AARMS Vol. 20, No. 1 (2021) 81–93.

10.32565/aarms.2021.1.6

Security and Military Relevancies of Digitisation, Globalisation and Cyberspace[1]

Tibor BABOS[2] – Alexandra Lilla BEREGI[3]

The goal of this study is to explore security threats and challenges of digitisation. Digitisation as one of the key technological factors has a significant impact on the development of today's modern world. Beyond general security circumstances, this impact touches upon economic, financial, social, technological, medical, educational, defence and military issues, as well all over the world.

The argument of this study is that the modernisation of defence systems is an essential key to successfully responding to new security challenges in our digital explosion era. Therefore, it is a must that government organisations, including defence and military systems fundamentally upgrade their own technical, structural and operational capabilities and accept digitisation as the driving factor of future defence and military development.

In light of the above, the study first examines digitisation as a global security challenge and then presents a comparative analysis of the relationship between hybrid warfare and cybersecurity. Finally, before drawing conclusions, it takes stock of the military policy relevance of the cybersecurity challenges relevant to Hungary.

Overall, it can be stated that digitisation and digital transformation are present all over the world as a result of globalisation. Developed nations, including Hungary must be connected to digitisation and by digitisation to each other's various systems and technologies. This system has to be integrated, but independent at the same time, as well as connected but separable in order to be able to be involved in the whole cyberspace and get the benefits of it or get separated from it to defend threats or direct attacks coming from the outside. The Hungarian Defence Forces has a key role in this very important process.

Keywords: *Hungary, cybersecurity, digitisation, globalisation, hybrid warfare*

---

[1] 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).

[2] Founding Director, Szent István Security Research Center; Associate Professor, Hungarian Agricultural and Life Sciences University Faculty of Mechanical Engineering; Founding Director, Security Science Center; Founding Director, Security Science College, Professor, Doctoral School of Security Sciences; Honorary Professor, Óbuda University; Honorary Professor, University of Public Service Doctoral School of Military Sciences, Doctoral School of Public Administration; e-mail: babos@mil.hu

[3] PhD student, Óbuda University Doctoral School on Safety and Security Sciences; Vice President, College of Security Sciences; e-mail: beregi.lilla@uni-obuda.hu

Introduction

In his presentation entitled *The Four Global Trends and Nine Challenges of Security* delivered at the Annual Conference of the Hungarian Military Science Society on 5 November 2019, Tibor Babos first presented his thesis according to which European security today is fundamentally determined by four global trends and nine risk factors. The aim of his study was to find answers to the following dilemma: in order to research or understand our current security environment, which factors and contexts should be taken into account and what are their contents? According to Babos, its content can be summarised as follows.[4]

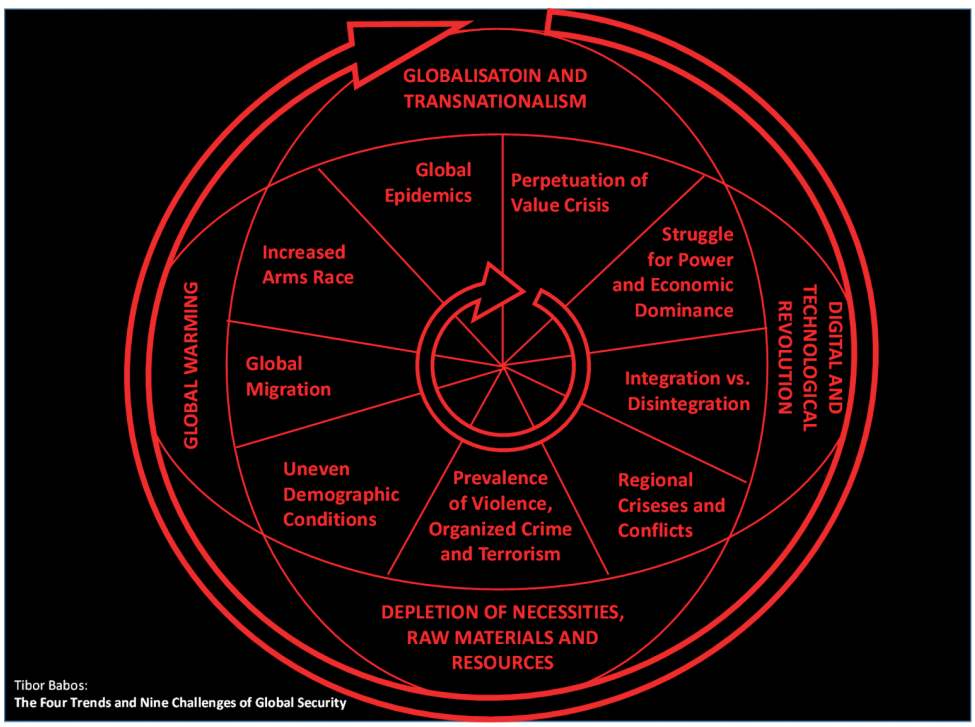

Figure 1: The Four Trends and Nine Challenges of Global Security

Source: Compiled by the author.

The four trends interact with the challenges and the challenges greatly influence the development of the trends, the challenges are clearly not the dominant factors though. It can also be stated that these four trends are not a permanent phenomenon in our time, but they are definitely a long-term one, while the challenges can be apostrophised as temporary or changing factors. Challenges, in addition to prioritising trends, shape each other's nature

[4] Tibor Babos, 'A biztonság globális és európai összefüggései', in *Kutatás és innováció a hazáért*, Conference Preceedings, Budapest, 5 November 2019.

according to a complex mechanism of action. Based on global and continental conditions known today, it can be stated with great certainty that these security factors must be taken into account even in the medium term and their role and impact may increase even more in the future than at present.[5]

Based on the reasoning of the above presentation, the argument of this study is that today's most defining security challenges are (1. the expanding globalisation; 2. the boom of digitisation; 3. the perpetuation of global warming; and 4. the increasing depletion of raw material resources).[6] These global and Europe-wide security policy trends define national ambitions and objectives all over the world. Among the above trends, this paper explores digitisation as a security challenge because digitisation, as the only technological factor of the above four, has the greatest impact on the development of today's modern world. This trend has an impact on the security of Europe as well as of Hungary.[7]

As a result of the IT revolution, politics, public administration, economy, industry, agriculture, education and science, health, transport, logistics, energy, diplomacy, national security and military systems have been transformed. We can say that this process is a global change of our era and it is therefore necessary to examine how nation states are adapting to the challenges of the technological revolution. However, with the development of digitisation, there are not only benefits but also serious dangers. Statistical data and case studies show that today we are increasingly counting on a rise in the number of cyberspace attacks and the quality and success of these acts. As a result of the rapid development of the technological level of mankind, new challenges emerge that determine the security of the world and thus of our country.[8] Although the recently released digital space is not the most important security factor, it is undoubtedly continued, sometimes defining other known challenges.

As a result of digitisation and smart cities, almost everything becomes more accessible to members of society more easily and quickly. Cyberspace attacks in many cases result in irreversible political or economic damage. Nation states, including Hungary, must have the ability to detect and address cyberspace threats, build cybersecurity, ensure the smooth functioning of critical information infrastructure, fend off attacks and properly carry out cyber defence tasks. However, the upsizing of digitisation takes place not only in cyberspace but also has a major impact on the following 4 global common spaces, which are also operational spaces from a military point of view: 1. land; 2. sea; 3. air; 4. outer space.[9]

The study looks for answers to the following questions: How can digitisation be identified in the global space as a security challenge? What are the main elements of hybrid warfare and cybersecurity in Hungary? What are the military policy relevancies

---

5 Ibid.

6 Tibor Babos, 'A biztonság globális és európai összefüggései', *Hadtudomány* 29, no 4 (2019), 16–29.

7 Alexandra Lilla Beregi, 'A Magyar Honvédség digitalizációja a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program tükrében', in *Digitális Biztonságpolitika Konferencia*, Conference Proceedings, Budapest, 25 May 2020.

8 Tibor Babos, 'A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái', *Hadtudomány* 28, E-publication (2018), 122–145.

9 Tamás Csiki Varga and Péter Tálas, 'Magyarország új nemzeti biztonsági stratégiájáról', *Nemzet és Biztonság* 13, no 3 (2020), 89–112.

of cybersecurity challenges relevant to our country? How could we characterise the cyber capabilities of the Hungarian Defence Forces nowadays?

The argument of this study is that the modernisation of defence systems is an essential key to successfully responding to new security challenges in our digital explosion era. Therefore, it is a must that government organisations, including defence and military systems fundamentally upgrade their own technical, structural and operational capabilities and accept digitisation as the driving factor of future defence and military development. In order to ensure that our country has knowledge of and capabilities to overcome the new security challenges created by digitisation in all operational areas the Hungarian Defence Forces need to switch to a new type of digital platform.

In light of the above, the study first examines digitisation as a global security challenge and then presents a comparative analysis of the relationship between hybrid warfare and cybersecurity. Finally, before drawing conclusions, it takes stock of the military policy relevance of the cybersecurity challenges relevant to Hungary.

Digitisation as a global security challenge

The current security processes, challenges, changes and trends need to be examined equally in order to pursue a successful policy both domestically and internationally. In the current unstable security environment, the factors and risks and threats to security are also changing. This means that, in addition to the economic, financial, social, cultural, religious, environmental, public security and migration problems, digitisation is causing us to face an increase in technical, IT systems and with it, cyberspace risks as well.[10]
As a result of the digital revolution, the centres of gravity of the new global power centres in Europe are being transformed and redefined. The success of the development of new power centres consists in the active and conscious use of digital, technological and information systems. In the meantime, we are seeing a mutation of global and European security challenges, which means that the security factors of our time are smaller in space, but more diverse and dynamic, easily cross state borders and may become global as well. We can conclude that globalisation can bring security challenges together, multiply smaller threat level to a significant and more complex one, as well as interconnect foreign and domestic security issues. Cultural and religious reasons stand in the way of globalisation and urbanisation, which are the scene of conflicts in the digital space. The contrast between radicalism and technology poses a great danger because rapid technological advances make the rich even richer and the poor even more poor and peripheral.[11]

The use of weapons of mass destruction and terrorism as an asymmetric security risk factor pose the greatest threat to developed countries. Due to proliferation of weapons of mass destruction and the lack of control of technologies, the world's balance of power is being transformed. Parties opposed to developed countries are more often using asymmetric devices for example viruses in cyberspace. Even with their low or limited

[10] Tibor Babos, *Az európai biztonság öt központi pillére* (Budapest: Zrínyi Kiadó, 2007).
[11] Babos, 'A Digitális Jólét Program'.

sources, they are able to cause a significant, or even a universal destructive effect. All this means that beyond nuclear, chemical, biological technologies, genetic engineering, proliferation of weapons of mass destruction, the massive use of IT and technology is one of the greatest security risks and threats of our time.[12]

NATO issued a new strategic concept at the Lisbon Summit in November 2010 to ensure that NATO capabilities provide more reliable protection against modern challenges. This means that action against hybrid threats, the protection of IT systems and electronic warfare will be at the heart of capability development.[13] The Global Commons Project has been launched with the aim of examining the seas and oceans, airspace, space and cyberspace in depth. These common dimensions are interrelated because everyone uses them, allowing information, goods and services to flow. Globalisation has made these spaces accessible to all and can therefore be used for good purposes as well as for malicious purposes and therefore the strategic importance of these spaces is increasing. NATO's aim is to provide the ability to combat damage against common dimensions through political, diplomatic and military domains. The importance of the ever-changing security challenges inherent in dimensions is very high from a military point of view because the army, air force and navy actively uses the seas, oceans airspace and outer space to transport military troops, units, navigation devices, reconnaissance and command control and communication systems. Cyberspace became the newest, most complex and most dangerous domain of global commons today.[14]

From the point of view of security challenges, cyberspace is the most important because it is not clearly delineated and cannot be delineated at all and technological developments have led to an increasing number of uncharted opportunities for the widespread use of cyberspace. Cyberspace is physically dependent on the physical devices that operate it: computers, servers, modems, cables, satellites. This means that the primary attackers of cyberspace, the activities of hackers can be physically traced. Despite the fact that the four dimensions are not just connected but also interconnected, cyberspace is different from the others. Its information base and infrastructure is largely non-state-owned, so private companies, and non-state actors operate and determine future developments, weakening the state's control role over it. For this reason, it is important to strengthen the cyberspace influence of state actors. In order to detect attacks on national and state digital systems, nations and states have to build right tools and capabilities to combat them.[15] Successfully facing new security challenges, especially in the cyberspace nations, states and their military systems need to invest more into digitisation and states need to review their strategy documents on cyber issues in the same way as new security risks.

---

12 Ibid.

13 Gergely Varga, 'A NATO új, lisszaboni stratégiai koncepciója', *Nemzet és Biztonság: Biztonságpolitikai Szemle* 3, no 10 (2010), 79–86.

14 Tibor Babos, '„Globális közös terek" a NATO-ban', *Nemzet és Biztonság: Biztonságpolitikai Szemle* 4, no 3 (2011), 34–46.

15 Babos, 'A Digitális Jólét Program'.

Hybrid warfare and cybersecurity in Hungary

Hybrid warfare and cybersecurity today are developing parallelly; at the same time, they have direct connection to each other. Although hybrid warfare has a longer history than cyber, cyber is the dominant factor of the subject, due to the fact that its relevance and space is much wider. As a result of the rapid development of the technological level of mankind, new opportunities and challenges emerge that determine the security of our country. As a result of digitisation, everything becomes more accessible to members of society. Today, there is a strong need for cities and villages to be more intelligent and able to effectively address the challenges of urbanisation and to successfully adapt to new situations and provide adequate answers to emerging issues.[16] Therefore, DJP2.0 places a special emphasis on the topic of Smart City developments to integrate smart solutions into the everyday life of settlements that make the lives of the people living there easier, more livable and safer. The basic task of the management of a settlement is both to create the safety of the people living in the settlement and their environment and to preserve the property of the institutions and companies operating under control. By building smart security systems, all of these above-mentioned goals can be achieved. Ensuring the security of networks is an essential condition for interconnecting and deploying systems.[17] In many cases, cyberattacks cause irreversible political or economic damage. Cyberspace, alongside land, seas, air and space is now a separate operational space.

Cyberattacks such as attacks on countries, international and world organisations, government and economic operators, are among the most significant security challenges of the 21st century. Hungary must be able to identify, address and cope with cyber threats, build cybersecurity, ensure the smooth functioning of critical information infrastructure, counter attacks and carry out cyber defence tasks. The number of attacks on IT systems is steadily increasing, so it is necessary to strengthen their protection and to increase the level of information security of users.[18]

Cybersecurity, like global pandemics, organised crime or terrorism, cannot be blocked by state borders today, spreading as a result of globalisation. Since computing systems became the basic tools of our societies and science and technology is available to all of us, we must be prepared to unexpected cyberspace attacks. It is necessary to adequately protect against cyberspace attacks, such as disrupting the functioning of governmental or public information and communication systems. Particular emphasis should be placed on cyber defence and the provision of international critical infrastructure.[19]

---

16 Alexandra Lilla Beregi, 'Magyarország Nemzeti Biztonsági Stratégiája (2012) a mai biztonságpolitikai kihívások tükrében', *Hadmérnök* 15, no 2 (2020), 205–217.

17 Digitális Jólét Program, 'A Digitális Jólét Program 2.0.', Budapest, 2017.

18 Péter Tálas, 'Changes in International Power Relations and Their Geopolitical Consequences', in *Security Challenges in the 21st Century*, ed. by Géza Finszter and István Sabjanics (Budapest: Dialóg Campus, 2017), 13–36.

19 László Kovács, 'Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I.', *Hadmérnök* 7, no 2 (2012), 302–311.

On 21 April 2020, the latest Hungarian National Security Strategy was released in which digitisation and cyberspace is one of the most dominant factors of new security challenges.

In the face of hybrid attacks, the defence and law enforcement forces are collectively able to combat civilian infrastructure. We can protect against new security risks including cyber warfare and technological advances that facilitate information flow, by adapting the right systems and improving our tools. This will make capacity improvements available with the support of the government, for the cybersecurity of our country. Continuous technical improvements are extremely important given the rapid rise in attacks on IT systems as a result of technological developments, a threat that is only further escalated by a low level of users' awareness on information security. For this reason, it is necessary not only to improve our tools and capabilities but also to increase user awareness.[20]

In addition to cyberspace, power struggles are underway for dominance over international waters and their resources, the Arctic and space. Cyberspace is now a separate operational space alongside oceans and seas, airspace and space and land. It is most likely to be adapted that future conflicts will increasingly culminate in cyberspace.[21]

In strategic common spaces, digitisation and globalisation have led us to face new challenges such as technological and revolutionary developments in 5G and space technology. It is important that our national security and military systems continue to invest into and develop cyber defence capabilities since unexpected attacks not only may cause fatal damages but also are more expensive.

Changes to international security policy, such as non-state actors; organised crime groups; international terrorist organisations; cybercriminal organisations; extremist religious communities; privately owned security companies; and other non-governmental actors have an impact on our country's security policy. This means that cyberspace is used to obtain critical data and to harm both different states and non-state actors.[22]

Increasing technological progress as a result of globalisation is based on digitisation. The vulnerability of information systems is a new security challenge. The number of malicious actions committed in cyberspace is increasing, it gets more sophisticated in their method and causes increasing damage. There is a great risk in the mass availability of information, which poses an information technology challenge but access to information can only be partially ensured for our country for the time being. Therefore, the introduction of processes supported by machine learning is no longer to be seen.[23]

With the rapid development of space technology, there is a growing technological gap between those who use technologies significantly and those who try to catch up. Hungary needs to play a prominent role in the knowledge and application of space technologies,

---

20 Government Resolution 1163/2020 (IV.21.) on Hungary's National Security Strategy.

21 Károly Szkála and Sándor Munk, 'A kibertér fogalma, értelmezése és fejlődése', *Földrajzi Közlemények* 142, no 4 (2018), 344–355.

22 László Kovács, 'A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában', *Honvédségi Szemle* 148, no 5 (2020), 3–18.

23 Dániel Berzsenyi, 'Kiberbiztonság', in *A globalizált világ kihívásai*, ed. by Péter Tálas, Tamás Csiki Varga, Alex Etl and Dániel Berzsenyi (Budapest: Ludovika Egyetemi Kiadó Iroda, 2021), 341–356.

because their use can become decisive in relation to development, economic indicators and political advocacy.

The unpredictability resulting from new security challenges is further undermined by the proliferation of weapons of mass destruction and their means of transport. Terrorist organisations, terrorist groups and various criminal organisations also possess and use weapons of mass destruction. Though these attacks induced by such means are not effective today due to the strong collective international community efforts, thus we must treat them as a major threat. It is in Hungary's interest to fight hybrid warfare within both national and allied frameworks. Hungary interprets cyber threats that causes direct attack against the state as conventional weapons. Cyberattacks, as aggression, is therefore considered classical attacks and may be responded by complex governmental domains with the approval and prior agreement of government agencies. Hungary pays particular attention to research and development, especially in the areas of cyber defence, artificial intelligence, autonomous systems and biotechnology. Today development of revolutionary technologies in Hungary are treated as strategic issues.[24]

Military relevancies in fighting against cyber threats

Any cyber violation against Hungary can therefore be identified as a direct attack against all elements of government systems, E-administration, critical infrastructure and critical information infrastructure, public and non-state companies and organisations. Constitutionally, the Hungarian Armed Forces must be able to cope with these challenges as well. Therefore, the digital transformation of the Hungarian Defence Forces is a vital task to the government to create new digital and network-based military systems. As a result of the improvements, national defence as a whole could be set up on a digital platform, which would result in the operation of defence, military and national security systems for market high-tech systems and infrastructures used by the public administration independently and disconnected in order to support the government's information communication.[25]

For Hungary to be able to face new security challenges, especially in cyberspace, the Hungarian Defence Forces need well-equipped and properly trained forces, effective, deployable and sustainable capabilities in the spirit of qualitative capability development rather than quantity. This means that the traditional tasks of the defence systems are complemented by new security challenges such as mass illegal migration, terrorist threat, hybrid attacks and disaster management. Therefore, the development of defence capabilities must be prioritised in such a way that it has the capacity to cope with all sorts of challenges up to war level. From the point of view of the armed forces, cyberspace

[24] Zoltán Rajnai (ed.), *Kiberbiztonság – Cybersecurity 2.* (Budapest: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2019).

[25] Tibor Babos and Miklós Szakali, 'Magyarország biztonsága a transzatlanti kapcsolatok tükrében', *Felderítő Szemle* 19, no 1 (2020), 29–44.

support for force operations is important and it is therefore necessary to develop the military's cyber defence and cyber operations forces as planned.[26]

To manage cybersecurity tasks, maintain cybersecurity and ensure the proper functioning of critical infrastructure, Hungary will take the following measures, based on the Hungarian National Security Strategy:

- identifying and monitoring challenges, risks and threats in cyberspace
- integrated and specific coordination of government agencies
- improving the legal regulation of cyberspace
- raising user awareness
- government information communication systems, national critical information infrastructure, the protection of open and classified information and the strengthening of the protection of national data assets, as well as the expansion of international cooperation on cybersecurity
- strengthening home-based research and development
- develop partnerships between public and non-state actors as well as between educational and scientific institutions and users
- fight against hybrid attacks should be based on the cooperation of state actors in the prevention, detection, intelligence and counter-response tools
- identifying cyberspace risks and addressing particular challenges
- being actively involved in international cooperation[27]

Developing digital and cyber capabilities

The process of transformation of the Hungarian Defence Forces is very significant since the government announced the so-called Zrínyi 2026 Defence Development Program in 2016. Complex transformation, acquisition of new military equipment, restructuring military command system and introducing new training requirements lays the foundations for research, development and innovation in the whole defence architecture and beyond. Digital and cyber capabilities of the military is the core part of the Zrínyi 2026 Defence Development Program.

The theatre of information warfare is cyberspace; however, changes are taking place in all other theatres of operations as well. It seems to be proved that conventional forces are no longer able to act effectively, especially against terrorist organisations, non-state actors or hybrid threats, thus the age of fourth generation warfare has begun. Against this background, the most important issue for forces is to increase responsiveness and to seek solutions for the successful implementation of digital transformation in all fields of use of force.

Interestingly, the key of the 21st century military operations is to build a threat-responsive command system, which is decentralised and at the same time integrated. In other words,

---

[26] Klára Fekete-Karydis and Bence Lázár, 'A kibervédelem katonai dimenziói', *Honvédségi Szemle* 148, no 3 (2020), 44–54.

[27] Government Resolution 1163/2020 (IV.21.) on Hungary's National Security Strategy.

a command structure, which is integrated and complex, at the same time its parts are separable but more operable and can recognise and address current challenges faster. To this end, problem solving, critical thinking, creativity, networking and rapid adaptation to changing circumstances are inevitable, as well as development of human abilities. The innovation of warfare is not only new technology, but also a kind of combination of skill-level application, rapid acquisition and innovative use of these technologies and latest weapons and machines. All of this together may help the state to create a stronger, more flexible and rapid reactive force, as well as to develop an appropriate organisational defence structure that is able to absorb all new developments of technology.[28]

Institutional transformations and, with it, organisation development have started in the Ministry of Defence and the Hungarian Defence Forces in 2019, three years later than the Zrínyi 2026 Defence Development Program was introduced. The Institute for Modernisation, the Hungarian Defence Forces and the Institute for Defence Research have been established in the same year. The Ministry of Defence has started to cooperate with different higher education institutions and launched a number of defence and military research projects. The National University of Public Service has also restructured its own educational and training focus. Professional education of new technologies, cybersecurity, engineering and hybrid warfare became the core curriculums of the Faculty of Military Sciences.[29]

Among the new security challenges facing the world and Europe, special attention should be paid to cyberattacks and cyber defence for digitisation and network systems. In the face of hybrid warfare, the military plans to create a cyber defence system that can withstand third-party incursions into command and control systems and detect activity suggesting an attack on the network. In order to counter threats in cyberspace, up-to-date direct, specialised and sustainable training is needed for soldiers, to this end the Cyber Training Centre of the Hungarian Defence Forces was transferred to Szentendre in June 2019.[30]

In order to achieve the comprehensive digitisation of the Hungarian Defence Forces, it is essential to develop the Hungarian Army's Separate Communications Network for Government Purposes. This is a special closed-end ICT network that should be able to support the management and command systems of the Hungarian Defence Forces, either in peacetime or during a qualified alert period, by providing a technological, technical and service background and an operating environment. A system is a network-based critical infrastructure based on special IT systems and tools. The network is responsible for serving the IT needs of higher military management, providing the technological and technical foundations of command systems, and enabling access to IT services during peace and classified alert periods. It is also responsible for connecting to and unloosing other ICT networks, that is, ensuring independent operation. The fundamental objective is to make the IT system, service and information centric. It also has to be user-friendly, multifunctional, convergeable and modern, and be able to satisfy both needs of the

[28] Áron Bencze, 'Digitális ugrásra készül a Magyar Honvédség', *Innotéka*, 03 May 2019.
[29] 'Középpontban a katona', 01 May 2019.
[30] 'Átadták a Magyar Honvédség Kiber Képzési Központját', 13 June 2019.

government and military sector. Another goal is to provide services to soldiers on the battlefield via real-time image streaming. The network should ensure cooperation with the networks of civil and law enforcement agencies on the one hand, and independent smooth operation in the event of a cyberattack or special legal order, on the other.[31]

As far as the international issues of digital and cyber capability development is concerned, it has to be mentioned here that Hungary is a founding member of the EU's Permanent Structured Cooperation (PESCO) project. PESCO is one of the European Union's permanent cooperation frameworks, which essentially supports defence-type projects and initiatives of member states. Many of these projects are already being organised by the European Defence Agency (EDA). The main objective of the PESCO project is to set up a cyber and information space, an information sharing centre, to create a common cyber situational awareness at the site of EU military operations. Hungary joined this initiative as a founding member. Establishing the Cyber and Information Domain Coordination Centre was carried out under the PESCO umbrella.[32]

Conclusions

The argument of this research paper was that the modernisation of defence systems is an essential key to successfully responding to new security challenges in our digital explosion era. Therefore, it is a must that government organisations, including defence and military systems fundamentally upgrade their own technical, structural and operational capabilities and accept digitisation as the driving factor of future defence and military development. To ensure that our country has skills and capabilities to overcome the new security challenges created by digitisation in all operational areas, the Hungarian Defence Forces need to switch to a new type of digital platform. In other words, modernising the Hungarian Defence Forces was essential to successfully address new security challenges during the digital explosion period.

Considering the above, the study first examined digitisation as a global security challenge and then presented a comparative analysis of the relationship between hybrid warfare and cybersecurity. Finally, before drawing conclusions, it took stock of the military policy relevancies of the cybersecurity challenges applicable to Hungary. In detail, the first chapter presented digitisation as a security challenge in the global space by analysing the goals of NATO's 'global commons' project. The second part analysed and evaluated the topicalities of the cybersecurity situation in Hungary and gave a presentation of the relevant parts of the new National Security Strategy. Chapter three has lined up the military political relevance needed to guarantee our country's cybersecurity.

Overall, it can be concluded that digitisation and digital transformation are present throughout the world as a result of globalisation, so that Hungary, through the capability

[31] Szabolcs Jobbágy, 'A Magyar Honvédség kormányzati célú elkülönült hírközlő hálózata', *Hadmérnök* 12, no 3 (2017), 223–236.

[32] Lajos József Komjáthy, 'A hatékony haderő felkészítésének néhány területe a várható alkalmazás szempontjából', *Hadtudományi Szemle* 11, no 1 (2018), 71–84.

development of the Hungarian Defence Forces, must be connected to the various systems and technologies in order to allow the defence, military and national security systems used for market high-tech systems and the infrastructures used by the administration to operate independently and separately in order to support the government in information communication.

Overall, it can be stated that digitisation and digital transformation are present all over the world as a result of globalisation. Developed nations, including Hungary must be connected to digitisation and by digitisation to each other's various systems and technologies. This system has to be integrated, but independent and separated at the same time, as well as connected to each other but separable, too. In other words, on the one hand we have to use the benefits of the whole global cyber system, as well as be ready to get separated from it, to defend threats or direct attacks coming from there and protect our own system. The Hungarian Defence Forces has a key role in this very important process. The Hungarian Defence Forces must therefore have the ability to detect, address and cope with cyberspace threats, build cybersecurity capabilities and forces to fully carry out cyber defence tasks and to guarantee the smooth functioning of governmental and critical information infrastructure at all times, in accordance with its constitutional obligation.

References

'Átadták a Magyar Honvédség Kiber Képzési Központját', 13 June 2019. Online: https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat

Babos, Tibor, *Az európai biztonság öt központi pillére*. Budapest: Zrínyi KIadó, 2007.

Babos, Tibor, '„Globális közös terek" a NATO-ban'. *Nemzet és Biztonság: Biztonságpolitikai Szemle* 4, no 3 (2011), 34–46. Online: http://nemzetesbiztonsag.hu/cikkek/babos_tibor-___globalis_kozos_terek____a_nato_ban.pdf

Babos, Tibor, 'A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái'. *Hadtudomány* 28, E-publication (2018), 122–145. Online: https://doi.org/10.17047/HADTUD.2018.28.E.122

Babos, Tibor, 'A biztonság globális és európai összefüggései', in *Kutatás és innováció a hazáért*, Conference Proceedings, Budapest, 5 November 2019.

Babos, Tibor, 'A biztonság globális és európai összefüggései'. *Hadtudomány* 29, no 4 (2019), 16–29. Online: https://doi.org/10.17047/HADTUD.2019.29.4.16

Babos, Tibor and Miklós Szakali, 'Magyarország biztonsága a transzatlanti kapcsolatok tükrében'. *Felderítő Szemle* 19, no 1 (2020), 29–44.

Bencze, Áron, 'Digitális ugrásra készül a Magyar Honvédség'. *Innotéka*, 03 May 2019. Online: www.innoteka.hu/cikk/digitalis_ugrasra_keszul_a_magyar_honvedseg.1909.html

Beregi, Alexandra Lilla, 'A Magyar Honvédség digitalizációja a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program tükrében', in *Digitális Biztonságpolitika Konferencia*, Conference Proceedings, Budapest, 25 May 2020.

Beregi, Alexandra Lilla, 'Magyarország Nemzeti Biztonsági Stratégiája (2012) a mai biztonságpolitikai kihívások tükrében'. *Hadmérnök* 15, no 2 (2020), 205–217. Online: https://doi.org/10.32567/hm.2020.2.14

Berzsenyi, Dániel, 'Kiberbiztonság', in *A globalizált világ kihívásai*, ed. by Péter Tálas, Tamás Csiki Varga, Alex Etl and Dániel Berzsenyi. Budapest: Ludovika Egyetemi Kiadó Iroda, 2021, 341–356. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16247/A_globalizalt_vilag_kihivasai_elektronikus.pdf?sequence=1#page=12

Digitális Jólét Program, 'A Digitális Jólét Program 2.0.', Budapest, 2017. Online: https://digitalisjoletprogram.hu/files/58/f4/58f45e44c4ebd9e53f82f56d5f44c824.pdf

Fekete-Karydis, Klára and Bence Lázár, 'A kibervédelem katonai dimenziói', *Honvédségi Szemle* 148, no 3 (2020), 44–54. Online: https://doi.org/10.35926/HSZ.2020.3.4

Government Resolution 1163/2020 (IV.21.) on Hungary's National Security Strategy.

Jobbágy, Szabolcs, 'A Magyar Honvédség kormányzati célú elkülönült hírközlő hálózata'. *Hadmérnök* 12, no 3 (2017), 223–236. Online: http://hadmernok.hu/173_20_jobbagy.pdf

Komjáthy, Lajos József, 'A hatékony haderő felkészítésének néhány területe a várható alkalmazás szempontjából'. *Hadtudományi Szemle* 11, no 1 (2018), 71–84. Online: https://epa.oszk.hu/02400/02463/00038/pdf/EPA02463_hadtudomanyi_szemle_2018_01_071-084.pdf

Kovács, László, 'Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I.'. *Hadmérnök* 7, no 2 (2012), 302–311. Online: http://hadmernok.hu/2012_2_kovacsl.pdf

Kovács, László, 'A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában'. *Honvédségi Szemle* 148, no 5 (2020), 3–18. Online: https://doi.org/10.35926/HSZ.2020.5.1

'Középpontban a katona', 01 May 2019. Online: https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/kozeppontban-a-katona

Rajnai, Zoltán (ed.), *Kiberbiztonság – Cybersecurity 2.* Budapest: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2019. Online: https://bdi.uni-obuda.hu/sites/default/files/oldal/csatolmany/kiadvany-2019.pdf

Szkála, Károly and Sándor Munk, 'A kibertér fogalma, értelmezése és fejlődése'. *Földrajzi Közlemények* 142, no 4 (2018), 344–355. Online: https://doi.org/10.32643/fk.142.4.6

Tálas, Péter, 'Changes in International Power Relations and Their Geopolitical Consequences', in *Security Challenges in the 21st Century*, ed. by Géza Finszter and István Sabjanics. Budapest: Dialóg Campus, 2017, 13–36.

Varga, Gergely, 'A NATO új, lisszaboni stratégiai koncepciója'. *Nemzet és Biztonság: Biztonságpolitikai Szemle* 3, no 10 (2010), 79–86. Online: http://nemzetesbiztonsag.hu/cikkek/varga_gergely-a_nato_uj__lisszaboni__strategiai_koncepcioja.pdf

Varga, Tamás Csiki and Péter Tálas, 'Magyarország új nemzeti biztonsági stratégiájáról'. *Nemzet és Biztonság* 13, no 3 (2020), 89–112. Online: https://doi.org/10.32576/nb.2020.3.7