30. évfolyam (2020) 2. szám 127–142. • DOI: 10.32562/mkk.2020.2.10

MŰSZAKI
KATONAI
KÖZLÖNY

Gergely Kovács[1]

Possibilities and Dangers of the Use of Digital (VR, AR) Devices in the Training System of the Defence Personnel

A kiterjesztett valóság és virtuálisvalóság-alapú eszközök felhasználásának lehetőségei és veszélyei a védelmi szféra kiképzési rendszerében

Modernising the methods of adult education is an essential issue not only because of the generational change and the pertaining transformation of its learning style, but also because of the current digital changes and the reduction in costs and efficiency gains. In the civil sector, this change has already started, but the use of modern procedures and digital tools in education and training in the defence sector is just as important. Effectiveness and security depend not only from indicators known in the civil sphere, but also from a number of other conditions, due to a much more complex system. Due to the digital nature of modern training solutions and tools, it is also important to look at the issue of cyberspace security separately before future application and deployment. The author will review the development potential of the defence bodies' training system in IT tools. This study also analyses the use of modern procedures and digital devices, such as augmented reality and virtual reality goggles, and what potential security issues are raised during training.

Keywords: *disaster management, fire department training, training, digitisation, cybersecurity, augmented reality, virtual reality*

A felnőttképzés módszereinek modernizálása nemcsak a generációk változása és tanulási stílusának átalakulása miatt létkérdés, hanem a jelenlegi digitális változások és a költségek csökkenése és a hatékonyság növelése miatt is elengedhetetlen. A civil szférában ez a változás már elindult, de modern eljárások és digitális eszközök felhasználása a védelmi szférában történő oktatásban, képzésben ugyanolyan fontos. Itt az eredményesség és a biztonság nemcsak a civil szférában ismert

[1] University of Public Service, Doctoral School of Military Technology, e-mail: kovacs.gergely@uni-nke.hu, ORCID: 0000-0002-1995-394X.

mutatókon múlik, hanem – a jóval komplexebb rendszerből adódóan – több más feltételen is. A modern képzési megoldások és eszközök digitális jellege miatt fontos, hogy a későbbi alkalmazás és bevezetés előtt külön vizsgáljuk a kibertér biztonságának kérdését is. A szerző a cikkben áttekinti, hogy a védelmi szervek állománya képzési rendszerében milyen fejlesztési lehetőségek rejlenek az informatikai eszközökben. Elemzi, hogy a korszerű eljárások és digitális eszközök használata, mint például a kiterjesztett valóság és a virtuálisvalóság-szemüveg, milyen lehetséges kiberbiztonsági kérdéseket vetnek fel a képzés során.

Kulcsszavak: *katasztrófavédelem, tűzoltóság, felkészítés, kiképzés, digitálizáció, kiberbiztonság, kiterjesztett valóság, virtuális valóság*

1. Introduction

Reading the daily news one can see that the challenges we face over the next decade will have a significant impact on the lives and health of the population. Protection against threats is a social task, so all states respond to this. Current security challenges, such as natural disasters, migration, new modern chemical plants and the associated increased road, air and water transport, the accelerated pace of life, create a changing environment in which resilience to threats is a prerequisite for survival. Over the past decade, our country has responded adequately to the threats to our security. The complex system of domestic protection works, and an integral part of it is preparation. Whether we are talking about defence or disaster management tasks, it is the responsibility of professional bodies and the defence management to train and prepare those involved in the performance of defence tasks. The question arises, if the responses to the new challenges mentioned above are available, what kind of new and efficient methods and tools can be used to encourage the specialised personnel to utilise them, and whether, in the era of the Fourth Industrial Revolution, we have integrated into training all sophisticated digital tools which NGOs routinely use in education. The question is what tools can be included in the training system that can increase the efficiency of education, and what dangers we need to address when using these tools. Because of the digital nature of these devices, we need to think most about the security challenges of cyberspace. It is known that as soon as a new technology develops, one tries to exploit it and in many cases attack or weaken it. This was also true for the internet, smartphones, social media networks and online games.[2] It is important to understand these vulnerabilities and find a solution.

[2] In the information society, information is collected from many sources, which are layered and overlapped. The qualitatively new and compressed information, which is multi-controlled and synchronised with automatic data fusion and correlation information technology, is a so-called ‘re-enactment’ for society or for certain groups and organisations. Information superiority, the long-term existence of information control, ultimately provide driving superiority over the other party. The holder of the information superiority enables him/her to gain advantage in different areas of social life by taking advantage of his/her information communication systems and their capabilities, or to constantly control the situation in such a way that the other parties are deprived of these abilities. László Üveges, *A Magyar Köztársaság katasztrófa-veszélyeztetettsége és az arra adandó válaszok,* doktori értekezés (Budapest: ZMNE, 2002).

In this article, I set out to examine the possibilities of using digital educational tools in the framework of domestic and international e-learning methods in the training of defence personnel that are not yet prevalent in all areas of current training. The main focus of this study is the application of virtual reality solutions (hereinafter referred to as VR)[3] during training. I am also looking for answers to cybersecurity questions about the use of these new tools. In order to be able to propose ways to apply these digital[4] procedures, it is important to know what we want to use and what training system we want to include. The defence organisations operating in our defence system are diverse and therefore it is not possible to examine all of them within the framework of this article. Therefore, in the next chapter I will examine the modern techniques that can be used in the training and preparation of those involved in disaster eradication and the performance of defence tasks.

This analysis is based on the processing of relevant legislation and other regulators (for example educational strategies) and an evaluation of studies and analyses related to the subject. Below I examine the 'traditional' teaching methods currently used in the defence sphere, analysing the applicability, effectiveness and security challenges of modern e-learning and some digital tools. Due to limitations in text length, I have not explored in a greater detail those possibilities of adult education and e-learning that cannot be linked to the field of civil protection and firefighting 'vocational training'. In addition, I have not analysed the supporting digital solutions related to the topic, such as applications, smart devices, and IoT[5] capabilities; and I have not studied extensively those areas of cybersecurity that are fundamental to the use of e-learning, such as DoS[6] attacks or malware; they will be the subject of a further research.[7]

2. Disaster training system and current challanges

Hungary's disaster risk is not particularly high, but events that have occurred in the past and recently have to be constantly kept in mind. According to the website of the National Directorate-General for Disaster Management, the dangers and types of disasters currently available

[3] VR: virtual reality.

[4] László Kovács, *Kiberbiztonság- és stratégia* (Budapest: Dialóg Campus, 2018).

[5] The 'Internet of Things' or 'IoT' in English, with which devices like household appliances, cars, cash machines can also be used via the Internet available, and they are able to interact and also communicate with each other. Digitalhungary conference, 2018. Available: www.digitalhungary.hu/konferenciak/ (22. 01. 2020.)

[6] Denial of Service (DoS) attacks, which are denial of service or overload attacks, are of paramount importance among security problems on the Internet. During DoS attacks, the attacker attempts to prevent the network from working properly and in operation. This is achieved by paralysing the respondent system with false requests, so that it can no longer serve real requests from other sources. These attacks are difficult to prevent as it is very difficult to decide which request is real and which is not. On the other hand, their implementation is not too complicated, as an attacker only needs an adequate amount of automated systems, which is sufficient to disable the target. Among DoS there are two large types of attacks: protocol attacks and so-called flooding attacks. Kovács, *Kiberbiztonság- és stratégia,* 26.

[7] Computer network attack tools include various malicious malware. Malware is the collective name of software whose common feature is that they enter the system without being authorised by the user. Any software that does not ensure the proper functioning of the computer system or network can be considered malicious. Kovács, *Kiberbiztonság- és stratégia,* 28.

in Hungary can be divided into two main groups: natural and civilisational hazards.[8] Natural disasters in Hungary, including flooding, are the most significant hazards, but the global environmental changes and recent socio-political transformations do not leave Hungary untouched, thus drawing attention to new or less pronounced aspects of the defence system. It is natural that this need affects the way that knowledge of tools and skills are acquired and transferred, that is, any form of institutionalised or organised education and training.

In addition to the emergence of new risks in hazard preparation, the development of education and training and its methodology make it essential to plan and organise training and the process of further training in the defence area in a continuous review of previous strategies and methods. The new didactic and methodical methods that appear offer a number of options for preparing for protection, including professional disaster management and the preparation of the personnel of related civil protection organisations, but also those working in the interest of defence. Prioritising and securing digitisation will also allow greater space for digital, modern solutions, e-learning systems and motivational models such as 'gamification'.[9] E-learning, for example, can be an effective tool for addressing the challenges of adult education, as it motivates and helps adults adapt their learning to their current lives.

The question arises as to how e-learning as a form of training and the up-to-date digital tools can be used in this field and what new security challenges we must face. Here, the safety and security issues of the use of the procedures and tools are most important, because, bearing in mind how important cyber security is, we have accumulated quite a few question marks. We already have responses to many challenges in this area, but researchers and specialists have yet to find solutions to 'cover' the new security gaps. New procedures are emerging in this area every year or even day by day.

3. Current forms of disaster management training

Professional disaster management personnel are involved in the planning, organisation and implementation of the tasks from three large areas. These are fire protection, civil protection and industrial security. The reform of the preparation of professional staff for civil protection tasks and the redesign of related processes in parallel with the reform of the preparation of civil protection organisations are based on citizenship and have achieved significant success. Preparation for fire protection – preventive and rescue – tasks also has a long history. Traditional forms of training were well combined – as a result of reform pedagogical research – with elements already prevalent in the civil sphere, which were comparable to training objectives. However, research into didactic and methodical areas is a constant demand, moreover, new scientifically based options may always arise.

[8] Zsolt Haig and László Kovács, *Kritikus infrastruktúrák és kritikus információs infrastruktúrák* (Budapest: Nemzeti Közszolgálati Egyetem, 2012).

[9] Gamification: playing.

In order to propose new procedures and to look at the application of their authority, it is important to see what methods and themes are currently used. The recent act, Act CXXVIII of 2011, was created to increase the security of the country, to increase the effectiveness of civil protection from disasters and to increase the effectiveness of the protection measures. Coming into effect on 1 January 2012, it created a unified system of legal, institutional and instrumental industrial security. The relevant regulators accurately describe the expectations and objectives which form the basis of the current training methods and themes.[10]

The current training system for professional disaster recovery protection is based on both the former firefighter and civil protection systems, and it combines theoretical and practical training. During the training, the participants will acquire the knowledge, skills and capabilities essential to the performance of the professional tasks.[11] The disaster management training system is both a school system and extracullicular system (adult training). Each form of training can be daytime, correspondence and distance learning. If you look at it according to the level of image, we can talk about basic vocational training. In this way, we must also mention university-level training. Specialist training takes place in the framework of the KOK (Katasztrófavédelmi Oktatási Központ)[12] and NKE (Nemzeti Közszolgálati Egyetem)[13] Disaster Management Institutes. The Task of KOK and the Institute of Disaster Management is to train and prepare firefighters to respond to professional tasks and challenges arising from diverse dangers of interventions, and the ability to professionally manage modern high-value technical equipment.

In addition to initial and tertiary training, various forms of preparation are used which are adapted to the trainee and the theme of the material to be transferred. Examples include vocational courses – where special requirements, specific workspaces are prepared within different disciplines – or courses which take place outside a school system. An important form of implementation is practical training, which is the main form of preparation for the core vocation of leaders, governing bodies and organisations. Looking at training and teaching methods, and at training tools, the effectiveness of training can be further enhanced by the use of new opportunities in IT. Training raises the question of how practices already used in the civil sphere could be applied in this area as well.

4. The importance, methods and tools of modern adult education

The professional knowledge and skills of defence professionals to respond to the complexity of education is also affected by a number of other factors, as well as a change in the process and system of learning in this context. Therefore, this is closely linked to the field of adult

[10] 62/2011 OF 2. BM rendelet (regulation by the Ministry of Interior), 9/2015 OF 25. BM, KOK rendelet (regulation by the Ministry of Interior and the Disaster Management Education Centre). See https://kok.katasztrofavedelem.hu/32423/jogszabalyi-hatter.

[11] Gyula Vass, 'Gondolatok a katasztrófavédelmi felsőoktatásról,' *Védelem Tudomány*, no 2 (2017), 193.

[12] Disaster Management Education Centre.

[13] University of Public Service.

education, distance learning, e-learning, which are of course also related to each other as modern training methods.[14]

Due to the implementation of protection tasks, the rapid change in the challenges and tools and methods used mainly affects the adult target group, so preparation mainly applies to them. One of the defining features of adult training and training in the public education sector is that workplace constraints make it difficult for adults entering the labour market to participate in traditional education. Thus, e-learning in adult education enables you to learn flexibly in space and time and to spread knowledge, and the demand for an efficient, high-quality but cost-effective form of learning has now increased. It is therefore no coincidence that relatively new educational opportunities have undergone a surge, such as open training or distance learning, including e-learning; and the so-called 'ICT' have been created in the rapid development of information and communication technologies.[15] These forms of education and areas have been created in response to needs that can also be used in the education system of the defence sector.

The main determinant of electronic distance learning is its device system which makes it electronic. The benefits of e-learning, such as cost-effectiveness, motivated learner and new types of tools such as the VR simulator (as a possible tool for practical training), show benefits compared to traditional methods, which are increasingly prevalent not only in the civil sphere but also in the defence sector for the development of an effective training system. There are many good solutions to the use of the aforementioned areas, but I do not have access to all of these, so I will show you the possibilities of using VR and gamification through a few examples below. VR and gamification – that is, playfulness – are among the most popular forms of digital solutions in adult education. Gamification in different areas of life (for example learning, sports, work, shopping) means the use of game elements and game mechanisms. Brian Burke's definition already shows the advantage of the mechanism in the given area: 'Gamifies the motivation of people with digital tools for gaming mechanisms and gaming experiences, and to develop their commitment to achieve their goals.'[16] Various applications and programs encourage them to learn more strongly, so gamification is almost essential for them. One of the good examples is the VR earthquake simulator for adults in Japan in which you can earn points and medals after well-completed tasks and tracks – and thus gain an ever higher rank in the game. This example is interesting not only because of the playfulness used, but also because of the VR – that is, virtual world – used, and its motivational power.

[14] Gyula Vass, Lajos Kátai-Urban, and Zoltán Cséplő, 'A katasztrófavédelmi felsőoktatási képzés gyakorlatorientált felkészítési tevékenységének elemzése,' *Védelem Tudomány* no 2 (2017), 227.

[15] Distance learning (d-learning): an educational form in which the teacher is at a distance from the students, not in the same space during the educational process. Distance learning may combine or use exclusively traditional correspondence, emailing and satellite transmitted video systems. E-learning is teaching and learning via information technology tools. M-learning is the latest version of distance learning, when one can learn permanently without being connected to the Internet. The tools used are: laptop, notebook, Intact Tablet PC, PDA, mobile phone and so on.

[16] Brian Burke, *Gamify: How Gamification Motivates People to Do Extraordinary Things* (New York: Routledge, 2018), 112.

Figure 1. Japan Virtual Reality Earthquake Simulation Game

Source: 'Japan Virtual Reality Earthquake Simulation Game Source,' Virtual World. Available: https://virtualworld.co.kr/board/review/article/1685?exin=1 (26. 12. 2019.)

When using VR technology, you are more likely to maintain ongoing interest in participants, and the tool also helps to unlock the monotony of traditional lessons. Unlike traditional education tools, VR makes it easier to keep participants' attention, so that the information provided on this platform is retained in the minds of students. VR technology also offers new learning dimensions for educational participants. At the same time, VR is a good opportunity to replace the practice as an alternative classroom pedagogical method.

In recent years, many companies have used VR technology to make the learning process more efficient and shorter. For example, UPS has launched training for its drivers that uses VR technology to realistically simulate emergencies on public roads and to teach trainees to detect and identify them.

5. Possibilities of application of the VR systems during defence training

The examples in this article highlight an extremely wide range of possibilities for e-learning and VR. Predicting the direction and future of the training of those involved in the performance of defence tasks is very difficult, but new e-learning methods and innovative digital tools such as VR can have a very large and positive impact on the effectiveness of education, training and preparation. Its advantages include collaborative learning communities, the possibility of rapidly variable knowledge, measurable and customisable training, rapid monitoring, immediate feedback, and the curriculum that can be shaped by the individual. The advantage is also efficient training resource allocation, continuous availability, simultaneous preparation of many people, fast and consistent accountability, efficient communication, and knowledge available from anywhere. The advantage of VR simulators is also to complement and replace practical training. VR can be useful for defence agencies to simulate and practice specific, special events because of the often unexpected and unique precedent-free nature of exceptional situations. The VR simulator can be used to ensure a more pragmatic and higher degree of preparedness of the defence personnel in cases that have not been before or cannot be tested at a real event.

This technology can also help to raise industrial safety to a higher level, as simulation practices for defects and malfunctions associated with the operation of certain hazardous plants and facilities can be used to develop safer protection capabilities.

6. The bohemia interactive VR simulator

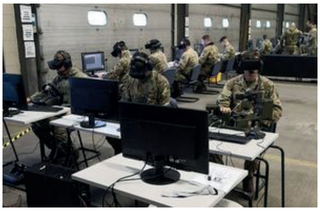

Figure 2. Bohemia VR Simulator during use

Source: VBS4.com. Available: www.bisimulations.com/ (26. 12. 2019.)

The following is an investigation into the possibility of using a software that could be a possible alternative to defence training. Bohemia Interactive Simulation (BISim) is a company that manufactures simulation software for the defence sphere for simulation tactical training. The company's main product is Virtual Battlespace 3 (VBS 3), which has now been organised by more than 50 armies worldwide.

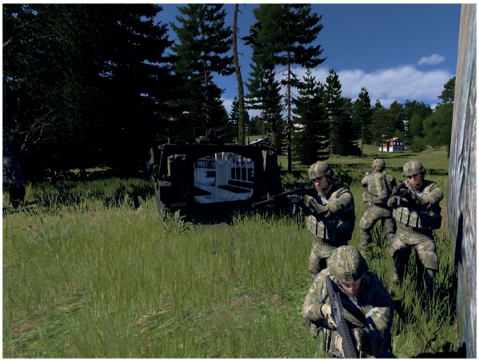

Figure 3. Bohemia VR Simulator Virtual Space

Source: VBS4.com. Available: www.bisimulations.com/ (26. 12. 2019.)

The simulation software offers various tasks to perform in a realistic virtual environment during training. The software contains all realistic models of vehicles and weapons that are used in the user's armies, and it is very useful for newer customers that the interoperability of the software is extremely wide. The system is modularly structured, that is, the basic simulator can be supplemented by the module needed to simulate all types of tasks. VBS 3 is suitable for simultaneous management of up to 200 soldiers – that is, connected computers – in combat simulation centres, where each soldier operates a computer and performs the task from his own perspective, which can be either cleaning a building from enemy forces or securing a convoy. The goal during the use of the program is to practice communication, decision-making and strategic thinking. BISim recently announced their latest product, specially developed for the U.S. Army under the name VBS STE (synthetic training environment).[17] This software is already capable of carrying out the training task anywhere in the world, as it contains a complete realistic virtual map of the Earth. VBS is suitable for VR glasses, that is, soldiers perform the task in a 360-degree virtual reality world during exercise. To model missions as realistically as possible, operators have an extremely wide range of options to parameterise the mission. You can adjust the weather, the number and role of the enemy and civilian population in the mission – powered by artificial intelligence – and any means that is deployed in that army can support our mission. Of course, one of the basic conditions for using such software in the disaster management training system is to learn about the possibilities of the program and to map its modular system. Due to the scope of this article, I do not have the opportunity to do so here, but it may be useful to examine the use of VBS or another type of VR simulator for further research in the future.

7. The possible dangers of using the VR simulator in cyberspace during the training of the defence personnel

In order to examine the e-learning solutions used in training, including the security issues of the use of the VR simulator, it is important to mention essential and special areas of the defence sphere, such as national defence. Since these modern procedures are essentially carried out using the information space, we can assume without any evidence that the 'traditional' attack methods that arise here can also be applied to the means used in the defence sector education system. Furthermore, it will be important to examine the dangers of using the VR simulator as an e-learning platform, possible attack surfaces and possible motives for attacks.[18]

As for information about VR simulators, and especially collaborative VR technology based on multi-user collaborations, there is still a long way to go for security research. Since it is a complex system, it is worth examining the vulnerability of each component separately. Moreover, in the defence sphere, and in particular in defence and risk management and data protection against threats that exploit the vulnerability of VR technology, hardware and software components are of paramount importance, as they are also capable of obtaining a strategic advantage in transnational competition. That is why it is appropriate for vulnerabilities and attack vectors to take into account beyond an operator's information security also a cybersecurity approach.

[17] A. Muspratt, 'VBS STE: The future of simulated training,' Defence IQ, 12. 11. 2018. Available: www.defenceiq.com/defence-technology/articles/vbs-ste-bohemia-simulations-on-creating-a-cloud-based-synthetic-training-environment (27. 10. 2020.)

[18] László Kovács, 'Az információs terrorizmus eszköztára,' *Hadmérnök*, special issue (Robothadviselés 6. konferencia), 22 November 2006. Available: http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html (27. 10. 2020.); Iván Sibalin and Gyula Vass, 'Az ENISA által meghatározott aktuális technológiai kihívások kezelése a katasztrófavédelem szemszögéből,' *Védelem Tudomány* 3, no 2 (2018), 124.

The VR technology and users correspond to the triple division of cyberspace, such as physical, logical and cognitive layers, so threats and vulnerabilities can be interpreted from the perspective of cyber operations.[19] Potential attackers are organisations, governments, armies or non-state actors, hackers, hacktivists, industrial spies or terrorists, and so on.[20] Obtaining or influencing information superiority within information operations can be physical destruction[21] against hardware components of VR technology, a logical threat to the software layer that affects the user, or the armed force at the cognitive capability level.[22]

The following are the security issues of the use of VR simulator in the training of the defence sector, using a triple split: 1) VR components based on different dimensions of cyberspace; 2) based on some attack vectors; 3) based on the possible motives for the attack, in particular in the context of cyber operations between nation states.[23] In the case of each hazard, we will also propose a possible protection measure.[24]

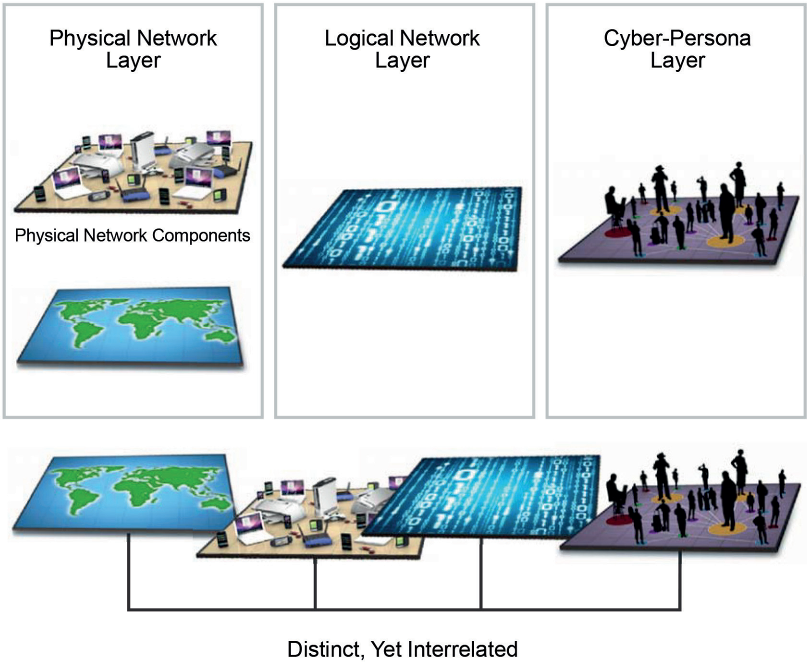

Figure 4. Three interconnected layers of cyberspace.

Source: Cyberspace Operations, JP 3-12. Joint Staff, U.S. Department of Defence, June 2018, I-3. Available: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (22. 01. 2020.)

[19] Haig and Kovács, *Kritikus infrastruktúrák,* 16.

[20] Ibid.

[21] Ibid.

[22] See www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (22. 01. 2020.).

[23] Ibid.

[24] Zsolt Haig, *Információs műveletek a kibertérben* (Budapest: Dialóg Campus, 2018).

The VR device and its user fit into the three-way division shown above, which has become decisive in cyberspace security policy and military approach based on American literature. Furthermore, geographical and network components within the physical layer can be distinguished, within which the network component indicates the types of network hardware and infrastructure.[25] VR technology includes platforms, sensors, data storage centres, servers, routers, wires, optical cables, radio frequency data transmission devices, satellite devices, and so on. The logical layer is a virtual space in the network, which basically contains software-based elements of cyberspace. The logical layer can be mind-treated information, transmission and addressing protocols, software applications, network service providers and users' data, internet domain names, information security solutions, virtual reality content and software, and so on.[26]

The layer of cyber personality consists of the interface, the user and the community components. This layer displays the identity of cyberspace actors that are used, for example, to obtain and influence information, while their true identities and affiliations remain hidden. In the cyber personality layer, the interface component connects people with and through the logical and physical layers of cyberspace with the users' own hardware and software tools. This includes the user's own personal information communication tools related to the network, such as personal computers, laptops, tablets, smartphones, navigation devices, and so on.[27] For virtual reality, this includes, for example, VR (headset), treadmill, gloves, and so on. The cyber personality layer is the third social component, that represents interactions of people in the network. The community component is therefore related to human interaction.[28]

Since VR technologies used for training in the defence sector are in many cases the same as commercially available technologies and devices, they can easily become an attack target, even though they are not used in combat situations. Therefore, in the light of the information assurance vulnerabilities associated with these technologies, it is worth taking stock of some potential threats and motivational factors in the context of cyber warfare.

In this study, we use the term INFOSEC introduced by NATO, which is formed by merging the words of *information security*. It is used in the relevant Hungarian literature in the form of electronic information protection and, in some cases, electronic document protection. The NATO INFOSEC means 'application of security arrangements in communication, information and other electronic systems against the accidental or intentional loss of confidentiality, integrity or availability of processed, stored or transmitted information and against the loss of integrity or availability of those systems.'[29] This definition concerns the protection of IT systems and the data processed therein.[30]

Cyberspace operations can be defined as follows: 'Cyberspace operations are a set of activities for the integrated, coordinated and harmonized application of cyberspace information

[25] Haig, *Informacios műveletek.*

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] 'Security within the North Atlantic Treaty Organisation (NATO),'NATO Document C-M (2002) 49. Available: www.cni.es/comun/recursos/descargas/DOCUMENTO_21_-_Security_within_NATO_-_C-M49-COR1-12.pdf (22. 11. 2020.)

[30] Lajos Muha, 'Az informatikai biztonság egy lehetséges rendszertana,' *Bolyai Szemle* 17, no 4 (2016), 146.

capabilities, which, in order to achieve the objectives of operations, using networked information systems, directly with cognitive capabilities and indirectly with technical capabilities, have impacts on the target audience involved in the operations.'[31] For example, you can include the following activities within the technical capabilities:

- access to and detection of computer networks;
- access to databases, modifying them, destroying them;
- preventing access by overloading servers;
- interception of telecommunications networks;
- interference with data-recording and communication tools and systems;
- similar activities of the opposing party, as detailed above;
- protection against the environment.

Cognitive capabilities in cyberspace can be achieved through networked ICT systems to deliver real and false messages to the target audience, as well as information and collaborative information. The VR simulator requires a huge real-time data flow from many data sources, so in most cases this is done on a cloud basis.[32] Therefore, it can be a priority target for electronic discovery or reconnaissance computer network operations to gain access to them and detect them. Cloud-based technology can be attacked at both the physical and logical layers, and in the case of defence, only a closed private cloud solution built up from its own devices would have a *raison d'etre*. As the military application of the cloud service still faces many difficulties,[33] this can definitely slow the military application of VR technology – and this also affects its use in education. VR systems continuously collect data from the environment through a variety of sensor networks. Communication between sensors, nodes and data processing centres is usually done using wireless technologies. From this point of view of information protection, the fact should be highlighted that sensors are fully open to the processing system on the Internet, which may result in a significant risk to data confidentiality.[34] As a result, the VR sensor network also includes typical vulnerabilities in technology, which most often include:

- detect network traffic and determine the location of network sensor nodes, gateways, data processing centers;
- modifying and compromising sensor data;
- overload attack of the sensor network;
- destruction in the case of physical access.[35]

The VR simulator is particularly suitable for cognitive influence and psychological work through logical and interface layers. VR simulators are the most immersive among multimedia digital devices that we know of and that affect perception. At the same time, experiments have

[31] Haig, *Információs műveletek*, 94.

[32] Ibid.; Géza Vasvári, 'A katonai szervezetek elektronikus információvédelmi képességeinek fejlesztésével kapcsolatos feladatok,' *Honvédelmi Szemle* no 5 (2018), 73–89.

[33] Haig, *Információs műveletek*.

[34] Vasvári, 'A katonai szervezetek.'

[35] Haig, *Információs műveletek*.

shown that security was not a primary concern in the development of VR systems and thus is particularly vulnerable to certain malware attacks. For example, researchers at The New Haven University in Connecticut demonstrated that a malware submitted via e-mail can be used to change the virtual reality content that is perceived by the user. This can fail the training itself, and the user can be physically or mentally injured.[36]

As mentioned above, simulators can be particularly good scouts and intelligence targets because they collect and store an extraordinary amount of sensitive data. There is a huge threat, among other things, in the designs of map bases or critical infrastructure systems that are the basis for the scenarios used for simulator practices, which are the same as the databases and IT systems used by that defence organisation for real-world planning and operations. At the same time, the simulator continuously collects data about users, including its biometric data, such as pupil movement, or the so-called skeleton movement, which allows you to analyse the user's behavior and status. On the basis of these ADT's, however, it is possible to use false personalities or so-called *deep fake persona* as well. VR's 360-degree space scanner data is also available, enabling the data holder to reconstruct a site realistically. With the help of some malwares, attackers can penetrate the VR system and even map the physical space surrounding it.[37] From the data collected about how to train, and the performance of the participants, opponents can learn about the skills, knowledge, current performance and operational planning of the training staff.

The interface with civil Internet networks is particularly sensitive in the context of data leaks and malicious programmes. Researchers have already demonstrated that the content of a commercially available VR simulator can be manipulated through an e-mail malware, which should limit direct network communications to encrypted networks closed for military or national security purposes. A separate problem connected with VR simulation systems is that their closed, encrypted communications also need to be solved.[38]

It is a significant danger and security risk factor that the global supply chain cannot be controlled. In terms of cost-effectiveness, the production and development of certain hardware or software components is the so-called 'commercially available' software *off-the-shelf* devices, where it is very difficult to guarantee the reliability of all components. At the same time, manufacturers are trying to keep up with the very rapid development of the technology, and therefore there is not enough time and capacity to test the safety of the developments.[39] To eliminate this, electronic information security requirements should be a priority in the public procurement procedure of the defence sector.

[36] Alfred Ng, 'VR systems Oculus Rift, HTC Vive may be vulnerable to hacks,' Cnet, 2018. Available: www.cnet.com/news/hack-a-vr-system-lead-a-player-astray-yes-say-researchers/ (22. 01. 2020.)

[37] Leif Johnson,,'Someone Could Be Watching You Through Your Oculus Rift's Tracking Sensors,' Motherboard, 2017. Available: www.vice.com/en_us/article/jpdpm4/should-you-worry-about-the-oculus-sensor-spying-on-you-we-asked-the-expert (22. 01. 2020.)

[38] Ng, 'VR systems.'

[39] Steven T. Kroll, 'Is Virtual Reality The Next Generation in Security Awareness Training?' *Cybercrime Magazine*, 2019. Available: https://cybersecurityventures.com/is-virtual-reality-the-next-generation-in-security-awareness-training/ (27. 10. 2020.)

In summary, the use of VR technology during training as a complex IT system carries the risks from the physical, logical and cognitive dimensions. Because of these vulnerabilities and the large amount of data stored here, electronic or computer network discovery operations can be a particularly suitable target, so ensuring confidentiality among electronic information protection requirements can be the biggest challenge. Thus, the development of electronic information security requirements should play a key role in this aspect.

8. Conclusion

The above thoughts can be summarised stating that as challenges become more diverse, the preparation of defence professionals must also be more diverse. This may affect not only the content issues, but also the methods used. In addition to traditional forms of learning and teaching, new ones appear. Some of the new methods used in civil society education and farming organisations, based mainly on pedagogical research, can be applied well in initial conservation and further training. For example, e-learning opportunities can be useful as a complement to teaching methods in initial education and as a major form of education in further education.

However, it is important to note that the aim here is not only to acquire theoretical knowledge, but also to acquire practical knowledge in order to become familiar with the subject and to acquire applicable knowledge. The benefits of e-learning include a constant and direct individual relationship with a teacher or instructor and the possibility to collaborate with other members of the group. In addition, modern e-learning systems focus on the learning process, the needs and capabilities of the individual to be prepared, unlike previous models of education. The use of the state-of-the-art IT tools presented in this article is becoming increasingly important in VR, for example, they can be highly efficient in the field of training. However, particular attention should be paid to cyber security. In addition, these devices, such as VBS software, provide field opportunities without live practice, as they provide a hands-on experience through VR simulation, which are essential for such training in real life. When using VR devices, traditional ICT devices are a security experience challenge of cybersecurity.

It can be concluded that methodological innovations, VR instruments and the development started to have a major impact on the preparedness of those assigned to defence organisations in the field of training of defence personnel. Curriculum, teaching tools and methods must be constantly modernised, using the latest tools presented, mainly in IT. However, the use of tools, particularly in defence education, should pay particular attention to the security aspects of the applicability of hardware and software and the new cybersecurity implications of its application.

Overall, modern forms of education, such as e-learning and VR solutions, are new educational opportunities that, due to their benefits, have a *raison d'être* in defence-themed training. VR and AR tools are useful and can provide new opportunities for knowledge transfer, but their application requires rethinking of the forms and methods of education systems, developing appropriate software, and last but not least, keeping cybersecurity rules in mind at all times.

References

Burke, Brian: *Gamify: How Gamification Motivates People to Do Extraordinary Things.* New York, Routledge, 2018. DOI: https://doi.org/10.4324/9781315230344

Haig, Zsolt – Kovács, László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* Budapest, Nemzeti Közszolgálati Egyetem, 2012.

Haig, Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.

Kovács, László: *Kiberbiztonság- és stratégia.* Budapest, Dialóg Campus, 2018.

Kovács, László: 'Az információs terrorizmus eszköztára.' *Hadmérnök*, special issue (Robothadviselés 6. konferencia), 22 November 2006. Available: http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html (27. 10. 2020.)

Muha, Lajos: 'Az informatikai biztonság egy lehetséges rendszertana.' *Bolyai Szemle* 17, no 4 (2016), 137–156.

Sibalin, Iván – Vass, Gyula: 'Az ENISA által meghatározott aktuális technológiai kihívások kezelése a katasztrófavédelem szemszögéből.' *Védelem Tudomány* 3, no 2 (2018), 119–134.

Üveges, László: *A Magyar Köztársaság katasztrófa-veszélyeztetettsége és az arra adandó válaszok.* Doktori értekezés, Budapest, ZMNE, 2002.

Vass, Gyula – Kátai-Urbán, Lajos – Cséplő, Zoltán: 'A katasztrófavédelmi felsőoktatási képzés gyakorlatorientált felkészítési tevékenységének elemzése.' *Védelem Tudomány* no 2 (2017), 223–236.

Vass, Gyula: 'Gondolatok a katasztrófavédelmi felsőoktatásról.' *Védelem Tudomány*, no 2 (2017), 188–203.

Vasvári, Géza: 'A katonai szervezetek elektronikus információvédelmi képességeinek fejlesztésével kapcsolatos feladatok.' *Honvédelmi Szemle* no 5 (2018), 73–89.

Internet references

Cyberspace Operations. JP 3-12. Joint Staff, U.S. Department of Defence, June 2018, I-3. Available: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (22. 01. 2020.)

Digitalhungary conference, 2018. Available: www.digitalhungary.hu/konferenciak/ (22. 01. 2020.)

'Japan Virtual Reality Earthquake Simulation Game Source.' Virtual World. Available: https://virtualworld.co.kr/board/review/article/1685?exin=1 (26. 12. 2019.)

Johnson, Leif: 'Someone Could Be Watching You Through Your Oculus Rift's Tracking Sensors.' Motherboard, 2017. Available: www.vice.com/en_us/article/jpdpm4/should-you-worry-about-the-oculus-sensor-spying-on-you-we-asked-the-expert (22. 01. 2020.)

Kroll, Steven T.: 'Is Virtual Reality The Next Generation in Security Awareness Training?' *Cybercrime Magazine*, 2019. Available: https://cybersecurityventures.com/is-virtual-reality-the-next-generation-in-security-awareness-training/ (27. 10. 2020.)

Muspratt, A.: 'VBS STE: The future of simulated training.' Defence IQ, 12. 11. 2018. Available: www.defenceiq.com/defence-technology/articles/vbs-ste-bohemia-simulations-on-creating-a-cloud-based-synthetic-training-environment (27. 10. 2020.)

Ng, Alfred: 'VR systems Oculus Rift, HTC Vive may be vulnerable to hacks.' Cnet, 2018. Available: www.cnet.com/news/hack-a-vr-system-lead-a-player-astray-yes-say-researchers/ (22. 01. 2020.)

'Security within the North Atlantic Treaty Organisation (NATO),' NATO Document C-M (2002) 49. Available: www.cni.es/comun/recursos/descargas/DOCUMENTO_21_-_Security_within_NATO_-_C-M49-COR1-12.pdf (22. 11. 2020.)

VBS4.com. Available: www.bisimulations.com/ (26. 12. 2019.)

Legal references

62/2011 OF 2. BM rendelet (regulation by the Ministry of Interior).
9/2015 OF 25. BM–KOK rendelet (regulation by the Ministry of Interior and the Disaster Management Education Centre).