TECHNOLOGICAL AND INFORMATION WARFARE IN THE XXI. CENTURY

TECHNOLÓGIAI ÉS INFORMÁCIÓS HADVISELÉS A XXI. SZÁZADBAN

BABOS Tibor[1] – BEREGI Alexandra Lilla[2]

Abstract

The thesis of the paper is that an effective management of traditional and new security challenges can be achieved through a complex international cooperation, knowledge and data exchange, while at the same time developing adaptive capabilities of the defense sector. In addition, to advance national defense and military capabilities, the defense sector, including armed forces, need to adapt to the new security threats that have appeared and are developing continuously. To recognize and properly manage complex and coherent new security risks as well as to perform conventional military tasks at the same time, it is necessary to transform and fully modernize warfare based on existing and new technological and information capabilities. In order to verify the thesis, the first chapter of the study presents the grouping of new security challenges and then, based on that, the second part evaluates the individual stages of the military revolution. The third chapter presents the characteristics of information warfare, while the fourth chapter highlights the waves of the military revolution explaining the four stages of their development.

Keywords

digitization, globalization, security challenge, technological development, force reform, military technology

Absztrakt

A dolgozat tézise, hogy a hagyományos és az új biztonsági kihívások hatékony kezelése komplex nemzetközi együttműködéssel, a szövetségesek vonatkozó tudás és adatcseréjével, ugyanakkor a védelmi szektor adaptív képességfejlesztésével érhető el. A védelmi szektornak, ezen belül a fegyveres erőknek, a hagyományos országvédelmi feladatai ellátása mellett szükséges az új kockázati tényezők mentén kialakult/kialakuló biztonsági fenyegetésekhez alkalmazkodni, azokra reagálni. Ahhoz, hogy a hagyományos katonai feladatok ellátása mellett a komplex és koherens új biztonsági kockázatokat a fegyveres erők felismerjék és megfelelően kezeljék, szükséges a hadviselés átalakítása, teljeskörű modernizációja. A tézis igazolása érdekében a dolgozat első fejezete bemutatja az új biztonsági kihívásokat, míg a második rész értékeli a tudományos-technológiai forradalom, azon belül pedig a haditechnikai boom egyes szakaszait. A harmadik fejezet az információs hadviselés jellemzőit mutatja be, majd arra alapozva, a negyedik fejezet a hadügyi forradalom egyes hullámait, a szakirodalomban is fellelhető négy fejlődési szakaszban jeleníti meg.

Kulcsszavak

digitalizáció, globalizáció, biztonsági kihívás, technológiai fejlődés, haderőreform, haditechnika

[1] babos@uni-nke.hu | ORCID: 0000-0001-7459-8349 | director, Security Science Center University Óbuda | igazgató, Biztonságkutató Központ

[2] beregi.lilla@uni-obuda.hu | ORCID: 0000-0003-0436-4875 | contracting rapporteur, Eötvös Loránd University | szerződéskötési referens, ELTE

INTRODUCTION

Security is a state of a sort of conditions without threats, when there is no active threat to endanger us, our life or our environment. Security challenges that can become threats are complex in nature and interact with each other. This conceptual framework may be further complicated or even reinforced by changes in society, especially in the face of rapid technological development.

The process of globalization, i.e. the free and rapid flow of information, capital, labor, goods, services and political principles and ideologies, has been accompanied by technological development, i.e. electronics, informatics, biogenetics, space, the explosive development of artificial intelligence and many other technical fields of science [1] The thesis of the paper is that an effective management of traditional and new security challenges can be achieved through a complex international cooperation, knowledge and data exchange, while at the same time developing adaptive capabilities of the defense sector. In addition, to advance national defense and military capabilities, the defense sector, including armed forces, need to adapt to the new security threats that have appeared and are developing continuously. To recognize and properly manage complex and coherent new security risks as well as to perform conventional military tasks at the same time, it is necessary to transform and fully modernize warfare based on existing and new technological and information capabilities.

In order to verify the thesis, the first chapter of the study presents the grouping of new security challenges and then, based on that, the second part evaluates the individual stages of the military revolution. The third chapter presents the characteristics of information warfare, while the fourth chapter highlights the waves of the military revolution explaining the four stages of their development. Finally, the paper concludes that modern countries and their defense sectors need to be prepared to deal with new security risks, among them with cyber space, therefore digital capability development for the armed forces is not just needed, but inevitable.

A XXI. SECURITY CHALLENGES OF THE 21ST CENTURY

The goal of first chapter is to present those new and main security challenges that reshape our security perception and dominate every-day life. These are the globalization, the migration, the terrorism and the digital-technological revolution and its challenges to the information society. The transformation of security continued at the beginning of the 21st century, in line with the post-Cold War trends of the previous decade. The political, economic and social changes that began in the late 1980s, the culmination of globalization, swept away the bipolar world order, which changed the balance of power, accelerated scientific and technological development, and the interdependence of states, while threats have become universal and common. [1] The "old" armed conflicts, which can be called traditional, have been replaced by "new" security challenges: low-intensity security risks, proliferation of weapons of mass destruction, uncontrolled development of nuclear, chemical and biological technologies, cyber threats from the mass use of computers. Conflicts of interest arising from unequal social and economic development, or attacks organized by non-state actors and terrorist groups, all states to set new target systems of a preventive and protective nature in order to survive. [2]

The new security challenges can be grouped along the following lines:

- global, regional, local and specific threats based on geographical aspects;
- military "hard" or non-military, ie "soft" hazards due to their nature;
- direct, immediate or long-term, preventable risks according to their occurrence;
- occasional, short, medium and long-term hazards in terms of their duration;
- in terms of their nature and origin, armed conflicts, natural and industrial disasters, social crises, threats to civilization and forensic phenomena. [3]

With the emergence and globalization of new types of security risks, the chances of armed conflicts in democratic and modernized countries show a declining trend, as they stand today. With regard to Hungary, on the one hand, collective defense due to NATO membership reduces the chances of a direct armed conflict, and on the other hand, a significant proportion of Hungarians living across the border increase the possibility of violence against Hungarian interests, e.g. low-intensity 'below-threshold' violent armed conflicts. Therefore, maintaining and strengthening the border protection system, the presence of law enforcement and military forces nationwide cannot be indispensable as new security challenges come to the fore.

Ecological, natural or industrial disasters are emerging as new security challenges. The above phenomena are becoming more common in Hungary and Europe as well, and technological development further escalates the problems. Floods, rainfall and epidemics can have secondary consequences, as well as animal and human epidemics from the West or East, which, in addition to testing the health system, pose a serious threat to the economy, in particular COVID-19. The prevention of natural disasters and the management of disasters and epidemiological situations in the spirit of a comprehensive approach can be effective through complex civil-military cooperation. The domestic method of developing a signaling system necessary for the prevention of disaster situations, prevention damages in infrastructure, with international cooperation is a priority task for Government institutions, especially for military, disaster management and law enforcement agencies. [2]

Today, migration has been shown to be a natural part of globalization. The 2015 wave of migration, highlighted the shortcomings of the asylum system, the inadequacy of immigration, border and civil protection capacities. [2] As a consequence of migration, it is accompanied by the black labor market and cross-border crime, international crime, the increase in drug trafficking, the transmission and spread of epidemics, and the emergence of human trafficking. As a result of migration, the threat of terrorism also increases, and the expulsion and return of migrants and the emergence and criminalization of ethnic minorities may also lead to international disputes. While controlled migration can bring economic and demographic benefits in the medium and long term, it also poses serious risks to public security and national security in the short term. In terms of illegal migration, Hungary is primarily a transit country, but there is also a chance that in the long run, the peoples of Africa and South Asia will find Hungary as a destination country, especially if relative prosperity continues to improve economically and socially. Our country is tackling illegal migration with the help of organized crime, stepping up the fight against human trafficking and developing a policy of expulsion, return and readmission. In connection with the above, it can be stated that the recognition of the security challenges affecting Hungary and the

action against them can be effectively applied by deploying the appropriate national self-sufficiency and meeting the requirements of transatlantic and European integration. [4]

The relegation of traditional war to the background also greatly reduced the likelihood of total nuclear warfare during the Cold War. According to the general opinion in the global media space and social networks created in direct proportion to globalization, nuclear war should not be in the 21st century. instrument of the political goal of the 21st century. However, the nature of the new warfare resulting from the development of information and technology requires global and international treatment, especially with regard to the proliferation of weapons systems, the use of super-technical systems and the development of application technologies.

In terms of the scale of the threats, despite the above, the use of weapons of mass destruction and terrorism as asymmetric security risk factors pose the most fatal threat to developed countries. Due to the proliferation of weapons of mass destruction and the uncontrolled nature of technologies, the balance of power in the world is changing, so counterparts to developed countries are more likely to use asymmetric instruments in view of their smaller budgetary needs but greater universal destructive effects. All this means that the unauthorized access to nuclear, chemical, biological technologies, genetic engineering, the proliferation of weapons of mass destruction, the mass use of information technology and technology by computers is one of the greatest security risks and threats today. [5]

With the advent of globalization, terrorism is gaining ground, manifesting itself in different and changing ways in space and time. Although terrorism knows no borders, Hungary's level of terrorist vulnerability is rather low, but at the same time foreign terrorist acts can have an economic and security impact on Hungary. The country participates in the international fight against terrorism, in the development of the international anti-terrorist organization system, and in the implementation of the obligations of the United Nations, the EU and NATO. [6]

Today's cyber threats, like terrorism, know no borders and are spreading more and more as a result of globalization. Computer systems are driving societies, science and technology are becoming available to all of us, so we have to deal with unexpected attacks in cyberspace. Adequate protection against cyber-attacks, such as disruption, blocking, or overloading of information and communication systems or the government backbone, is necessary. In addition to the development of national security and national defense, emphasis must be placed on cyber defense and the provision of international critical infrastructure. [6]

Thus, in addition to its benefits, the IT explosion can be identified as a new risk. Both governmental and non-governmental actors are adapting the advantages and disadvantages of cyberspace. "Hacker" or "pirate" attacks may include governmental, political, and economic, non-state actors exposed to malicious intent, terrorist acts, data acquisition, or data theft and use. It is worth mentioning here the deletion and theft of information of public interest and the smuggling of falsified, false information.

Overall, traditional and new security challenges are often interlinked, inducing each other, so threats are clearly interlinked, interacting, continuously influencing a given level of stability. One of the surest places to deal effectively with traditional and new security challenges is through international cooperation. In order for Hungary to properly manage the complex and coherent risks presented in this chapter, it is necessary to adapt the force

and its use. This is basically a structural, procedural, warfare and comprehensive modernization transformation that began in 2016 with the Zrínyi 2026 Force Development Plan.

THE TRANSFORMATION OF THE ARMED FORCES, THE AGE OF MILITARY TECHNICAL REFORMS

The period from the French Revolution to the middle of the 20th century can be called the age of mass warfare. Which means that during that period, the military force consisted of an enlisted mass army, meaning those who had a larger army were the most successful on the battlefield. However, the age of mass armies is over. The almost complete destruction of Iraq, the world's fourth-largest army, in 1991 was a breeze that that outdated military technology could be surpassed by advanced weapons. [7]

In the 19th century and the 20th century, for the most part, the armies of countries had the same weapons worldwide. By the time of the First World War, greater differences could already be discovered in this field, until the Allies began mass tank production, until the Germans developed this land capability. During World War II, the contrast increased even more. The United States and Great Britain developed heavy bombers at this time, but neither the Soviet Union nor their enemies followed this example. Nevertheless, in World War II and during the Cold War, the weapon systems were fundamentally similar. The great change began at the end of the 20th century, by which time weapons had developed rapidly, which meant the development of actual means of destruction, the emergence of unique armaments solutions, and the creation of military technology systems. [8]

In most countries of the world, compulsory, conscript military service was abandoned, thereby reducing the size of the armed forces and bringing military technical developments to the fore. Together with more advanced military technology and appropriately trained soldiers, a change in power can result in a 1: 3 victory against a larger force that uses more outdated techniques. Quality, which is a combination of a trained soldier and technique, therefore overcomes quantity.

"Force reform," that is, the change of the armed forces, is a constant historical process. In the modern age, this process is present as a budgetary, developmental, and political issue. The reorganization of the force depends on changes in the image of the war. The mode of warfare depends on the particular, developed or under development military technique, political interests and economy. In addition, the geopolitical situation and military geographical position also determine the parameters of the forces. In the current changing security environment, the management of new security risks and conflicts is based on different principles of warfare than before, where mobility, flexibility, capability development and the functional use of knowledge, i.e. quality, come before quantity. At the same time, the military revolution, electronic and information-based warfare, namely the change in the human-machine ratio, is emerging. This chapter takes the stages of the above process by presenting the milestones that have shaped its major recent events leading to the transformation of the army.

Defense and military cooperation need to be implemented within an international framework, which means that international interoperability is important. With regard to our NATO allied and EU membership, the elements and capabilities of the Hungarian Armed Forces are modern, up-to-date and useful, which can be deployed outside the country, and

thus can also be used in an international environment. Therefore, the center of force development is provided by the achievement of the above capabilities. As a result, it is conceivable that some skills that have become redundant in the meantime will disappear completely and be replaced by new, modern ones. The goal is to train an army that is not based on the principle of a "mass army" with full capabilities before the change of regime, but is new and innovative, based on technology and capability development. [9]

Military technology is constantly changing and evolving. The military revolution is based on the combined presence of change. Military technology changes evolution-like, at greater or lesser rates, it transforms hectically, that is, it develops unevenly. During development, the merging of some technical innovations induces a greater transformation, while other areas have become secondary (see mass nuclear capabilities today).

Changes in warfare first appeared in the 1991 Gulf War [7], where the effectiveness of high-precision weapons was first demonstrated, a range of supporting military techniques emerged, and this brought about a fundamental change in warfare. Analyzing the specifics of the Gulf War, we can conclude that (1) quality versus quantity, (2) the specialization of military equipment, (3) and the military application of civilian-developed technologies provide the triple tooth that characterizes the new technological era of warfare. [8]

Today, the weapon systems between the leading powers are not as balanced as in the past. The United States is at the forefront of military advances such as the heavy B-2 bomber, which uses heavy-range stealth technology. [10] Few countries are able to follow this technological development, but many are able to sustain ballistic missiles. This process suggests that arms competition between countries and major powers is / has become asymmetric.

Military development is greatly influenced by the state of comprehensive systems. Because of its ability to cooperate in combat, the U.S. Navy is able to see and manage the common picture created by the data in the system simultaneously for all ships in service. Space guidance systems, which can be used to track all objects moving in orbit around the Earth and coordinate the movements of vehicles, will become available to military leadership. These advanced systems are now only shadows of traditional military command and control systems. The United States and some European countries are successful in aerospace development, with Japan having little success, while China and Russia have mixed results. [11] Systems integration, namely the targeted integration of complex technologies in the States, is developed by interconnecting weapons systems and sensors in order to enable these systems to operate in an ever-changing environment.

The military use of civilian-developed technologies is not new, as some of the developments have always come from the civilian sector. Civilian technical devices basically had a great impact on warfare (railway, telegraph). However, after the Second World War, a large number of countries interested in technical development set up research institutes, as a result of which military developments were transferred to the civil sector (transistor, jet engine). A similar finding can be made with regard to the ARPANET, which emerged at the beginning of the information age and was referred to as the "ancestor of the Internet" developed by the U.S. Department of Defense — a messaging and receiving network system created during the nuclear war. [12]

Today, as a turning point in the information age, the military sector is once again relying on developments in the civil sphere. Civilian technology is leading the way in military applications. The interdependence of governmental and non-governmental, economic and market actors is becoming more and more important in terms of technical innovations and developments.

It takes time for new military technology to take effect. It is a burden on modern armies to cope with the challenges of the information revolution. One of the biggest challenges is retaining human strength. At the time of the Industrial Revolution, the civil sector and private enterprises did not have to be fought. In the information revolution, however, the gap between civil-military organizations is widening. It is much more difficult to keep trained forces on the defense field in an age where the civilian sector offers more freedom, better wages and opportunities. That is why the development of the military career is very important. As a result of technological advances, the military faces another challenge: warfare takes place within the framework of cameras and satellite communications. This means that armed clashes can be affected by cyberspace, some battles can unfold on the World Wide Web, so real and virtual battlefields are inseparable.

INFORMATION WARFARE

This part of the study is written as an introduction to the fourth and final chapter, which aims to provide the reader with a comprehensive picture of the information society and warfare, as well as the threats to information infrastructures. The secure functioning of the information society depends on the information infrastructure and information systems. Through these, physical, electronic and IT attacks can be launched against the political, economic and cultural life of a developed industrial country. A successful information attack can cause damage that makes an actual military attack unnecessary, and in the event of a crisis, it can cripple strike forces, early warning systems, and immediate and rapid response forces. In the information society, the chances of an information attack are increasing. This predicts the short-term economic and social decline of an industrialized country dependent on information infrastructures. This means that information attacks affect both the civilian population and the military. [13]

However, cyber-terrorism is a global threat, so every country must catch up with the dangers of the information society. Nowadays, it is unpredictable when and from which country a cyber-attack will be launched. It is beneficial for a country or terrorist organization launching a cyber-attack to be able to weigh on the stability and international prestige of a target country with cost-effective information attacks, especially if it can do so without hiding its identity. [14]

In conclusion, information terrorist attacks and aggressions are as much a threat as challenges, risks and threats to international, global, regional or national interests. Therefore, in order to prevent them and fight, every country must act. This statement has already been recognized by many NATO allies, including Hungary. To this end, the establishment of a number of legal acts, institutions and organizations has begun.

Information infrastructures are complex systems that build on each other, assume each other and consist of a set of mutually supportive infrastructures. The information society depends on functional information infrastructures and the continuous operation of supporting infrastructures. Therefore, if this complex infrastructure system is attacked, it will

also affect the smooth operation of other infrastructures. There is interdependence between infrastructures. The functioning of information society information infrastructures can therefore be disrupted, damaged or destroyed altogether. Maintaining the operation of information infrastructures is important for companies, government institutions and organizations alike. The global availability of info-communication systems also provides an opportunity for their global vulnerability. Threats may come from different groups and individuals or non-governmental entities. The motivation behind threats are usually (1) political; (2) economic; (3) financial; (4) soldiers; (5) social, (6) cultural; (7) industrial; (8) ethnic; (9) regional; (10) or may be of individual interest.

Threats can be summarized as follows:

- unauthorized data entry, access to information;
- entering malicious software and viruses into the system;
- database degradation, modification, destruction;
- theft of information system data;
- electronic attacks on both military and civilian communications, reconnaissance, systems;
- destruction and destruction of elements of military command, communication, arms control systems and civilian systems that can be used for military purposes. [15]

The above threats may come from individuals, unauthorized users, terrorists, international organizations, foreign intelligence, or military organizations. In peacetime, the most common information activity is intrusion into computers, thus assessing the weaknesses of the system, so that in times of crisis or war, more direct attacks can be expected. They are able to attack the initiation or unfolding of military actions through coordinated information activities. Attacks against information systems include GPS, unmanned devices, or satellites. Attacks on civilian and military information infrastructures and info-communication systems are the primary targets of the information battlefield. [16]

The waves of the military revolution

By the beginning of the 21st century, warfare had undergone changes, new technical means had developed on the battlefield for centuries, new principles of application had appeared, and this chapter aims to present this process by analyzing the four waves of development of the military revolution.

The information revolution led to the new Revolution in Military Affairs (RMA) [17], which uses the achievements of the information, scientific and computer revolution to modernize the military and transform the 21st century force model to protect the information society. In the United States, the Army Transformation Programs [18] are undergoing a force transformation program, and in Hungary, the Zrínyi 2026 Defense and Force Development Program [19] provides a framework for capability development. Force development and force transformation programs are in line with the development of the information age and the information society. This developmental process unfolds in developmental stages that follow each other in a wave-like manner, producing higher performance. In these waves, new military-technical tools and capabilities are emerging for the army to promote the development of the information society. In parallel with the new military capabilities and weapon systems created in the development stages, new military, operational and tactical principles and methods are emerging.

The waves of the new military revolution:

- first wave (1950-2010)
- second wave (2010-2030)
- third wave (2030-2050
- fourth wave (2050-2100). [15]

The chapter goes on to take a closer look at the main features of each wave without claiming to be exhaustive. The first wave of development is related to the IT and science-based technical revolution, especially the development of precision weapons and computing, software, networking, telecommunications, control and command technology. The army's armaments feature first-generation air and ground robots, miniaturized nuclear weapons, that can serve as a response to asymmetric and terrorist acts, thereby reducing the size and deployment threshold of nuclear weapons.

The main military capabilities of the first wave are:

- the military use of the results of science;
- state-of-the-art military equipment;
- emergence of intelligent missile weapons, integrated weapon systems;
- the emergence of prototypes of miniaturized nuclear weapons;
- high-capacity bombs and missiles, warheads that destroy air pressure and fire;
- the first generation of unmanned, remotely controlled / programmed aerial and ground reconnaissance and combat robots;
- the emergence of high-performance, precision-networked reconnaissance systems;
- total force command;
- increasing team maneuverability;
- combat use of satellite reconnaissance, navigation and news systems;
- combat and news equipment unlikely to be detected;
- global information environment, information battlefield, digital battlefield, emergence of digital soldiers;
- digital signal processing, news, control;
- network-based management systems;
- combat computers, tactical internet, complex military computer networks;
- advanced computer information, management and complex reconnaissance systems (C4ISR); [20]
- information operations, information warfare, command warfare. [15]

The mechanized-motorized, analog-system armies of the traditional production era are thus being replaced by digital armies that utilize new types of scientific results and have digital command superiority and precision fire superiority. The battlefield of digital forces is the digital battlefield where information operations take place.

In the second wave, the weapons and weapon systems that were developed as prototypes in the first wave will appear. Hence, the digital army continues to evolve, creating a digital, precision, and network-centric army. [21] This means that the transformation of warfare is directed towards high-mobility and high-powered airborne combat equipment.

The military characteristics of the second wave are as follows:

- the emergence of digital and precision armies in developed countries; the emergence of digital, precision and network armies in more developed countries;
- the emergence of first-generation unmanned aerial vehicles and ground robotic systems; development of second generation robots;
- making cruise missiles with stealth technology;
- the emergence of aerial, space and ground laser weapons;
- the emergence of electromagnetic pulse weapons, microwave, laser and infrared jamming equipment, devices that interfere with navigation satellites;
- the emergence of sixth-generation triple-speed multi-purpose aerial combat robots with stealth technology;
- testing of hypersonic aircraft (NASA) [22];
- development of seventh generation voice-controlled test aircraft;
- regularization of multi-purpose aerial combat robotic aircraft;
- development of aeronautical motherships for small aerial combat robots;
- proliferation of advanced chemical, biological, genetic and psychological warfare tools;
- further development of precision weapons;
- increase of remotely launched precision weapons;
- emergence of precision, multi- and hyperspectral, unsupervised detection sensor systems;
- systematization of battlefield - ground, air, sea, cosmic - attacking combat robots;
- the emergence of voice-controlled combat equipment;
- modernization of news systems and devices for multimedia data transmission, audio and video transmission, tactical internet connection and network combat management;
- further development of non-contiguous battlefield warfare, new-minded urban combat, network-based warfare, impact-based operations, information operations;
- development of networked military programs, which is a complex program of force digitization. [15]

Central to the second wave of development is the development of a networked, digital military program, the prevention of information attacks by international terrorism, with special regard to the protection of information infrastructures and computer networks. In this wave of development, the digital, networked, precision army provides leadership and technical superiority, which means it is up to three to six times more efficient in proportions than a traditional army.

In the third wave of development, multi-purpose second-generation robots and a hybrid army of mixed-composition robots and humans will most likely appear. [23] The formation of the first phase of the hybrid army is expected to consist of a larger share of living force and a smaller proportion of the presence of robots.

In the fourth wave of development, it can be assumed that the proportion of robots and humans in the hybrid army will be split in half, or in greater proportion in favor of

robots. Scientific results will have an increasing influence on military technical developments. Weapons are evolving using nano, bio, and genetic technologies, and military techniques are evolving using molecular computers. This creates a hybrid army based on nanotechnology that represents scientific and military superiority.[24]

In principle, all information societies are able to acquire the skills that have developed / are developing in connection with the waves outlined above, therefore fierce skills competition can be expected. Some of the characteristics of the development waves are that they have a close connection in each other's direction, they are built on each other, they are connected to each other, because the individual abilities, tools and systems have already appeared in the previous stages. These changes result in the emergence of new military doctrines, a reduction in the size of formations, an increase in the number of areas of application, and a multiplication of destructive force.

CONCLUSIONS, SUMMARY

The thesis of the dissertation was that the effective management of traditional and new security challenges can be achieved through international cooperation and capability development of the army. In addition to performing its national defense and military tasks, the army needs to adapt to the security threats that have developed / are developing along the new risk factors. In order for the military to recognize and properly manage complex and coherent new security risks in addition to performing traditional military tasks, it is necessary to transform and fully modernize warfare.

To substantiate the thesis, the first chapter of the dissertation presented a grouping of new security challenges and analyzed the challenges that are relevant to information technology warfare. The second part analyzed and evaluated each stage of the military technology revolution, providing a comprehensive and general picture of the historically significant points of force reform. The third chapter aimed to present the characteristics of information warfare with special regard to the characteristics of information infrastructures. The fourth chapter analyzed the waves of the military revolution in four stages of development with a focus on military-military capabilities.

Overall, the effects of globalization and the technological revolution will sooner or later reach all nations. As a result of the development of information societies, new threats know no borders. The chances of cybercrime, terrorism, migration, disasters are growing. The proliferation of asymmetric warfare and weapons of mass destruction carries great danger. All countries need to be prepared to deal with new security risks, so digital capability development for the military is needed. Through four chapters, the study draws attention to the fact that digitization, military-military technical development, total force capability development, and professional training of human resources have already begun. The only question is which country, how, in what way and to what extent has it caught up with the challenges of the information society? Or were you aloof from them instead of catching up? In the latter case, it is certain that there will be serious breaks between the countries that have caught up and those that have caught up, the conflicts of which can be assured.

"This research was supported by the Ministry of Innovation and Technology within the framework of the Thematic Excellence Programme 2020, National Challenges Subprogramme (TKP2020-NKA-16)."

BIBLIOGRAPHY

[1] T. Babos, The Five Central Pillars of European Security, Brussels: NATO Public Office, 2006.

[2] T. Babos and A. L. Beregi, "The Security Policy Context of the Defence Economy Today," 9 2018.
[Online]. Available: http://hadmernok.hu/183_25_babos.pdf Engineer. [Access date: 19 12 2020].

[3] P. Deák, "Security Policy in Everyday Life," Budapest, Zrínyi Publishing House, 2009, pp. 107-114.

[4] T. Babos and A. L. Beregi, "Security Hungary european processes," 4 2020. [Online]. Available: https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/945 Engineer. [Access date: 19 12 2020].

[5] T. Babos, "Security, Defense and Military Policy Relevances of the Digital Prosperity Program," 2018. [Online]. Available: http://mhtt.eu/hadtudomany/2018/2018_elektronikus/2018ebabos2.pdf Military Science. [Access date: 15 11 2020].

[6] A. L. Beregi, "national security strategy Hungary (2012) in the light of today's security policy challenges," 2020. [Online]. Available: https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/748/3924 Engineer. [Access date: 12 11 2020].

[7] L. Szűcs, "Ten Less Well-Known Facts about the Gulf War," 13 9 2014. [Online]. Available: https://honvedelem.hu/hatter/multidezo/tiz-kevesbe-kozismert-teny-az-obolhaborurol.html honvedelem.hu. [Access date: 1 12 2020].

[8] E. Cohen, "Technology and Warfare," in A Strategy in *the Modern Age*,P. Tálas, Ed., Budapest, Zrínyi Publishing House, 2005, pp. 295-316.

[9] P. Deák, "Security Policy in Everyday Life," Budapest, Zrínyi Publishing House, 2009, pp. 101-103.

[10] "B-2 SPirit," [Online]. Available: https://www.military.com/equipment/b-2-spirit military.com. [Access date: 4 12 2020].

[11] "The Hungarian Aerospace Cluster," [Online]. Available: http://hunspace.org/ hunspace.org. [Access date: 10 12 2020].

[12] "ARPANET," [Online]. Available: https://www.darpa.mil/about-us/timeline/arpanet darpa.mil. [Access date: 5 12 2020].

[13] A. Treasures, "Technology and Society in the Age of Information," in The Information *Society*,R. Pintér, Ed., Budapest, Thought-New Mandate, 2007, pp. 47-64.

[14] Z. I. Papp, Doctoral Thesis "Methods, Possible Means and Alternatives to Cyberterrorism," 2018. [Online]. Available: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/Papp_Zoltan_PhD_ertekezes_tervezete.pdf. [Access date: 10 12 2020].

[15] Z. Haig and I. Várhegyi, "Warfare in the Information Theatre," Budapest, Zrínyi Publishing House, 2005.

[16] Z. Haig, L. Kovacs, L. Vana and S. Vass, "Electronic Warfare," 2014. [Online]. Available: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10964/webview.pdf?sequence=1&isAllowed=y. [Access date: 1 11 2020].

[17] R. F. James and M. V. T. Jan, "Revolution in Military Affairs," 25 2 1990. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a360252.pdf. [Access date: 10 12 2020].

[18] „United States Army: 2004 Army Transformation Roadmap," 7 2004. [Online]. Available: https://www.hsdl.org/?abstract&did=464516. [Access date: 2 11 2020].

[19] "Law No 1298/2017 on the implementation of the Zrínyi 2026 Defence and Force Development Programme (VI. 2) Gov. Decision," 2018. [Online]. Available: http://njt.hu/cgi_bin/njt_doc.cgi?docid=202263.355813. [Access date: 12 12 2020].

[20] "C4ISR," [Online]. Available: https://www.c4isrnet.com/. [Access date: 13 12 2020].

[21] A. Robertson, America's Digital Army: Games at Work and War, London: University of Nebraska Press, 2017.

[22] „NASA Armstrong Fact Sheet: Hyper-X Program," 28 2 2014. [Online]. Available: https://www.nasa.gov/centers/armstrong/news/FactSheets/FS-040-DFRC.html. [Access date: 16 11 2020].

[23] Z. Somodi and Á. P. Kiss, "Interpretation of the concept of hybrid warfare in international literature," 6 2019. [Online]. Available: http://real.mtak.hu/105176/1/SomodiZoltC3A1n-C591rnagy-E28093-Kiss-C381lmos-PC3A9ter_A-hibrid-hadviselC3A9s-fogalmC3A1nak-C3A9rtelmezC3A9se-a-nemzetkC3B6zi-szakirodalomban.pdf. [Access date: 10 11 2020].

[24] „Digital Army Program-for maximization of combat force effectiveness," [Online]. Available: https://elbitsystems.com/media/DAP.pdf. [Acces date: 12 12 2020].