-level authentication, data backup and recovery, as well as protection of network connections and simulation environments from unauthorized interference. The combination of these parameters determines the stability of the digital system to cyber threats and technical failures during the implementation of educational CBRN scenarios.

Each indicator is evaluated in the range from 0 to 1, after which the results are integrated into the CEI - an index of the efficiency of integration of cloud and simulation technologies.

CEI was determined by using the formula (1):

$$CEI = (0.30 \times TG) + (0.25 \times PI) + (0.20 \times OA) + (0.15 \times ST) + (0.10 \times CI) \quad (1);$$

The weighting coefficients were determined based on the results of an expert survey conducted using the Delphi method in three stages. The assessment was based on comparing the importance of each indicator relative to the others, which ensured the objectivity and balance of the results. Experts independently determined the priority of the five components of the model, after which the assessments were agreed upon using the pairwise comparison method (AHP) and checked for consistency. The study involved 20 specialists (5 each from Ukraine, Italy, Germany, and Austria) with over 10 years of experience in digital education, military training, information security, and CBRN protection. This sample size corresponds to the principles of the Delphi method, which is focused not on representativeness, but on achieving professional consensus, which is sufficient for the reliability of the assessments.

The experts were selected according to the principle of purposive sampling, taking into account academic degree, military rank, participation in international projects, and the availability of publications. Information about the survey was distributed via LinkedIn, ResearchGate and personal electronic invitations within the NATO CBRN Defence Education Consortium. In the first stage, experts completed an online questionnaire (12 questions) in Google Forms, assessing the importance of the components on a five-point scale. In the second stage, the results were agreed upon during online focus group discussions in Zoom, where the moderator coordinated the discussion for 60–90 minutes and recorded the argumentation during the agreement of weighting factors. In the third stage, a statistical check of consistency was carried out using the Kendall coefficient (W = 0.84), which confirmed the stability of the estimates.

The resulting integral CEI indicator reflects the level of digital readiness of institutions and allows for interstate comparison of military training models according to technical and pedagogical parameters: CEI ≥ 0.75 - high level of integration, 0.50–0.74 - medium, < 0.50 - initial stage of digital maturity.

3.3. Methods of analysis

Quantitative processing of the results was carried out using correlation and regression analysis, which made it possible to establish statistically significant relationships between CEI and key variables: the share of practical classes using cloud simulators (in % of total training time); the level of success in completing CBRN training scenarios (in % of tasks completed without security violations); the digital maturity index of the educational institution (*E-Readiness Score*), calculated according to the OECD methodology [35]. Structural differences between countries were determined through clustering using *k-means* in order to distinguish three models of digital integration: highly consolidated (Italy, Germany), balanced (Austria), and scalable (Ukraine). At the qualitative level, pedagogical modelling of digital interaction processes between cadets, teachers, and simulation environments was used. Content analysis of regulatory acts (NATO STANAG 6001 [27]; STANAG 2520 [37]; ISO/IEC 27001 [28]; Directive (EU) 2018/1972 [31]; Regulation (EU) 2024/1183 [eIDAS 2.0] [36]; MIL-STD-3020 [30]; Order of the Ministry of Internal

Affairs of Ukraine No. 579/2018 [34]) provided an assessment of the level of harmonization of national educational and security standards with international requirements for cyber security, digital identification, and interoperability. The MIL-STD-3020 standards [30] defined the requirements for the secure operation of training simulators, while Regulation (EU) 2024/1183 [36] established the regulatory framework for digital identification of users in the EU military and educational systems. The stability of the obtained results was checked though bootstrap modelling (n = 500), which made it possible to calculate confidence intervals (α = 0.05) and ensure the statistical reliability of the parameters of the author's digital readiness matrix.

3.4. Technical environment

The CEI calculation, statistical calculations, and data visualization were performed in the Python 3.12 environment using the Pandas, NumPy, SciPy, scikit-learn, Matplotlib, and Seaborn libraries. Microsoft Power BI and Tableau Public were used to build interactive charts and comparative data panels, which made it possible to display the dynamics of CEI by country and cluster groups in accordance with the requirements of MIL-STD-3020 [30] regarding the safety and control of simulation environments. The analytical background was formed on the basis of materials from the NATO CBRN Defence Centre of Excellence [33, 37], OECD Digital Government Index (2025) [35], EU Digital Education Action Plan (2023) [32], ISO/IEC 23247 (2022) [29], as well as open data from the official websites of military educational institutions in Ukraine, Italy, Germany, and Austria. This methodological architecture provided a comprehensive reproduction of the relationship between the technical, pedagogical, and organizational components of digital training and made it possible to reasonably compare the effectiveness of national models of using cloud platforms and network simulators in the CBRN training system.

4. RESULTS

4.1. Validation of the authors' digital readiness matrix

The validity of the author's Digital Readiness Matrix was tested based on the results of an expert survey conducted using the Delphi method among 20 specialists from Ukraine, Italy, Germany, and Austria. The purpose of the survey was to determine the agreed weights of the five components of the model: TG, PI, OA, ST, and CI. The obtained values shown in Table 2 reflect the average expert ratings normalized in the range of 0–1.

Table 2: Distribution of weight coefficients of the components of the author's Digital Readiness Matrix (Delphi method)

Country	TG	PI	OA	ST	CI	Coefficient of consistency W
Ukraine	0.32	0.24	0.18	0.16	0.10	0.83
Italy	0.29	0.27	0.21	0.14	0.09	0.85
Germany	0.31	0.23	0.22	0.15	0.09	0.86
Austria	0.28	0.25	0.20	0.17	0.10	0.84
Average value	0.30	0.25	0.20	0.15	0.10	0.84

Source: calculated by the authors based on the results of an expert survey (Delphi–AHP, n = 20) and the data from [27–37].

A comparative analysis of Table 2 showed that there are national differences in the structure of weighting factors due to different levels of digital maturity and pedagogical integration of simulation technologies. In Ukraine, experts prioritized technical readiness (TG = 0.32), which reflects the stage of intensive deployment of cloud platforms and modernization of IT infrastructure in military educational institutions. Italian experts highly rated pedagogical integration (PI = 0.27), emphasizing the widespread implementation of VR/AR technologies in preparation for CBRN scenarios. In Germany, organizational adaptability (OA = 0.22) dominates, which indicates the systematic management of digital learning environments and the integration of simulators into interdepartmental platforms. Austria demonstrated the highest security and technical stability (ST = 0.17) due to the combination of the requirements of ISO/IEC 27001, 23247 and MIL-STD 3020 standards in the national military education system.

The Kendall consistency coefficient (W = 0.84) demonstrated the stability of the assessments and a high level of consensus among experts. So, the results of the validation of the author's Digital Readiness Matrix confirmed its ability to reflect real structural differences between national models of implementing cloud and simulation technologies in the military education system. The identified priorities — the technical vector of development in Ukraine, the pedagogical orientation of Italy, the managerial systematicity of Germany, and the security balance of Austria — outline different strategies for digital transformation of CBRN training. The resulting agreed weighting coefficients

create an analytical basis for constructing CEI and further cluster analysis of the digital maturity levels of the studied countries.

4.2. Calculation of CEI

Based on data collected in HMEIs of Ukraine, Italy, Germany, and Austria, the average normalized values of the five components of the author's matrix were calculated: TG, PI, OA, ST, and CI. The CEI was calculated according to formula (1), taking into account the weight coefficients obtained during expert evaluation using the Delphi method. The results of the calculations are given in Table 3.

Table 3: Average values of the components and the CEI in the participating countries

Country	TG	PI	OA	ST	CI	CEI	Digital Maturity Level
Ukraine	0.60	0.52	0.48	0.53	0.57	0.54	Initial
Italy	0.83	0.86	0.80	0.78	0.77	0.81	High
Germany	0.79	0.75	0.80	0.76	0.70	0.78	High
Austria	0.70	0.67	0.65	0.68	0.63	0.69	Medium

Source: calculated by the authors based on data from HMEIs, expert assessments (Delphi–AHP, n = 20) and regulatory documents [27–37].

The results obtained in Table 3 show that Italy (CEI = 0.81) and Germany (CEI = 0.78) have achieved the highest level of digital integration of cloud and simulation technologies in military training. Austria (CEI = 0.69) occupies an intermediate position due to a stable technical base and a moderate pace of pedagogical adaptation. Ukraine (CEI = 0.54) is at the stage of forming institutional mechanisms for digital integration, demonstrating high technical potential, but an insufficient level of organizational coherence and communication interaction. The comparative structure of the CEI indicates three levels of digital maturity: high (≥ 0.75) - Italy, Germany; medium (0.50–0.74) - Austria; initial (< 0.50) - Ukraine. These results confirm the effectiveness of using the Digital Readiness Matrix as an analytical tool for further cluster analysis. Therefore, the results presented in Table 3 are interpreted not only through the numerical values of the index, but also in the form of levels of digital maturity (low, medium, high), which allows the model to be generalized and adapted to different educational and technical contexts. This approach enables assessing not specific values, but general trends in the development of digital integration, which ensures the universality of the model for comparative analysis between countries and institutions.

4.3. Cluster analysis of digital integration models

In order to identify typological differences between countries in terms of the level of digital maturity and the effectiveness of using cloud and simulation technologies in military education, data clustering was performed using the *k-means* method. The input variables were the average values of the five components of the author's Digital Readiness Matrix (TG, PI, OA, ST, CI) and the integral CEI indicator obtained in the previous subsection. The optimal number of clusters ($k = 3$) was determined using the elbow method, which revealed three stable groups of countries with similar digital profiles. The structure of digital integration is shown in Figure 1.

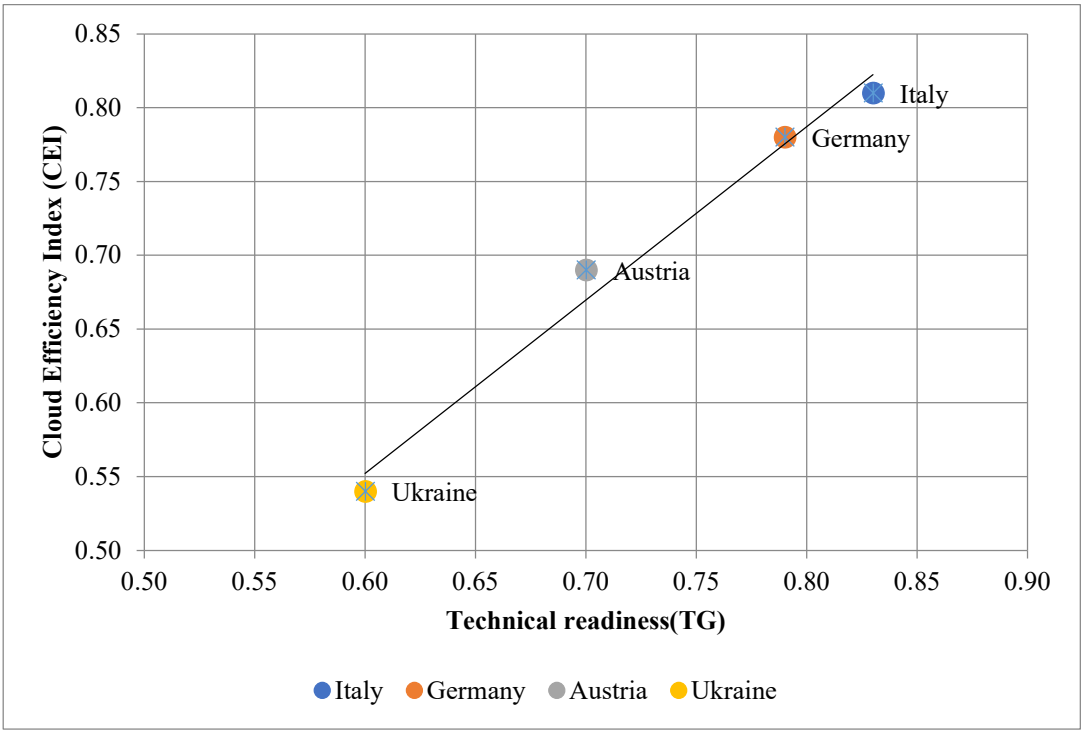

Figure 1: Cluster structure of digital integration of systems for CBRN training (k-means)
Source: constructed by the authors based on empirical data from HMEIs and expert assessment (Delphi–AHP, n = 20)

The clustering results shown in Figure 1 show that Italy and Germany form a highly consolidated cluster, characterized by a combination of high technical readiness (TG > 0.75) with advanced pedagogical integration (PI > 0.80) and stable organizational mechanisms to support digital transformation. This cluster corresponds to the NATO digital maturity model, where cloud platforms and VR/AR simulators are integrated into joint CBRN training systems. Austria belongs to a balanced cluster, characterized by a harmonious combination of technical, organizational and security parameters (TG ≈ 0.70; ST ≈ 0.68; OA ≈ 0.65). Its model is characterized by a moderate pace of digital integration, an emphasis on ISO/IEC 27001 and 23247 standards, and a high level of interagency coordination between military and civilian structures. Ukraine has formed a developing cluster in which the process of digitalization of military education is at the stage of formation. It is characterized by high variability of the TG (0.60) and CI (0.57) indicators with relatively lower values of PI (0.52) and OA (0.48), which indicates the gradual introduction of simulation technologies within the framework of limited resources and modernization of IT infrastructure. So, the cluster analysis confirmed that the depth of digital integration in the field of CBRN training is determined not only by the technical potential, but also by the level of pedagogical adaptation, managerial support, and regulatory harmonization. The resulting three-level structure – highly consolidated (Italy, Germany), balanced (Austria) and developing (Ukraine) – creates a conceptual basis for further analysis of the relationships between CEI and the parameters of the effectiveness of practical training.

4.4. Correlation and regression analysis of relationships

The relationship between the level of digital readiness of military educational institutions and the results of practical training was quantitatively confirmed through a correlation and regression analysis. The study used CEI, the share of practical training using simulators (% of the total training time), and the success rate of CBRN training (% of tasks completed without violating safety requirements). The results showed statistically significant positive correlations: between CEI and the share of practical training using simulators ($r = 0.82$, $p < 0.05$), as well as between CEI and the level of success in performing CBRN scenarios ($r = 0.77$, $p < 0.05$). This indicates that an increase in the level of digital integration directly correlates with the quality of practical training and a decrease in the

number of safety violations during training. The constructed linear regression model demonstrated a high coefficient of determination ($R^2 = 0.68$), which means that almost 70% of the variation in learning outcomes is explained by changes in the level of digital readiness. Testing the stability of the results using the bootstrap method ($n = 500$) showed minimal fluctuations in the mean values, and the 95% confidence intervals remained within ± 0.03, which confirms the reliability of the model. Figure 2 presents a graphical interpretation of the regression relationship between CEI and the level of success in implementing the CBRN scenarios, which demonstrates an increasing linear trend and the absence of outliers that could indicate structural distortions in the data.

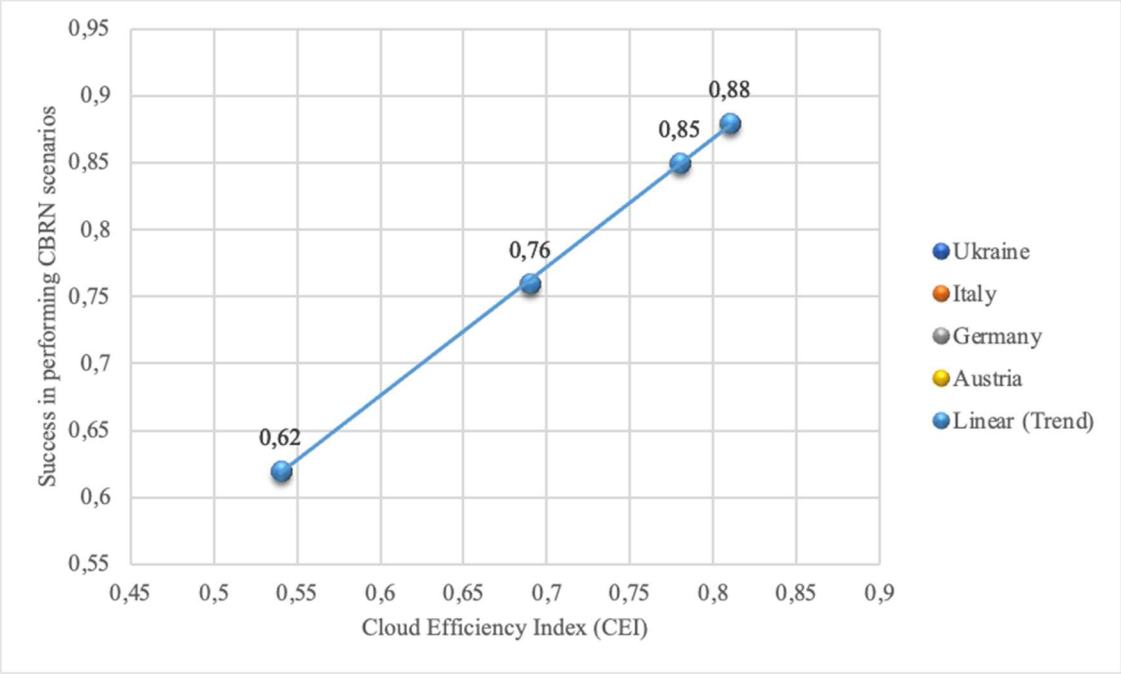

Figure 2: Regression relationship between CEI and the level of success of implementing CBRN scenarios (bootstrap model)

Source: calculated and built by the authors in Python 3.12 using Pandas, NumPy, SciPy, and Matplotlib libraries based on data from higher education institutions of four countries (Ukraine, Italy, Germany, Austria)

Figure 2 shows that there is a clear positive linear relationship between CEI and the level of success in implementing the CBRN scenarios: the observation points tend to an upward regression line, and the value of the coefficient of determination $R^2 = 0.68$ confirms that approximately two-thirds of the variation in learning outcomes is explained by changes in the level of digital readiness. Italy and Germany are located in the upper right sector of the graph with higher CEI values and, accordingly, higher success in implementing the scenarios. Austria occupies an intermediate position with moderate values of both indicators, while Ukraine is located in the lower left part of the field, demonstrating lower results, but consistent with the trend. No outliers were recorded; bootstrap estimation (n = 500) provided narrow 95% confidence intervals (±0.03) for the model parameters, which further confirms its stability and suitability for further interpretation.

Summarizing the results of the correlation and regression analysis, it can be stated that the digital integration of cloud platforms and network simulators in the military education system has a direct impact on the effectiveness of practical CBRN training. The obtained values of the correlation and determination coefficients indicate a strong linear relationship between the level of digital readiness of educational institutions and the quality of implementation of practical scenarios, which confirms the pedagogical and technical feasibility of using simulation technologies. The consistency of the data and the stability of the bootstrap evaluation results demonstrate the reliability of the constructed model and its suitability for predicting learning outcomes in further studies. So, the digital maturity of military educational institutions is a key factor in increasing the safety, accuracy, and effectiveness of personnel training for actions in crisis conditions.

4.5. Comparative characteristics of participating countries

A comparative analysis of the systems for CBRN training students of HMEIs has shown that the level of digital integration of cloud platforms and network simulators differs significantly depending on the national strategies for digitalization of defence education, regulatory support, and technical capabilities. In Italy and Germany, digital technologies are a component of the integral infrastructure of military training, while in Ukraine and Austria the modernization process is evolutionary and is at the scaling stage. The comparative characteristics are given in Table 4.

Table 4: Comparative characteristics of the implementation of cloud platforms and network simulators in military educational institutions of the participating countries

Country	Nature of cloud platform implementation	Use of VR/AR technologies	Level of network integration	Compliance with international standards	Existing regulations
Ukraine	Initial scaling phase; deployment of individual cloud environments	Partial use of VR modules in CBRN protection courses	Local simulation networks without inter-agency integration	Partial compliance with ISO/IEC 27001, MIL-STD 3020	Orders of the Ministry of Internal Affairs No. 579/2018, Ministry of Defence No. 331/2023
Italy	Full integration into *CBRN Training Cloud*	VR/AR complexes developed in Modena, Turin academies	Inter-agency integration with *NATO CBRN Network*	Full compliance with STANAG 2520, ISO/IEC 23247, eIDAS 2.0	*EU Digital Education Action Plan (2023)*
Germany	Usage of cloud solutions in *Bundeswehr Simulation Center*	VR/AR modules in CBRN response scenarios	High integration in *Defence Cloud Germany*	Compliance with STANAG 2520, MIL-STD 3020, ISO/IEC 27001	*NATO Standardization Office (2023)*
Austria	Partial deployment within *Digital Defence 2025*	Using AR environments for joint exercises	Medium level of integration with *EU CBRN Resilience Network*	High compliance with ISO/IEC 27001, 23247	Focus on civil-military interaction; *Regulation (EU) 2024/1183*

Source: compiled by the authors based on the data from NATO CBRN Defence Centre of Excellence [33, 37], *OECD Digital Government Index (2025)* [35], *Regulation (EU) 2024/1183 [eIDAS 2.0]* [36], *ISO/IEC 27001* [28], *STANAG 2520* [37], *MIL-STD 3020* [30], *orders of the Ministry of Internal Affairs and the Ministry of Defence of Ukraine [34]*

Table 4 shows that Italy has the highest level of integration of cloud platforms and VR/AR modules into the CBRN Training Cloud system, which combines simulation environments and automated evaluation of training scenarios in accordance with STANAG 2520, ISO/IEC 23247, and Regulation (EU) 2024/1183 [eIDAS 2.0]. Germany is implementing the Bundeswehr Simulation Centre and Defence Cloud Germany model with a high level of interdepartmental integration, compliance with MIL-STD 3020 and ISO/IEC 27001 and multi-level access protection. Austria is developing a balanced Digital Defence 2025 system in cooperation with the EU CBRN Resilience Network and focusing on ISO/IEC 27001 and 23247, where VR/AR environments are used mainly in joint exercises. In Ukraine, digital modernization is at the formation stage and is regulated by Orders of the Ministry of Internal Affairs No. 579/2018 and the Ministry of Defence No. 331/2023; although the regulatory framework is still partially aligned with international standards, there is a gradual increase in technical and pedagogical readiness. In general, Italy and Germany represent a highly consolidated type of digital integration. Austria is balanced, while Ukraine is moving towards the systematic implementation of cloud and simulation technologies; the effectiveness of digital transformation depends on the degree of compliance with international standards and the level of strategic management of educational processes. The relationship between CEI components, the level of technical readiness, and the effectiveness of cadet training is presented in Figure 3.

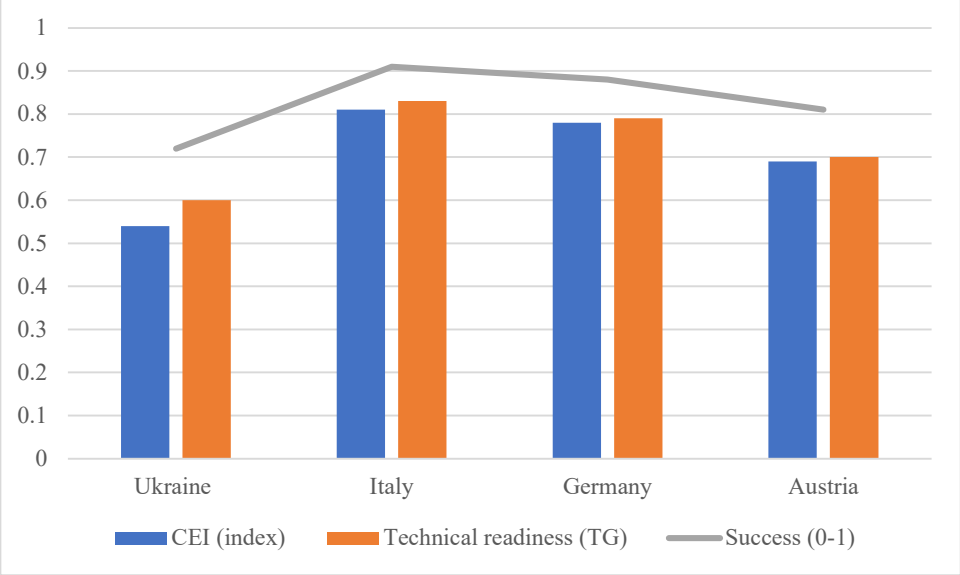

Figure 3: Integrated visualization of CEI indicators in the CBRN training system
Source: calculated and built by the authors in the Power BI / Tableau environment

Figure 3 shows that Italy demonstrates the highest indicators for both the integral CEI (0.81) and the level of technical readiness TG (0.83), which correlates with the highest success rate of implementation of CBRN scenarios (91%). Germany has slightly lower values – CEI = 0.78, TG = 0.79 and success rate of 88%, which indicates stable but less intensive digital integration. Austria has a slightly lower level (CEI = 0.69, TG = 0.70, success rate of 81%), which may be due to the limited use of simulation environments. Ukraine showed the lowest values (CEI = 0.54, TG = 0.60, success rate of 72%), which indicates the initial stage of integration of cloud platforms into the training of cadets. The general trend indicates a direct relationship between digital maturity, technical readiness, and the effectiveness of the educational process. Summing up the results of the study, it should be noted that the comprehensive analysis made it possible to empirically confirm the relationship between the level of digital readiness of military education systems and the effectiveness of practical CBRN training. Validation of the author's Digital Readiness Matrix using the Delphi method demonstrated its reliability and representativeness for assessing the technical, organizational and pedagogical aspects of digital integration. Calculation of the CEI revealed significant inter-country differences: Italy and Germany have achieved a high level of digital maturity due to the integration of VR/AR systems and standardization according to STANAG, ISO and eIDAS, Austria is characterized by a balanced combination of security and technical components, while Ukraine is at the stage of institutional formation of digital infrastructure. Clustering of CEI indicators confirmed the existence of three types of digital integration – highly consolidated, balanced and scalable. Correlation and regression analysis (R^2 = 0.68) proved that the level of digital readiness directly determines the quality of practical training. The obtained results showed an increasing relationship between technical readiness, CEI and training effectiveness, which confirms the strategic role of cloud platforms and network simulators as key elements of the modern military education system in Ukraine, Italy, Germany, and Austria.

5. DISCUSSION

The obtained results of the study confirmed that the effectiveness of using cloud platforms and network simulators in CBRN training of students of HMEIs is determined not only by the level of technical equipment, but primarily by the degree of integration of digital technologies into the pedagogical and organizational structure of the educational process. This pattern is consistent with the conclusions of the authors [20], who emphasize that the effectiveness of CBRN training systems directly depends on the quality of data exchange between training environments, detection means, and management systems. High CEI values in Italy (0.81) and Germany (0.78) are explained by the complex interaction of VR/AR modules, as well as command and training networks, which ensures the unity of technical, analytical and pedagogical aspects of training. This is consistent with the approach of [21], which considers digital simulation systems as a

key element of dual-use risk management in the CBRN sphere.

The German and Italian models confirmed the findings [22] regarding the growing role of MASINT systems in improving the analytical functions of training simulators: it is the combination of sensor networks and cloud architectures that creates the conditions for operational analysis of threat scenarios. The obtained results revealed that an increase in CEI by 0.1 is accompanied by an average increase in the success rate of CBRN training scenarios by 6–8%, which confirms the correlation relationship ($r = 0.77$; $p < 0.05$) between the level of digital readiness and the quality of practical training. The positive slope of the regression model indicates that technical modernization directly affects pedagogical results, i.e. digital tools are not only auxiliary, but become the basis of practical training.

The Austrian model, as evidenced by the data, has a balanced but cautious nature of integration, which is consistent with the studies [23], indicating the complexity of implementing sensor networks in urban environments because of the risks of communication channel overload and regulatory constraints. This partly explains the lower values of CEI = 0.69, combined with moderate indicators of technical readiness (TG). At the same time, the Austrian strategy demonstrates the benefits of interagency coordination and harmonization with the civilian sector, which confirms the appropriateness of integrating defence and crisis services within a single digital infrastructure. The results for Ukraine indicated a gradual but clear trend towards increasing digital readiness (CEI = 0.54). As the authors [24] emphasized, optimization of investments in CBRN training is possible only if simulation platforms are standardized and common cloud resources are created. In the Ukrainian context, the limitations are associated with the fragmentation of the regulatory framework and the insufficient level of technical unification between the departments of different HMEIs, however, the positive dynamics of the implementation of digital simulators indicates a sustainable trend.

The obtained results are consistent with the findings [25], which prove that the effectiveness of CBRN training depends on the readiness of personnel to act in a multi-level digital crisis management system. In this regard, the CEI model developed in the study confirmed the key role of the integration of VR/AR environments, cloud services and pedagogical strategies in increasing the practical competence of cadets.

The general trends are consistent with the findings [26], which emphasize that simulation models based on CFD and artificial intelligence provide accurate reproduction of chemical and biological processes, building real-time decision-making skills in applicants. Accordingly, the results of correlation and regression analysis and clustering in this work showed that only countries with a high level of technical consolidation (Italy, Germany) achieve a stable pedagogical effect and safety of training.

The study not only confirmed the general conclusions of the modern military and pedagogical literature, but also proposed a new quantitative model for assessing the effectiveness of digital integration in the context of CBRN threats. Comparison of the obtained results with international studies showed that the success of digital transformation in military education is determined by the balance between technical capabilities, pedagogical adaptation, and regulatory coherence. This opens up prospects for further interdisciplinary research aimed at developing tools for assessing digital maturity, the resilience of educational systems to cyber threats, and the integration of international standards STANAG 2520, ISO/IEC 27001 and ISO/IEC 23247 into the structure of military education. So, the hypothesis put forward in the study that the integration of cloud platforms and network simulators into the training system for applicants to HMEIs increases the effectiveness of the educational process and the readiness of officer cadres to act in conditions of CBRN threats was fully confirmed.

6. LIMITATIONS

The results of the study must be interpreted taking into account a number of methodological and practical limitations. First, the analysis of digital integration of cloud platforms and network simulators covered only four countries – Ukraine, Italy, Germany and Austria, which limits the possibility of generalizing the conclusions to other countries with different levels of digital maturity, technical infrastructure or regulatory regulation. Second, the CEI was formed on the basis of five components (TG, PI, OA, ST, CI), while additional factors – financing, staffing, level of cyber protection, socio-psychological readiness of personnel – were not included in the model due to limited empirical data. Third, the determination of weighting coefficients using the Delphi–AHP method was carried out on a relatively small sample of experts ($n = 20$), which may affect the accuracy of interpretation and reproducibility of the results. In addition, the analysis of practical effectiveness was

based on generalized indicators of the effectiveness of the implementation of training RCB scenarios without taking into account the specifics of individual subjects or levels of training. The socio-economic, cultural and ethical aspects of the digital transformation of military education, which potentially affect the pace of integration of innovations, were not considered. Further research should be directed at expanding the geography of the sample, involving time series for dynamic analysis of digital maturity, taking into account institutional and behavioural factors, as well as developing tools for monitoring the impact of digital integration on the quality of education and the safety of the educational environment. This will increase the validity of the CEI model and provide a deeper understanding of the mechanisms of the digital transformation of military education. It is worth noting that the results of the model may differ in other organizational contexts, technological conditions or implementation methods, in particular when changing the principles of data collection or calibration of weight coefficients. In further studies, it is appropriate to expand the sample of objects of analysis and detail the criteria for evaluating individual CEI components, adapting them to the specifics of different educational and military systems.

7. CONCLUSIONS

The study confirmed that the effectiveness of digital integration in military education directly depends on the level of technical readiness, pedagogical adaptability, organizational coherence, and compliance with international standards. A comparison of the models of Ukraine, Italy, Germany and Austria showed significant differences in the structure of digital maturity, which is reflected in the CEI. The highest CEI indicators were recorded in Italy (0.81) and Germany (0.78), where digital simulators are integrated into VR/AR complexes and interdepartmental cloud networks, fully consistent with STANAG 2520, MIL-STD 3020, ISO/IEC 23247 and Regulation (EU) 2024/1183 (eIDAS 2.0). Austria (CEI = 0.69) is characterized by a balanced combination of technical and security parameters within the *Digital Defence* 2025 programme, while Ukraine (CEI = 0.54) demonstrates a gradual transition from fragmented solutions to the systematic implementation of cloud and simulation technologies. Correlation and regression analysis confirmed a strong relationship between the level of digital readiness and training effectiveness ($r = 0.82$; $R^2 = 0.68$), which indicates the decisive role of digital tools in improving the quality of CBRN training. Data clustering distinguished three types of digital integration: highly consolidated (Italy, Germany), balanced (Austria), and buildable (Ukraine), each reflecting different levels of maturity of educational and technological systems. The practical value of the study is the formation of an analytical model of CEI suitable for assessing the effectiveness of the digital transformation of military education, planning the modernization of the educational infrastructure and harmonizing the regulatory and technical base with European standards. The academic novelty of the study is the combination of Delphi–AHP methods, cluster, correlation and regression, as well as bootstrap analysis in a single system for quantitative measurement of the digital maturity of military educational institutions. Prospects for further research are associated with expanding the sample of countries, developing an adaptive scale for assessing the digital competence of personnel and testing the impact of simulation technologies on behavioural readiness for action in crisis situations.

The scientific contribution of the work is the development of a CEI-based assessment model that advances the current state of the art from descriptive analysis of separate simulation technologies to a measurable framework for comparing national CBRN training systems. The study demonstrates that the effectiveness of cloud platforms and network simulators should be evaluated through the combined interaction of technical readiness, pedagogical integration, organizational adaptability, security and technical resilience, and communication interoperability. This contribution clarifies why the same category of digital tools may produce different training outcomes in different institutional environments and provides a transferable analytical basis for monitoring digital transformation in military education.

REFERENCES:

[1] V. Shemchuk, O. Khatsaiuk, V. Sokolovsky, A. Kovtunenko, O. Kornienko, & Yu. Mushtatov, “Formation of Professional Competencies of Future Officers to Act in Conditions of Radiation, Chemical and Biological Danger”, Military Education, Vol. 1, No. 43, 2021, pp. 360-380. https://doi.org/10.33099/2617-1783/2021-43/360-380

[2] V. V. Chepkii, V. V. Skachkov, O. M. Yefymchykov, V. K. Nabok, O. D. Yelchaninov, & S. M. Osypenko, “Cloud Solutions for the Implementation of Hybrid IT-Infrastructure of the Information and Educational Environment of

a Higher Military Educational Institution", Collection of Scientific Works of Odesa Military Academy, Vol. 1, No. 19, 2023, pp. 189–202. https://doi.org/10.37129/2313-7509.2023.19.189-202

[3] G. Regal, D. Pretolesi, H. Schrom-Feiertag, J. Puthenkalam, M. Migliorini, E. De Maio, ... & M. Murtinger, "Challenges in Virtual Reality Training for CBRN Events", Multimodal Technologies and Interaction, Vol. 7, No. 9, 2023, p. 88. https://doi.org/10.3390/mti7090088

[4] A. Alshowair, J. Bail, F. AlSuwailem, A. Mostafa, & A. Abdel-Azeem, "Use of Virtual Reality Exercises in Disaster Preparedness Training: A Scoping Review", SAGE Open Medicine, Vol. 12, 2024, Art. 20503121241241936. https://doi.org/10.1177/20503121241241936

[5] O. O. Popov, Y. O. Kyrylenko, I. P. Kameneva, A. V. Iatsyshyn, A. V. Iatsyshyn, V. O. Kovach ... & A. E. Kiv, "The Use of Specialized Software for Liquid Radioactive Material Spills Simulation to Teach Students and Postgraduate Students", CTE Workshop Proceedings, Vol. 9, 2022, pp. 306-322. https://doi.org/10.55056/cte.122

[6] P. Gaman, T. Yarovoi, T. Shestakovska, O. Akimov, & L. Akimova, "Institutional Platform to Ensure the Interaction between the Subjects of Combating Medical and Biological Emergencies Mechanism", Economic Affairs, Vol. 67, No. 4s, 2022, pp. 765-775. http://doi.org/10.46852/0424-2513.4s.2022.10

[7] O. Illiashenko, V. Kharchenko, I. Babeshko, H. Fesenko, & F. Di Giandomenico, "Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-powered Cyberattacks and Protection", Entropy, Vol. 25, No. 8, 2023, Art. 1123. https://doi.org/10.3390/e25081123

[8] Y. Liu, & K. Zhu, Application of virtual simulation technology in university laboratory safety education. In 3rd International Conference on Internet, Education and Information Technology (IEIT 2023). Paris: Atlantis Press, 2023, pp. 946-953. https://doi.org/10.2991/978-94-6463-230-9_114

[9] S. G. Fussell, & D. Truong, "Using Virtual Reality for Dynamic Learning: An Extended Technology Acceptance Model", Virtual Reality, Vol. 26, No. 1, 2022, pp. 249-267. https://doi.org/10.1007/s10055-021-00554-x

[10] R. Raman, & L. Vyakaranam, "IoT-Enabled Smart Military Training for Virtual Simulation and Real-Time Performance Analysis", In 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), IEEE, Chennai (India), 18-19 April 2024, pp. 1-6. https://doi.org/10.1109/ADICS58448.2024.10533460

[11] C. Nemeth, J. Sedehi, G. Rule, J. Di Pietrantonio, D. Laufersweiler, N. Keeney, & R. Clark, "Decision Support for CBRN Avoid and Protect Missions", Cognition, Technology & Work, Vol. 26, No. 3, 2024, pp. 375-384. https://doi.org/10.1007/s10111-024-00767-5

[12] T. Kegyes, Z. Süle, & J. Abonyi, "Machine Learning-Based Decision Support Framework for CBRN Protection", Heliyon, Vol. 10, No. 4, 2024. https://www.cell.com/heliyon/fulltext/S2405-8440(24)01977-7

[13] B. Altan, S. Gürer, A. Alsamarei, D. K. Demir, H. Ş. Düzgün, M. Erkayaoğlu, & E. Surer, "Developing Serious Games for CBRN-e Training in Mixed Reality, Virtual Reality, and Computer-Based Environments", International Journal of Disaster Risk Reduction, Vol. 77, 2022, Art. 103022. https://doi.org/10.1016/j.ijdrr.2022.103022

[14] M. Sedláček, D. Slatkovský, & J. Kompan, "Improving Explosive Ordnance Disposal Training: Determinants and Solutions in Virtual Reality Environments", In 2024 International Conference on Computing in Natural Sciences, Biomedicine and Engineering (COMCONF), IEEE, Shanghai (China), 9-12 August 2024, pp. 127-135. https://doi.org/10.1109/COMCONF63340.2024.00026

[15] A. C. Pogmore, R. J. Davies, & N. J. Cooke, "Virtual Versus Reality: A Systematic Review of Real-World Built Environment Tasks Performed in CAVEs and a Framework for Performance and Experience Evaluation", Virtual Worlds, Vol. 3, No. 4, 2024, pp. 536-571. https://doi.org/10.3390/virtualworlds3040028

[16] S. Sporrer, N. Niemann, & C. Hammer, "Critical Infrastructure Monitoring in CBRNe Scenarios: A Reliable and Robust Communication Network for Distributed Multimodal Sensors", The European Physical Journal Plus, Vol. 139, No. 9, 2024, p. 783. https://doi.org/10.1140/epjp/s13360-024-05583-4

[17] G. Sutlieff, L. Berthoud, & M. Stinchcombe, "Using Satellite Data for CBRN (Chemical,

Biological, Radiological, and Nuclear) threat Detection, Monitoring, and Modelling", Surveys in Geophysics, Vol. 42, No. 3, 2021, pp. 727-755. https://doi.org/10.1007/s10712-021-09637-5

[18] R. De Rouck, M. Benhassine, M. Debacker, C. Dugauquier, E. Dhondt, F. Van Utterbeeck, & I. Hubloue, "Creating Realistic Nerve Agent Victim Profiles for Computer Simulation of Medical CBRN Disaster Response", Frontiers in Public Health, Vol. 11, 2023, Art. 1167706. https://doi.org/10.3389/fpubh.2023.1167706

[19] F. Lamberti, F. De Lorenzis, F. G. Pratticò, & M. Migliorini, "An Immersive Virtual Reality Platform for Training CBRN Operators", In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), IEEE, Madrid (Spain), 12-16 July 2021, pp. 133-137. https://doi.org/10.1109/COMPSAC51774.2021.00030

[20] E. M. Abdelhadi, M. D. Watson, S. Purohit, Q. J. Wright-Mockler, B. R. Morton, & P. L. McKenzie, Countering Weapons of Mass Destruction Office (CWMD) Data Categorization Study: Chemical, Biological, Radiological, and Nuclear (CBRN) Detection Device Data (No. PNNL-36023). Pacific Northwest National Laboratory (PNNL), Richland, WA (United States), 2024. https://doi.org/10.2172/2479297

[21] A. Vaseashta, Existential Risks with Dual-Use Technologies Across Nano, Cyber, and CBRN Domains. In International Scientific Conference Management and Engineering, Dordrecht: Springer Netherlands, 2024, pp. 3-27. https://doi.org/10.1007/978-94-024-2316-7_1

[22] E. Rios, & D. Frascà, "Latest Trends in MASINT Technologies for CBRNe Threats", Advances in Military Technology, Vol. 19, No. 1, 2024, pp. 131-147. https://doi.org/10.3849/aimt.01876

[23] W. Seböck, B. Biron, & B. Pospisil, "Challenges and Implementation of CBRN Sensor Networks in Urban Areas", In International Conference on Information Technology in Disaster Risk Reduction, Cham: Springer Nature Switzerland, 2022, pp. 136-149. https://doi.org/10.1007/978-3-031-34207-3_9

[24] S. Choudary, G. P. Xerri, M. Carestia, O. Vybornova, J. L. Gala, M. F. Van De Vorst,... & D. Di Giovanni, "Development of a Methodology for Pooling Resources and Optimising Investments in the Field of CBRN Training and Capacity Building", International Journal of Safety and Security Engineering, Vol. 14, No. 3, 2024, pp. 933-940. https://doi.org/10.18280/ijsse.140324

[25] H. Farhat, G. Alinier, K. Chaabna, K. El Aifa, W. Abougalala, J. Laughton, & M. Ben Dhiab, "Preparedness and Emergency Response Strategies for Chemical, Biological, Radiological and Nuclear Emergencies in Disaster Management: A Qualitative Systematic Review", Journal of Contingencies and Crisis Management, Vol. 32, No. 3, 2024, Art. e12592. https://doi.org/10.1111/1468-5973.12592

[26] F. Marturano, L. Martellucci, A. Chierici, A. Malizia, D. D. Giovanni, F. d'Errico,... & J. F. Ciparisse, "Numerical Fluid Dynamics Simulation for Drones' Chemical Detection", Drones, Vol. 5, No. 3, 2021, p. 69. https://doi.org/10.3390/drones5030069

[27] NATO Standardization Office, STANAG 6001 – Language Proficiency Levels in the NATO Armed Forces. Brussels, Belgium: NATO, 2014. [Online]. Available: https://nuou.org.ua/assets/documents/dodb_stanag_6001.pdf [Accessed: February 12 2026].

[28] International Organization for Standardization, ISO/IEC 27001:2018 – Information security management systems – Requirements. Geneva, Switzerland: ISO, 2018. [Online]. Available: https://www.iso.org/standard/54534.html [Accessed: February 12 2026].

[29] International Organization for Standardization, ISO/IEC 23247 – Digital Twin Framework for Manufacturing. Geneva, Switzerland: ISO, 2022. [Online]. Available: https://www.iso.org/standard/75066.html [Accessed: February 12 2026].

[30] U.S. Department of Defense, MIL-STD-3020: Safety, Environmental, and Health Requirements for Training Simulations. Washington, DC, USA: DoD, 2020. [Online]. Available: http://everyspec.com/MIL-STD/MIL-STD-3000-9999/MIL-STD-3020_11625/ [Accessed: February 12 2026].

[31] European Union, Directive (EU) 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code, Official Journal of the European Union, L 321, pp. 36–214, 2018. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2018/1972/oj [Accessed: February 12 2026].

[32] European Commission, Digital Education Action Plan (2021–2027): Resetting Education and Training for the Digital Age. Brussels,

Belgium: European Commission, 2023. [Online]. Available: https://education.ec.europa.eu/focus-topics/digital-education/action-plan [Accessed: February 12 2026].

[33] CBRN Defence Response, Annual Report 2023, 2023. [Online]. Available: https://www.jcbrncoe.org/app/uploads/2024/09/CBRN_1_2023_web.pdf [Accessed: February 12 2026].

[34] Ministry of Internal Affairs of Ukraine, On Approval of the Charter of Actions in Emergency Situations of the Management Bodies and Units of the Operational and Rescue Service of Civil Protection and the Charter of Actions of the Management Bodies and Units of the Operational and Rescue Service of Civil Protection during Firefighting (Order No. 579, July 5, 2018). Kyiv, Ukraine: Ministry of Internal Affairs of Ukraine, 2018. [Online]. Available: https://zakon.rada.gov.ua/laws/show/z0801-18#Text [Accessed: February 12 2026].

[35] OECD, Government at a Glance 2025: Full Report. Paris, France: OECD Publishing, 2025. [Online]. Available: https://www.oecd.org/en/publications/government-at-a-glance-2025_0efd0bcd-en.html [Accessed: February 12 2026].

[36] European Union, Regulation (EU) 2024/1183 of the European Parliament and of the Council on a framework for a European Digital Identity (eIDAS 2.0), Official Journal of the European Union, L 2024/1183, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183 [Accessed: February 12 2026].

[37] NATO Standardization Office, STANAG 2520 – CBRN Defence Standards for Education, Training and Evaluation (ATP-3.8.1, Vol. III). Brussels, Belgium: NATO Standardization Office, 2023. [Online]. Available: https://nllp.jallc.nato.int/cmnt/ciedcoi/CIED%20PUBLICATIONS/STANAGs/STANAG%2520%20CBRN%20defence%20standards%20for%20Education%2C%20Training%20and%20Evaluation%20ATP%203.8.1.%20vol.%20III.pdf [Accessed: February 12 2026].