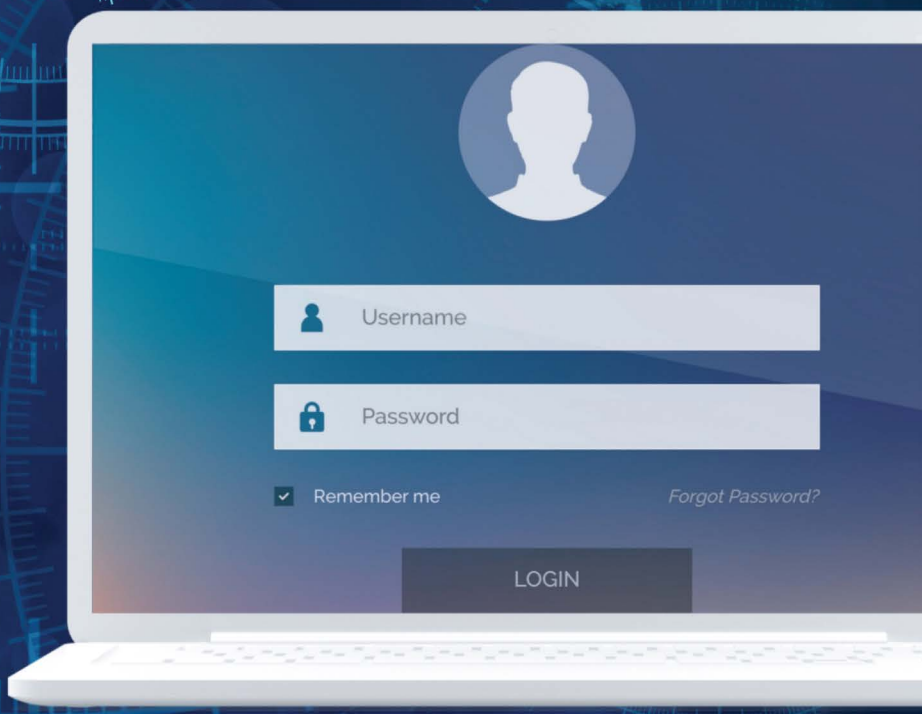
DIGITAL SECURITY POLICY IN THE CYBER SPACE

Edited by Tibor Babos



MATE

DIGITAL SECURITY POLICY IN THE CYBER SPACE

Hunexpert Hungarian Expert Systems Ltd. contributed
to the compilation of the volume and supported the publication.

DIGITAL SECURITY POLICY IN THE CYBER SPACE

Collection of studies

Edited by
Tibor Babos

Hungarian University of Agriculture and Life Sciences
Gödöllő, 2021

Authors:
Tibor Babos, Alexandra Lilla Beregi, Zsolt Csutak, Áron Drabancz,
Márton El-Meouch Nedim, Henrietta Hegyi, István Paráda

Editor-in-Chief:
Babos Tibor

Lectors:
Tibor Babos, László Jobbágy, Dóra Varga

Publisher:
Hungarian University of Agriculture and Life Sciences
H-2100 Gödöllő, Práter Károly u. 1.
Tel.: +36-28/522-000 https://www.uni-mate.hu

Published in 2021
Under the supervision of
Prof. Dr. Csaba Gyuricza, rector

Proofreading:
Hunexpert Hungarian Expert Systems Ltd.

DTP and layout:
Norbert Szalai

Printed by Szent István Egyetem Kiadó és Üzemeltető Kft.
Address: 2100 Gödöllő, Páter Károly utca 1.
Director: László Borbély

ISBN 978-963-269-976-9 (Printed)
ISBN 978-963-269-977-6 (PDF)

TABLE OF CONTENTS

FOREWORD

'Digital', 'security', and 'politics' – these words are commonly used in today's political, social, economic, technological or international relations. While their meaning seems self-evident, no systems theory, comparative analysis or research project on the relationships between the three words or their correlation has ever been published. Every day, researchers and the general public experience that the world's leading officials, experts and researchers interpret digital security policy differently, and prioritise its elements differently. Evaluations, arguments and positions are often radically influenced by factors arising from political, economic, cultural, historical, geographical, religious affiliations or circumstances. In fact, this is the basic dilemma of digital security policy—in the absence of common denominators and definitions, not only the approach to the problem, but also the results of research, negotiations and conferences aimed at solving it are different, and their outcome is ambiguous. This is further complicated by the incredible speed at which digitalisation is evolving. While digitalisation has solved many problems in recent years, it has become obvious that, in addition to the benefits, it raises a number of questions and dilemmas as well as it entails even some dangers. The Digital Security Policy research project, conference and the resulting book will help to reduce such differences, bring different views closer together and reach a common denominator for these concepts. It is rather unique as no other research project has ever been registered with such a title before. This book records this unique scientific and professional achievement. For this reason I recommend the Digital Security Policy research project, conference and book published by our University to all the researchers and interested readers who wish to acquire up-to-date knowledge regarding the current developments in this field. I am confident that the Digital Security Policy in the Cyber Space Vol. I. will be followed by many more volumes, as justified by the dynamic development of this field.

Prof. Dr. Csaba Gyuricza Rector
Hungarian University of Agriculture and Life Sciences

ACKNOWLEDGEMENTS

The editor-in-chief, the editor, the publisher and the authors would like to thank the organisations listed below for their professional knowledge, expertise, and human resources with which they contributed to the realisation of the research project and conference *Digital Security Policy* and the resulting publication of this book. This research project would not have been realised without the dedicated support of the Digitális Jólét Nonprofit Kft., especially László Jobbágy, CEO; the Association of Hungarian PhD and DLA Candidates; Hunexpert Hungarian Expert Systems Ltd.; the Hungarian University of Agriculture and Life Sciences and the Szent István Safety Research Centre; the Hungarian Atlantic Council; and The Council of the National Scientific Students' Associations.

Tibor Babos

Background and requirements for the Digital Security Policy in the Cyber Space research project

"Look to the future and measure the present with by what you wish to achieve"[1]
Kölcsey

The description of the situation

The pace, time constraints and prospects of today's international relations are greatly influenced by globalisation and the overall digital, technological revolution that has grown out of it. The digital and technological revolution has brought about wide-ranging, multi-faceted and at the same time rapid changes throughout society, radically transforming political, administrative, economic, industrial, agricultural, educational, scientific, health, transport, energy, diplomatic, national security and military systems.

Digitalisation, computer science and the Internet as interpreted today started to develop as part of the military systems during the Second World War, they gained momentum in the military blocks of the Cold War and by the 1950s the arms race reached their pinnacle in the technical control systems used in nuclear and conventional *high-tech* weapons. Today, information technology is equally present in the military organisations of the developed world and in the armed forces of emerging countries. The United States, France, Britain and Germany conduct all of the command-and-control of their military systems and that of their communications, logistics, supply chain management and military-industrial development on digital platforms, similarly to the practice of China, India, Brazil or Russia.

Once controlled by the military and military-industrial sectors only, digitalisation and the information revolution have become unstoppable; they permeate all the social systems of the world. Digitalisation radically transforms political, administrative, economic, industrial, agricultural, educational, scientific, health, transport, logistics, energy, diplomatic, national security and military systems as well. It can be established that security has also become digitalised, and this process can be interpreted as a global turning point that will determine the alternatives for human development in the long-term. This raises the fundamental question of how national (national security and military) strategies deal with the information revolution and the inherent fast-paced information and technological progress. Do they isolate themselves? Do they adapt? Or do they take the lead and exploit their potential?

1 Ferenc Kölcsey, Huszt. 29 Dec 1831, *The Complete Works of Ferenc Kölcsey*, National Széchenyi Library, (Budapest, 2019).

The description of the problem

This process has opened up a whole new dimension of development for humanity—resulting from the globalisation of information and communication; the quick availability of knowledge to the masses; the increased speed and relative reduction in distances; the universalisation of cultures, customs and languages; as well as the global interconnection of markets—we see how the daily routines that people follow have fundamentally changed, and previously held scientific theories are being refuted one after another. The current technical and technological explosion seems to be unstoppable and without specific boundaries. The dynamic rearrangement of the classical order has led to an unprecedented increase in the free competition of politics, economies, markets and technologies as well as rivalry between national, state, cultural and religious centres, which also prompted a growth of military power. The change in the economic dimension, the new structures of production, consumption and services, the integration of international finance, the increased demand for raw materials and the pursuit of the necessities of life are shaping the international order in an increasingly powerful and radical way, where the armed forces have an increasingly more important role. As the world 'shrinks', differences in development and conflicts of interest become even more pronounced.[2] In today's world, military capabilities based on advanced technology are gradually becoming more and more important.

It can established with great certainty that this process represents a turning point in history and it will determine the alternatives for the development of humanity in the long-term. In addition to the many benefits of the digital and technological revolution, certain negative consequences must also be taken into consideration. Widespread or targeted cyber attacks against networks of public interest and their critical elements; hacking into community systems, the theft, misuse and manipulation of personal data also for defamation purposes; and the disruption and manipulation of communication systems continue to pose a direct threat to states, organisations and individuals alike. There are unforeseeable potentials as well as dangers inherent to artificial intelligence, space research, genetic research or nanotechnology.[3]

Technical, IT or digital inventions have opened up new dimensions in military technology and the military industry. The proliferation of technological and IT-based systems, their changing content, along with their vulnerability, urge for new security requirements and different behavioural standards. Many actors cannot endure the resulting constant and intense pressure, and systems which are incapable of adapting or competing will collapse more frequently and much faster, become excluded or disconnected, and become antagonistic of the new processes.

2 Tibor Babos, *The Five Central Pillars of European Security*, NATO Public Diplomacy Division Brussels, Strategic and Defense Research Institute Budapest, NATO School Oberammergau and Chartapress, (Budapest, 6 October 2007).

3 Tibor Babos, 'A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái' (The security, defence, and military policy relevance of the Digital Welfare Programme), *Hadtudomány Journal*, electronic issue of 2018, (Budapest, 2018).

The system of objectives

This raises the fundamental question of how national (military and national security) strategies deal with the digital and technological revolution and the inherent fast-paced information progress. Do they isolate themselves from it? Do they adapt to it? Or do they take the lead and exploit its potential? Having regard to the fact that digital transformation is overwhelming and it permeates the entirety of the social systems of our developed world, Hungary should not only join but also take a leading role in this process, especially since Hungary is highly positioned in international comparison in terms of scientific, technological, IT skills and mathematical intelligence, and the achievements and scientific recognition of Hungarians have been widely acknowledged for centuries.

"Look to the future and measure the present with by what you wish to achieve" Kölcsey wrote in 1831, during the Reform era, when the country's development gained new momentum. By the beginning of the 19th century, in the Hungarian society—formerly lagging behind England, France, the model states of Western Europe and the Habsburg Empire—embarked upon national and innovative processes. In this era countless political, economic, social and cultural achievements were made, including the teaching of the Hungarian language, artistic works expressing national unity, the removal of obstacles to civic transformation as well as the creation of an independent modern industry and technology. These achievements later became pillars to the modern history of the Hungarian nation that was gaining self-awareness; and they led to the creation of a modern, civic Hungary. The information revolution challenges Hungary to accomplish its national aspirations and defend its 1000-year-old values in conditions similar to that of the Reform era. Therefore, it is important to take stock of the current international security developments, challenges and trends. The right conclusions must be drawn to ensure a successful policy both at a regional and international level.[4]

Thesis

The Digital Welfare Programme of the Hungarian Government, the Hungarian Atlantic Council, the Association of Hungarian PhD and DLA Candidates, The Council of the National Scientific Students' Associations and the Szent István Safety Research Centre of the Hungarian University of Agriculture and Life Sciences published an open research project and conference with the title *Digital Security Policy* that seeks to provide young Hungarian scientists with the opportunity to conduct research in the topic of security and digitalisation. Under the auspices of the *Digital Security Policy* research project and conference, young Hungarian scholars can apply for (1) writing a paper; (2) participating in and presenting at a conference; and (3) publishing in an edited and revised volume. The authors of outstanding papers were awarded with prizes and were invited to join the professional discussion regarding Hungarian security studies.

4 Tibor Babos, 'A Digitális Jólét Program biztonság'.

The competition organisers were looking for studies that correctly address the regional and international connections, processes and trends regarding the current security threats, challenges and the topic of digitalisation that can be utilised in the development of the national (military and national security) strategies. The application deadline was 30 April 2020.

Conclusion

The progress of the research project entitled *Digital Security Policy* that was launched in 2020, and the publication of the edited and revised book were greatly delayed by the COVID-19 global pandemic. At the same time, the call for competition organisers could draw lessons and even benefit from this turn of events. Probably the most important lesson drawn was that security of humankind could change unexpectedly and even radically at any time. It was the first time that humankind acted in a more or less united and collective way against such a threat by essentially limiting the physical contact between people, in which *Digital Security Policy* has become a key element. This is the first Hungarian and even international book on the topic to be written under these circumstances. The founders seek to ensure a future for this topic and the continuation of the scientific research initiative to go beyond the first conference and the first published book.

Tibor Babos

The defence and military policy context of *Digital Security Policy*

"The price of light is less than the cost of darkness."[1]
Arthur C. Nielsen

Resume

Digital transformation is unstoppable; it permeates the social systems of the developed world. Hungary should not only join it, but should also take a leading role in this process. This paper briefly summarises the military aspects and connections of the Digital Welfare Programme (DWP); outlines the directions of the Zrínyi 2026 National Defence and Armed Forces Development Programme; proposes a set of requirements for military systems that can be linked to the DWP; and it draws general conclusions on the representation of security, defence and military policies in the DWP.

Executive summary

The information revolution radically transforms political, administrative, economic, industrial, agricultural, educational, scientific, health, transport, logistics, energy, diplomatic, national security and military systems. It can be established with great certainty that this process represents a turning point in history and it will determine the alternatives for the development of humanity in the long-term. This raises the fundamental question of how national (military and national security) strategies are dealing with the information revolution and the accelerating information and technological progress that comes with it. Do they isolate themselves from it? Do they adapt to it? Or do they take the lead and exploit its potential? Considering that digital transformation is unstoppable and it pervades the entire social systems of the developed world, Hungary should not only join, but also take a leading role in this process. Especially since Hungary is highly positioned in international comparison in the field of scientific, technological, IT and mathematical skills, and the achievements and scientific recognition of Hungarians are undisputed worldwide. In light of this, following the presentation of the impact mechanism of security threats and information technology, this paper briefly summarises the military aspects and connections of the DWP and DWP 2.0; outlines the open-source elements and directions of the Zrínyi 2026 National Defence and

1 Arthur C. Nielsen, Colorado State University, Denver, online: http://social.colostate.edu/2015/06/19/the-price-of-light-is-less-than-the-cost-of-darkness/, accessed on 05.07.2019.

Armed Forces Development Programme; proposes the definition of requirements for military systems that can be linked to the DWP and DWP 2.0; and draws general conclusions on the representation of security, defence and military policy in the DWP.

Introduction

The information revolution has induced sweeping and large-scale changes in society as a whole, and it has radically transformed political, administrative, economic, industrial, agricultural, educational, scientific, health, transport, logistics, energy, diplomatic, national security and military systems. It can be established with great certainty that this process represents a turning point in history and it will determine the alternatives for human development in the long-term. This raises the fundamental question of how national (national security and military) strategies deal with the information revolution and the inherent fast-paced information and technological progress. Do they isolate themselves? Do they adapt? Or do they take the lead and exploit their potential?[2] Having regard to the fact that digital transformation is unstoppable and it permeates all the social systems of our developed world, Hungary should not only join but also take a leading role in this process, especially since Hungary is highly positioned in international comparison in terms of scientific, technological, IT skills and mathematical intelligence, and the scientific achievements of Hungarians have been widely recognised all over the world.

One of the most important tasks of the Digital Welfare Programme is to support Hungary's public systems, public administration, businesses and all citizens to be the winners of digitalisation and the information revolution. In recognition of this, the Programme aims to prepare Hungarian citizens, economic actors and state systems for this global transformation. The medium-term goal is for Hungary to become a world leader by transforming its scientific, technological, industrial, educational and other systems into digital opportunities within a decade.[3] The Hungarian Government intends to coordinate the interdependent and complementary governmental info-communication programmes within the framework of the DWP aimed at the digital development of Hungarian society and the Hungarian economy, adopted by Government Decision No 2012 of 2015 (XII.29.). The objectives of the DWP to be implemented in line with the National Info-communications Strategy (NIS) is based on the achievements and ongoing results of the Digital Nation Development Programme (DNDP). Government Decision No 1456 of 2017 (VII.19.) on the monitoring report of year 2016 of the National Info-communications Strategy, on the Digital Welfare Programme 2.0 (DWP 2.0), that is the extension of the Digital Welfare Programme, the adoption of its Working Plan for

2 Tibor Babos, *The Five Central Pillars*.

3 Government Decision No 2012 of 2015 (XII.29.) on the Digital Welfare Programme to be implemented by the Government based on the results of the national consultation on the Internet and digital developments (InternetKon), Netjogtár, https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A15H2012.KOR&timeshift=fffffff4&txtreferer=00000001.TXT, accessed on 10.01.2018.

2017–2018, and on further developments in digital infrastructure, competences, economy and public administration.[4]

Having regard to the fact that in addition to the political, public administration, economic, industrial, agricultural, educational, scientific, health, transport, energy and other civilian systems, digitisation and information technology have a major impact on defence, military and national security structures, this papers states that security, defence, military and national security considerations should be part of the Digital Welfare Programme and its updated, 2.0 version. More specifically, the defence, military and national security sector must be developed in the DWP and DWP 2.0 because (1) security processes directly affect digital prosperity; (2) defence, military and national security systems must support it; (3) military systems themselves apply and develop IT, digital and network-based capabilities; and (4) the defence and national security sector as a whole must be connected to the larger Hungarian digital development project in order to avoid disconnection or isolation from it. The implementation of the DWP should also be subject to a continuous professional assessment regarding the security conditions and threats, as well as protection by defence, military and national security aspects.

In light of this, following the presentation of the impact mechanism of security threats and information technology, this paper briefly summarises the military aspects and connections of the DWP and DWP 2.0; outlines the open-source elements and directions of the Zrínyi 2026 National Defence and Armed Forces Development Programme; proposes the definition of requirements for military systems that can be linked to the DWP and DWP 2.0; and draws general conclusions on the representation of security, defence and military policy in the DWP.

Digital aspects in the transformation of security

"Look to the future and measure the present with by what you wish to achieve"[5] Kölcsey wrote in 1831, during the Reform era, when the country's development gained a new momentum. By the beginning of the 19th century, in the Hungarian society—formerly lagging behind England, France, the model states of Western Europe and the Habsburg Empire—embarked upon national and innovative processes. In this era countless political, economic, social and cultural achievements were made, including the teaching of the Hungarian language, artistic works expressing national unity, the removal of obstacles to civic transformation as well as the creation of an independent modern industry and technology.[6] These achievements later became pillars of the modern history to the Hungarian nation that was gaining self-

4 Government Decision No 1456 of 2017 (VII.19.) on the monitoring report of 2016 of the National Info-communications Strategy (NIS), on the Digital Welfare Programme 2.0, that is the extension of the Digital Welfare Programme, on the adoption of its Working Plan for 2017–2018, and on further developments in digital infrastructure, competences, economy and public administration; Netjogtár, https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT, accessed on 18.01.2018.

5 Ferenc Kölcsey, 'Huszt', Cseke, 29 Dec 1831, *Kölcsey Ferenc összes művei* (The complete works of Ferenc Kölcsey), National Széchenyi Library, Budapest, http://mek.oszk.hu/06300/06367/html/01.htm#120, accessed on 12.10.2015.

6 András Gergely, 'A polgári átalakulás programja, A reformkor' (The programme of bourgeois transformation, The Reform Era), *Rubicon Historical Journal*, (1996/10). Kormányfők (Heads of Government), (1996/4-5), Államtörténet (State History) (1996/1-2), Ezer év, Budapest.

awareness; and they led to the creation of a modern, civic Hungary. The information revolution challenges Hungary to accomplish its national aspirations and defend its 1000-year-old values in conditions similar to that of the Reform era. Therefore, it is important to take stock of the current international security developments, challenges and trends. The right conclusions must be drawn to ensure a successful policy both at a regional and international level.

In the late 1980s, a radically new global strategic situation emerged when the confrontation between the East and the West ended. One after another, Central and Eastern European states broke with the practice of communism and the centralised state system and declared an opening towards the West and its social system. These occurrences led to widespread disintegration, as well as integration trends. The Eastern European events radically changed the political landscape of the world, and the resulting changes are still decisive on the European continent. In the new, more diverse and unstable situation, those factors, sources of danger and risks that affect security have received a different emphasis along with new aspects.[7] Other components of security have come to the forefront—besides the economic, financial, social, cultural, religious, environmental, public security and migration issues there are now technological and IT risks that are dominantly present.

The security of our planet is still characterised by the transitory nature of the consequences resulting from the comprehensive historical changes, as well as by a dynamic restructuring, market and political competition, regionalisation, localisation and nationalism, while the digital revolution and its development are becoming the defining historical phenomenon. As the order of the Cold War has been dissipating since the 1980s, the new global centres of power are being transformed and redefined in Asia, North America and Europe. In this process, the economic potential of the US and Western Europe, while still important, is no longer clearly dominant. The emergence and success of centres of power depend on the more active, targeted and widespread use of digital, IT and information systems.

Concurrently, both global and European security challenges are undergoing a comprehensive and large-scale change. Today, threats that cannot always be linked to nation states, but which manifest a transnational character, are becoming more and more clearly and forcefully expressed. Factors under the war-risk threshold such as nationalism; separatism; extremism; economic, technological, social and cultural disparities; divergences in development perspectives; ethnic and religious contrasts; contradictions between territorial integrity and national and ethnic self-determination; the proliferation of weapons of mass destruction; terrorism, transnational organised crime; money laundering; trafficking in drugs, arms and human beings; migration; environmental pollution; industrial and other man-made disasters or the spread of pandemics are clearly no longer constrained by the country borders. By nature, the security risks of our times are less spread out geographically, but they are more complex, diversified and dynamic. Their impact can easily reach global proportions and their temporal scope is almost impossible to be defined.[8]

The potential confrontation of national economic, political and military strategies targeted at global strategic goods continue to remain a potential security threat even in the 21st century. While in the developed world, competition between global centres is intensifying at

7 Tibor Babos, *The Five Central Pillars*, pp. 69-92.
8 Tibor Babos, *The Five Central Pillars*, pp. 69-92.

an increasingly dynamic pace, regions of insecurity and in transition are experiencing a steady accumulation of security deviations. The struggle for survival between countries at different levels of economic development is actually independent of prosperity. Developed countries compete with each other just as much as underdeveloped countries, or as underdeveloped countries compete with developed countries, and vice versa. To put it in simple terms—everyone wants to have more, irrespective of the fact whether they already have a lot or only a little. At the same time, most global strategic goods are still finite. IT platforms are developed and used by all public and non-public entities; therefore, digital spaces tend to merge, forming a global entity and multiplicity.

Social and cultural values influenced by globalisation, digitalisation, information and media are causing serious identity disorders in community both at macro and micro levels. Traditional national traits, consciousness types, rules and other values are being reinterpreted, and in this multi-faceted process, national strategic goals are also undergoing a major transformation. One of the main reasons for this is that, as a result of more open borders, the free flow of information and the globalisation of information, the categories and levels of analysis of international relations—*national, nation state* and *international*—are being radically reassessed.[9]

The universalisation of security challenges as a result of globalisation has greatly blurred the distinction between *foreign* and *domestic security policies*. In this process, state-centred institutions and rules are dissolved and give way to laws dictated by global networks and actors. The universalisation of risk factors is leading to an intensification of the debate on common security policy action, and to nation states raising their advocacy a level higher, to that of international security institutions. This is a trend that entails an increase of responsibility on the international institutional system. In this process, the role and competence of the state as a *factor in international relations* is being transformed. Today, states operate in an era of post-international dynamics, which makes borders easier to cross, institutions less efficient and political power to be more muddled. State institutions remain important, but they function less efficiently, with fewer resources and with a diminished legitimacy. However, in light of the fact that international organisations are losing prestige and legitimacy more rapidly than states, the power of national actors is relatively increasing.[10]

There are many, mostly cultural, religious and nationalist strongholds that still stand in the way of globalisation and modernisation. The question is whether very closed communities organised around traditional slogans, such as Islamic societies or contemporary dictatorships, will be able to resist or confront this complex and multi-level process without engaging in conflicts. Since Islam itself is not homogeneous, it is likely that conflicts will erupt along the fault lines between extremism—that is between overly closed, fundamentalist dictatorships on the one hand, and open, liberal societies on the other. These two opposing forces will certainly confront each other until the contrasts balance each other out, or, appropriately, one weakens the other one to a minimum.[11] Digital networks are open arenas for this confrontation. While the Internet has a huge cultural impact on closed societies, it is increasingly being used by fundamentalist systems to carry out their attacks with it.

9 Tibor Babos, *The Five Central Pillars*, pp. 69-92.
10 Tibor Babos, *The Five Central Pillars*, pp. 69-92.
11 Tibor Babos, *The Five Central Pillars*, pp. 69-92.

Perhaps the greatest danger today lies in the contrast between radicalism and technology. The growing risk of confrontation due to unequal social and economic foundations and disproportionate resources is exacerbated by cultural, civilisational, religious, ethnic rhetoric and political interests. This complex social polarisation may then interact with the military potential that remains as a legacy of the Cold War, in which the almost immeasurable technological contrasts and the relative ease of access to weapons of mass destruction play a decisive role. This is causally linked to further rapid and broad-scale scientific and technological progress, with the rich becoming even richer and more advanced and the poor even further marginalised. How and when these contrasts will balance each other out remains to be seen.

Asymmetric security risks, such as the use of weapons of mass destruction, their capacity to reach targets and/or strikes caused by terrorist attacks, are nowadays a more likely threat for developed countries. Today, in the turbulent security environment of the post-Cold War era, the world's strategic balance of power is being restructured by the uncontrolled proliferation of weapons of mass destruction and other destructive technologies. Countries, nations and non-state actors in opposition to the developed world, in the absence of, or instead of, *regular* instruments of international advocacy, are resorting to asymmetric tools that require relatively limited resources, which can have a universal impact. The developed countries where such technologies were developed, are now potential targets of these solutions. With the growing possibility of certain political forces in the Third World resorting to *dirty* means of warfare in their conflicts with each other or with the developed world, the wide range of threats posed by nuclear, chemical and biological technologies, genetic manipulation, the means of delivery for weapons of mass destruction, the widespread use of computers, and technologies becoming used by unauthorised parties, are perhaps the threats that could most easily materialise in our time.

Terrorism is a reaction or rather a by-product of globalisation. Terrorism is no longer a domestic problem, because it poses a direct threat to international security. Inequality, poverty, the ambitions of dictatorships to expand and their related cultural roots serve as breeding ground for terrorism. Terrorism, as a universal threat, is manifested by the scale of attacks, the qualitative and quantitative indicators of global casualties. The activity is conducted by transnational, professional, mobile, fully uninhibited terrorist organisations that operate beyond any borders and that pose a potential security threat to each and every nation state.

From a cultural point of view the question regarding the future of globalisation, digitalisation and IT development is whether each nation, country, federation, community of states, region, alliance or organisation will be able to mobilise its resources to engage in this process without any conflict, or to transform it, or maybe even put an end to it? And if not, which one(s) will not be able to do so? When? And at what cost?

The *cyberspace* of the Global Commons

At the NATO Summit organised in Lisbon on 19-20 November 2010, Secretary General Anders Fogh Rasmussen announced that the Heads of State and Government had adopted a new strategic concept for a stronger, more effective Alliance, which is more open and cooperative towards global actors and processes. NATO leaders pledged to shape NATO capabilities in the future to provide a more reliable defence against the modern challenges of our time. Ballistic missile defence, countering hybrid threats, the protection of information systems and electronic warfare will be a priority in the future development of the Alliance's capabilities.[1] The Allied Command Transformation (ACT), which has been actively involved in the preparation of the Strategic Concept, has launched the Global Commons project to examine modern challenges more in-depth, which in fact explores the potential geographic and virtual dimensions that cannot be linked to a specific country or region but are crucial to the security of NATO and its member states. These common dimensions are basically the seas and oceans, the atmosphere, outer space, and cyberspace.

The ACT study titled *Global Commons*[2] explores the security challenges and power control opportunities inherent in geographic and virtual spaces that cannot be linked to a particular nation, country or region, but are of critical importance to NATO and its member states. The shared seas and oceans; the airspace; outer space and cyberspace are globally interconnected, overlapping and interdependent spaces. Since they allow the flow of information, goods, services and other products important to humanity as well as the movement of people, everyone uses them.[3] In a globalising world, the strategic importance of shared spaces is gradually increasing, not only for bona fide users but also for malicious ones.[4] Organisations at the forefront of security research, including NATO, have been driven by the realisation that strategic damage can be caused on one or more of these dimensions with relatively limited financial investment and innovation. For NATO and its member states to be able to meet these challenges, they need to take serious political, diplomatic and military steps in both external and internal regulation. This task is urgent because the problem is twofold. On the one hand, security conditions are changing rapidly and are difficult to monitor due to the increasing level of globalisation and the technological revolution, and delays can only be compensated later at considerable additional cost, which can therefore become a strategic disadvantage. On the other hand, the global common spaces defined—and otherwise so far dominated—by the United States and its Western allies are increasingly being exploited by malicious, usually non-state actors who can inflict damage or even direct blows on the Western world.

The four dimensions are important from a military point of view, since they are constantly used in manoeuvres—but above all in command, control and liaison activity—from the

1 'NATO Summit paves way for renewed Alliance', NATO HQ, (20 Nov, 2010), http://www.nato.int/cps/en/SID-A807E092-E5343B66/natolive/news_68877.htm, accessed on 01.12.2010.
2 The Global Commons Initiative, The Global Commons Homepage, Allied Command Transformation, NATO, http://www.act.nato.int/globalcommons, accessed on 01.12.2010.
3 Security and Defence Agenda, Atlantic Council, *Protecting the Global Commons*, (Brussels, November 2010).
4 Scott Jasper, *Securing Freedom in the Global Commons*, (Stanford University Press, California, USA), p. 3.

highest level of command to the smallest units.[5] For example, the Alliance actively uses the oceans and airspace for the transportation of troops and military material; the airspace and space for command-and-control, reconnaissance and navigation; or the cyberspace to maintain command, control and for communications. Having regard to the fact that NATO's military formations are not only tasked with defending themselves, but also the interests of the member states—including their trade, research or telecommunications infrastructure—they must also be ready to carry out military missions in any of the four dimensions. Obviously, this requires significant reconnaissance, strategic analysis, planning, command-and-control, capability development, logistics and operational preparation regarding the global space.

It is clear that the four dimensions share common features in many respects and are therefore interlinked and overlapping, but in other respects they have a number of unique and different characteristics. Consequently, they must be examined both from a general and a specific point of view.[6] In terms of security, cyberspace is the global dimension that receives the most attention, since it was created by humanity in the last few decades, and therefore there is no sufficient international legal or historical experience to regulate and manage it. Unlike the seas and airspace, cyberspace cannot be clearly defined or delineated as it does not have clearly identifiable boundaries. Technological development does not occur in a confined space, but rather, as technology improves, the possibilities and horizons of cyberspace are dynamically expanding. Understanding the characteristics of Global Commons and the rules that govern them is important not only because we use them all the time in our daily lives, but primarily because they can also be used by opponents to gain strategic advantage or to suffer losses.

In some ways, cyberspace is the most unique dimension of all, since it cannot be connected to or described only by physical or geographical terms. At the same time, cyberspace is highly dependent on physical devices, technologies, computers, servers, terminals, cables, antennas, satellites, which are no longer virtual, and their ownership and location can also be determined.[7] Once a piece of information starts its journey through artificially designed channels, it becomes extremely difficult to determine its exact location at any given time. Information launched from a computer travels to its destination via a multitude of servers, signal transmission towers, optical cables, and satellites. In this case, the data set does not follow the shortest path, but its journey is basically determined by the free and cheaper capacity of the available networks. The information may travel on optical or other types of cables on the ground, in the air as a set of electronic signals, on flexible optical cables in the seas, or on satellite systems located in space. This type of information traffic is already happening million times every hour all over the world, and its quantity and quality are on an exponential increase. It can be clearly predicted that cyberspace systems will become bigger, faster and more complex over time.

5 Linton Wells II, 'Manoeuvre in the Global Commons – The Cyber Dimension', *SIGNAL Magazine*, (December 2010), http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2472&zoneid=306, accessed on 25.01.2011.

6 Tara Murphy, 'Security Challenges in the 21st Century Global Commons', *Yale Journal of International Affairs*, Volume 5, Issue 2 – Spring/Summer 2010, Spotlight on Security, (July 20, 2010), http://yalejournal.org/2010/07/security-challenges-in-the-21st-century-global-commons/, accessed on 09.12.2010.

7 Ron Deibert, 'Toward a Cyber Security Strategy', *Vanguard*, Canada, http://www.vanguardcanada.com/CyberArmsRaceDeibert, accessed on 28.01.2011.

The vulnerability of cyberspace lies precisely in its complexity, with hackers being the primary attackers as we know it today. Up until recently, attacks have mainly focused on software, meaning that hackers have attacked programmes and virtual systems. But this has changed dramatically. Unlike the other dimensions, the information base and technological infrastructure of cyberspace is predominantly owned by civil and commercial actors.[8] Therefore, cyberspace is primarily not dependent on states or governments, nor is the security of different systems first and foremost guaranteed by them. It is NGOs that are responsible for that. The situation is further complicated by the fact that the owners are economic operators and therefore operate according to market rules and are in strong financial competition with each other.[9] Under such circumstances, cyberspace providers have a strong interest in resisting external constraints, evading state and international regulation and pushing the security aspect imposed by the rules to the background. This obviously provides them with freedom, more creative developments and an equally important aspect—cheaper maintenance. It means that they spend the money on their own security and developments, rather than on strict compliance with the obligations imposed by external regulations. As long as this paradox persists, state control—ensured by international law—will continuously become weaker and weaker.

One of the best examples of the extremes, unregulated features and dangers that characterise cyberspace is the WikiLeaks scandal that erupted in autumn 2010. It is well-known that WikiLeaks and its supporters specialise in disclosing confidential or even top-secret information, no matter whether it comes from individual, company or government sources. As their activity has caused serious damage and harm to the interests of a number of NGOs and the state, the victims decided to launch a major counter-campaign. Currently, there is a high intensity and wide-ranging hacking attack, government intelligence operation, police action, diplomatic coordination, as well as economic and financial activity to undermine wikileaks.com.[10] It is likely that the harsh WikiLeaks attack on state interests will serve as the ground for strengthening state defence mechanisms, including the development of intelligence IT capabilities.

From a military perspective, the cyber attack against Estonia in May 2007 and the Russian-Georgian conflict in the summer of 2008 provide the most recent lessons in this respect. The cyber attack on Estonia is now described by analysts as the first large-scale, real, country-to-country cyber war in military history. The cyber attack against Tallinn was a so-called DDoS attack, which overloaded the Estonian IT systems and made them inoperable. The attack targeted the servers of the Estonian Parliament, government offices, ministries, banks, telecommunication and media companies. The experts agreed that the selection of the targets, the well-organised and unified nature of the attacks, the timing and the sheer force of the operation point far beyond an action carried out by a simple hacker group or even an organised crime group. Estonian IT networks were supposed to handle thousands of times

8 The White House, The National Strategy to Secure Cyberspace, (Washington, February 2003), http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf, accessed on 17.12.2010.

9 Ziad I. Akir, 'Space Security: Possible Issues & Potential Solutions', *Space Journal*, Issue 6, (2004).

10 'Invisible armies fight the WikiLeaks war', *Origo.hu*, http://www.origo.hu/nagyvilag/20101209-wikileaks-julian-assange-internetes-haboru.html, accessed on 16.12.2010.

the regular traffic, which they were obviously not able to do.[11] Since Estonia requested the convocation of the North Atlantic Council, a broad international coalition was formed to investigate the incident. Nevertheless, they have not been able to verify where the attacks originated from and exactly which country was behind them. The data streams that made the targets inaccessible were infected with viruses and came from temporary servers installed in various locations around the globe. One can only suspect that Russian governmental authorities were behind the attacks.

The cyber dimension of the Russian-Georgian conflict shows a much clearer picture. The radio-electronic reconnaissance agencies of Moscow, in close cooperation with the Russian military, launched a coordinated strike against the civilian and government IT systems of Georgia, as a result of which both the open civilian as well as the classified government IT networks collapsed.[12] In this case, not only the virtual systems were attacked, but also the physical infrastructure. This has fully paralysed the defence capabilities of the Georgian government for a long time. It is no exaggeration to say that the above-mentioned situations can destroy the defence systems of even leading NATO members, not to mention attacks that are followed by specific armed interventions.

In response to the ongoing attacks on the IT systems of NATO, the Alliance published its cyber defence concept in 2009, which provides a complex description on the protection of virtual and physical infrastructures, as well as areas that NATO considers to be of interest.[13] However, in addition to the attacks on the IT systems of NATO, the pressure of technological advances also played a role in the decision to take a stance in this respect. The leadership of NATO recognised it many years ago that the transition to the so-called digital warfare and digital command of the operations are now basic requirements, the principles and defence of which must be included even in the highest level conceptual documents.[14] NATO has thus conceptualised strategic principles and standards in a top-down regulatory mechanism, and at the same time it also builds on an operational, counter-intuitive, bottom-up working method for decision-makers, responsible bodies and implementers.[15] In all of this, NATO considers the human factor to be the most important, as human activity is behind all cyber attacks as well as their prevention. The defence-related training and preparedness of NATO users, system administrators and maintenance personnel are therefore more important than ever.

11 Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian*, (17 May 2007), http://www.guardian.co.uk/world/2007/may/17/topstories3.russia, accessed on 16.12.2010.

12 Gadi Evron, 'Internet Attacks Against Georgian Websites', *CircleID*, (Aug 11, 2008), http://www.circleid.com/posts/88116_internet_attacks_georgia/, accessed on 16.12.2010.

13 Evgeny Morozov, 'The Fog of Cyberwar, NATO military strategists are waking up to the threat from online attacks', *Newsweek*, (18 April 2009), http://www.newsweek.com/2009/04/17/the-fog-of-cyberwar.html#, accessed on 16.12.2010.

14 Rex B. Hughes, *NATO and Cyber Defence, What steps have been taken by NATO against the threat of cyber attacks? What needs to be done to prevent them in the future? Mission Accomplished?* Ap: (2009), nr 1/4, http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf, accessed on 28.12.2011.

15 Rex B. Hughes, *NATO and Cyber Defence Mission Accomplished?*, (2009), nr 1/4 http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf, accessed on 16.12.2010.

International overview

NATO and the United States

NATO first encountered cyber warfare during the 1999 Kosovo bombing. The military intervention was launched on 24 March 1999 against the forces of Slobodan Milosevic. Following the military intervention, Serbian hackers launched an attack against the website of NATO. On several occasions, the website of NATO became unavailable for long periods of time due to continuous Distributed Denial of Service (DDoS) attacks. The Serbian hacker group known as the Black Hand, which was responsible for the attacks, also posted political messages on several government sites and tried to hack into NATO command servers on several occasions, mostly unsuccessfully, as they managed to reach the IT network of the Air Force but were unable to access classified information. Following the bombing of the Chinese embassy in Belgrade, Chinese and later Russian hackers joined them, also using DDoS attacks and deface techniques to sabotage both NATO and US embassy websites. The Russian hacker group *From Russia with Love* has been the most prominent actor in the attacks against NATO. According to the statistics, they hacked at least fourteen military and state websites together with Serbian hackers during the 1999 Balkan war. It was largely the cyber incidents following the Kosovo intervention that helped decision-makers to recognise the importance of cybersecurity. Consequently, NATO's cyber defence programme was launched at the Prague Summit in 2002, which included the establishment of the Cyber Incident Response Capability. The Technical Centre behind this tool is able to detect intrusions into NATO systems. This marked the beginning of the North Atlantic Treaty Organisation's preparations for cyber warfare.[16]

Nowadays NATO, in line with the US conceptual and strategic development system, treats digitalisation and cyberspace as a complex system. On the one hand, NATO applies, builds on it and develops it in its own systems, and on the other hand—as one of the Global Commons—it considers it to be its raison d'être and as one of its war theatres[17] with regard to the doctrinal systems (NNEC DJTS etc). Although NATO has not yet established its own cyber forces, it has the so-called NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). Founded in Tallinn in 2010, NATO CCDCOE functions as a NATO-accredited knowledge centre, research institute, training and education base and training centre. This international military organisation conducts interdisciplinary applied research and initiates and hosts educational curricula, training courses and exercises. The organisation is made up of international experts, scientists, lawyers, strategic planners and military personnel who jointly conduct cyber and technology research along the military, governmental, administrative and industrial interests of NATO and its member states. Membership is open to all allied countries. The countries currently actively participating are the Czech Republic,

16 Gergely Szentgáli, 'A NATO kibervédelmi politikájának fejlődése' (The Evolution of NATO's Cyber Defence Policy), in: *Nemzet és Biztonság*, Budapest, http://uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf, accessed on 28.12.2017.

17 Tibor Babos, 'Globális közös terek a NATO-ban' (Global Commons in NATO), *Nemzet és Biztonság*, Centre for Strategic and Defence Studies, (Budapest, April 2011), http://www.nemzetesbiztonsag.hu/cikkek/babos_tibor-___globalis_kozos_terek____a_nato_ban.pdf.

Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States. Austria and Finland, as non-NATO partner countries, have signed a cooperation agreement.[18]

China

The Chinese economic miracle and the resulting complex expansion of power have become commonplaces by now. China has, without doubt, been at the political and economic forefront of the world in the last 25 years, and no other power can ignore Beijing's interests and its continuous expansion. But the Chinese miracle and imperialism does not end here, as cyberspace is not a neglected portfolio when it comes to the global extension of power by China.[19]

According to Internet Live Stats, China had 721 434 547 Internet users in 2016, or 52.2% of the country's population of 1 382 323 332. It accounts for 21.1% of the world's total Internet users, which is 3 424 971 237.[20] This is all the more shocking because less than a decade ago the entire Internet network was censored by the central government in China. Today, the country boasts of the most structured and largest public IT system in Asia.[21] Maintaining and developing this position, China is conducting significant developments in IT, both internationally and in absolute terms, and is nowadays present in the digital market not only as a user but also as a developer.

As the most populous nation and Asian power with the largest digital system on the globe, China has recognised the dangers and the potentials of cyberspace, including its military applications, at an early stage. The direct presence of Chinese security and military systems and their increased activity on the world wide web can be clearly detected by international Internet measurements. This is confirmed by the fact that China has built up globally significant assets and mobilised special experts in order to assist digital transformation. However, the Chinese government does not see the digital revolution as a separate topic, therefore they have not yet established separate cyber organisations or hierarchies. Rather, the complexity of the Chinese public administration structures and known conceptual documents suggest that all government portfolios and state segments are being transformed all at once to become IT capable.[22]

The President of the People's Republic of China, Xi Jinping, established the Central Internet Security and Information Management Group in 2016, under his personal supervision, with the main task of preparing a cyber strategy for China. This clearly shows that Beijing sees digitalisation and IT as a natural part of social development and therefore does not separate it from the ideology of the government or that of the Chinese Communist Party. Several conclusions can be drawn from this very interesting approach, which are as follows:

18 History, Structure, NATO Cooperative Cyber Defence Centre of Excellence, http://www.ccdcoe.org./history.html, accessed on 10.01.2018.
19 Mikk Raud, China and Cyber: Attitudes, Strategies, Organization, NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf, accessed on 27.04.2017.
20 Internet Live Stats, http://www.internetlivestats.com/internet-users/china/, accessed on 25.01.2018.
21 Desmond Ball, China's Cyber Warfare Capabilities, https://indianstrategicknowledgeonline.com/web/china%20cyber.pdf, accessed on 20.12.2017.
22 Mikk Raud, China and Cyber: Attitudes, Strategies, Organization, accessed on 26.01.2018.

- the world's largest national Internet community is centrally governed;
- given the size of the community, this governance directly affects and influences the Internet network as a whole;
- China has thus not only become part of the online world, but it is also a dominant player, and since the main content on the Internet—at least in the early stages—was a representative of Western values and culture, it has become a direct information gateway and China has in the meanwhile adapted to the West in many areas;
- the reverse is not true, as almost no Chinese content appears on the web in the West;
- adapting to the opportunities offered by the Internet, China has gained access to additional information and networking capital in a wide range of areas.[23]
- Taking advantage of these circumstances, China has also consciously expanded its national security and military capabilities in this area. It is a proven fact that the Chinese military, Chinese private companies and individuals are actively engaged in IT and information activities towards Western powers and neighbouring states at the behest of the Chinese government. These operations target scientific research, technological secrets, industrial developments, government systems and classified information. Beijing clearly shows that, as in the past 30-40 years, it is prepared to steal technology and *know-how* illegally and aggressively in order to seize the strategic initiative and gain direct economic, political or military advantage. Nothing proves the success of Chinese information operations more than the theft of an entire American F–35 fighter jet and bomber aircraft weapons system, the most expensive military development of the United States.[24]

Russia

Russia interprets and treats cyber warfare very differently from the Western countries. Cyber warfare is not a new element, but it fits well with the general and traditional Russian strategic concepts as a new opportunity and new space where war is fought. According to Kremlin strategists, Russia is under geostrategic pressure from the US-dominated and expanding NATO, which threatens the country's security through its IT systems and networks, as in all other areas. The information space is seen by Russia as essentially permanent and infinite. For Moscow, the Internet, the free flow of information, open access to data, is both a threat and an opportunity to be exploited. At the same time, the Kremlin is relatively less ambitious in terms of large-scale cyber developments than the US military leadership, but it is investing heavily in the knowledge base and human capital to support the field.

Russian military writers do not use either the word *digital* or *cyber* in relation to military systems. The conceptual documents are more concerned with the so-called *information systems* and *information warfare*, which serve as a general framework for the topics of computer systems, information technology, electronic warfare, information operations and psychological warfare. Consequently, cyber and IT are rather tools than a strategic dogma

23 Mikk Raud, *China and Cyber: Attitudes, Strategies, Organization*, accessed on 13.01.2018.
24 Mikk Raud, *China and Cyber: Attitudes, Strategies, Organization*, accessed on 06.01.2018.

for Russia. Due to its nature as an asset and space, and in line with the information system concept, the military is increasingly emphasising this issue in conventional operations. Many experts, who study cyber operations today, have also suggested that the development of a complex information operations capability could become part of Russia's strategic deterrent capabilities in the short-term.

Even though the Red Army can be considered rather backward in terms of IT developments, as digitisation has so far only been present in the traditionally *high-tech* space, missile, aircraft, naval and fire control systems, the armed force was also doctrinally and structurally deprived of the basic achievements of the information age. One of the main reasons for this was to protect military systems from the threats posed by global networks. However, the operations during the Russian-Georgian conflict that erupted in August 2008 clearly indicate that the Red Army's cyber offensive and counter-attack capabilities have already been created and they operate successfully. The Red Army's cyber capabilities made their world-class début in the Russo-Ukrainian crisis, when it became clear that they could dominate the cyber battlefield and deter external forces supporting the enemy with high-level equipment, excellent procedures and operational readiness.

All the findings of the international cyber-event investigations confirm that Russia was directly or indirectly involved in almost all significant cases and that it was acting in its own interests. Beyond information support for military operations, Russian information capabilities are being deployed on a daily basis, be it cybercrime; electronic banking systems, transactions; communications channels and media or IT attacks against certain state or administrative systems.

Military links between the DWP and the DWP 2.0

Digitalisation, computer science and the Internet as interpreted today started to develop as part of the military systems during the Second World War, gained momentum in the military blocks of the Cold War and by the 1950s the arms race escalated in the technical control systems used in nuclear and conventional high-tech weapons. Today, information technology is equally present in the military organisations of the developed world and in the armies of emerging countries. The United States, France, Britain and Germany conduct all of the command-and-control of their military systems and that of their communications, logistics, supply chain management and military-industrial development on digital platforms, similarly to the practice of China, India, Brazil and Russia.

In terms of the DWP and the DWP 2.0, this means that Hungarian defence, national security and military systems must meet the following four requirements: (1) they must be embedded in the current Hungarian digital system; (2) resulting from our memberships, the interconnection and interoperability of the Hungarian defence, military and military-industrial systems with the NATO and the EU must be ensured; (3) the military IT system developed in peacetime must also be able to ensure the management of Hungary and the operation of the public administration independently—with restrictions—in any legal order other than the peacetime one.

In line with the general tasks set out in the DWP in the short-term, the following set of objectives for defence, military and national security should be defined:

- the Hungarian defence, national security and military systems as a whole—including the equipment, personnel and procedures that operate it—should make progress in the field of digital preparedness;
- all defence, military and national security subsystems that are based on or linked to IT and technology should increase their competitive, defence and operational capabilities in a timely manner by recognising and acknowledging the importance of digitalisation;
- the development of defence, military and national security IT, digital and network-based systems should form an interdependent, interconnected and complementary unit that can also function as a redundant system if necessary, it should represent a leap forward in the international military and cyber warfare arena to become a winner of the digital transformation, and thus it shall ensure Hungary's defence and the realisation of its national interests;
- all in all, the military IT systems must be developed in such a way that they are protected against attacks from civilians or civilian platforms, can be disconnected from them at any time and can operate autonomously at any time, in order to enable the continuous running of the country in peacetime.

In line with the implementation of the governmental goals set out in Government Decision No 1456 of 2017 (VII.19.) on the monitoring report of 2016 of the National Info-communications Strategy, on the Digital Welfare Programme 2.0, that is the extension of the Digital Welfare Programme, on the adoption of its Working Plan for 2017–2018, and on further developments in digital infrastructure, competences, economy and public administration the following defence, military and national security areas should be linked to the initiative (following the structure of the Government Decision):[25]

- (Preamble) the Government should involve the defence and national security organisations (Ministry of Defence, Hungarian Defence Forces, National Military Security Service) in the forums for broad social dialogue, the cooperation and collaboration of professional, social, advocacy and scientific organisations during the implementation of the Digital Welfare Programme 2.0;
- the development of the defence, military, military-industrial and national security divisions and connections (defence management, military management, military national security and military-industrial aspects) of the Monitoring Report 2016 of the National Info-communications Strategy (NIS Monitoring Report) presented by the Minister of National Development;

25 Government Decision No 1456 of 2017 (VII.19.) on the monitoring report of 2016 of the National Info-communications Strategy (NIS), on the Digital Welfare Programme 2.0, that is the extension of the Digital Welfare Programme, on the adoption of its Working Plan for 2017–2018, and on further developments in digital infrastructure, competences, economy and public administration; Netjogtár, https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT, accessed on 01.02.2018.

- the development of the defence, military, military-industrial and national security divisions and connections (defence administration, military administration, military national security and military-industrial aspects) of the strategic document Digital Welfare Programme 2.0 presented to the Prime Minister's Commissioner responsible for the coordination and implementation of governmental tasks related to the Digital Welfare Programme;
- the development of the Superfast Internet Programme, the development of the National Telecommunications Backbone Network, the further development of the National Information Infrastructure Development Programme, the self-sustained digital network development investments of the Hungarian telecommunications operators, and the development of the defence, military, military-industrial and national security divisions and connections of the programme (defence administration, military administration, military operations, command-and-control, military national security and military-industrial aspects) aimed at increasing the reaching of superfast Internet access at an appropriate pace;
- new technological solutions for mobile telecommunications, the 5G network and application developments, the deployment of self-driving vehicles, and the development of their defence, military, defence industrial and national security divisions and connections (operational, command-and-control, military-technical and defence industrial aspects);
- the development of the Hungarian 5G Coalition and the 5G Strategy and Action Plan of Hungary, with the participation of professional, scientific and advocacy organisations, and the development of their defence, military, defence industrial and national security divisions and connections (operational, command-and-control, military technology and defence industrial aspects);
- the development of digital readiness and competences, and their defence, military, military-industrial and national security divisions and connections for specialised digitally-skilled employees (defence administration, military administration, military supplementation, military operations, command-and-control and military-industrial aspects);
- the development of the implementation of the Digital Workforce Programme with its defence, military, military-industrial and national security divisions and connections (defence administration, military administration, military supplementation, military-industrial company connections under the control of the Ministry of Defence);
- the development of a comprehensive programme for micro, small and medium-sized enterprises of high national economic importance, aimed at improving their digital readiness, the development of their defence, military, military-industrial and national security divisions and connections (defence administration, military administration, military supplementation, military operations and military-industrial company connection under the control of the Ministry of Defence);

- the development of a unified methodological manual as well as measurement and rating system that supports the digitalisation of the national economic sectors. Furthermore, the development of the defence, military, military-industrial and national security divisions and connections of the Digital Service Trade Development Strategy (defence administration, military administration, military supplementation and military-industrial companies under the control of the Ministry of Defence);
- the development of the Hungarian Digital Agricultural Strategy and the elaboration of the defence, military, military-industrial and national security divisions and connections of the measures that support the implementation of the strategy (complex digital content and foil systems for military and operational maps);
- the role of digital tools and technologies in health preservation, disease prevention in healthcare, and the development of the Hungarian Digital Healthcare Development Strategy created for the digital innovation in healthcare, as well as development of the defence, military, military-industrial and national security divisions and connections of the Info-communications Model Programme for the Elderly (military health, Hospital of the Defence Forces, NATO Health Centre of Excellence);
- the development of the defence, military, military-industrial and national security divisions and connections of the Hungarian Digital Sports Strategy established for the accelerated application of digital technologies (operational, training, educational, military sports (Defence Sports Association), competitive sports aspects);
- effective support for digital public administration services, comprehensive monitoring and coordination of tasks related to the digitalisation of public administration to help citizens and businesses, and the development of a common reference framework, training materials and educational framework for public administration employees with their defence, military, military-industrial and national security divisions and connections (defence administration, military administration, military supplementation, military operations, command-and-control and military-industrial aspects);
- development of the defence, military, military-industrial and national security divisions and connections of measures that support the innovation activities and product development of Hungarian micro, small and medium-sized IT enterprises and think tanks (defence and technological research, military-industrial aspects);
- the development of the defence, military, military-industrial and national security division and connections for a unified digital development of public cultural treasures in public collections, the making accessible of the digitalised cultural assets for public education and training, and raising the interest of citizens towards digital cultural content objectives (military history, historical archives (Military History Museum and Institute), military heritage preservation);
- the elaboration of defence, military, military-industrial and national security divisions and connections regarding the cyber security of citizens, businesses and public institutions as well as Hungarian digital networks (Ministry of Defence, Hungarian Defence Forces, military-industrial companies operating under the supervision of the Ministry of Defence, Military National Security Service);

- the review of the National Cyber Security Strategy and the development of the resulting detailed action plan, including the identification of tasks and responsibilities, with the development of their defence, military, military-industrial and national security divisions and connections (Ministry of Defence, Hungarian Defence Forces, military-industrial companies operating under the supervision of the Ministry of Defence, Military National Security Service);
- validation of defence, military, military-industrial and national security divisions and connections in the development of the information security aspects of the Digital Welfare Programme 2.0 (Ministry of Defence, Hungarian Defence Forces, military companies operating under the supervision of the Ministry of Defence, Military National Security Service);
- the direct use of network research and its results for the operation and development of the digital ecosystem in public administration, education and training, and the development of their defence, military, military-industrial and national security divisions and connections (Ministry of Defence, Hungarian Defence Forces, military-industrial companies operating under the supervision of the Ministry of Defence, Military National Security Service);
- the elaboration of digital development programmes for local, municipal and regional communities, as well as the Smart City working group together with the Smart City and Smart Region public administration model project that was launched in the wake of the Smart City developments and the development of their defence, military, military-industrial and national security divisions and connections (Ministry of Defence, Hungarian Defence Forces, defence administration, military-industrial companies operating under the supervision of the Ministry of Defence, Military National Security Service);
- the assessment of the social, physiological and environmental impacts of digitalisation, the development of research to mitigate the negative impacts, and the management of the adverse social impacts of digitalisation and the sanctioning of these impacts in the legal system along with the development of their defence, military, defence industry and national security sectors divisions and connections (Ministry of Defence, Hungarian Defence Forces, defence administration, defence industry companies operating under the supervision of the Ministry of Defence, Military National Security Service).

Digital, IT and network-based military target systems

In accordance with the Fundamental Law and Act CXIII of 2011 on defence and the Hungarian Defence Forces (HDF) and on measures that may be introduced in special legal order (Act on the Defence of the Hungarian Defence Forces, Htv. in short), the Hungarian Defence Forces—for the purposes to perform their defence tasks—must have the forces, means and capabilities prepared in peacetime to avert an external armed attack. Consequently, the Hungarian Defence Forces must already in peacetime build up and operate its own communications, IT and information protection systems required for command-and-control. Pursuant to

Government Decree No 290 of 2011 (XII.22.) on the implementation of certain provisions of the Act on the Defence Forces (Implementing regulation of the Act on the Hungarian Defence Forces), the Hungarian Defence Forces operate a Governmental Purpose Isolated Communications Network (HDF GPICN) for their management and leadership functions, the development and operation of which is the responsibility of the Minister of Defence. Annex 2 of Government Decree No 346 of 2010 (XII.28.) specifies the Governmental Purpose Isolated Communications Network of the Hungarian Defence Forces as an isolated communications network that is operated by the Minister of Defence.

This HDF GPICN is obliged to ensure the following main tasks:

- pursuant to the implementing regulation of the Act on Defence Forces, the HDF GPICN of the Hungarian Defence Forces operate a permanent and field-based communications, IT and information protection system for the command-and-control tasks of the Defence Forces;
- pursuant to paragraph (1) of Article 15 of the implementing regulation of the Act on Defence Forces, the special operating conditions of the Defence Forces Operational Command System shall be provided if the conditions for decision-making, the operation of the command-and-control system cannot be ensured in peacetime or the threat to the peacetime command-and-control of the facility is so wide-scale that the conditions for command-and-control cannot be ensured (in such a case, the strategic and operational command elements of the Defence Forces shall operate at a location other than the peacetime facility, where the security conditions for command-and-control shall equally be ensured);
- pursuant to paragraph (2) of Article 15 of the implementing regulation of the Act on Defence Forces, the info-communication support of the special operation of the Operational Command System of the Defence Forces is provided by the systems of the Governmental Purpose Isolated Communications Network of the Hungarian Defence Forces, as well as by leased systems;
- subject to the legislative provisions, the basic purpose of the HDF GPICN is to provide high availability info-communication support to the command-and-control of the Hungarian Defence Forces, including the Operational Command System of the Hungarian Defence Forces even in peacetime and during special legal order.

The strategic management of the HDF GPICN is implemented at three levels, as follows:

- Minister of Defence: pursuant to Article 2 (2) 17 of the implementing regulation of the Act on the Defence Forces, the Minister of Defence is responsible for the development and operation of the HDF GPICN, he determines the cooperation tasks required to ensure the operability of the intelligence, IT and information protection services important for the performance of the tasks of the Hungarian Defence Forces;

- Chief of the Defence Staff:
  - pursuant to Article 11 (1) 2 and 3 of the implementing regulation of the Act on the Defence Forces, the Chief of Staff of the Hungarian Defence Forces is responsible for the preparation, implementation and control of the national armed defence plan, the tasks related to the introduction of the special legal order of the Defence Forces, the order for maintaining and enhancing the level of preparedness, and the protection of Hungarian territory by air defence with standby forces;
  - according to Article 11 (1) 6 of the implementing regulation of the Act on the Defence Force, he manages the development of the communications, IT and information protection strategy and service system, the planning, development, continuous provision, operation and maintenance of the services of the HDF GPICN and the HDF Information Management System;
  - pursuant to Article 11 (1) 7 of the implementing regulation of the Act on the Defence Forces, he is responsible for the operation of the Operational Command System of the Defence Forces, for the implementation of tasks related to ensuring its operational conditions, and for the operation of the necessary infrastructure and info-communications system;
  - pursuant to Article 11 (1) 8 of the implementing regulation of the Act on Defence Forces, he contributes to the protection of the transport network, communications, information technology and information protection services, airborne, radiation monitoring, signalling and alarm systems important for the fulfilment of tasks by the Hungarian Defence Forces, as well as protection of systems and installations that are vital in the energy networks.
- News, Information Technology and Information Protection Group Leader of the National Defence Staff: in accordance with the by-laws of the Hungarian Defence Forces, he performs the network management tasks of the HDF GPICN under the authority delegated to him by the Minister of Defence.

Military aspects related to the Digital Welfare Programme

Development related to the DWP are of national and relatively wide scope, therefore it is justified from a national security and economic point of view to open and make the digital infrastructures under development available to defence and military systems. If there is a positive decision at a leadership level about this, a defence, military and national security segment or bloc of the DWP must be created. This would enable the requirements regarding the telecommunication networks and info-communication systems of the Hungarian Defence Forces to be taken into consideration during the planning and implementation of the developments. Military requirements for digital infrastructure, including public and government wired and wireless networks, are proposed to be defined as follows:

- ensure high availability and, to this end, be robust, complex and redundant;
- ensure the confidentiality, integrity and timely transmission of data;
- ensure that failures, network incidents and security incidents are detected immediately

and can be responded to quickly in order to take immediate action, contain and prevent failures, minimise damage and take the necessary countermeasures in the event of a security incident;

- ensure the use of networks, systems, services and applications by the Hungarian Defence Forces;
- ensure that the Hungarian Defence Forces are connected to the networks at all access points or, by special arrangement, that access points are installed at locations determined by the HDF;
- the fixed, mainly optical, transmission paths are terminated in all HDF-managed installations in use (command-and-control facilities, barracks, firing ranges and training areas, etc.);
- fibre optic cable transmission lines to be established at all district headquarters;
- ensure a nationwide coverage of wireless networks (public mobile, EDR) and provide the highest possible data transfer besides voice communications;
- provide support for the project to launch and operate a Hungarian (possibly V4) telecommunications satellite with at least European coverage, which could also be used for military purposes;
- a central database of the digital infrastructure—reflecting real-time changes and failures –should be created and online access to it should be provided to the HDF, especially during periods when a special legal order is applied;
- in justified cases and during periods of special legal order, the potential prioritisation of the services to be used by the HDF should be to ensure, with the definition of the priority group of users and, where appropriate, to exclude public users from the data traffic;
- the designated organisations of the HDF should have online access to data stored in government and public IT systems—relevant for operations, logistics and military supplementation—on the basis of predefined rights and purposes of use, e.g. location of electricity and gas distribution centres, water wells, chemical plants, logistics centres, load capacity and width of bridges, number of patients and injured persons admitted to hospitals, addresses of employees of hospitals, medical practices, mayor's offices, data from the population register relevant for military supplementation, road closures, traffic jams, current events, etc.;
- the designated organisations of the HDF must be able to use the IT services of disaster management, rescue, border and law enforcement organisations, to obtain up-to-date information from them and to send data to them.

The above requirements are justified by Hungary's international obligations and tasks related to the defence of the country, for the implementation of which it is essential to establish and operate the digital infrastructure required for the continuous and reliable functioning of the Operational Command System, military command-and-control, airborne and other weapon control systems in accordance with the above requirements.

Hungarian defence and military developments—*Zrínyi 2026*

From January 2017, the Hungarian Defence Forces launched *Zrínyi 2026*, the largest defence and armed forces development programme of the last 26 years. Government Decision No 1298 of 2017 (VI.2.) on the Implementation of the Zrínyi 2026 National Defence and Armed Forces Development Programme states that the Government has discussed the Zrínyi 2026 Defence and Armed Forces Development Programme and approved its main directions, and agrees that the Programme should be implemented in the priority order determined by the National Security Cabinet at its meeting of 1 February 2017, having regard to the security situation in Hungary and the development needs of the Hungarian Defence Forces. In order to implement the tasks included in the Programme, it called on the Minister of Defence to prepare and submit to the Government further proposals on the implementation of its elements.[26] In accordance with the Government's decision pursuant to Government Decision No 1273 of 2016 (VI.7.) on the provision of budgetary resources for defence expenditure and the establishment of the conditions for long-term planning, the government decided to increase the main financial provision by 0.1 percentage point of the GDP, and to provide other surplus amounts (including HUF 5 000 million for the renewal of military equipment), thus, the amount of the main financial support was increased by HUF 72 048.7 million compared to the original amount designated back in 2017.[27]

The details of the complex armed forces development plan are contained in highly classified documents, although press reports suggest that it focuses on the replacement of highly obsolete Soviet-made equipment and the procurement of modern, NATO-compatible and interoperable military equipment, as well as IT, digital and network-based developments for the next ten years. This requires careful planning and well-scheduled, precise implementation, since it is not about a one-time additional expense and its utilisation, but of a comprehensive military technology and military-industrial development process that is based on a step-by-step approach. In line with our national objectives and commitments made to our allies, the main pillars of *Zrínyi 2026* programme as currently outlined, are the following: procurement of transport aircraft, helicopters, air defence systems; weapons, ammunition, all-terrain transport vehicles; and command, control, communications, IT and cyber defence systems.[28] Another important requirement of the legal, professional regulators and the strategic management system, as detailed in the previous chapter on *the military relevance of the DWP*, is to serve and ensure the development of *high-tech* weapon systems and the military defence industry.

The development of military-technical, military engineering, command, control, intelligence, communications, and reconnaissance systems is unthinkable without the use of the modern IT platforms available today. Therefore, the armed forces development objectives

26 Government Decision No 1298 of 2017 (VI.2.) on the implementation of the Zrínyi 2026 Defence and Armed Forces Development Programme, *Hungarian Gazette*, Budapest, http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK17081.pdf, accessed on 29.12.2017.

27 http://www.parlament.hu/irom40/15381/adatok/fejezetek/13.pdf, (02.02.2018).

28 Ádám Draveczki-Ury, 'Zrínyi 2026, The era of comprehensive development is upon us', *Magyar Honvéd Journal*, (January 2017), Zrínyi Publishing House, Budapest, http://www.honvedelem.hu/cikk/61339, accessed on 22.12.2017.

of Zrínyi 2026 should include the need for the HDF to make a shift and start using the world's most developed IT, digital and network-based solutions, and thus, the technologically leading military systems in the short-term. Since the defence policy objectives are significant, just like the resources allocated for the upcoming modernisation, it is important that these developments are implemented with the correct definition of the focal points and the calculation of the return of investment, so that the whole of the defence activity can be shifted onto a new digital platform. This can only be achieved by linking defence, military and national security systems to the high-tech systems available on the market and to the infrastructures used by civil administrations, so that they can be disconnected and operated independently at any time, with limited takeover of the functions of attacked, damaged or corrupted government networks to support the specific ICT operations of the government.

Potential military development directions that can be aligned with the DWP and DWP 2.0

In light of the above, the specific defence, military and military-technical development directions to be set for the DWP and DWP 2.0 are as follows:

- Digital Hungarian domination in the international division of labour regarding the defence industry;
- prioritisation of military, operational, command-and-control, communications, defence and military technology developments based on 5G technology;
- development of precision weapons (small arms, self-guided weapons systems, bombs, missile systems);
- development of smart military equipment, individual and sub-unit equipment system (smart clothing, sensor system, individual and relative positioning, real-time biophysiological condition measurement, video camera system, digital audio communication, temperature, humidity, chemical and radiation measurement, etc.);
- self-driving military vehicles (trucks, armoured vehicles, armoured transport vehicles, combat vehicles, aircraft [transport, reconnaissance, jamming], helicopters);
- creation of a digital military map and film system and a navigation system;
- the large-scale digital and network-based development of the Hungarian space programme, the development and launch of Hungarian satellites;
- development of a complex digital and network-based command, control, military communications system;
- comprehensive digital literacy training (courses) for soldiers and civilian employees serving in the Hungarian defence system;
- addition of digital and network-based capabilities to the military training and education system;
- addition of digital capabilities to the defence management and military management systems;
- addition of a real-time digital and network-based platform to military supplementation and personnel record systems;

- shifting the military logistics and combat supply (arms, ammunition, munitions, equipment, clothing, fuel, etc.) inventory system to a real-time digital and network-based platform;
- migration of the entire enterprise resource planning and development systems of companies and military enterprises under the control of the Ministry of Defence to a digital and network-based platform.

Conclusions

In addition to affecting political, public administration, economic, industrial, agricultural, educational, scientific, health, transport, energy and other civilian systems, digitisation and information technology are also having a major impact on defence, national security and military structures. From the perspective of the DWP and DWP 2.0, this means that Hungarian defence, military and national security systems must meet the following four main requirements: (1) be embedded in the entire Hungarian digital and network-based system; (2) ensure the interconnection and interoperability of the Hungarian defence, military and military-industrial systems with NATO and the EU, resulting from Hungary's membership in the two organisations; (3) the military IT, digital and network-based systems developed in peacetime should be able to operate independently in any legal order other than the peacetime one, and ensure the management of the country as well as the smooth functioning of the public administration with restrictions. With regarding to the design and implementation of the DWP and DWP 2.0, this implies that security, defence, military and national security considerations must be part of the DWP, i.e. a defence, military and national security branch or block must be developed within the DWP. The defence, military and national security sectors would analyse and assess the security challenges, support and protect the Programme with their expertise, capabilities and tools, and would also carry out their own IT, digital and network-based capability development within this complex system to open the possibility of interconnection to other segments of the DWP, and thus creating interoperability and making the Hungarian digital and IT systems and networks compatible with one another.

Bibliography

1. Government Decision No 2012 of 2015 (XII.29.) on the Digital Welfare Programme to be implemented by the Government based on the results of the national consultation on the Internet and digital developments (InternetKon), Netjogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A15H2012.KOR&timeshift=fffffff4&txtreferer=00000001.TXT, accessed on 04.09.2017.
2. Government Decision No 1456 of 2017 (VII.19.) on the monitoring report of 2016 of the National Info-communications Strategy, on the Digital Welfare Programme 2.0, that is the extension of the Digital Welfare Programme, on the adoption of its Working Plan for 2017–2018, and on further developments in digital infrastructure, competences, economy and public administration; Netjogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT, accessed on 04.09.2017.
3. Government Decision No 1298 of 2017 (VI.2.) on the implementation of the Zrínyi 2026 Defence and Armed Forces Development Programme, Hungarian Gazette, (Budapest), online: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK17081.pdf, accessed 28 December 2017, http://www.parlament.hu/irom40/15381/adatok/fejezetek/13.pdf, accessed on 22.12.2018.
4. Babos, Tibor, 'Globális közös terek a NATO-ban' (Global Commons in NATO), *Nation and Security*, Centre for Strategic and Defence Studies, (Budapest, April 2011), Online: http://www.nemzetesbiztonsag.hu/cikkek/babos_tibor-___globalis_kozos_terek____a_nato_ban.pdf.
5. Babos, Tibor, *The Five Central Pillars of European Security*, NATO Public Diplomacy Division, Brussels, Strategic and Defence Research Centre, Budapest, NATO School, Oberammergau, (2008).
6. Ball, Desmond, *China's Cyber Warfare Capabilitie*s, online: https://indianstrategicknowledgeonline.com/web/china%20cyber.pdf, accessed on 27.08.2017.
7. Draveczki-Ury, Ádám: 'Zrínyi 2026, Az átfogó fejlesztések időszaka következik' (Zrínyi 2026, The era of comprehensive development is upon us), *Magyar Honvéd Journal*, (January 2017, Zrínyi Publishing House, Budapest), online http://www.honvedelem.hu/cikk/61339.
8. Internet Live Stats: online: http://www.internetlivestats.com/internet-users/china/, accessed on 27.01.2018.
9. History, Structure: NATO Cooperative Cyber Defence Centre of Excellence, Online: http://www.ccdcoe.org./history.html, accessed on 19.01.2018.
10. Raud, Mikk: *China and Cyber: Attitudes, Strategies, Organization*, NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf, accessed on 30.01.2018.
11. Szentgáli, Gergely: 'A NATO kibervédelmi politikájának fejlődése' (The Evolution of NATO's Cyber Defence Policy), in: *Nemzet és Biztonság*, (Budapest), online: http://uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf, accessed on 28.01.2018.

Alexandra Lilla Beregi

The digitalisation of the Hungarian Defence Forces in the light of the Zrínyi 2026 Defence and Armed Forces Development Programme

Resume

The aim of the study is to present the capability developments, procurements and recommendations that contribute to the digitalisation of defence in accordance with the Zrínyi 2026 Defence and Armed Forces Development Programme. It can be concluded that if the objectives of the Zrínyi 2026 Programme are achieved and the digital platforms are treated with the same weight and intensity, national defence as a whole could be shifted onto a digital platform, which would mean that the *high-tech* systems on the market and the defence, military and national security system infrastructures used by the public administration could operate independently and separately in order to support the Government's info-communications activities.

Executive summary

The aim of the study is to present the capability developments, procurements and recommendations that contribute to the digitalisation of defence in accordance with the Zrínyi 2026 Programme. The thesis discusses that the integration of defence, military and national security systems into the Hungarian digital network is required to ensure that military IT, digital and network-based systems which function properly in peacetime would be able to operate independently and perform the public administration functions and the governance of the country when a special legal order (other than peacetime) is applied.

"Nothing is more outdated than what was modern yesterday"
István Csukás

Introduction

The most pressing current security challenges are (1) globalisation; (2) digitalisation; (3) global warming; (4) and the depletion of raw material resources.[1] Security trends in Europe shape Hungary's security challenges, ambitions and objectives. Of the above challenges, this paper presents digitalisation as a security challenge, because digitalisation is increasingly present in today's modern world and thus has an impact on the security of Europe and Hungary.

With the development of digitalisation, we should expect an increase in the number of attacks in cyberspace and an increase in the quality and success rate of the attacks. Resulting from the rapid development of technologies, new challenges are emerging that determine the security of our country.

Digitalisation makes everything more accessible to the members of society. Cyber attacks in cyberspace often result in irreversible political or economic damage. Hungary must have the capability to identify and manage cyber threats, build cybersecurity, ensure the smooth functioning of critical information infrastructure, prevent attacks and perform cyber defence tasks in an appropriate way. But digital revolution is not confined to the virtual space, it also affects the following four operational areas: (1) land; (2) sea; (3) air; (4) space.

According to the author, in order for Hungary to be familiar with the new security challenges that have emerged as a result of digitalisation in all operational areas and to have the capability to overcome them, the Hungarian Defence Forces need to apply a new approach and shift onto a digital platform.

In the era of the digital explosion, the modernisation of the army is essential to successfully face new security challenges, which is supported by the Zrínyi 2026 Defence and Armed Forces Development Programme (hereinafter referred to as Zrínyi 2026 Programme) that the Ministry of Defence (MoD) launched together with the HDF in 2017.[2]

The Zrínyi 2026 Programme objectives include the upgrading of the HDF IT, digital and network-based military systems. With the implementation of the developments the Hungarian national defence as a whole could be shifted onto a digital platform, which would mean that the high-tech systems on the market and the defence, military and national security system infrastructures used by the public administration could operate independently and separately in order to support the Government's info-communications activities.[3]

The thesis discusses that the integration of defence, military and national security systems into the Hungarian digital network is required to ensure that military IT, digital and network-based systems which function properly in peacetime would be able to operate independently and perform the public administration functions and the governance of the country when a special legal order (other than peacetime) is applied.[4]

---

1 Tibor Babos, 'A biztonság globális és európai összefüggései' (The global and European context of security), in: *Hadtudomány Journal*, (Budapest, 2019/4), http://real.mtak.hu/105840/1/016-029_Babos.pdf, accessed on 12.02.2020.

2 Government Decision No 1298 of 2017 (VI.2.) on the implementation of the Zrínyi 2026 Defence and Armed Forces Development Programme.

3 Tibor Babos, 'A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái' (The security, defence, and military policy relevance of the Digital Welfare Programme), in: *Hadtudomány Journal*, (Budapest, 2018), http://real.mtak.hu/82604/1/2018ebabos2.pdf, accessed on 26.01.2020.

4 Tibor Babos, 'A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái'.

It is essential to align the development and modernisation efforts of the Zrínyi 2026 Programme with the full-scale digitisation of the HDF. In order to prove this claim, the first chapter of the thesis presents the military development and digital platforms along which the Zrínyi 2026 Programme sets the long-term goals and instruments for the digitalisation and modernisation of the HDF. In the second chapter, without being fully comprehensive, it lists recommendations for the full digitalisation of the Hungarian Defence Forces by presenting international examples.

The Zrínyi 2026 Programme in the spirit of digitalisation

Presentation and objectives of the Zrínyi 2026 Programme

Upgrading obsolete skills and techniques is essential for the digitalisation of the Hungarian Defence Forces. The HDF's land and air assets and capabilities are in need of modernisation. To achieve the above goal, the Zrínyi 2026 Programme identifies the modernisation, defence and military force development capabilities and activities that will contribute to the full digitalisation of the Hungarian Defence Forces.
The first chapter of this thesis seeks to answer the following questions:

- What are the platforms for which the Zrínyi 2026 Programme will define its modernisation, defence and military force development activities? What are the objectives?
- What procurements and capability upgrades have been made to modernise the air and land forces? What are the future goals?

The Zrínyi 2026 Military Force Development and Modernisation Programme was launched in January 2017,[5] for the purposes of providing the Hungarian Defence Forces with the technical equipment, capabilities and personnel that meet today's challenges and requirements. An army needs continuous training, new capabilities and advanced technical equipment to effectively perform its defence-related tasks, to defend the homeland—in addition to our cooperation with the allied forces—by maintaining and developing Hungary's self-reliance in such a way that the education of citizens to patriotism and participation in the defence of the homeland would also be achieved.

The Zrínyi 2026 Programme is the largest and most comprehensive military development programme of the last 25 years. The programme includes (1) an increased budget for the overall development and modernisation of the HDF; (2) a secure career path to create predictability and security; (3) a defence programme to ensure a secure supply through the establishment of the Voluntary Territorial Defence Reserve, the Voluntary Defence Training and the Defence Sports Association; (4) the development of the Voluntary Reserve System to fill the gap in conscription and general military service; (5) financial and in-kind support for families of military personnel; (6) the establishment of national defence camps to familiarise the military with the tasks of the armed forces; (7) the defence scholarship programme for secondary and higher education students; (8) promotion of the Youth for the Defence, Defence Education

5 Government Decision No 1298 of 2017 (VI.2.) on the implementation of the Zrínyi 2026 Defence and Armed Forces Development Programme.

Programme within the framework of the Defence Cadet Programme; (9) modern training for the preservation and development of the capabilities of the HDF through the further training of the personnel to be able to use modern military equipment; (10) honouring the heroes of World War I and II within the framework of the Military Heroes' Commemoration Programme and the Sacrifices by Hungarian Soldiers in the Great War Programme; (11) development of the military through digitalisation.[6]

The Zrínyi 2026 Programme is based on several pillars, the most important of which are military development; modernisation of the army; modernisation, development and digitalisation of capabilities. The development and modernisation programme covers both land and air forces. However, the programme will also modernise the logistics, military health and management systems as a whole.[7]

The development of the military force aims to renew the combat equipment of the individual soldiers; modernise the helicopter fleet, artillery and anti-tank artillery capabilities; modernise the fixed and rotary wing airlift capabilities of the armed forces and modernise the radars; the modernisation of the air defence missile units; the modernisation of the Defence Information Technology and Command-and-Control System; the further development of special operations capabilities and the development of cyber defence within hybrid warfare to effectively address the new security threats of our time. The complex military development serves the purposes of implementing mission tasks and military operations, as well as the professional management of disasters and, possibly, the provision of civil assistance.[8]

The HDF seeks to spend at least 20% of its defence budget on development and modernisation by 2024, in line with the NATO Recommendations. In the context of Zrínyi 2026 Programme, the upgrading of the personal equipment and clothing of the soldiers is already underway. The Defence Forces have also purchased RÁBA H series off-road trucks of various designs, passenger cars and special vehicles. The Mi-17 transport and Mi-24 combat helicopters have undergone major overhauls, the replacement of the Jak-52 training aircraft with new Zlin training and reconnaissance aircraft has been completed, and the procurement of sixteen Airbus H145M helicopters has been completed. The Airbus H145M helicopters will also be suitable for air rescue missions by 2021. In the framework of the development of the defence industry, 100 modular modern buses have also been manufactured.[9] Furthermore, the development of shoulder-launched anti-tank capability and the procurement of artillery optical devices and Leopard 2A4 tanks have also been completed. The latter ones are not new tanks, but upgraded and refurbished equipment to prepare the military for the use of the new Leopard 2A7 Western state-of-the-art technology that will be procured between 2023 and 2025. Self-propelled guns, the air defence missile system, anti-aircraft missiles are under procurement and there are also plans to upgrade the Gripen software.[10]

6 'Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében' (Zrínyi 2026 Defence and Armed Forces Development Programme, In Defence of the Homeland), in: *Honvedelem.hu*, (Budapest), https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf, accessed on 24.01.2020.

7 'A haza védelme, a nemzet szolgálata' (Defending the homeland, serving the nation), in: *Honvedelem.hu*, (Budapest, 2019), https://honvedelem.hu/files/files/116159/honvedseg_kiadvany_165x235mm_v2_6_.pdf, accessed on 14.02.2020.

8 'A haza védelme, a nemzet szolgálata'.

9 Ádám Draveczki-Ury, 'Zrínyi 2026', *Honvedelem.hu*, (Budapest, 16 January 2017), https://honvedelem.hu/cikk/zrinyi-2026/, accessed on 27.01.2020.

10 'A járványról és a haderőfejlesztésről is beszélt a honvédelmi miniszter' (The Minister of Defence spoke about the epidemic and the development of the armed forces as well), in: Honvedelem.hu; (Budapest, 05.12.2020), https://honvedelem.hu/hirek/a-jarvanyrol-es-a-haderofejlesztesrol-is-beszelt-a-honvedelmi-miniszter.html, accessed on 27.02.2021.

For the Kecskemét airbase of the Hungarian Defence Forces, the Zrínyi 2026 Programme includes the renovation and the development of the runway, lighting equipment, operational areas and general infrastructure. The creation of tank and self-propelled artillery and helicopter capabilities requires the infrastructural development to be launched in Tata and Szolnok, as well as the modernisation of the barracks and buildings concerned, such as the buildings in Hódmezővásárhely.[11]

The conditions for applying the MEDEVAC capability for the two Airbus A319 troop-carrier aircraft and the self-defence capabilities for the A319s and the two Dassault Falcon 7X courier aircrafts have already been developed. With such capabilities, logistical operations such as the transport of personnel and supplies can be carried out, and special operations forces armed with Bren 2 assault rifles have been trained to successfully master these operations.[12]

Modernising the Air Force's capabilities

The renewal of our air force capabilities, maintaining air transport as a military capability is of strategic importance for the Hungarian Defence Forces. The preparation and training of soldiers for operational and mission tasks, the supply and replenishment of equipment and tools for foreign service, and participation in humanitarian and disaster relief activities can be achieved by renewing and modernising our aircraft and by procuring helicopters equipped with new types of digital instruments. Air transport capability can be deployed even in the event of a major accident, natural disaster, terrorist attack, armed conflict or mass casualty.

The Airbus H145M light helicopters procured first as part of the Zrínyi 2026 Programme—which serve as a step towards modernising the Air Force's capabilities—arrived in Szolnok in November 2019. The HDF also provides a logistics programme for the helicopters, through which the training of pilots has already been completed and the supply of the new aircraft is ensured. The helicopters are armed with a 20mm machine gun and unguided missiles, but can also be equipped with laser-guided anti-tank missiles.[13] In June 2020 there were three additional Airbus H145M helicopters delivered to the 86th Helicopter Base of the Hungarian Defence Forces in Szolnok. Two of the newly procured helicopters are already equipped with search and rescue equipment.[14] By December 2020, a total of 16 H145M Airbus helicopters had arrived in Szolnok.[15]

The Hungarian Defence Forces have planned to procure a total of twenty Airbus H145M helicopters by 2021. Hungarian soldiers can be trained to use the helicopters, which are equipped with modern, state-of-the-art equipment, digitalised instruments and digital,

11 'Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében'.

12 'Irán támadást intézett két amerikai bázis ellen Irakban' (Iran attacks two US bases in Iraq), *Hirtv.hu*, Budapest, (08.01.2020), https://hirtv.hu/hirtvkulfold/iran-ballisztikus-raketakkal-tamadott-meg-amerikai-celpontokat-irakban-2492968, accessed on 31.01.2020.

13 'Már a szolnoki bázison vannak a honvédség első új helikopterei' (The first new helicopters of the Hungarian Defence Forces are already at the base in Szolnok), *Honvedelem.hu*, (Budapest, 19.11.2019), https://honvedelem.hu/cikk/mar-a-szolnoki-bazison-vannak-a-honvedseg-elso-uj-helikopterei/, accessed on 25.01.2020.

14 'Tovább gyarapodó légi képesség' (Further developing air capability), *Honvedelem.hu*, (Budapest, 22.06.2020), https://honvedelem.hu/media/aktualis-videok/tovabb-gyarapodo-legi-kepesseg.html, accessed on 27.02.2021.

15 'Újabb helikopterek érkeztek' (Additional new helicopters have arrived), *Honvedelem.hu*, (Budapest, 10.12.2020), https://honvedelem.hu/hirek/ujabb-helikopterek-erkeztek.html, accessed on 27.02.2021.

network-based weapons, at the helicopter base in Szolnok. Equipped with high-performance cameras and an electronic protection system, the multi-purpose and light helicopters have all the features of a training helicopter, search & rescue helicopter as well as a helicopter that supports weapons fire.[16] Besides the H145M, additional sixteen Airbus H225M medium military helicopters are in the process of being procured. The French-made aircraft will arrive in Hungary in 2023-2024 as part of Zrínyi 2026 Programme.[17]

In order to improve the capabilities of the air force, the Zrínyi 2026 Programme will purchase trainer jet aircraft, which will improve the Hungarian pilot training. In addition, the modernisation of the Gripen weapon system, the development of MISTRAL M2 short-range missiles and the procurement of additional short- to medium-range missile complexes are also planned. The programme will also include the procurement of gap-filler and mobile three-dimensional radar stations to complement the airspace control function of fixed radars that monitor the country's airspace, as well as the modernisation of military airfields.[18]

With the acquisition of new Airbus H145M and H225M helicopters and trainer jet aircraft, as well as the modernisation of Gripen aircraft and the development of MISTRAL M2 missiles, the modernisation of the Hungarian air force capabilities has taken on a new dimension, opening the way to the digitalisation of air force capabilities. The results and goals presented in this chapter all lead one step closer to shifting the HDF onto a fully digital platform.

The modernisation of the land forces

The Hungarian Defence Forces must have the deterrent power and military capabilities to effectively deal with threats to security. This requires not only the improvement of the air force but also that of the land forces, which is why the development and digitalisation of the HDF's land capabilities will also be carried out within the framework of the Zrínyi 2026 Programme.

The modernisation of the soldiers' personal combat equipment—with a preference for new, modern equipment that is manufactured in Hungary—has already begun. In peacetime, individual combat equipment contains the tools required for daily work and training tasks, and in wartime it increases the survival chances of soldiers while also ensuring the performance of their tasks. Within the Defence Force Development Programme, the Digital Soldier Programme has been launched, which seeks to provide soldiers with fully digitalised equipment.[19]

Structural changes are also being made to modernise the ground forces. This will include a three-brigade development that means the creation of a heavy, medium and light infantry brigades. The elements of the three-brigade development will also be in accordance with international requirements, allowing for national defence tasks to be carried out concurrently

16 Béla Révész, 'Csúcstechnika a levegőben' (High-tech in the air), *Honvedelem.hu*, (Budapest, 18.11.2019), https://honvedelem.hu/galeriak/csucstechnika-a-levegoben/, accessed on 25.01.2020.

17 Gábor Baranyai, 'Megérkeztek a honvédség új helikopterei a német gyárból' (The new HDF helicopters have arrived from the German factory), *Magyarnemzet.hu*, (19.11.2019) https://magyarnemzet.hu/belfold/megerkeztek-a-honvedseg-uj-helikopterei-a-nemet-gyarbol-7505657/, accessed on 25.01.2020.

18 'Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében.'

19 'Katonás infotér' (Military Information Space), *Honvedelem.hu*, (Budapest, 16.10.2019) https://honvedelem.hu/hirek/hazai-hirek/katonas-infoter.html, accessed on 27.01.2020.

with NATO requirements. The procurement of modern equipment and armament for the brigades will also be ensured as part of the Zrínyi 2026 Programme. The concept implementation will be accompanied by the deployment of a modern military command, control and communication system for the brigades, which will enable information and command to be shifted onto a new platform.[20]

In order to develop and modernise the artillery and anti-tank artillery capability, the procurement of new equipment, as well as carrier platforms and additional equipment, and the upgrading of the technical teams of the Hungarian Defence Forces, the modernisation of technical equipment, the modernisation of medium tracked floating vehicles and the war bridges will also be carried out with the involvement of the Hungarian defence industry.

Of the new security challenges facing the world and Europe, cyber attacks and cyber defence need to be a key focus for digitalisation and network systems. To combat hybrid warfare, the Hungarian Defence Forces plan to create a cyber defence system that can resist third-party intrusions into the command-and-control systems and detect activity that could indicate an attack on the network. In order to counter threats in cyberspace, soldiers need up-to-date training, and for this purpose the Cyber Training Centre of the Hungarian Defence Forces was inaugurated in Szentendre in June 2019.[21]

A modern logistics, placement and storage system is essential for the proper placement of the new and modernised equipment, which will be implemented as part of the barracks reconstruction programme. The military development programme also includes plans to set up a field hospital and purchase the required equipment that enable the saving of lives, performance of surgical operations and the running of diagnostic tests in the field.[22]

In order to modernise the ground forces, twelve Leopard 2A4 leased tanks[23] will arrive in Tata by December 2020, followed by the procurement of 44 Leopard 2A7+ battle tanks, 24 PzH 2000 self-propelled guns and Ejder Yalcin type armoured Multi-purpose Modular Tanks.[24]

Further Hungarian production of small arms, development of combat equipment for individual soldiers, continued development of cyber capabilities and the creation of the infrastructure required to receive new equipment are all in the pipeline.

Thus, the Zrínyi 2026 Programme will contribute to the short- and long-term transition of the Hungarian Defence Forces to the full application of IT, digital and network-based military systems by way of modernising both the air force and the ground forces. All this supports the thesis that, as the developments are implemented, the entire defence activity can be transferred onto a digital platform in order to ensure that defence, military and national security systems are able to operate independently, decoupled from other systems, and maintain the country's management and public administration in peacetime and in times of special legal order.

---

20 'Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében', accessed on 24.01.2020.

21 'Átadták a Magyar Honvédség Kiber Képzési Központját' (The Cyber Training Centre of the Hungarian Defence Forces was inaugurated), *Kormany.hu*, (Budapest, 13.06.2019) https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat, accessed on 13.02.2020.

22 'Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében', accessed on 24.01.2020.

23 'Aki már huszonöt éve ismeri a "nagymacskákat"' (Some have known the "big cats" for 25 years), *Honvedelem.hu*, (Budapest), https://honvedelem.hu/hirek/aki-mar-huszonot-eve-ismeri-a-nagymacskakat.html, accessed on on 27.02.2021.

24 'A haza védelme, a nemzet szolgálata' (Defending the homeland, serving the nation), *Honvedelem.hu*, (Budapest, 2019), https://honvedelem.hu/files/files/116159/honvedseg_kiadvany_165x235mm_v2_6_.pdf, accessed on 14.02.2020.

The digitalisation of the Hungarian Defence Forces

Nowadays, we are on the threshold of a new warfare era that is radically different from the past. The HDF also needs to adapt to the new way of waging war by going through a digital transformation.

In the following chapter, the author seeks to examine, analyse and project the full-scale digitisation of the defence sector, mostly by presenting international examples, in order to prove her thesis. For this reason there are ten recommendations that are presented below.

The second chapter seeks to determine the weight and intensity that digitalisation represents in the defence sector when it comes to the following platforms:

1. Hungarian participation in the international defence industry.
2. The application of 5G technology in military, operations, command-and-control, communications, defence and military technology.
3. Development of smart weapons, with particular regard to the digitalisation of small arms, self-propelled weapon systems, bombs and missile systems.
4. Development of smart military equipment, in particular smart clothing and digital sensor systems, development of digital military maps and navigation systems.
5. Self-driving military vehicles—the modernisation of trucks, armoured vehicles, armoured transport vehicles, combat vehicles, aircraft, helicopters; their fitting with digital instruments, artificial intelligence on the battlefield.
6. Comprehensive training of soldiers and civilians in digital literacy, ensuring trainings and courses for acquiring knowledge and learning the professional use of digital tools.
7. Addition of digital and network-based capabilities to the military training and education system, defence administration as well as military management system.
8. Completion and migration of personnel record systems, military logistics and combat supply record systems to a digital and network-based platform.
9. Digital development of the Hungarian space programme, development and launch of a Hungarian satellite.
10. Development of a complex network-based and digitised command, control, military intelligence and communications system.[25]

Hungarian participation in the international defence industry

In order to boost the Hungarian defence industry, the Ministry of Defence, the Ministry of Innovation and Technology and the Government Commissioner responsible for National Defence Industrial and Defence Developments and the Coordination of Modernising the Defence Forces are jointly responsible for the development of the defence industry. However, the defence industry developments of the Government may require the involvement of small and medium-sized enterprises as well as *start-ups* in order to ensure faster and more effective development. The flagship priority is to develop the Hungarian defence industry and attract

25 Tibor Babos, 'A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái', pp. 143-144, http://real.mtak.hu/82604/1/2018ebabos2.pdf, accessed on 26.01.2020.

world-leading investors to Hungary, such as Airbus, one of the world's leading aerospace companies. Airbus' plans for Hungary include an aerospace industrial cluster in addition to the manufacturing of components.[26]

Within the framework of the Zrínyi 2026 Programme, the MoD and the HDF started the armament of the forces by launching the procurement of twenty Airbus H145M and 16 H225M helicopters, while the purchase of 44 Leopard 2 A7+ tanks and 24 PzH 2000 self-propelled guns is planned from the German company Krauss-Maffei Wegmann. In order to boost the Hungarian arms industry, the production of P-07, P-09 pistols, Bren 2 assault rifles and Scorpion Evo three submachine guns is planned to take place in Kiskunfélegyháza.[27]

The 5G technology

With the transition to 5G mobile networks, the world is entering a technological era. The 5G network is much faster than the current 4G mobile network, allowing faster data transfer and reduced response times. The transition to 5G will be utilised in the automotive industry, in transport, manufacturing, agriculture, healthcare, energy management, retail, entertainment and media. 5G offers a minimised response time and near real-time communication that contribute to the creation and/or development of intelligent transport, self-driving cars and e-health.[28]

With a public role in the deployment of the 5G network, Hungary could become a European leader, and the network could be deployed faster, avoiding duplication, in partnership with the private sector. In addition to the United States, the UK, Germany, Switzerland, China, South Korea and Australia are also urging the introduction of the new network.[29]

From a defence perspective, connecting digital instruments to the 5G network would not only improve their use on the battlefield, but also develop military training and education. The application of 5G technology in military, operational, command-and-control, communications, defence and military-industrial developments will ensure the transfer of the Hungarian defence activities onto a digital platform.

The development of smart weapons

The development and mass production of smart weapons for the military first was started by the United States in 2019. The idea is that future handheld weapons would have their own operating system. New technology small arms will change the way weapons are handled and used and they will increase the efficiency of the army. In terms of how smart weapons work,

26 'Védelmi ipar ágazati koncepciója' (Sectoral concept for the defence industry), *HMarzenal.hu*, (Budapest, 2018), http://www.hmarzenal.hu/vedelmi-ipar/vedelmi-ipar-agazati-koncepcioja.pdf, accessed on 13.02.2020.

27 Áron Bencze, 'Digitális ugrásra készül a Magyar Honvédség' (The Hungarian Defence Forces about to make a digital leap), *Innoteka.hu*, (Budapest, 03.05.2019), https://www.innoteka.hu/cikk/digitalis_ugrasra_keszul_a_magyar_honvedseg.1909.html, accessed on 31.01.2020.

28 '5GK-Magyarországi 5G Koalíció' (5GK – Hungarian 5G Coalition), *Digitalisjoletprogram.hu*, Budapest, https://digitalisjoletprogram.hu/hu/tartalom/5gk-magyarorszagi-5g-koalicio, accessed on 13.02.2020.

29 Colin Blackman, Simon Forge, *5GDeployment*, Europarl.europa.eu, Brussels, (2019), https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631060/IPOL_IDA(2019)631060_EN.pdf, accessed on 13.02.2020.

the idea is that the operating system built into the weapon can prevent unauthorised use of the device and the applications can help to achieve more accurate targeting. This will not only transform, but also facilitate the future training of soldiers. However, with the digitisation of weapons and their fitting with an operating system, the possibility of hacker attacks increases, and the government needs to prepare for this eventuality by strengthening its cybersecurity system.[30]

The United States is exploring new deployment options for the F-35 II JSF stealth fighter as part of its efforts to develop missile defence capabilities. The aim of the development is to use the F-35's sensors and data link systems to detect or destroy intercontinental ballistic missiles, even already at launch phase. China and North Korea are also interested in such developments.[31]

On 8 January 2020, Iran launched eighteen short-range ballistic missiles against US Army bases in Iraq. Almost 200 Hungarian soldiers are posted in Erbil, but they were not injured in the rocket attack. Following the attacks, Iran said in a statement that any country allied with the United States could be seen as an enemy and a target for them.[32]

Given the increasing trend of threats, the expansion of the defence system capabilities cannot be delayed any longer. Consequently, not only the United States, but also NATO and EU Member States, including Hungary, must focus on state-of-the-art defence capabilities.

The digital soldier

The idea of smart military equipment was pioneered by the United States in the late 1990s. Developments included laser-based technology, a digital tactical map that acts as a built-in computer and a helmet-mounted display system capable of displaying the own position of the soldiers as well as their team's. A much lighter bullet-proof Kevlar helmet has been developed that can be fitted with a special display which shows the image of the camera mounted on another soldier's weapon, or even the enemy's position along with events on the battlefield. Future plans include the addition of 3D displays and a 3D audio system to the hermetically sealed helmet with attachable gas mask, which will enable the soldier to detect the enemy from a distance. In the US Army, soldiers are issued with a protective vest (interceptor) that protects the upper body, the thighs and the arms. In the future, the aim will be to develop armour designs that are lighter in weight and more effective in protection than the current ones, using titanium composite protective panels capable of stopping even close-range machine bullets.[33]

Military uniforms must be adapted to different climate zones. However, modern technology has led to major improvements in uniforms, making them increasingly adaptable

30 Adorján Kiss, 'Okosfegyverekkel látnák el a hadsereget' (The army to be equipped with smart weapons), *Vg.hu,* (21.10.2019), https://www.vg.hu/gazdasag/gazdasagi-hirek/okosfegyverekkel-latnak-el-a-hadsereget-2-1821681/, accessed on 31.01.2020.

31 'Lockheed Martin - F-35 Lightning II', *Aerotech.hu*, http://www.aerotech.hu/f-35.php, accessed on 28.02.2021.

32 'Rakétatámadások Irakban: Irán gyorsan megtorolta Szulejmáni likvidálását' (Rocket attacks in Iraq: Iran quickly retaliates Suleimani's liquidation), *Hvg.hu*, (Budapest, 2020.01.08), https://hvg.hu/vilag/20200108_Iran_raketacsapast_mert_az_amerikaiak_egy_iraki_tamaszpontjara, accessed on 13.02.2020.

33 Miklós Cifka, 'A jövő gyalogos katonája: baka a digitális korszakban' (The future infantryman: soldier in the digital age), *Sg.hu,* (Budapest, 29.03.2005), https://sg.hu/cikkek/tudomany/36233/a-jovo-gyalogos-katonaja-baka-a-digitalis-korszakban, accessed on 13.02.2020.

and providing soldiers with more comfortable, practical wear, thus contributing to improved performance in combat. The future vision is that the uniforms will be made of well-ventilated, water-repellent, durable materials, with cooling and heating functions adapted to specific climates. Cooling vests contain a crystalline material that turns into a gel when it comes into contact with water, thus providing the cooling function. This solution was already successfully used by soldiers fighting in Iraq in the mid-2000s.[34]

The clothing and equipment pattern of the US Army has evolved over generations. The camouflage uniforms have been replaced by digitalised patterns. The new pixelated cadpat camouflage pattern was first used by the Canadian military in 1996, followed by the US Marine Corps' marpat pattern in 2001 and finally the US Army's acupat pixel pattern in 2005, which is now in use by many military forces all over the world. The Americans are exploring the possibility of how the digitised uniforms could pick up the colours of the background like a chameleon, or how the suit could fully merge with the landscape behind it.[35]

The US has developed smart military uniforms and digital military equipment under the Land Warrior and then the Objective Force Warrior programmes. The aim of digital warfare is for every soldier to have a transceiver that can transmit voice, data and images between the soldier on the battlefield and the headquarters. The idea is that the cables for the radio system, computer and electrical systems would be housed in the harness and clothing, ensuring the soldier' unhindered movement.[36]

In the 21st century, it is important that Hungarian soldiers have electronic equipment that can receive or send voice, text and picture messages over a secure communication channel. Therefore, in line with international developments, Hungary has also launched the Digital Soldier Programme within the framework of Zrínyi 2026 Programme, with a main focus on the soldiers themselves. The Programme seeks to provide new, modern combat equipment—clothing, boots, flak jackets, load-bearing vests, helmets, rucksacks and personal weapons for the duration of the training period and for soldiers in the field.[37]

Since the digital suit developed by the US does not provide good enough camouflage in the Hungarian setting, the old darker-coloured training suits were replaced by lighter-coloured infrared-absorbing training suits in the first phase of the Digital Soldier Programme. The personal weapons of the Hungarian soldiers are produced in the arms factory in

34 Zoltán Gácser, 'A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben' (The possibilities of developing a modern, network-integrated individual equipment system in the Hungarian Defence Forces to increase the combat capability of our soldiers), PhD thesis, (Budapest, 2008), https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12102/ertekezes.pdf;jsessionid=E53B0E3B1B43A817529E3C72C25CEF01?sequence=1, accessed on 28.02.2021.

35 *Key Issues Relevant to The U.S. Army's Transformation to the Objective Force, An AUSA Torchbearer Issue*, Vol. II. USA, (2002), https://www.ausa.org/sites/default/files/TBNSR-2002-The-US-Armys-Transformation-to-the-Objective-Force-Vol2.pdf, accessed on 09.02.2020.

36 'Land Warrior Integrated Soldier System', *Army-technology.com*, USA, https://www.army-technology.com/projects/land_warrior/, accessed on 09.02.2020.

37 'Military Information Space' (Katonás Infotér), *Honvedelem.hu*, (Budapest, 16.10.2019), https://honvedelem.hu/hirek/hazai-hirek/katonas-infoter.html, accessed on 27.01.2020.

Kiskunfélegyháza, where pistols, submachine guns and assault rifles are manufactured. As part of the military industry developments, the Zrínyi 2026 Programme will include the Hungarian production of small arms, and gunpowder.[38]

Self-driving vehicles, artificial intelligence

The use of robots in the battlefield to make the job of soldiers easier is becoming increasingly common. This means that you can see miniature military robots with wheels, tracks or legs, but there are larger robots that can carry heavy loads and can transport even several tonnes of military equipment. Furthermore, in the various theatres of war there are remotely piloted aircraft performing air reconnaissance or strike missions and improvised explosive device (IED) bomb-neutralizing robots. In the future, demining robots, explosive disarming robots and remote-controlled robots equipped with weapons will be upgraded to be able to patrol a predefined area and eliminate the enemy.[39]

The development of a new generation of combat robots has started, which means that tracked, rubber-wheeled, longer-range and smarter systems can be also deployed. The United States, Russia and China are also engaged in the military development of artificial intelligence.[40]

Robotisation can be achieved not only by harnessing newly developed artificial intelligence, but also by rebuilding the autonomous operation of existing vehicles and aircraft. This is how the US Navy uses the MQ-8C remotely piloted helicopter, a modified version of the Bell 407 helicopter. In Russia, the BMP-3 infantry fighting vehicle has been rebuilt with computers replacing the operators. The Russian Uran-6 bomb squad robot is an upgrade of the Croatian MV-4 DOK-Ing, a large tracked demining system. In China, Sharp Claw, a rubber-wheeled light armoured vehicle that can autonomously approach enemy territory, was introduced in 2014. This robotics vehicle has its own reconnaissance and weapons systems, but the latter requires a soldier to operate it. The vehicle is able to perform reconnaissance both in the air and on the ground, since it is equipped with a short-range quadrocopter.[41]

Although Hungary has little interest in developing robotic ships and submarines, it must be mentioned that the United States and Russia have already started testing submarine hunters and warships, and the US Navy is developing robots to extinguish fires on ships and submarines.[42]

Based on international examples, the military use of artificial intelligence on land, sea and air clearly has an important role on the battlefield. As part of the Zrínyi 2026 Programme, new procurements and the modernisation of existing equipment described above are the first steps for the HDF to effectively deploy artificial intelligence in the theatre of operations.

38 Draveczki-Ury, Ádám, 'Digitális világ a haza szolgálatában' (The digital world at the service of the homeland), *Honvedelem.hu*, (Budapest, 30.04.2019), https://honvedelem.hu/media/aktualis-videok/digitalis-vilag-a-haza-szolgalataban.html, accessed on 09.02.2020.

39 Imre Négyesi, 'A mesterséges intelligencia és a hadsereg I.' (Artificial Intelligence and the Army I.), *Hadtudományi Szemle*, (Budapest, 2017/2), http://epa.oszk.hu/02400/02463/00035/pdf/EPA02463_hadtudomanyi_szemle_2017_2_023-034.pdf, accessed on 13.02.2020.

40 'Robotok uralják a jövő harctereit?' (Will robots rule the battlefields of the future?), Honvedelem.hu, (Budapest, 05.08.2010), https://honvedelem.hu/hirek/robotok-uraljak-a-jovo-harctereit.html, accessed on 13.02.2020.

41 Balázs Trautmann, 'Fémharcosok' (Metal warriors), *Honvedelem.hu*, (Budapest, 24.07.2016), https://honvedelem.hu/hatter/haditechnika/femharcosok.html, accessed on 09.02.2020.

42 Balázs Trautmann, 'Fémharcosok'.

The development of digital capabilities

The Hungarian Defence Forces are undergoing a major transformation, with the procurement of state-of-the-art equipment that lays the foundations for research, development and innovation. Information warfare is taking place in cyberspace and changes are occurring in all theatres of war. Conventional forces are no longer effective against terrorist organisations, ushering in the era of fourth generation warfare. In light of the situation, the most important issue for the armed forces is to increase their responsiveness and find solutions to successfully implement digital transformation within their organisations.

The key to success in the 21st century is to decentralise leadership and recognise and address the challenges of the day. This requires the development of problem-solving skills, critical thinking, creativity, networking skills and the ability to quickly adapt to changing circumstances. Innovation in warfare does not merely mean new technology, it also entails the easy and professional application and mastering of these technologies, and their use in state-of-the-art weapons and machines. All this will help to ensure that the Hungarian armed forces become flexible, and have an appropriate organisational structure for the application of the new technologies.[43]

The institutional transformation and organisational development of the Ministry of Defence and the Hungarian Defence Forces started in 2019. The Hungarian Defence Forces Modernisation Institute and the Defence Research Institute were established. The Ministry is in cooperation with Hungarian higher education institutions to launch a number of research projects. The curricular and additional courses and trainings of the National University of Public Service ensure the professional use of new technologies and the effective confrontation with new security challenges, both in engineering and in cybersecurity training which are relevant to the development of hybrid warfare.[44]

The military training and education system

The development of new technologies, modern weapons and that of defence capabilities not only place an additional physical burden on soldiers, but also require the development of their cognitive skills. The development of cognitive skills can be accomplished similarly to how physical stamina is built. Digital tools, weapons, clothing and equipment for military development and modernisation are based on algorithms, just like in the applications which are used in civilian life. They are based on *deep learning*, which involves the use of neural networks.[45]

The United States Defense Advanced Research Projects Agency (DARPA) and the Platypus Institute are engaged in the neurotechnological development of military performance. These institutes are exploring the potential for improving cognitive skills by studying the brain's

43 Áron Bencze, 'Digitális ugrásra készül a Magyar Honvédség', accessed on 31.01.2020.

44 'Középpontban a katona' (The soldier in the focus), *Kormany.hu*, (Budapest, 01.05.2019), https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/kozeppontban-a-katona, accessed on 13.02.2020.

45 'Digitális megoldások a jövő hadseregében' (Digital solutions for the army of the future), *Uni-nke.hu*, (Budapest, 2019), https://www.uni-nke.hu/hirek/2019/08/07/digitalis-megoldasok-a-jovo-hadseregeben, accessed on 31.01.2020.

adaptability in a dynamic technological environment.[46] This research is an investigation of the individual cognitive abilities of soldiers and of a group of soldiers during joint operations. Furthermore, the research also covers interactions between humans and robots. Research is required because digital technology is advancing faster than what the human brain is capable of processing, and this is the reason why the cognitive development of individual skills is needed. There is a simulation programme also used by the US Army's Special Operations Forces in their training programme. The *online* simulation system is used to teach leadership behaviour and methods within the command training programme.[47]

In Hungary, the VR-based simulation system developed as part of the Digital Soldier Programme contributes to the development of the cognitive skills of the soldiers.[48]

The digitisation of record-keeping systems

The Integrated Legislative System (ILS) was launched in 2016 to reduce the burden on public administration and increase the service delivery capacity.[49] The aim of the ILS is to improve the quality of legislation, and to this end all activities related to legislation within the system are supported by IT, from the first draft all the way to its publication in the Hungarian Gazette.

The ILS consists of several subsystems, such as the Electronic Legislative Drafting System (ELDS), which supports the drafting of legislation, that is the codification process. Other subsystems of the ILS are GovLex, Parlex and LocLex. GovLex is responsible for preparing government legislation. It has an IT platform for commenting on and sharing legislation, proposals and reports, and it also boasts of organisational, query, recording and executive control functions. ParLex is the Parliamentary Information System for Legislation, a system for parliamentary document editing and process management. It ensures the drafting and electronic submission of individual documents, with appropriate user and data security.[50] The LocLex system supports the legislation preparatory, drafting and uploading processes of local authorities.

In the spirit of electronic administration, since February 2015 the Ministry of Defence has been successfully using the Customer Service System of the Budget Management Information System of the Ministry of Defence, which is a universal portal enabling in-person administration as well as quick and non-personal electronic administration of financial records and personnel administration, available to the entire staff.[51] The Ministry of Defence has also joined the ILS project, so following the test run the live system will be launched within the Ministry. The ILS will go live after the test run on 1 August 2020.[52]

46 'DARPA, Army & Team Platypus, Big Boosts for Artificial Intelligence', *Breakingdefense.com*, (2018), https://breakingdefense.com/2018/09/darpa-the-army-team-platypus-artificial-intelligence-for-future-war/, accessed on 28.02.2021.

47 Darpa.mil, https://www.darpa.mil/, accessed on 13.02.2020.

48 'Digitális megoldások a jövő hadseregében'.

49 Governmental Decision No. 1004 of 2016 (I.18.) on the establishment of the annual development budget for the Public Administration and Civil Service Development Operational Programme.

50 'Elektronikus irományszerkesztés és benyújtás (ParLex rendszer)' (Electronic document editing and submission, ParLex system), *Parlament.hu*, Budapest, https://www.parlament.hu/elektronikus-iromanyszerkesztes-es-benyujtas-a-parlex-rendszer- accessed on 12.02.2020.

51 The Ministry of Defence Instruction No 80 of 2014 (XII.5.) on the National Defence Chapter of the Budget Management Information System.

52 Government Decision No 1612 of 2019 (X.24.) on the introduction of the Integrated Legislative System and related tasks.

The Hungarian space programme

In order to boost the Hungarian space programme, the Hungarian Minister of Foreign Affairs and Trade held talks with the director of the Russian state space corporation Roscosmos in November 2019. The aim of the Hungarian-Russian coalition is to formally continue Hungarian space programmes of technical and technological value currently running in Russia as Hungarian-Russian space projects. The goal of the long-term cooperation is to have a Hungarian astronaut working on the International Space Station (ISS) by 2024/2025, and to ensure that the Hungarian astronaut researcher can take the space instruments of intellectual value which have been developed by Hungary to the ISS and perform their research activity on the ISS for 3-6 months.[53]

The Hungarian-Russian coalition will provide a new opportunity for Hungarian space companies and researchers from Hungarian universities engaged in space industry and space technology for the development of the Hungarian space industry and the dissemination of existing Hungarian technologies. For the purposes of a successful coalition and the development of the Hungarian space industry, the portfolio of the Ministry of Foreign Affairs and Trade is expanded to include space research, which included the establishment of the National Space Research Fund.[54]

The digitisation of military communications system

Last, but not least, in order to achieve the comprehensive digitalisation of the HDF, it is essential to implement the Hungarian Defence Forces' Governmental Purpose Isolated Communications Network (HDF GPICN) development. The HDF GPICN is a specialised, closed-purpose info-communications network that must be capable of supporting the HDF's command-and-control systems in peacetime or in special times by providing the technological, technical and service background as well as the operational environment. The system is a network-based critical infrastructure that is based on communication and information systems and devices. The purpose of the network is to serve the communication and information technology needs of the high-level military command, to provide the technological and technical basis for the command-and-control systems, and to enable access to communication and information technology services in peacetime and in times of special legal order. It is also tasked with connecting to and disconnecting from other info-communications networks, i.e. to ensure an independent operation.[55]

The availability of the HDF GPICN is an interest of the Hungarian Defence Forces. However, the development of a network based on digital age technologies and services cannot be delayed any longer. On the one hand, it has to meet the currently evolving international requirements for the purposes of cooperation with the networks and systems of other nations, and on the other hand, it has to be compliant with the requirements raised by our NATO membership.

53 'Oroszországgal közös cél, hogy magyar űrhajós kezdhessen el dolgozni 2025-re' (Common goal with Russia to have a Hungarian cooperating astronaut by 2025), *Magyarhirlap.hu*, (Budapest, 13.12.2019), https://www.magyarhirlap.hu/kulfold/20191213-magyar-orosz-urkutatasi-projektek-indulnak, accessed on 12.02.2020.

54 Urvilag.hu, http://www.urvilag.hu/, accessed on 12.02.2020.

55 Ministerial Direction No 55 of 2013 (IX.13.) on the operation and supervision regime of the Governmental Purpose Isolated Communications Network of the Hungarian Defence Forces in peacetime, and the rules for the use of centrally provided services.

The developments should be carried out in accordance with the following directions: (1) increasing bandwidth, data transmission speed; (2) increasing the capacity of hardware and software transmission paths; (3) replacing and upgrading hardware, software platforms, server farms; (4) creation and provision of reserves; (5) developing and increasing cyber defence capabilities; (6) building network, user, hardware and software security; (7) ensuring availability, reliability and flexibility; (8) increasing quality of service.[56]

The fundamental objective is to make the communications and IT system, services and information more centralised, to build a user-friendly, multifunctional, converged and modern digital network and to develop the defence sector in line with the general progress. A further objective is to bring services to soldiers fighting in the field, with real-time images. The network must ensure both cooperation with civil and law enforcement networks as well as continue to operate smoothly and independently in the event of a cyber attack or during times of special legal order.[57] The long-term objective for the development of the HDF GPICN is therefore to ensure that digital and network-based systems are capable of autonomously fulfilling the public administration functions as well as maintaining the country's management even in times of special legal order.

In summary, the ten platforms presented as recommendations for the full digitisation of the Hungarian Defence Forces vary in their intensity. This means that they do not weigh equally regarding the measures taken to achieve the digitisation goals. However, for the Hungarian Defence Forces to transfer onto and catch up with advanced military, IT, digital and network-based systems in order to ensure the autonomous and independent operation of such systems, it is necessary to treat the recommended platforms as equally important.

Conclusion

The thesis was written based on the assumption that in this era of digital revolution, the modernisation of the army is essential to successfully face new security challenges, the implementation of which has already been launched by the Ministry of Defence, in cooperation with the Hungarian Defence Forces in 2017 as part of the Zrínyi 2026 Programme.[58]

The Zrínyi 2026 Programme objectives include the upgrading of the HDF IT, digital and network-based military systems. With the implementation of the developments the Hungarian national defence as a whole could be shifted onto a digital platform, which would mean that the high-tech systems available on the market and the defence, military and national security system infrastructures used by the public administration could operate independently and separately in order to support the Government's info-communications activities.[59]

56 Szabolcs Jobbágy, 'A Magyar Honvédség kormányzati célú elkülönült hírközlő hálózata' ('The separate government communications network of the Hungarian Defence Forces), *Hadmérnök Journal*, (2017). XII. p. 233 Online: http://hadmernok.hu/173_20_jobbagy.pdf, accessed on 09.02.2020.

57 Szabolcs Jobbágy, 'A Magyar Honvédség kormányzati célú elkülönült hírközlő hálózata'.

58 Government Decision No 1298 of 2017 (VI.2.) on the implementation of the Zrínyi 2026 Defence and Armed Forces Development Programme.

59 Tibor Babos, 'A Digitális Jólét Program', accessed on 26.01.2020.

The main claim of this paper was that the integration of defence, military and national security systems into the Hungarian digital network is required to ensure that military IT, digital and network-based systems that function properly in peacetime would be able to operate independently and perform the public administration functions and the governance of the country when a special legal order (other than peacetime) is applied.[60]

As a proof of this claim, the first chapter of the thesis presented the military development and digital platforms along which the Zrínyi 2026 Programme set its long-term goals and instruments for the digitalisation and modernisation of the Hungarian Defence Forces, with a special regard to the presentation of the Zrínyi 2026 Programme and the modernisation of the air force and the ground forces. The second part, without being fully comprehensive, lists ten recommendations for the full digitalisation of the Hungarian Defence Forces by presenting international examples.

In conclusion, it can be established that the overall Zrínyi 2026 Programme is in accordance with the digitalisation efforts of the Hungarian Defence Forces. This means that the already implemented procurements, investments, trainings, further educational activities and defence programmes occurred to an increasing extent for the purposes of facilitating digitisation.

Based on the already achieved results and in light of the further objectives, the ten platforms presented in the second part of the thesis that were formulated as recommendations—if understood, applied and developed—could put the whole of the Hungarian defence on a digital footing.

However, for the Hungarian Defence Forces to shift to and catch up with IT, digital and network-based military systems, it is necessary to treat the recommended platforms as equally important. Provided that the objectives of the Zrínyi 2026 Programme are achieved and the digital platforms are treated with the same weight and intensity, national defence as a whole could be shifted onto a digital platform, which would mean that the high-tech systems available on the market and the defence, military and national security system infrastructures used by the public administration could operate independently and separately in order to support the Government's info-communications activities.

60 Tibor Babos, 'A Digitális Jólét Program', accessed on 26.01.2020.

Bibliography

1. 'A haza védelme, a nemzet szolgálata', (Defending the homeland, serving the nation), Honvedelem.hu, (Budapest, 2019), https://honvedelem.hu/files/files/116159/honvedseg_kiadvany_165x235mm_v2_6_.pdf, accessed on 14.02.2020.
2. The Ministry of Defence Instruction No 80 of 2014 (XII.5.) on the National Defence Chapter of the Budget Management Information System
3. 'A járványról és a haderőfejlesztésről is beszélt a honvédelmi miniszter' (The Minister of Defence spoke about the epidemic and the development of the armed forces as well), Honvedelem.hu, (Budapest, 05.12.2020), https://honvedelem.hu/hirek/a-jarvanyrol-es-a-haderofejlesztesrol-is-beszelt-a-honvedelmi-miniszter.html, accessed on 27.02.2021.
4. Governmental Decision No 1004 of 2016 (I.18.) on the establishment of the annual development budget for the Public Administration and Civil Service Development Operational Programme.
5. Ministerial Direction No 55 of 2013 (IX.13.) on the operation and supervision regime of the Governmental Purpose Isolated Communications Network of the Hungarian Defence Forces in peacetime, and the rules for the use of centrally provided services.
6. Government Decision No 1298 of 2017 (VI.2.) on the implementation of the Zrínyi 2026 Defence and Armed Forces Development Programme.
7. 'Aki már huszonöt éve ismeri a „nagymacskákat"' (Some have known the "big cats" for 25 years), Honvedelem.hu, (Budapest), https://honvedelem.hu/hirek/aki-mar-huszonot-eve-ismeri-a-nagymacskakat.html, accessed on 27.02.2021.
8. 'Átadták a Magyar Honvédség Kiber Képzési Központját' (The Cyber Training Centre of the Hungarian Defence Forces was inaugurated), Kormany.hu, (Budapest, 13.06.2019), https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat, accessed on 13.02.2020.
9. Government Decision No 1612 of 2019 (X.24.) on the introduction of the Integrated Legislative System and related tasks.
10. Babos, Tibor, 'A biztonság globális és európai összefüggései' (The global and European context of security), Hadtudomány Journal, (Budapest, 2019/4), http://real.mtak.hu/105840/1/016-029_Babos.pdf, accessed on 12.02.2020.
11. Babos, Tibor, 'A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái' (The security, defence and military policy relevance of the Digital Welfare Programme), Hadtudomány Journal, (Budapest, 2018), http://real.mtak.hu/82604/1/2018ebabos2.pdf, accessed 26.01.2020.
12. Baranyai, Gábor, 'Megérkeztek a honvédség új helikopterei a német gyárból' (The new HDF helicopters have arrived from the German factory), Magyarnemzet.hu, (19.11.2019), https://magyarnemzet.hu/belfold/megerkeztek-a-honvedseg-uj-helikopterei-a-nemet-gyarbol-7505657/, accessed on 25.01.2020.

13. Bencze, Áron, 'Digitális ugrásra készül a Magyar Honvédség' (The Hungarian Defence Forces about to make a digital leap), Innoteka.hu, (Budapest, 03.05.2019), https://www.innoteka.hu/cikk/digitalis_ugrasra_keszul_a_magyar_honvedseg.1909.html, accessed on 31.01.2020.
14. Blackman, Colin andForge, Simon, 5G Deployment, Europarl.europa.eu, (Brussels, 2019), https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631060/IPOL_IDA(2019)631060_EN.pdf, accessed on 13.02.2020.
15. Cifka, Miklós, 'A jövő gyalogos katonája: baka a digitális korszakban' (The future infantryman: soldier in the digital age), Sg.hu, (Budapest, 29.03.2005), https://sg.hu/cikkek/tudomany/36233/a-jovo-gyalogos-katonaja-baka-a-digitalis-korszakban, accessed on 13.02.2020.
16. 'DARPA, Army & Team Platypus: Big Boosts for Artificial Intelligence', Breakingdefense.com, (2018), https://breakingdefense.com/2018/09/darpa-the-army-team-platypus-artificial-intelligence-for-future-war/, accessed on 28.02.2021.
17. Darpa.mil, https://www.darpa.mil/, accessed on 13.02.2020.
18. 'Digitális megoldások a jövő hadseregében' (Digital solutions for the army of the future), Uni-nke.hu, (Budapest, 2019), https://www.uni-nke.hu/hirek/2019/08/07/digitalis-megoldasok-a-jovo-hadseregeben, accessed on 31.01.2020.
19. Draveczki-Ury, Ádám: 'Digitális világ a haza szolgálatában' (The digital world at the service of the homeland), Honvedelem.hu, (Budapest, 30.04.2019), https://honvedelem.hu/media/aktualis-videok/digitalis-vilag-a-haza-szolgalataban.html, accessed on 09.02.2020.
20. 'Electronic document editing and submission (ParLex system)' Parlament.hu, (Budapest), https://www.parlament.hu/elektronikus-iromanyszerkesztes-es-benyujtas-a-parlex-rendszer-, accessed on 12.02.2020.
21. Gácser, Zoltán: 'A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben' (The possibilities of developing a modern, network-integrated individual equipment system in the Hungarian Defence Forces to increase the combat capability of our soldiers), PhD thesis, (Budapest, 2008), https://nkerepo.uninke.hu/xmlui/bitstream/handle/123456789/12102/ertekezes.pdf;jsessionid=E53B0E3B1B43A817529E3C72C25CEF01?sequence=1, accessed on 28.02.2021.
22. https://honvedelem.hu/media/aktualis-videok/tovabb-gyarapodo-legi-kepesseg.html, accessed on on 27.02.2021.
23. 'Irán támadást intézett két amerikai bázis ellen Irakban' (Iran attacks two US bases in Iraq), Hirtv.hu, (Budapest, 08.01.2020), https://hirtv.hu/hirtvkulfold/iran-ballisztikus-raketakkal-tamadott-meg-amerikai-celpontokat-irakban-2492968, accessed on 31.01.2020.

24. Jobbágy, Szabolcs: 'A Magyar Honvédség kormányzati célú elkülönült hírközlő hálózata' (The separate government communications network of the Hungarian Defence Forces), Hadmérnök Journal, (2017). XII. p. 233, http://hadmernok.hu/173_20_jobbagy.pdf, accessed on 09.02.2020.
25. 'Key Issues Relevant to The U.S. Army's Transformation to the Objective Force', An AUSA Torchbearer Issue, Vol. II. USA, (2002), https://www.ausa.org/sites/default/files/TBNSR-2002-The-US-Armys-Transformation-to-the-Objective-Force-Vol2.pdf, accessed on 09.02.2020.
26. Kiss, Adorján: 'Okosfegyverekkel látnák el a hadsereget' (The army to be equipped with smart weapons), Vg.hu, (21.10.2019), https://www.vg.hu/gazdasag/gazdasagi-hirek/okosfegyverekkel-latnak-el-a-hadsereget-2-1821681/, accessed on 31.01.2020.
27. 'Land Warrior Integrated Soldier System', Army-technology.com, USA, https://www.army-technology.com/projects/land_warrior/, accessed on 09.02.2020.
28. 'Lockheed Martin - F-35 Lightning II', Aerotech.hu, http://www.aerotech.hu/f-35.php, accessed on 28.02.2021.
29. 'The first new helicopters of the Hungarian Defence Forces are already at the base in Szolnok', Honvedelem.hu, (Budapest, 19.11.2019), https://honvedelem.hu/cikk/mar-a-szolnoki-bazison-vannak-a-honvedseg-elso-uj-helikopterei/, accessed on 25.01.2020.
30. Négyesi, Imre: 'A mesterséges intelligencia és a hadsereg I.' (Artificial Intelligence and the Army I.), Hadtudományi Szemle, (Budapest, 2017/2), http://epa.oszk.hu/02400/02463/00035/pdf/EPA02463_hadtudomanyi_szemle_2017_2_023-034.pdf, accessed on 13.02.2020.
31. 'Oroszországgal közös cél, hogy magyar űrhajós kezdhessen el dolgozni 2025-re' (Common goal with Russia to have a Hungarian cooperating astronaut by 2025), Magyarhirlap.hu, (Budapest, 13.12.2019), https://www.magyarhirlap.hu/kulfold/20191213-magyar-orosz-urkutatasi-projektek-indulnak, accessed on 12.02.2020.
32. https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf, accessed on 24.01.2020.
33. 'Rocket attacks in Iraq: Irán gyorsan megtorolta Szulejmáni likvidálását' (Rocket attacks in Iraq: Iran quickly retaliates Suleimani's liquidation), Hvg.hu, (Budapest, 2020.01.08), https://hvg.hu/vilag/20200108_Iran_raketacsapast_mert_az_amerikaiak_egy_iraki_tamaszpontjara, accessed on 13.02.2020.
34. Révész, Béla: 'Csúcstechnika a levegőben' (High-tech in the air), Honvedelem.hu, (Budapest, 18.11.2019), https://honvedelem.hu/galeriak/csucstechnika-a-levegoben/, accessed on 25.01.2020.
35. 'Robotok uralják a jövő harctereit?' (Will robots rule the battlefields of the future?), Honvedelem.hu, (Budapest, 05.08.2010), https://honvedelem.hu/hirek/robotok-uraljak-a-jovo-harctereit.html, accessed on 13.03.2020.
36. 'Tovább gyarapodó légi képesség' (Further developing air capability), Honvedelem.hu, (Budapest, 22 June 2020), https://honvedelem.hu/media/aktualis-videok/tovabb-gyarapodo-legi-kepesseg.html, accessed on 27.02.2021.

37. 'Újabb helikopterek érkeztek' (Additional new helicopters have arrived), Honvedelem.hu, (Budapest, 10 December 2020), https://honvedelem.hu/hirek/ujabb-helikopterek-erkeztek.html, accessed on 27.02.2021.
38. 'Védelmi ipar ágazati koncepciója' (Sectoral concept for the defence industry), HMarzenal.hu, (Budapest, 2018), http://www.hmarzenal.hu/vedelmi-ipar/vedelmi-ipar-agazati-koncepcioja.pdf, accessed on 13.02.2020.
39. 'Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében' (Zrínyi 2026 Defence and Armed Forces Development Programme, In Defence of the Homeland), Honvedelem.hu, (Budapest), https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf, accessed on 24.01.2020.
40. Trautmann, Balázs: 'Fémharcosok' (Metal warriors), Honvedelem.hu, (Budapest, 24.07.2016), https://honvedelem.hu/hatter/haditechnika/femharcosok.html, accessed on 09.02.2020.
41. Draveczki-Ury, Ádám, 'Zrínyi 2026', Honvedelem.hu, (Budapest, 16 January 2017), https://honvedelem.hu/cikk/zrinyi-2026/, accessed on 27.01.2020.
42. 'Középpontban a katona' (The soldier in the focus), Kormany.hu, (Budapest, 01.05.2019), https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/kozeppontban-a-katona, accessed on 13.02.2020.
43. 'Katonás infotér' (Military Information Space), Honvedelem.hu, (Budapest, 16.10.2019), https://honvedelem.hu/hirek/hazai-hirek/katonas-infoter.html, accessed on 27.01.2020.
44. Urvilag.hu, http://www.urvilag.hu/, accessed on 12.02.2020.
45. '5GK-Magyarországi 5G Koalíció' (5GK – Hungarian 5G Coalition), Digitalisjoletprogram.hu, (Budapest), https://digitalisjoletprogram.hu/hu/tartalom/5gk-magyarorszagi-5g-koalicio, accessed on 13.02.2020.

Zsolt Csutak

In the maze of networks, the social impact and security risks of 21st century technologies

Resume

In the 21st century, humanity must face and cope with such new revolutionary technological challenges and trends that had never been encountered before. These factors feature brand new psychological, social challenges and obviously also pose serious security risks. In this interconnected digital ecosystem, various actors commit diverse acts simultaneously, which altogether constitute global security risks. Issues, such as cyber warfare, weaponisation of digital information and the growing impact of social media platforms cannot be neglected any more. However, finding proper solutions proves to be a bigger intellectual and political challenge than identifying the emerging problems.

Executive summary

In the last decade, cyberspace has become a theatre of war, digital information has become a destructive tool that can be used as a cyber weapon, while the Internet user base has become globalised in an untraceable and uncontrollable way.

The social and psychological impact of new technological applications and the safety, human and ethical risks of using artificial intelligence are hardly discussed, it is therefore increasingly important to carry out in-depth, holistic and anthropocentric analyses and research at the level of both individual and public users.

Policymakers need to take action to regulate cyberspace processes, digital applications and highly influential online media providers, and to identify and control the growing number of cybersecurity risks.

The basic premise

"Imagination is more important than knowledge"
Albert Einstein

Starting this paper with Albert Einstein's famous thought—in the age of biological pandemics and cyberspace viruses at the beginning of the 21st century—it is worth examining the ideas of science fiction writers and futurologists, even from the beginning of the last century, as we can find eerie similarities and fulfilled dystopian happenings in today's globalised societies. It is enough to think of the ideas of the British H. G. Wells, Arthur C. Clarke, William Gibson or that of the great master in American science fiction, Isaac Asimov, that included a worldwide computer-based library, a habitable space station or an interconnected network of smart talking machines and humans.[1]

In these science fiction works you can also read about viral attacks on humanity's existence, and even about secondary virtual reality duplication (matrix), which, if we heed Einstein's wisdom, actually make it easier to understand the real challenges of our present time. In the seven millennia or so of written history, there had never been such fast-paced changes in technology and in people's lifestyle as the ones that characterise the recent decades.

In the following pages, the author seeks to find the characteristic features that describe the complex relationship and interrelationship between postmodern societies and new digital technologies. This paper primarily examines and analyses the less studied social aspects and epistemological problems of the subject, along with the sources of security threats.

It can be established that the unforeseeable development horizon and prospects of entirely new digital technologies and artificial intelligence entail in themselves a real set of risks. Furthermore, given the intrinsic development potential of these technologies, and taking into account humanity's historical experience to use new technologies both to build and destroy, such new technologies present numerous and significant risks for the functioning of democratic societies and the evolution of human relations.

According to holistic philosophers who examine human existence and the entirety of increasingly intertwined globalised societies, today, in the age of computer-driven digital systems and the development of artificial intelligence (AI), people are witnessing a transformation and paradigm shift as dramatic and shocking as the advent of the printing press half a millennium ago or the spread of electricity at the end of the 19th century.[2] Perceptibly, the book and paper-based, knowledge-sharing civilisation era, called by McLuhan as the Gutenberg Galaxy[3], is coming to the end of its life, or rather it is becoming radically transformed, digitised, virtual and, perhaps most tellingly, organised into networks of specialised media platforms. Never in human history have human and machine networks been so important and influential as they are today, in the age of the largest man-made

1 Really telling is the visionary interview with Isaac Asimov in *The New York Times* in 1964, in which the author talked about the technical wonders of the World Exhibition in 2014, titled 'Visit to the World Fair of 2014'.
2 Martin Ford, *Robotok kora*, (Budapest, HVG, 2017), pp. 10-13.
3 Marshall McLuhan, *The Gutenberg Galaxy*, (Toronto, University of Toronto Press, 2011).

artificial network, the Internet, which, as presented later, is already excessively shapes and defines the post-postmodern societies of the 21st century in their entirety.

According to surveys[4] since 2018 more than half of humanity (over 4 billion people) have been using some form of an online digital device on a daily basis, and the size of the globally connected *smart devices*, the so-called Internet of Things (IoT), is now estimated to consist of 25 billion gadgets, and this number could reach a staggering 75 billion by 2025.[5] This new, virtually autonomous, gigantic pool of devices (from smart watches to self-driving mini-submarines and military robots to the fully automated Budapest underground line 4) is already partly under the supervision of artificial intelligence, which in itself poses a security risk even without malicious external interference.

In the following pages, the author presents the main characteristics of the new paradigm that consists of computer-based or as more commonly referred to, digital devices and millions of application types, and in particular the security implications of this new global phenomenon that significantly defines and affects the security not only of individual end-users, but also of multinational corporations and nation states. The question is whether societies—that are based on human nature and traditional interpersonal cooperation—are prepared for a revolutionary and radical digital lifestyle and transition, and what would be the resulting cultural, social and political consequences of it? As many renowned thinkers such as Albert Einstein, John von Neumann, Stephen Hawking or Yuval Noah Harari and revolutionary technological entrepreneurs such as Elon Musk have already asked the uncomfortable question: are we sufficiently concerned with the moral and human implications of new, often human-substituting smart technologies (such as artificial intelligence and robotics), or are we leaving these sensitive questions to be answered by future generations?[6]

The virtual *global interconnectedness* of the web is unprecedented in human history and, unfortunately, the associated proliferation of fake news, pseudo-scientific forums and conspiracy theories also poses a serious social and security risk at an individual, community and state level. The duality of human nature means that the Internet and new digital technologies can serve as weapons or be educational, training and healing tools in the hands of the users. At the same time, based on historical experience and the philosophical position derived from Hobbesian anthropological pessimism[7], with some generalisation it can be concluded that people (both at an individual and community level) tend to use any tool, be it social media or artificial intelligence, to satisfy their egoistic interests and desires in a rather harmful and unhelpful way.

Consequently, in addition to the growing security concerns and potential cyber threats, it is important to examine the socio-psychological, cultural transformation process and key factors of the new digital technology-based societies, which are even more drastic and radical than the security challenges they pose. According to social scientists and critical analysts[8], the

4 Statista 1: https://www.statista.com/topics/1145/internet-usage-worldwide/, accessed on 15.01.2020.
5 Statista 2: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide, accessed on 28.01.2020.
6 Catherine Clifford, 'Elon Musk on AI', *CNBC.com*, https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html, accessed on 19.03.2020.
7 Leo Strauss, *A politikai filozófia története*, (Európa, Budapest, 1994), pp. 409-412.
8 Yuval Harari, *Homo Deus*, (Budapest, Animus, 2017), pp. 195-200.

designers and producers of digital information technologies systematically forget the indirect individual and social impact of their new solutions, or they face such impact only years later, with mixed feelings, as described below regarding the birth of the Internet.

In general it could be stated that the analysis or the taking into consideration of medium and long-term social, cultural and other human consequences are the main priorities of programmers and software engineers. Obviously, they are not to be condemned for it, since the design and production of a digital product or service requires completely different skills and knowledge than the analysis of its subsequent security policy or overall social impact. At the same time, analysing the impact of all these technologies is no small intellectual challenge because of their novelty, their history of one or two decades or even just a few years. Researchers and analysts, both well versed in new digital technologies and sensitive to the social implications and human responses, as well as able to explore the wider social-scientific context are required.

Presumably for this very reason, i.e. due to the lack of such experts, these softer technological aspects have been less researched and explored until now, to the point where many of their negative effects are becoming apparent even to laypeople by now. With this regard, it is worth noting two particular and thought-provoking examples that already very much determine our everyday lives in this cyber era. On the one hand, the comment that became a one-liner by Norton A. Schwartz, a US Air Force general and cyber defence commander is really telling—nowadays "a blackout may be just a blackout, but in cyber warfare it may be part of a pre-emptive military strike."[9]

On the other hand, it is worth recalling the bitter interviews of Vinton Cerf and Sir Tim Berners-Lee, two of the founding fathers of the Internet, in *The Guardian*, about the transformation and fate of the web they developed.[10] In the three decades since 1991, the two world-renowned experts argue that the computer-based Internet has evolved from its original vision as a global digital knowledge marketplace into something completely different in an era dominated by social media and mass online gaming. It is sufficient to think of the depressing data that around 80% of the dark web that dominates the underworld, is filled with stomach-churning child pornography and other illegal content,[11] which poses great danger for individuals and society alike. Not to mention the depressing fact that, according to research by international law enforcement organisations and Internet security companies, Internet-based cybercrime has taken over the global lead from drugs, illegal arms and human trafficking since 2016. A staggering figure is that the damage caused by these new, invisible and anonymous cyber criminals around the world amounts to $5.5 trillion a year, the equivalent of about one and a half years of the US federal budget.[12]

The world wide web, and in particular the world of social media networks, have extremely democratised the flow of information, the exchange and spread of ideas, and because of the

9 Richard A. Clarke, Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (Harper Collins, New York, 2010), p. 25.

10 Olivia Solon, 'Tim Berners-Lee on the future of the web: "The system is failing"', The Guardian, https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-web-net-neutrality, accessed on 29.12.2019.

11 Hsinchun Chen, Dark Web: *Exploring and Data Mining the Dark Side of the Web*, (Springer, New York, 2012).

12 *CyberCrime Magazine*, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, accessed on 15.01.2020.

deliberately damaging Internet actors and the previously referred to realist-pessimistic human traits, it did so with a tilt towards the negative aspects. In recent decades, the level of faith and trust in traditional social, political and academic elites has significantly eroded, and inversely, the popularity of Internet-based conspiracy theories, superstitions, false esoteric doctrines, and the influence of uneducated soothsayers, self-proclaimed expert vloggers and influencers that are like religious substitutes[13] has unfortunately skyrocketed.[14]

Although it is not the primary focus of this paper to examine the relational evolution between the diffusion of smart devices and human intelligence, it is considered to be a very important aspect that will most probably be discussed in great detail in the future. Some of the more critical US researchers and studies have already pointed out[15] that the unprecedented and unimaginably rapid digitalisation of recent years has led to people becoming mentally impoverished, losing intellectual creativity and agility as end-user consumers through ever smarter devices and applications, and members of the examined focus group even showed a slight decline in their overall measured intelligence level.[16]

For millions of users, especially a significant part of the younger generation, the digitalised, virtual (or cyberspace) secondary reality has become an extension of our primary physical reality, and for many of them the web is now a primary source of information and experience, a lived reality, with all its personality-distorting and even mind-altering dangers.

In a virtual maze of concepts

In the following, this paper examines the scientific paradigms and perceptions that characterise our digital world, and the conceptual framework that best captures the current processes.

Nowadays, the terms *digital* and *cyber* are often used as each other's synonyms and in an overlapping way, however, the latter is a more appropriate and more realistic term, as opposed to the much narrower meaning of the adjective *digital*. Obviously, both concepts have a raison d'être, as well as a Hungarian scientific relevance, primarily due to the outstanding research work conducted by Hungarian nuclear physicists and theoretical mathematicians who fled to the United States after World War II. It was the young American mathematical genius John W. Tukey of Princeton and his Hungarian-born Professor colleague John von Neumann who developed and set the foundations for the *binary digit* algorithm system with bit-based units (where the digit is either 0 or 1, true or false), which created the new digital computing paradigm of the 20th century.[17] So, the term digital is mainly related to electronic computing processes and binary algorithms. However, the unintentional and misleading interchange and confusion of the terms *cyber* and *cybernetics* is a source of much misunderstanding.

13 They are online media personalities and celebrities who regularly publish mostly self-produced multimedia content and are able to actively influence their target audience.

14 Péter Krekó, 'Netes konteók' (Conspiration theories on the Internet), Index TNT Podcast, https://index.hu/techtud/2020/04/12/tnt_osszeeskuves_kreko_peter_podcast/, accessed on 12.04.2020.

15 Nicholas Carr, *The Shallows: What the Internet is doing to our Brains*, (W. Norton, New York, 2011).

16 Brett Frischmann, 'Is Smart Technology Making Us Dumb?', *Scientific American*, (27 December 2018).

17 'Father of digital computer John von Neumann was born 114 years ago', About Hungary blog, http://abouthungary.hu/news-in-brief/father-of-digital-computer-janos-neumann-was-born-114-years-ago/, accessed on 20.03.2020.

Cybernetics, the new science of information retrieval and the control, computer modelling and programming of dynamic systems, has been linked to Norbert Wiener ever since 1946, and the term was used in a scientific context quite different from how cyber is used today. Wiener, who borrowed the name of this new discipline from the Greek term *kybernḗtēs*, saw the dynamics and control of man-made artificial machines as similar to that of animals. It was later Hungarian American Nobel Prize-winning scientists in computer science, John von Neumann and János Harsányi who, through game theory and other revolutionary affiliate scientific disciplines, extended it to the modelling of social processes (especially war conflicts) as most of the technology was in the service of US defence research.[18] In this context, Bertrand Russell, the famous British mathematician and pacifist philosopher, was right to say that in wartime, science cannot be conducted unless it has some kind of military connection or relevance.[19]

The much-used term *cyber*, in the modern sense of the word, is primarily associated with the Canadian physicist and science fiction writer William Gibson, who first used the expression in his 1982 novel *Burning Chrome* as a metaphor of the system that is based on the interaction between the computer and humans. However, for completeness, Arthur C. Clarke's brilliant *The City and the Stars* must also be mentioned from 1956, in which the British master of science fiction already used the concepts of a virtual matrix and virtual reality in a very similar context.[20]

According to its professional application and the context in which it is used today, primarily based on the glossaries used in military science and security studies, *cyberspace* refers to a system of electronic devices and information networks that operate across the entire electromagnetic spectrum,[21], a term with a much broader dimension and content than the much older term *digital*, which is also used as its synonym. *Joint Vision* 2020, a US Joint Forces strategic document issued in 2000 was the first to identify the various military *warfighting domains* and *operational environments* and *terrains*, including cyberspace in the information environment. After the dramatic cyber attack, the famous *web war one*[22] against Estonia in April 2007, cyberspace was also included in the new NATO cyber defence strategy from 2008 as part of the dynamic military and civilian information environment and as a potential new theatre of war.[23]Furthermore, in 2014 the proliferation of hidden and overt cyber attacks and ransomware, which are a cause for serious concern, led NATO's main decision-making body, the North Atlantic Council, to declare a demonstrable and traceable cyber attack against one of its member states a real *casus belli* in the future and to include it in the provisions of the famous Article 5 of the Washington Treaty on collective defence.[24]

18 'Norbert Wiener', https://www.britannica.com/biography/Norbert-Wiener, accessed on 10.03.2020.
19 Olivier Esteves, 'Bertrand Russell: the utilitarian pacifist', *French Journal of British Studies*, XX-1/(2015), https://journals.openedition.org/rfcb/308, accessed on 25.03.2020.
20 William Gibson, *Cyberspace*, http://www.technovelgy.com/ct/content.asp?Bnum=53, accessed on 25.12.2019.
21 Zsolt Haig, *Információs műveletek a kibertérben* (Information operations in cyberspace), (Dialóg Campus, Budapest, 2019), pp. 22-26.
22 Stephen Blank, 'Web War I: Is Europe's First Information War a New kind of War?', https://www.tandfonline.com/doi/full/10.1080/01495930802185312, accessed on 12.01.2020.
23 Ulf Häußler, 'Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO's Treaty', https://www.sbs.ox.ac.uk/cybersecuritycapacity, accessed on 10.01.2020.
24 Laura Brent, 'NATO's role in cyberspace', in *NATO Review*, (Feb 2019).

In a similar way to NATO's strategic approach and definition of cyberspace, Colonel Zsolt Haig and General László Kovács are at the forefront of clarifying the concept of cyberspace in Hungary through their military science work. According to Hungarian experts in information operations and cyber warfare, cyberspace in a primarily military context is nothing more than "the use of the part of the information arena by the various networked electronic systems on the battlefield where the various electronic information processes (electronically executed data acquisition, data processing, communication, etc.) are realised, and the activities and defence against electronic systems are carried out. This range of the information space is often referred to as cyberspace."[25] For the sake of clarity and in order to avoid conceptual and semantic confusion, it is therefore worthwhile and recommended to use the term cyber dimension, or *cyberspace*, instead of the term digital ecosystem, which is limited to the narrower computing dimension. This term covers the physical network that transmits and processes data (*internet hardware*), the system of smart devices (*the Internet of Things*) and the multitude of applications and *software* packages running on them, all across the entire electromagnetic spectrum.

In fact, the revolutionary technological paradigm shift that took place at record speed has left millions of ordinary people and a significant proportion of state actors still in the dark, especially if they approach the new challenges with a mentality and habits entrenched in the 20th century.

Data and Information as power and weapon in the cyber era

"Data is the oil of the 21st century."[26]

This paper seeks to find answers to the problems and phenomena of how the growing amount of digital data and information is perceived, what general properties it has, what it can be used for and what cybersecurity threats it can pose to a wide range of users.

For centuries, information—intended as processed data (sets)—has been a key instrument of power, a key tool in the hands of decision-makers for military, political or economic advantage. This statement is even more true today, when an amount of virtual electronic data unimaginable to the human mind is generated on the world wide web. The average daily data that is generated by human users (plus IoT and AI) on the Internet amounted to about 8,000 petabytes in 2019[27]), which for the sake of proportionality is twice the size of the 40-million-volume collection of the Library of Congress in Washington DC. Obviously, this ever-increasing and mostly unintelligible amount of data is both a burden on the digital storage system and a serious mental challenge for humans, as the human mind is not capable of processing such quantity of data and external inputs that change this rapidly in terms of size and quality. It is most tangible in the multitude of people who feel lost, confused

25 Zsolt Haig, László Kovács, 'Fenyegetések a cybertérből' (Threats from cyberspace), *Nemzet és Biztonság* Journal, (2008/5). p. 63.
26 This sentence is attributed to Clive Humby, British mathematician and corporate marketing manager from 2006, https://www.quora.com/Who-should-get-credit-for-the-quote-data-is-the-new-oil, accessed on 30.01.2020.
27 Statista 3, https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic, accessed on 26.12.2019.

and disoriented in this ocean of electronic news, and in the renaissance of fake news and pseudo-scientific superstitions spread on social networks, which reach half of the world's population and constitute a fairly considerable social, political and security problem today. Internet security experts and social scientists have concluded that the unlimited freedom of information and uncontrolled democratism which is unfolding in cyberspace pose a worrying and serious security risk, as noted by Professor R. Waltzman, a defence technologies researcher at Rand Corporation in the USA. According to the Professor Waltzman's findings, over the last three decades, a vast knowledge base has been created and made available in a unique and unprecedented way in human history, and concurrently, an even larger amount of malicious and harmful information content was generated.[28] To produce and distribute online digital content or malware, you now only need two things: a networked computing device and some skills in info-communications and software management or programming.

Generation Z and the alpha generation consists of hundreds of millions of young people worldwide who were born already in the age of the Internet, or cyber age, and a significant proportion of them possess the two basic prerequisites to become a hacker. According to Rand's researchers, the scandalous cyberspace events of the past decade have shown that information has become over-democratised and it turned into a weapon.[29]

However, since WikiLeaks[30]—that shook the basic tenets of the system when Edward Snowden[31] leaked information—as well as since the spy scandals, a lot of people think that the virtual world and communication on the Internet is subject to serious government surveillance and control, but this is only partially true. The United States, China, the United Kingdom (and to a lesser extent Russia) have the largest, most advanced and comprehensive personal and physical means and capabilities to monitor and even restrict digital traffic in the world[32], but even the most technologically advanced powers are unable to exercise total control due to the gigantic amount of data in cyberspace and the multi-node cellular network structure of the physical Internet network.

The case of *Cambridge Analytica*[33], the small data analytics IT company that had a cardinal influence on the outcome of the Brexit referendum in the UK, which also shook Europe, and on the external influencing scandals that cast a shadow on the 2016 US presidential election, highlighted the operational risks of uncontrolled social networks and their very troubling data usage practices, which can be used as *soft power tools*.[34] Mark Zuckerberg, founder and CEO of Facebook, the world's best-known online social media platform, voiced his concern and demanded more serious and transparent cybersecurity, data use and privacy legislation during his April 2018 US Senate hearing on the alleged or real business relationship between Cambridge Analytica and Facebook.

---

28 R Waltzman, *The Weaponization of Information*, (Rand Corp., Sta Monica, CA, 2017).

29 R Waltzman, *Weaponization*, p. 24.

30 D Leigh, L Harding, *WikiLeaks-akták*, (Geopen, Budapest, 2011).

31 Glen Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, (Metropolitan Books, 2014).

32 See Bruce Sussman's summary in *The Secured World*, https://www.secureworldexpo.com/industry-news/top-10-most-powerful-countries-in-cyberspace, accessed on 31.01.2021.

33 Tom Warren: 'The Cambridge Analytica Scandal', *The Verge*, (April 2018), https://www.theverge.com/2018/4/10/17165130/facebook-cambridge-analytica-scandal, accessed on 10.12.2019.

34 According to Joseph S. Nye's typology of power, culture and communication can also be a component for the projection of power. See Maxime Gomichon 'Joseph Nye on Soft Power', *E-International Relations*, (8 March 2013).

The world's population comes from different cultures and possesses different levels and types of digital literacy, with huge gaps in between them. On the one hand, there is the well-known generational gap regarding the use of digital tools, and on the other, there is the North-South divide or developed/developing/underdeveloped world axis, which also reflects the fragmentation of the world economy. It reveals that Europe, North America and the Far East is in juxtaposition with Africa, South America and South Asia, which in fact means the coexistence of parallel worlds and societies.[35]

For millions of people living in the digital technological civilisation of the 21st century, the right and opportunity to access appropriate information, as well as the ability to filter, process and interpret the available data, has become almost a primary necessity, alongside water, food, and fuel. The Internet service providers behind the much talked about online platforms and social media sites, mostly US tech giants such as Facebook, Twitter, Amazon, Apple, Microsoft or Alphabet (the parent company of the Google group), have a greater role and responsibility than ever before to provide trustworthy, reliable and verified digital data and information. However, the world's major data controllers and opinion leaders do not really meet all these expectations for economic considerations but exploit the various legal loopholes. Large swathes of British and American citizens have recently joined the involuntary call of Zuckerberg for Congressional clampdown. On the one hand, because of the well-known scandals surrounding the 2016 Brexit referendum and US presidential election, and especially because of the proliferation of Internet trolls[36], a large number of conspiracy theories and fake news in the early 2020s, the majority of Britons and Americans want stricter laws on data management, information sharing and the control and supervision of Internet services, if not with global scope, at least regarding their own countries' cyberspace.[37]

The unimaginable and often contradictory information overload, as well as the diminishing of scientific filters, so-called gatekeepers, the drastic reduction of editorial boards of electronic media outlets and their frequent replacement by AI-based applications, altogether have a negative effect on the masses of users and online media consumers. This unfortunate global trend is well demonstrated and observed in media studies and social psychology studies[38] conducted in recent decades on the influence of conspiracy theories and pseudo-scientific news portals, various *influencers*, *vloggers* and social media content sharing. New cyber-psychological terms such as echo-chamber, media bubble and cognitive dissonance, i.e. the belief in your own truth and believing that your comfortable, self-justifying preconceptions are true and real, have become a common characteristic of billions of users living and working in cyberspace. Alongside the malicious and damaging programs and ransomware spreading in cyberspace, there have been a proliferation of conspiracy theories regarding the coronavirus pandemic, the biggest global health and social challenge of the 21st century that nearly a third of the US population surveyed actually believe in.[39]

35 Parag Khanna, *Konnektográfia*, (HVG, Budapest, 2017), pp. 28-32.
36 Paid reviewers and commentators on online social networking sites.
37 James Tapper, 'Social Media Giants…', *The Guardian*, https://www.theguardian.com/technology/2020/apr/04/social-media-giants-must-tackle-trolls-or-face-charges-poll, accessed on 15.04.2020.
38 Péter Krekó, *Tömegparanoia* (Mass paranoia), (Athaeneum, Budapest, 2018).
39 Analysis by Katherine Schaeffer on *FactTank*: https://www.pewresearch.org/fact-tank/2020/04/08/nearly-three-in-ten-americans-believe-covid-19-was-made-in-a-lab/?utm_source=Pew+Research+Center&utm_campaign=9a8a1fc2a0-EMAIL_CAMPAIGN_2020_04_09_06_59&utm_medium=email&utm_term=0_3e953b9b70-9a8a1fc2a0-400906701, accessed on 12.04.2020.

The belief in alternative realities and distorted, pseudo-scientific explanations has gained unprecedented momentum with the global spread of online social media, which, as explained earlier, is obviously in stark contrast with the original noble ideas of the creators of the world wide web. According to the wisdom attributed to the world-famous American writer and journalist Mark Twain, "A lie can travel halfway around the world while the truth is still putting on its shoes".[40] In the early days of the telegraph, telephone and tabloid press at the end of the 19th century, and more than a century before the birth of cyberspace that now pervades the whole world, this witty statement was a particularly sophisticated insight into human nature and society, which unfortunately is still valid today. Needless to say, this global phenomenon, this human trait, poses a very serious social and political security risk, both for the leadership of countries as well as regarding the survival or disintegration of human communities. With regard to the unleashed flow of data and uncontrolled information sharing, we are faced with a dilemma from a moral-philosophical point of view similar to the one faced by the American nuclear physicists in July 1945. On the eve of the first use of the atomic bomb in World War II, several leading scientists of the top-secret Manhattan Project, led by the Hungarian Leó Szilárd, expressed their scientific and general moral concerns and reservations in a petition presented to President F. D. Roosevelt. They did not consider mankind to be mentally or morally prepared to use nuclear energy, especially not for the destructive purpose of war against civilian targets.[41]

Today's radically transforming digital ecosystem presents humanity with a similar, if not greater, and even more profound scientific-technological and socio-psychological challenge. After all, the purpose and method of using nuclear energy (and nuclear weapons) concentrated around a few dozen top decision-makers and experts in the last year of World War II, as it was the case during the long years of the Cold War, while today's secondary virtual universe is accessible to anyone, without any real safety valves and no limits to its use—either for good or evil. Just think of the untapped potential of artificial intelligence, or the vulnerabilities of critical infrastructures driven by computers that determine the basic needs, security and physical existence of our human societies.

It is on the level of imagination, but there are specific cases, for example, when a young Hungarian hacker from Transylvania, propelled by a narcissistic desire to show off (or by a reward of the Russian military intelligence service), hacks into the private correspondence and mobile phone of the US Secretary of State from Oradea with the help of a notebook and intermediate IT skills,[42], hacks into the control system of a thermal power plant responsible for the energy supply of hundreds of thousands of people, or the case of the 13-year-old boy who organised a far-right terrorist cell in the United States from an island in Estonia on the Internet.[43]

40 See Mark Twain quotes, http://www.twainquotes.com/Lies.html, accessed on 12.04.2020.

41 Leó Szilárd's letter of petition, http://www.dannen.com/decision/45-07-17.html, accessed on 12.04.2020.

42 Cimpanu, Catalin, 'Hacker Guccifer...', *Zero Day News*, https://www.zdnet.com/article/hacker-guccifer-who-exposed-clinton-private-email-server-ready-for-us-prison-sentence/, accessed on 14.04.2020.

43 Deutsche Welle News, 'Far Right Terrorist Ringleader found to be teenager in Estonia', https://www.dw.com/en/far-right-terrorist-ringleader-found-to-be-teenager-in-estonia/a-53085442, accessed on 15.04.2020.

The legendary US Army General Herbert Norman Schwarzkopf Jr. might have said, somewhat irritated, on the eve of the Gulf War in 1991 that "you can't fight a war with a goddamn laptop, only with bullets and bombs"[44] but today this statement is no longer appropriate, but neither was it applicable during the second Gulf War, already in 2003...

Surrounded by robots, at the dawn of Singularity?

"Who can say
Why Today Tomorrow will be Yesterday?"
Lord Alfred Tennyson, English poet

The security challenges posed by virtual networks and artificial intelligence, not to mention social problems or moral concerns, increasingly define everyday life in the 21st century. We have no answer to the poetic, philosophical question from 200 years ago, featured as the motto, nor do we know what to expect in the coming years and decades in terms of the changes, events and phenomena induced by technological development of an unimaginable scale. In the following pages, the author reviews the potential for self-driving smart devices, robots and artificial intelligence, and the technological development dimensions of defence. Furthermore, he seeks to answer the complex philosophical question of how useful or harmful this segment of the technological revolution can be for humanity.

In the 21st century generations are living and socialising as they are surrounded by fast, instant digital and Internet-based solutions, the young generation is growing up under the spell of revolutionary quantum computing and self-learning artificial intelligence that can answer almost any computational or prediction-related problems. Obviously, in the early days of the technological "magic" that we are witnessing today, users will not be thinking primarily about the downsides and negatives, as this is primarily the task of analysts and experts who are more sensitive and drawn to social and security issues. However, experience suggests that any tool or application that can be used for destructive purposes will be used unscrupulously by a significant proportion of people (states) to achieve their classic Hobbesian (self-interest-driven) goals. As Professor Waltzman and his colleagues have noted, the militarisation of information and digital solutions, the weaponisation of information has been happening for long decades, and cyberspace (as a theatre of war), or *cyborgs* and the artificial intelligence that controls them, cannot be exempt from its influence.[45] The latter, in particular, has given rise to much international debate and concern, although the theoretical debate and futurological thinking on the subject is much older than one might presume.

Concurrently with the birth of modern digital computing, towards the end of World War II, some scientists, in particular the British Alan Turing and the Hungarian American John von Neumann, began to think about the development of an artificial (machine) intelligence. The theoretical problems (and caveats) that they were pondering nearly a century ago have now become increasingly pressing technological and philosophical questions that have to be

44 R. A. Clarke, R. K. Knake, *Cyber War*, (2010), pp 19-21.
45 R. Waltzman, *Weaponization*, p. 28.

answered. For example, will artificial intelligence, which in 2020 is already capable of machine learning, achieve (or even surpass) the complexity and operational level of the human mind? If so (and why couldn't it happen?), the question is, when will this revolutionary "singular moment" occur in human history? Will the computer designer John von Neumann and his fellow American mathematician and science fiction writer Vernor Vinge prove right when they argued as early as the 1950s for a paradigm shift in technology and information technology—a certain technological singularity—which, if happened, they said, could end history as we know it[46].

According to Ray Kurzweil, the popular American engineer futurologist—who was also Google's first director of technical development and co-founder of the Silicon Valley Singularity Research University—the often referred to singularity, or even *human machine interface/interaction* (HMI), is inexorably approaching and it is expected to happen around 2045.[47] In his view, which many researchers agree with, that historical moment will mark the big moment of AI's coming of age and the beginning of the era of "humanity 2.0". Whether this event will be good or bad for us, well, that's another matter to be discussed extensively, but Kurzweil is clearly a committed advocate of the optimistic, people-friendly AI scenario.

Due to length limitations, the technological details about simple and *advanced AI* and the phases of its development will not be discussed, but this paper will briefly review the security policy and social, socio-psychological aspects that are closely related to robotics and the development of AI.

In recent years there has been a widespread reaction to comments made by renowned scientists and technological innovators who have publicly criticised the development of so-called human-substituting smart technologies, especially artificial intelligence and robotics. The late Stephen Hawking, world-famous British physicist and cosmologist, together with Martin Ford, American sociologist and AI researcher, as well as Elon Musk, entrepreneur and technological revolutionary, have argued that it is not advisable or even dangerous to experiment with technological solutions that can be used as weapons, that have undisclosed security risks and that could take millions of jobs if massively deployed.[48] Musk, the renowned manufacturer of self-driving cars (and space rockets), is quite critical and hostile to AI-controlled machines capable of autonomous decision-making, considering them more dangerous to human security than nuclear weapons of mass destruction.[49] In 2015, over a hundred acknowledged scientists and global technology entrepreneurs, led by Elon Musk, raised their voices and concerns in a joint manifesto against the use of AI-driven intelligent robots for military offensive purposes.[50]

A similar, albeit academically more sophisticated opinion was expressed much earlier by Professor Hawking, who pointed out the evolutionary contradiction of how a frail, mortal

46 Vernor Vinge, 'Technological Singularity', *Whole Earth Review*, (January 2003), http://cmm.cenart.gob.mx/delanda/textos/tech_sing.pdf, accessed on 05.04.2020.

47 Christianna Reedy, https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045, accessed on 15.04.2020.

48 Martin Ford, *Robotok kora*, p. 228.

49 Catherine Clifford, 'Musk: mark my word', *CNBC*, https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html, accessed on 15.04.2020.

50 Samuel Gibbs, 'Elon Musk leads 116 experts calling for outright ban of killer robots', *The Guardian*, (20 Aug 2017), https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-banlethal-autonomous-weapons-war, accessed on 11.03.2019.

human with limited mental abilities could compete with a metallic, much faster-minded, more intelligent artificial robot, a *cyborg*, especially if the creation could theoretically become even more perfect than its human creator?[51] Hawking also shared the views of the head of the British Government Communications and Intelligence Organisation (GCHQ) and the concerns of *Internet founders* Sir Berners-Lee and Vinton Cerf about the security risks of the web, which has become a global forum for cyber criminals and may even make the dystopian world of runaway or malicious AI as smaller concerns. According to the laws of humanistic robotics, dreamed up and formulated by the American master of science fiction Isaac Asimov and his friend John W. Campbell as early as in 1940,[52] a robot must not harm a human or turn against its creator. Unfortunately, these are only rules set on paper, they are completely useless and inapplicable in reality. Like most revolutionary technical scientific innovations, smart, self-propelled military (combat) devices and robots are primarily the product of the military defence technology sector, and have been designed by American, Russian, Chinese or Israeli military engineers for non-peaceful purposes for decades.

Russian President Putin's futuristic statement at a student science conference in 2017 went viral. He said that "In the 21st century, artificial intelligence will pose both an enormous opportunity and threat. It is the future not only for Russia, but for all states (...) in any case, the country that succeeds in mastering AI will also dominate the system of international relations".[53] Of course, this statement prompted many heads of state and researchers to pay attention, given the facts that in line with the Russian Federation's cyber strategy, there are several special military projects that deal with the specialised uses of robotics and artificial intelligence,[54] although there is no reliable data on the nature and development level of Russian defence research due its confidential nature. At the same time, the press début of FEDOR in 2017, a Russian humanoid robot for aerospace applications—with a revolver in its hand—spoke louder than any words[55].

Compared to Russian AI and robotics research, the American and Chinese efforts are likely to be far more advanced, especially given the gigantic scale of public achievements and financial resources invested. In terms of technological and scientific military developments China wants to become the world's number one and most advanced AI manufacturer and user by 2030, overtaking the United States. To achieve this ambitious goal, China allocates around $7-10 billion a year, and with over $2 billion funding, the world's largest 55-hectare AI research centre has been built outside Beijing, where tens of thousands of scientists, engineers and computer scientists are researching *deep and machine learning*, artificial intelligence, cloud *computing services* and *big data* applications.[56]

---

51 Rory Cellan-Jones, 'Stephen Hawking warns A.I. could end mankind', *BBC*, https://www.bbc.com/news/technology-30290540, accessed on 15.04.2020.

52 Isaac Asimov, *Én, a robot*, (Móra Kiadó, 1950).

53 James Vincent, 'Putin says on AI...', *The Verge*, https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world, accessed on 11.12.2019.

54 Bilyana Lilly, Joe Cheravitch, *The Past, Present and Future of Russia's Cyber Strategy and Forces*, (NATO CCDCOE, Tallinn, 2020), p. 149.

55 See FEDOR Russian robot press conference https://nerdist.com/wp-content/uploads/2017/06/FEDOR-Feature-Image-06212017.jpg, accessed on 08.03.2019.

56 David Cyranoski, 'China enters the battle for AI talent', *Nature*, (15 January 2018), https://www.nature.com/articles/d41586-018-00604-6, accessed on 07.03.2019.

Given the political context of China's dictatorial one-party system, there are serious human rights and moral concerns with the 2014 introduction of the so-called *Social Credit System*, which is the individual assessment system of China that is even more impersonal than the Orwellian dystopia. With the help of over 500 million public cameras and AI-based *big data analytics* algorithms, 450 million individual assessments have been carried out so far, and by 2020, more than 5 million unreliable Chinese citizens have been filtered out by the system, in accordance with the interests of the Chinese Communist Party and its distorted security concerns that violate basic human rights.[57] The fate of those "filtered out" is highly questionable and difficult to track, as they have become disenfranchised citizens—stripped of their rights—in the country with the world's largest population and highest level of digital control.

It is fully understandable that cyber warfare and the application of artificial intelligence is specified as important objectives of the US defence and national security strategy, along with the need to contain and counter the efforts of hostile state and sub-state actors.[58] The United States, which conducts extensive research in this area in the amount of $100 billion a year,[59] already considers China its number one economic and military rival in their struggle for remaining or becoming the superpower, including cyber warfare and AI research. Therefore, the US administration seeks and expects defence and research cooperation with all possible allies, primarily within NATO, in order to achieve the *cyber containment* of China and secondarily that of Russia, as well as other smaller, but dangerous state actors such as Iran or North Korea.[60] Former US Secretary of Defence, Chuck Hagel, in his 2014 presentation on the "Third Offset Strategy", stated that smart device solutions, in particular applications involving artificial intelligence, are at the forefront and going to define defence technologies in the 21st century.[61] According to him, the United States, through the world's largest scientific-technological research organisation, the Pentagon, withholds no research expense and dedication to maintain the American strategic primacy and dominance in this field. In the US, hardware manufacturing is pioneered by giants such as Boston Dynamics, Texas Instruments, Lockheed Martin, Boeing, Raytheon, Space X, while artificial intelligence and software development is led by research centres such as MIT, NASA, Google, Apple and Microsoft. In fact, the activities of all major scientific technology players are determined by the trend-setting base research conducted at the Pentagon's Defence Advanced Research Projects Agency, or DARPA, which is the cradle of the Internet.

A telling statistic of this era is that in almost a decade, the US Air Force has more unmanned combat aerial vehicle or remotely piloted aircraft pilots (nearly 2,000) than it has actual active-duty combat pilots (1,700).[62] The '*eyes in the sky*', such as the iconic *MQ-1 Predator, MQ-4*

57 Nicole Kobie, 'The complicated truth about China's social credit system', *Wired*, https://www.wired.co.uk/article/china-social-credit-system-explained, accessed on 11.04.2020.

58 US National Security Strategy, 2017 and National Defence Strategy of the U.S., (Washington D.C., 2018).

59 The National Artificial Intelligence Research and Development Strategic Plan, NSTC NITRD, (October 2016), https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf, accessed on 28.02.2020.

60 Yasmin Tadjdeh, 'DoD seeks alliance to counter China and Russia', *National Defense*, https://www.nationaldefensemagazine.org/articles/2020/3/3/algorithmic-warfare-dod-seeks-ai-alliance-to-counter-china-russia, accessed on 16.04.2020.

61 Chuck Hagel, '*A game-changing third offset strategy*', https://warontherocks.com/2014/11/a-game-changing-third-offset-strategy/, accessed on 15.11.2019.

62 'US Drone Milestone...', *The Military*, https://www.military.com/daily-news/2017/03/08/drone-milestone-more-rpa-jobs-any-other-pilot-position.html, accessed on 25.11.2019.

Global Hawk or the dreaded *MQ-9 Reaper*, are controlled from the Nevada desert container control centres in the US, and they can carry out surveillance or precision strike engagement missions anywhere in the world. In the 12 years of the Obama and Trump administrations, this is exactly what has happened, more than 2,000 times, against targets in Yemen, Somalia, Pakistan, Afghanistan, Iraq and Syria.[63]

The scope of advocating one's great power naturally extends to the new theatre of war, to cyberspace, but ever since 2019 even to outer space,[64] as well as to the closely related robotic and artificial intelligence solutions and devices.

Following the development trend of air and water drones, and the increasing influence and complexity of AI, many military analysts raise the potential security and moral risks of a scenario where a target (human or object) found and analysed by the reconnaissance drone is then destroyed by the also self-propelled air or water drone, without no human intervention whatsoever.[65] Given the current structure of the *command-and-control* as well as the communication system and hierarchy of the chain of command, this would be unimaginable today, but in light of the current trends, it cannot be excluded in the near future, which could result in a major paradigm shift in both our legal and moral systems.

Apart from the purely military aspects, robots and self-driving AI-based technological solutions can obviously cause social unrest, resentment and political upheaval. The first major concern could be that machine intelligence and humanoid smart robots actually substitute humans. Many experts and politicians agree with the controversial idea of introducing a universal basic income. One such person is Martin Ford, a sociologist and researcher on robotics, who expressed his support in his influential bestseller on the topic.[66] These people argue that this very equitable, unique social solution could adequately, but only partially, remedy the plight of millions who are becoming unemployed in the 21st century. In fact, Pope Francis, the head of the Roman Catholic Church, believes that in the short and medium-term it may be the most effective way to alleviate the massive unemployment caused by the global economic recession in the wake of the 2020 coronavirus pandemic.[67]

According to American labour market surveys and sociological calculations, in the developed world (mainly in the United States and Canada), one third of today's jobs and professions are at risk of being lost, and nearly 60% of adult workers with only secondary education are at risk of losing their jobs due to outsourcing and automation in the near future, which could lead to unprecedented tensions, conflicts, economic and political crises[68].

Unsurprisingly, the followers of the infamous English Luddites of the early 19th century (who destroyed machines)[69] are once again enjoying popularity in our days. There are

63 'Obama's Covert Drone War in Numbers', *Bureau of Investigative Journalism*, (2017), https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush, accessed on 29.12.2019.

64 On 20 Dec 2019, the *US Space Force* was created as the sixth independent US military force responsible for space as a war theatre, https://www.spaceforce.mil/About-Us/Fact-Sheet, accessed on 15.04.2020.

65 Imre Porkoláb, 'Digitális katona' (Digital soldier), TEDx, Győr, (2019).

66 Martin Ford, *Robotok kora*, p. 294.

67 Wooden, Cindy, 'Pandemic is time to consider "universal basic wage," Pope says', CruxNow, (April 2020), https://cruxnow.com/vatican/2020/04/pandemic-is-time-to-consider-universal-basic-wage-pope-says/, accessed on 14.04.2020.

68 Michael Webb, The Impact of AI on Labor Market, (Stanford University Press, January 2020), pp. 21-25.

69 With the instigation of Ned Ludd or Ludland (provided he ever existed), between 1799 and 1817 groups of masked men regularly smashed up textile spinning and weaving machines in England. Evan Andrews, 'Who were the Luddites?', https://www.history.com/news/who-were-the-luddites, accessed on 02.04.2020.

hundreds of thousands of people who joined the neo-Luddite *off-the-grid*, *into the woods* movement, mainly in the territory of the United States and Canada.[70]

In our rapidly changing and crisis-ridden world, anti-technological violence, even anarcho-terrorist actions cannot be fully excluded in the future if the aforementioned pessimistic labour market and technological forecasts become a reality or if they are not addressed by the leaders in a satisfactory manner.

However, not forgetting the risks and negative aspects, modern technologies and AI applications are not at all from the devil, since in an optimistic and technology-friendly interpretation, as advocated by the world-famous Japanese American astrophysicist Michio Kaku, they can make our lives much better and easier, help us to scientifically unravel the mysteries of the universe, not to mention other achievements in nanotechnology medicine or computing.[71]

Final thoughts

As seen above, we may have reviewed several segments of cyberspace digital applications and the human, social and security aspects of artificial intelligence and robotics, there are still many issues in the digital ecosystem or cyber matrix that remain unmapped and on which it might be important to make analytical, critical observations and to conduct in-depth research. Another important topic worthy of attention and research is the phenomenon of social media platforms and disinformation campaigns, fake news, which distort society and might even threaten democracy, and which may be used as a serious influencing tool or even as a soft weapon in the hands of state and non-state actors.

In conclusion, cyberspace dominated by computer systems has also become a war zone in the 21st century, and digital information can also be used as a weapon in the hands of state and non-state actors for political and other purposes. In a new paradigm shift, the world of book- and paper-based written communication and knowledge transfer has become electronic, digital and virtual, as once pictured by John von Neumann or Isaac Asimov. At the same time, the world of the Internet knowledge has not really evolved over the last three decades in the well-intentioned, idealistic way that its scientific creators had envisioned. Historical experience and anthropological pessimism compel us to say that almost all outstanding technological inventions have been used for strategic defence or offensive and destructive purposes, in accordance with the basic human trait. This is of course the case even for machine or advanced artificial intelligence and robotics, which will revolutionise not only warfare, but also our everyday lives, the labour market and human civilisation, as John von Neumann or Ray Kurzweil have explained.

On the basis of the opinions of the above-mentioned scientific experts and sharing Professor Hawking's concerns, we can say that humanity is not prepared for the challenges posed by 'overdeveloped artificial intelligence' and especially for its non-military applications,

70 John Bartlett, 'Will 2018 be the year of the neo-luddite?', *The Guardian*, https://www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite, accessed on 16.04.2020.

71 Michio Kaku, *Az emberiség jövője*, (Akkord, Budapest, 2019), pp. 110-126.

which could carry unforeseeable risks, even greater than nuclear weapons, and that the UN General Assembly should therefore also adopt a resolution condemning the deployment of killer robots (killbots). Also in this context, the research scandal involving the US Department of Defence and Google's AI-based robot technology received a lot of press coverage because of the moral and security risks posed by 'killer smart devices, robots'.[72]

As the fathers of the Internet bitterly noted, the information superhighway and the cyberspace that has been built on it have sadly become filled with mostly negative, harmful and destructive content, and cybercrime has become the number one and most damaging type of crime in the world in just a few years. It seems that even in the midst of a devastating coronavirus pandemic, criminal groups are not at rest, and they are still attacking biological research laboratories and hospitals with incredible ransomware programs even in these trying times.[73]

Seeing the global trend of digital mediatisation, we find contradiction in the dominance of social media platforms, multimedia information sharing applications and the influence of *vlogger* influencers, which have become the absolute primary sources of information for the Z and alpha generations of cyber age, even over the school and family media.[74] Every day, new digital information is being generated at a scale and in a volume that is incomprehensible and perplexing to the human mind, making it even more difficult for users to find their way around. From a psychological point of view, this can often lead to confusion, disinformation, individual and collective frustration and alienation, as well as to a comfortable but distorted world of virtual echo chambers, which may even endanger social peace and political order.

The development of cyberspace applications and machine intelligence seems to be unstoppable, which in itself poses security risks, not to mention the number of technology users with bad intentions, whose numbers we can only estimate when exact figures or statistics are not really available.

Renowned American Professor of philosophy and risk analyst Nassim N. Taleb evaluated that the technological complexity and the myriad of social and natural variables and unknown factors will lead to an increasing number of unknown and unpredictable global crises (the so-called 'black swan' phenomenon) or security challenges and problems that are downplayed and considered unrealistic ('grey swan').[75] Whether it is a pandemic of biological origin (a coronavirus), a small planetary impact, a widespread regional or continental blackout, not to mention the proliferation of much more realistic, devastating cyber crimes, or the impending singularity of artificial intelligence and its as yet unforeseen consequences.

One of the most difficult challenges for mankind is to find a way out of the technological trap outlined in the study and to find a user-friendly solution, for which there are two main options in simple terms. On the one hand, by restricting or fully banning access to technology,

72 Henry McDonald, 'Ex Google worker fears "killer robots" could cause mass atrocities', *The Guardian*, (Sept 2019), https://www.theguardian.com/technology/2019/sep/15/ex-google-worker-fears-killer-robots-cause-mass-atrocities, accessed on 04.12.2019.

73 See in https://healthitsecurity.com/news/560-healthcare-providers-fell-victim-to-ransomware-attacks-in-2020, accessed on 01.02.2021.

74 Greg Jarboe, 'Generation Z can't live without YouTube', *Tubular Insights*, (June 2017), https://tubularinsights.com/generation-z-youtube/, accessed on 16.04.2020.

75 Nassim Nicholas Taleb, *The Black Swan*, (New York, Random House, 2010), pp. 189-195.

which is a dictatorial and counter-productive evil, and on the other hand, by developing a clear and strict legal framework for digital media service providers and machine intelligence applications in cyberspace, to protect users and universal human values and interests, complemented by cybersecurity education, media literacy, critical thinking and net etiquette training in formal school and digital education.

It can be concluded that by teaching and practising critical and analytical thinking, many cybersecurity and social problems can be easily and effectively addressed for the broad masses of society. However, this requires the application of measured rationality on the part of decision-makers and users, and the separation of goals (e.g. humane social, scientific progress) and not their interchange with means (digital technologies, robotics, AI), in order to avoid Einstein's and Bertrand Russell's prophetic statement that a world of smart technology could lead to a dumbed-down and increasingly comfortable humanity.

Bibliography

1. Asimov, Isaac, 'Visit to the World Fair of 2014', *The New York Times*, (16 August 1964), http://www.nytimes.com/books/97/03/23/lifetimes/asi-v-fair.html, accessed on 02.12.2019.
2. Asimov, Isaac, *Én, a robot*, (Móra, Budapest, 1991).
3. Andrews, Evan: *Who were the Luddites?* https://www.history.com/news/who-were-the-luddites, accessed on 02.04.2020.
4. Bartlett, Jamie, 'Will 2018 be the year of the neo-Luddites?', *The Guardian*, https://www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite, accessed on 16.04.2020.
5. Blank, Stephen, *Web War I: Is Europe's First Information War a New Kind of War?*, https://www.tandfonline.com/doi/full/10.1080/01495930802185312, accessed on 12.01.2020.
6. Brent, Laura, 'NATO's role in cyberspace', *NATO Review*, (Feb 2019), https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html, accessed on 29.12.2019.
7. Bureau of Investigative Journalism, 'Obama's drone strikes', https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush, accessed on 29.12.2019.
8. Carr, Nicholas, *The Shallows: What the Internet is doing to our Brains* (W. Norton, New York, 2011).
9. Chen, Hsinchun, *Dark Web: Exploring and Data Mining the Dark Side of the Web* (Springer, New York, 2012).
10. Clifford, Catherine, 'Musk: mark my word...', *CNBC*, https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html, accessed on 19.03.2020.

11. Cimpanu, Catalin, 'Hacker Guccifer..', *Zero Day News*, https://www.zdnet.com/article/hacker-guccifer-who-exposed-clinton-private-email-server-ready-for-us-prison-sentence/, accessed on 14.04.2020.
12. Clarke, Richard A., Knake, Robert K., *Cyber War: The Next Threat to National Security and What to Do About It*, (Harper Collins, New York, 2010).
13. Cyranoski, David, 'China enters the fray for AI talent', *Nature*, (15 January 2018), https://www.nature.com/articles/d41586-018-00604-6, accessed on 07.03.2019.
14. Deutsche Welle English News, 'Far-Right Terrorist Ringleader', https://www.dw.com/en/far-right-terrorist-ringleader-found-to-be-teenager-in-estonia/a-53085442, accessed on 15.04.2020.
15. Esteves, Olivier, 'Bertrand Russell: the utilitarian pacifist', *French Journal of British Studies*, XX-1/(2015), https://journals.openedition.org/rfcb/308, accessed on 25.03.2020.
16. Galeon, Dom, Reedy, Christianna, 'Kurzweil Claims That the Singularity Will Happen by 2045', *Futurism*, (5 October 2017), https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045/, accessed on 22.12.2019.
17. Gibbs, Samuel, 'Elon Musk leads 116 experts calling for outright ban of killer robots', *The Guardian*, (20 August 2017), https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-banlethal-autonomous-weapons-war, accessed on 10.11.2019.
18. Gibson, William, 'Cyberspace', *Technovelgy* online sci-fi magazine, http://www.technovelgy.com/ct/content.asp?Bnum=53, accessed on 25.12.2019.
19. Gomichon, Maxime, 'Joseph Nye on Soft Power', *E-International Relations*, (8 March 2013).
20. Hagel, Chuck, 'A game-changing third offset strategy', https://warontherocks.com/2014/11/a-game-changing-third-offset-strategy/, accessed on 15.11.2019.
21. Haig, Zsolt, *Információs műveletek a kibertérben* (Information operations in cyberspace), (Dialóg Campus, Budapest, 2018).
22. Haig, Zsolt & Kovács, László, 'Fenyegetések a cybertérből' (Threats from cyberspace), *Nemzet és Biztonság Journal*, (2008/5), p. 63.
23. Haizler, Omry, 'The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking', *Cyber, Intelligence, and Security*. Vol. 1, No.1., (January 2017).
24. Harari, Yuval: *Homo Deus – a holnap rövid története*, (Animus, Budapest, 2017).
25. Häußler, Ulf: 'Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO's Treaty', https://www.sbs.ox.ac.uk/cybersecuritycapacity, accessed on 10.01.2020.
26. Ford, Martin, *Robotok Kora*, (HVG Könyvek, Budapest, 2016).
27. Greenwald, Glen, *A Snowden-ügy*, (HVG Könyvek, Budapest, 2014).
28. Jarboe, Greg, 'Generation Z can't live without YouTube', *Tubular Insights*, (June 2017), https://tubularinsights.com/generation-z-youtube/, accessed on 16.04.2020.
29. Jones, Rory Cellan, 'S. Hawking warns A.I. could end mankind', *BBC News*, https://www.bbc.com/news/technology-30290540, accessed on 15.04.2020.

30. Kaczysnki, Ted, 'The Unabomber Manifesto', *Washington Post Special Edition*, (22 Sept 1995), https://www.washingtonpost.com/wp-srv/national/longterm/unabomber/manifesto.text.htm, accessed on 11.04.2020.
31. Kaku, Michio, *Az emberiség jövője*, (Budapest, 2019).
32. Kaplan, Jerry, *Artificial Intelligence*: What Everyone Needs to Know, (Oxford University Press, New York, 2016).
33. Khanna, Parag, *Konnektográfia*, (HVG, Budapest, 2017).
34. Kobie, Nicole: 'The complicated truth about China's social credit system', *Wired Magazine*, https://www.wired.co.uk/article/china-social-credit-system-explained, accessed on 11.04.2020.
35. Krekó, Péter, *Tömegparanoia* (Mass paranoia), (Athaeneum, Budapest, 2018).
36. Krekó, Péter: 'Netes konteók' (Conspiracy theories on the net), Index TNT Podcast, https://index.hu/techtud/2020/04/12/tnt_osszeeskuves_kreko_peter_podcast/, accessed on 12.04.2020.
37. Lilly, Bilyanna & Cheravitch, Joe, *The Past, Present and Future of Russia's Cyber Strategy and Forces*, (NATO CCDCOE, Tallinn, 2020), p. 149.
38. Leigh, D, Harding, L., *WikiLeaks-akták*, (Geopen, Budapest, 2011).
39. Mazarr, Michael J., Bauer, Ryan, Casey, Abigail, Heintz, Sarah and Matthews, Luke J., *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*, (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2714.html, accessed on 10.03.2020.
40. Military, 'US Drone Milestone...' *The Military*, https://www.military.com/daily-news/2017/03/08/drone-milestone-more-rpa-jobs-any-other-pilot-position.html, accessed on 25.11.2019.
41. Molander, Roger C., Riddile, Andrew, Wilson, Peter A., *Strategic Information Warfare: A New Face of War*, (Santa Monica, CA: RAND Corporation, 1996), https://www.rand.org/pubs/monograph_reports/MR661.html, accessed on 11.03.2020.
42. Munk, Sándor, 'A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései' (Some issues for a common understanding of the concept of cyberspace), *Hadtudomány Journal*, (2018/1)
43. Newton, Casey, 'Lessons from Zuckerberg's Senate Hearing', https://www.theverge.com/2018/4/10/17222444/mark-zuckerberg-senate-hearing-highlights-cambridge-analytica, accessed on 10.12.2019.
44. NSTC NITRD, *The National Artificial Intelligence Research and Development Strategic Plan*, (October 2016), https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf, accessed on 28.02.2020.
45. Porkoláb, Imre, 'Digitális katona' (Digital soldier), TEDX Győr, (2019).
46. Póti, László (editor), *Nemzetközi Biztonsági Tanulmányok (Studies on International Security)*, (Zrínyi, Budapest, 2006).
47. Reedy, Christianna: 'Kurzweil on Singularity', *Futurism*, https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045, accessed on 15.04.2020.

48. Schaeffer, Katherine, 'COVID-19 origins', *FactTank* https://www.pewresearch.org/fact-tank/2020/04/08/nearly-three-in-ten-americans-believe-covid-19-was-made-in-a-lab/?utm_source=Pew+Research+Center&utm_campaign=9a8a1fc2a0-EMAIL_CAMPAIGN_2020_04_09_06_59&utm_medium=email&utm_term=0_3e953b9b70-9a8a1fc2a0-400906701, accessed on 12.04.2020.
49. Statista 1, https://www.statista.com/topics/1145/internet-usage-worldwide/, accessed on 15.01.2020.
50. Statista 2, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide, accessed on 28.01.2020.
51. Statista 3, 'Data volume of global consumer IP traffic from 2015 to 2021' https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic, accessed on 26.12.2019.
52. Strauss, Leo & Cropsey, Joseph, *A politikai filozófia története I.*, (Európa, Budapest, 1994).
53. Szilárd, Leó, 'Petíciós levél Roosevelt elnökhöz', (Washington D.C.) http://www.dannen.com/decision/45-07-17.html, accessed on 12.04.2020.
54. O'Neill, Patrick Howell, 'The cyber attack that changed the world', *The Daily Dot*, (2016), https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/, accessed on 08.10.2019.
55. Tadjdeh, Yasmin, 'DoD seeks alliance to counter China and Russia', *National Defense*, https://www.nationaldefensemagazine.org/articles/2020/3/3/algorithmic-warfare-dod-seeks-ai-alliance-to-counter-china-russia, accessed on 16.04.2020.
56. Taleb, Nassim Nicholas, *The Black Swan*, (Random House, New York, 2010).
57. Toonders, Joris, 'Data Is the New Oil of the Digital Economy', *Wired Magazine*, (July 2014), https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/, accessed on 25.01.2020.
58. Vinge, Vernor, 'Technological Singularity', *Whole Earth Review*, (January 2003), http://cmm.cenart.gob.mx/delanda/textos/tech_sing.pdf, accessed on 21.12.2019.
59. Vincent, James, 'Putin says on AI...', *The Verge*, https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world, accessed on 11.12.2019.
60. Waltzman, Rand, *The Weaponization of Information*, (Rand Corp., Santa Monica CA, 2017).
61. Warren, Tom 'The Cambridge Analytica Scandal', *The Verge*, (April 2018), https://www.theverge.com/2018/4/10/17165130/facebook-cambridge-analytica-scandal, accessed on 10.12.2019.
62. Webb, Michael, *The Impact of AI on Labor Market*, (Stanford University Press January 2020).
63. Wooden, Cindy, 'Pope on universal basic wage', *CruxNow*, (April 2020), https://cruxnow.com/vatican/2020/04/pandemic-is-time-to-consider-universal-basic-wage-pope-says/, accessed on 14.04.2020.

Áron Drabancz – Nedim Márton El-Meouch

The future of cyberspace, or examination of the state's cyber defence in a theoretical model framework

Resume

The study shows how technological developments have contributed to the proliferation of cyber warfare. In the framework of an optimality model, we have pointed out that the future cyberactivity of states may increase sharply (Nash equilibrium), moving further and further away from the pacifism that provides the welfare optimum. The introduction of sufficiently large and coordinated global sanctions could reduce countries' cyberactivity, but its feasibility is questionable.

Executive summary

Technological advances in computing power, the Internet of Things and artificial intelligence have made cyber warfare one of the most significant new forms of warfare. Based on our optimisation framework, cyberactivity and the resulting welfare losses could increase further in the future, and only the introduction of a sufficiently large and coordinated global sanctions regime would be able to slow down the process significantly.

"War is no longer declared, only continued"
Ingeborg Bachmann

Introduction

The first generation of computers, which appeared in the Second World War, have evolved continuously to the present day: from clumsy and slow machines the size of a room to fast and cheap ones, now available to everyone, which fundamentally alter our world. Increases in computing power and advances in software now allow computers to play an increasingly important role in areas previously unimaginable: the basic structure of mobility may be changed by the fully self-driving vehicles of the future, and workflows will be rewritten by the latest optimisation techniques based on artificial intelligence, which will require less and less human intervention in the monotonous, well-structured tasks. Technology is also becoming increasingly important for the armed forces: the US military now has partially self-guiding drones flying in foreign airspace,[1] and artificial intelligence can use satellite imagery and weather data from previous years to predict where drought, extreme weather and potentially turbulent political situations are likely to occur.[2]

The digitisation of activities is set to accelerate even further in the future: the complexity of integrated circuits continues to double every 18-24 months, based on Moore's Law,[3] the number of sensors providing data is growing exponentially,[4] and in 2019 Google announced its quantum supremacy, building a quantum computer with capabilities far beyond the upper limits of classical computing.[5]

Technological changes mean that the acquisition or manipulation of other countries' data gives the data controller significant power. The escalation of the situation is demonstrated by the growing number of cyber attacks against an increasing number of targets around the world, with key infrastructure and technology now being targeted alongside government institutions. Due to the lack of international regulations and the difficulty of deconstructing attacks, even serious cyber attacks are not usually considered an act of war, but rather a grey area, below the threshold of (classic) war, in the eyes of the international community.[6]

Our thesis is that in the future, the activity of cyberspace as a tactical space and the damage it causes will increase, making the problem of cyber warfare more and more important from a global perspective, due to its increasingly negative contribution to global well-being. To prove the thesis, we first briefly outline the technological, economic and social processes that are driving the digitalisation of the world and the increasing data-centricity, and how these should change the way societies and governments approach data protection in the future.

1 Gilmore, C. K., Chaykowsky, M., Thomas, B., (2019), *Autonomous Unmanned Aerial Vehicles for Blood Delivery: A UAV Fleet Design Tool and Case Study*, (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR3047.html, accessed on 15.06.2020.

2 Descartes Lab, (2020), https://www.descarteslabs.com/#overview, accessed on 15.06.2020.

3 Takahashi, D., (2017), https://venturebeat.com/2017/03/28/intel-moores-law-isnt-slowing-down/, accessed on 15.06.2020.

4 Dahlqvist, F., Mark Patel, M., Alexander Rajko, A., Shulman, J., (2019), 'Growing opportunities in the Internet of Things', https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things#, accessed in 15.06.2020.

5 Szepesi, A., 'Holnaptól borul a fél világ? Mit jelent a kvantumfölény, mire számíthatunk ezután?', (2019), (Half the world will be upended from tomorrow. What does quantum supremacy mean and what can we expect next?), https://hvg.hu/tudomany/20191028_google_sycamore_kvantumfoleny_jelentese_hogyan_mukodik_kvantumszamitogep_mukodese_egyszeruen_qubit_kubit_ibm_summit_szuperszamitogep, accessed on 15.06.2020.

6 Porche, I. R. III, (2019), 'Fighting and Winning the Undeclared Cyber War' https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html, accessed on 15.06.2020.

We then use a dynamic optimisation model framework to estimate how the growing number and increasing importance of electronic devices may make it more difficult for governments to protect our data. Chapter 2 describes the main technology trends related to this issue, followed by a discussion of the main concepts related to cyber warfare in chapter 3. In chapter 4, the elements of the dynamic optimisation model framework and the results under different scenarios are presented. In the final chapter, we summarise the results of the study, point out their limitations and formulate directions for further work in the field.

Technological development

In the context of technological development, we will explore the idea that, due to the dynamic technological developments of the last decades, computers are now able to process large amounts of unstructured data at once, which is a hotbed for the proliferation of online warfare. On the one hand, the computing capacity of computers has increased, on the other hand, more and more devices are providing digital data and the technology for processing data is becoming more advanced. The parallel evolution of these three factors has brought the solution of previously unfathomably difficult problems within reach. The aim of this chapter is to briefly describe the evolution of the three factors in recent years and possible future trends.

Computing capacity

Moore's Law is worth mentioning in the context of the computers' increased computing power. In line with this, the complexity of integrated circuits doubles every 18 to 24 months, meaning that the computing power you can buy for $1000 doubles every 1.5 to 2 years. It has been a fair description of the trends over the past decades (see Figure 1), which represents an outstanding improvement in computing capacity. To illustrate this, if you invested just $2 in 1920 and your return on investment followed Moore's Law, the value of your investment in 2014 would be roughly equal to the world's GDP, and today it would be sixteen times higher.[7] The example shows that the doublings in recent years have already taken place at a relatively high-level of capacity, so the jumps here can be considered as truly significant.

7 Own calculation from IMF (2020) data: https://www.imf.org/external/index.htm, accessed on 15.06.2020.

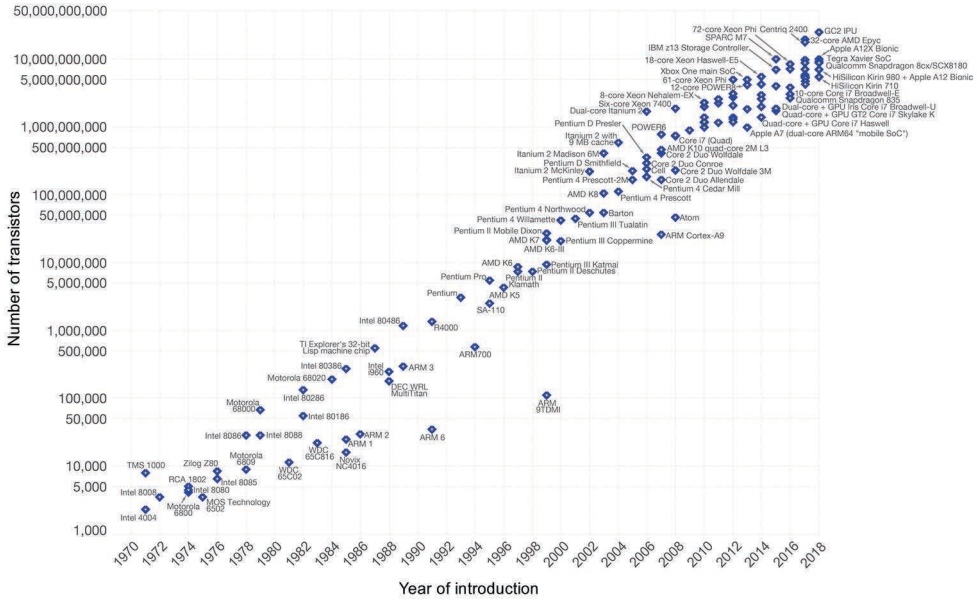


Figure 1. Growth in the number of transistors 1970-2018
(Source: Our World in data, 2020)

The Internet of Things

In parallel, the number of devices that can recognise and share essential information with another device on an Internet-based network, the Internet of Things (IoT), is also growing significantly around the world. The devices we wear on our bodies (e.g. smart watches), the smart sensors in our homes and the real-time monitoring of ever smaller industrial devices are all generating an increasing amount of data in cyberspace. The technology is based on RFID, which uses a radio frequency electromagnetic field to transmit data to the RFID reader. Falling prices allow more and more devices to be equipped with sensors, "smartened up" and connected via the Internet. Ericsson (2016) estimates that the number of IoT devices may grow by 21% per year between 2016 and 2022, with nearly 30 billion connected devices in the world by 2022.[8] Business Insider (2019) reports that the growth may be even more significant, estimating 64 billion IoT devices by 2025.[9] The proliferation of devices is helped by the rollout of the 5G network in the 2020s, which promises to be a major leap in data speed, efficiency, reliability, capacity and security, and is expected to open up new opportunities for IoT devices. With the significant increase in the number of devices and the amount of transmitted data, the security of data and the exposure of networks and devices to cyber attacks now frequently becomes an issue.

8 Ericsson, (2016), *Ericsson Mobility Report (2016 November) – on the pulse of the networked society*, https://www.ericsson.com/en/mobility-report/reports, accessed on 15.06.2020.

9 Business Insider, (2019), 'IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers', https://www.businessinsider.com/internet-of-things-report, accessed on 15.06.2020.

Artificial intelligence

The huge amount of data produced by different devices and the exponential increase in the computing power of computers alone are not enough to extract quality information from the available data, and algorithms for artificial intelligence and machine learning are also needed as a third component. Research into artificial intelligence began already in the 1950s, but after an initial boom, progress stalled in the second half of the 20th century, which the literature termed as the *winter of artificial intelligence*. The reason for this is precisely the stagnation in the development of the very factors that drove the resurgence of the artificial intelligence trend in the 2010s, which is now taking off with renewed vigour: the growth of data and computing power as well as cheap access to them.

Today, the biggest breakthrough in artificial intelligence is the ability to mine information autonomously on unstructured data, even without supervision. The most common examples of unstructured data are visual, audio and written data sources, and the best example of combining these is the data that can be extracted from social networking activity, which is often the target of cyber attacks. A good example is the Russian interference in the 2016 elections in the United States of America. Users were then manipulated by politically motivated messages targeted at them based on their activity on social networking sites, in an attempt to (successfully) shift or discredit their beliefs and voting preferences.[10] Artificial intelligence was essential to enable them to map voters well and accurately, using data from their social networking sites, on the contentious issues that are vital to their lives.

In addition, the machine learning algorithms behind artificial intelligence can also play a crucial role in protecting against cybercrime, including by helping to detect potential threats early enough to counter-attack suspicious (outlier) software, which behave in a conspicuous manner, different from the norm, before the problem grows out of proportion.[11] The main advantage is that the firewall can adapt in real-time without human intervention, based on incoming data, making it more flexible and at the same time more effective in blocking incoming attacks automatically.[12]

In the future, it is expected that individual entities will use artificial intelligence to defend themselves against incoming AI-driven attacks.[13] According to a survey of 850 business leaders conducted by Capgemini Research Institute (2019), the majority of these managers believe that AI is improving cyber defence by reducing the cost of detecting and responding to leaks (64 percent of respondents), enabling faster response times (74%) and helping to identify leaks more accurately (69%). In addition, the survey found that 63% of the companies

10 Bodine-Baron, E., Helmus, T. C., Radin, A., Treyger, E., (2019): *Countering Russian Social Media Influence*, (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR2740.html, accessed on 15.06.2020.

11 Ramachandran, R., (2019), 'How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks', https://www.entrepreneur.com/article/339509, accessed on 15.06.2020.

12 Cyber Security Intelligence (2019), 'The Future of Cyber Security Is AI', https://www.cybersecurityintelligence.com/blog/the-future-of-cyber-security-is-ai-4550.html, accessed on 15.06.2020.

13 Columbus, L., (2019), '10 Predictions How AI Will Improve Cybersecurity In 2020', https://www.forbes.com/sites/louiscolumbus/2019/11/24/10-predictions-how-ai-will-improve-cybersecurity-in-2020/#56712eb96dd7, accessed on 15.06.2020.

plan to implement AI-based cyber defence in their organisation.[14] In summary, we are at the beginning of a new era in which the computing processes applied will have a significant impact on the success of individual companies.

The age of cyber warfare

The exact scope of cyberspace and cyber warfare is difficult to define, but we believe that as more and more activities move online, the costs of this form of warfare could rise significantly. One of the main conclusions from the previous chapter points to this, as the results of information technology developments are increasingly shaping our everyday lives. In addition, in the 21st century, the activities of the economy and civil society have grown more extensive and diverse, and the state can no longer guarantee the protection of these activities by traditional means. In cyberspace, enemy forces are leapfrogging the traditional 20th century front lines and reach directly into the hinterland. The accelerating technological transformation is also reinforcing the restructuring of the elements of war: cyber defence has been included by NATO in its collective defence tasks, so that an attack against one member state of the Alliance can be interpreted as an attack against the Alliance as a whole.[15] The World Economic Forum's annual global economic ranking also ranks cyberspace threats higher. While in 2015, data theft and cyber espionage risks were the 9th and 10th most likely major risks in the world, in the 2019 report these were ranked 4th and 5th. In addition, the collapse of critical information infrastructure that is essential for the functioning of the state has now become a major risk.[16] Cybercrime has therefore started to cause significant economic damage, with Lewis (2018) estimating that the damage is now close to 1% of annual global GDP and growing continuously.[17] This is not a surprising amount given that computers with Internet access may suffer attacks every 39 seconds on average, and 62% of companies have experienced a phishing attempt in recent years.[18] The aim of this chapter is thus to briefly introduce the key concepts of cybersecurity, review the major cyber risks and introduce the concept of critical infrastructures.

To understand cyber warfare, it is important to clarify the 'theatre of war', where the attacks take place. Cyberspace is defined in the 2013 Hungarian National Cybersecurity Strategy as '... the set of globally interconnected, decentralised, and growing electronic information systems and the social and economic processes that take the form of data and information that are

14 Capgemini Research Institute, (2019), *Reinventing Cybersecurity with Artificial Intelligence – The new frontier in digital security*, https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf, accessed on 15.06.2020.

15 Tálas, P., (2016), 'A varsói NATO-csúcs legfontosabb döntéseiről' (The main decisions of the Warsaw NATO summit in Warsaw), http://www.nemzetesbiztonsag.hu/cikkek/nb_2016_2_09_talas_peter_-_a_varsoi_nato-csucs_legfontosabb_donteseirol.pdf, accessed on 15.06.2020.

16 WEF, (2015), *Global Risk 2015 – Insight Report*, http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf, accessed on 15.06.2020, and WEF (2019), Global Risk 2019 - Global Risk 201 – Insight Report, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf, accessed on 15.06.2020.

17 Lewis, J., (2018), *Economic impact of cybercrime*, https://www.csis.org/analysis/economic-impact-cybercrime, accessed on 15.06.2020.

18 Milkovich, D., (2019), '15 Alarming Cyber Security Facts and Stats', https://www.cybintsolutions.com/cyber-security-facts-stats/, accessed on 15.06.2020.

expressed through these systems'.[19] The definition itself highlights the difficulty of cyber defence: decentralised but globally interconnected IT systems make it difficult for states to decide where the IT network to be protected starts, and the large number and interconnectedness of networks makes it even more impossible to maintain permanent cybersecurity. The International Telecommunication Union (ITU), the UN's telecommunications agency, also defines cybersecurity in its Recommendations X.1205 of 2008 on cybersecurity in the broadest possible terms, taking a complex approach to the concept of cybersecurity: 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment."[20]

The targets of cyber warfare cover a wide spectrum: the government sector, the corporate sector and citizens are increasingly exposed. Attacks on the government sector can range from compromising public services, interception of government infrastructure, deliberate leaking of state secrets and publication of fake news to sabotage.[21]

In recent years, many public infrastructures have been attacked: In 2016, hackers accessed the Ukrainian electricity grid, leaving more than 80,000 people without power,[22] and India also reported that its newest nuclear power plant had been the victim of a cyber attack.[23] In the early 2010s, the Stuxnet virus, allegedly deployed by Israel and the United States, was aimed at slowing down Iran's uranium enrichment programme, which was largely successful: the computer program destroyed about 20% of the uranium centrifuges at the key Natanz plant for uranium enrichment. Analyses suggest that the attack set back Iran's nuclear programme by 1-2 years, and probably only by that little because a bug caused the worm to infect an engineer's laptop and then spread to computers around the world via the Internet, allowing it to be identified.[24]

The example illustrates the magnitude of the damage that computer software can cause. If a new worm were designed to manipulate the controls of a nuclear power plant or nuclear-powered submarine instead of controlling the speed of a uranium centrifuge, the damage would be unfathomable. In the event of an attack on the corporate sector, a meltdown of industrial installations or a paralysis of the stock market could cause a global economic crisis within days. The population is also increasingly exposed: our computers can be exploited

19 Government Decree 1139/2013. (III. 21.) on Hungary's National Cyber Security Strategy, https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf, accessed on 15.06.2020.

20 ITU, (2008), X.1205: *Overview of Cybersecurity*, https://www.itu.int/rec/T-REC-X.1205-200804-I, accessed on 15.06.2020, and Kovács, L., (2018), A kibertér védelme, (Protecting cyberspace), (Dialóg Campus Kiadó, Budapest), https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf, accessed on 15.06.2020.

21 Feledy, B., (2018), 'A kibertér mindent felfalhat' (Cyberspace can eat everything), https://index.hu/tech/2018/07/03/kiberter_cyber_kiberhadviseles/, accessed on 15.06.2020.

22 Wired, (2016), 'Everything We Know About Ukraine's Power Plant Hack', https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/, accessed on 15.06.2020.

23 FT, (2019), 'India confirms cyber attack on nuclear power plant', https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6, accessed on 15.06.2020.

24 Bányi, B., (2019), 'Szemelvények a kiberhadviselés jelenéből' (Snippets from the present of cyber warfare), Part III, *Nemzetközi haditechnikai szemle*, http://real.mtak.hu/98525/1/HT_2019-1_cikk-04.pdf, accessed on 15.06.2020.

as providers of extra capacity for attacks, but we can also fall victim to identity theft and ransomware.[25] In addition, cyber warfare can also subvert the institutional system: foreign hostile forces can compromise the purity of elections by hacking electronic voting systems or spreading disinformation (fake news) in the online information space.

The protection of critical infrastructure and vital system elements is of particular importance for governments. In Hungary, 2008 was an important milestone for the regulation of the protection of these system elements: the Government Decree on the *National Programme for Critical Infrastructure Protection* was published, which for the first time included a breakdown of these infrastructures by sectors and subsectors.[26] Article 1(f) of Act CLXVI of 2012 defines vital system elements as 'a system element of a device, facility or system belonging to a specific sector which is essential for the performance of vital social functions, in particular health care, the safety of persons and property, the provision of economic and social public services, the defence of the country, and the loss of which would have significant consequences due to the lack of continuity in the performance of these functions'.[27] As economic activities and social activity shift towards digitalisation, an increasing number of infrastructures may become a priority for cyber protection. In the context of the implementation of Government Decree 65/2013. (III. 8.), vital system elements are now identified on the basis of five main horizontal criteria.[28] The *loss criterion* considers potential casualties and serious injuries, the *economic impact criterion* looks at the ratio of damage to gross national income, the *social impact criterion* monitors the extent of disruption of public tranquillity in densely populated areas, the *political impact criterion* looks at the extent of trust in the state and its institutions, while the *environmental impact criterion* analyses damage to the built or natural environment.[29]

In order to minimise losses, it is becoming increasingly important for countries and companies to gear up for protection. The European Union has recognised this, and in 2016 the Commission launched a nearly €2 billion initiative to foster cybersecurity-related research and innovation in the public and private sectors. The initiative can both boost innovation in the EU and help to increase public confidence in e-services. Today, only 22% of European citizens have full trust in search engines, social networking sites and email services.[30]

The European cyber defence market is expected to grow steadily in the future, reaching €60 billion in 2025. In some sectors, the growth may be truly outstanding, for example, the banking sector's cyber defence costs are expected to double over this period.[31] Government

25 Feledy, B., (2018), 'A kibertér mindent felfalhat' (Cyberspace can eat everything), https://index.hu/tech/2018/07/03/kiberter_cyber_kiberhadviseles/, accessed on 15.06.2020.

26 Kovács, L, A kibertér védelme (Protecting cyberspace), accessed on 15.06.2020.

27 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Act CLXVI of 2012 on the Identification, Designation and Protection of Essential Systems and Facilities), https://net.jogtar.hu/jogszabaly?docid=a1200166.tv, accessed on 15.06.2020.

28 Government Decree 65/2013. (III. 8.) on the implementation of Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities, https://net.jogtar.hu/jogszabaly?docid=a1300065.kor, accessed on 15.06.2020.

29 Kovács, L. (2018): *A kibertér védelme* (Protecting cyberspace), (Dialóg Campus Kiadó, Budapest), https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf, accessed on 15.06.2020.

30 European Commission, (2019), 'Cybersecurity industry', https://ec.europa.eu/digital-single-market/en/cybersecurity-industry?fbclid=IwAR27gK72s-_GNuMDBwwUYZ8rkQB5v2-_gl3I-pEKHysdimcu53SyEpJAknM, accessed on 15.06.2020.

31 HelpNetSecurity, (2019), 'European cybersecurity market to exceed $65 billion by 2025', https://www.helpnetsecurity.com/2019/12/03/european-cybersecurity-market/?fbclid=IwAR3GcwGwXvd_zA1OKgHvJ3hsDTSdKNileHefuDVCGl0X0nJ2etqd9xK9eWk, accessed on 15.06.2020.

spending on cyber defence is not fully transparent due to national security concerns, but it is likely to be substantial in the public and military sectors, and these can increase significantly in the future. In the next section, we construct a model that attempts to estimate how cyber defence spending for government entities might evolve based on the above trends.

The modelling of cyber attacks

In this chapter, we explore our main thesis through modelling. In the future, the activity of cyberspace as a tactical space and the magnitude of damage it causes will increase, making the problem of cyber warfare increasingly important from a global perspective, due to its increasingly negative contribution to global well-being. This could potentially reduce future damage by strengthening the powers of supranational organisations and introducing sanctions related to cyber warfare.

The aim of the model framework is to create an abstract world where different simulations can be run to see what kind of warfare strategy would pay off for each member state in the field of cyber warfare. In the model, the participating agents make utility maximisation decisions throughout, i.e. at each decision point they decide whether and how to engage in cyber warfare. There are altogether twenty decision points in the model, giving agents this many opportunities to decide whether to go to war or not. For example, the twenty decision points can be considered as twenty decades/years and in that decade/year the agent is expected to decide how much resources to allocate to cyber warfare and cyber defence. The aim of the modelling is to assess the likely cyber warfare trends if future trends—the growth in the number and importance of electronic devices—take place. In the model, the deepening of digitalisation is proxied by the changing critical infrastructure. The framework of the model is only suitable for analysing cyber warfare between states, so we exclude the activities of non-state cybercrime groups, which may have a wide range of objectives (e.g. to make money, gain fame, or overthrow the current political structure), making them cumbersome to model.

In the 'model world', there are a total of three countries/alliance systems (A, B, C) that see each other as enemies (see Figure 2). Countries in the first model framework can only fight each other using cyber warfare alone, and their optimisation problem at each decision point is to decide whether or not to go to war with the other party or parties in a given year, and to what extent to protect their own critical infrastructure from attacks from an enemy country.

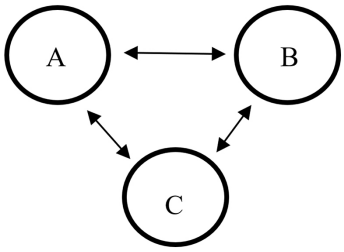


Figure 2. Relative roles of the constructed world

Countries are solving an optimisation problem, their aim being to maximise their own utility. Countries know each other's utility functions, which are maximised according to the following formula:

$$\max u = (av - bx - cy - dz) \qquad (1)$$

where "a" is the size of the reward for a successful cyber attack, "b" is the cost of a cyber attack, "c" is the cost of cybersecurity protection of a critical infrastructure, and "d" is the cost of having one of their critical infrastructures hacked. The country then decides how many cyber attacks to conduct (x) and how many sets of critical infrastructure (y) to protect. The number of successful cyber attacks (v) depends on the activity of the other countries. If the attacked infrastructure is equipped with protection, the attack fails; if it is not equipped with protection, the attack succeeds. The attacked country is only informed of successful attacks (z) against it, but not of failed ones. (For details of model parameters "a", "b", "c", "d", see Annex A.)

The digitisation of the sectors in the countries is ongoing. At the first decision point, there are only five critical infrastructures, and their numbers increase by 25% between each decision point. The technological evolution makes the protection of previously protected infrastructures obsolete, so that the cost of cyber insurance protection in the country has to be paid again to provide protection for the object. At a given decision point, countries decide how many cyber attacks to launch and how many sets of critical infrastructure to protect, taking into account the events of the previous two periods (see Annex A for details on the specification of the model). In addition, the decision structure of countries also includes a forgetting parameter, meaning that if infrastructures are not cyber attacked for a long period of time, states will pay the cost of cybersecurity protection for less and less infrastructure. Random variables are also built into the model so that, for example, if it is not worthwhile to launch a cyber attack against an enemy country for a certain period of time, after a few periods the country may try again with smaller attacks to assess the current situation, even at the cost of some reduction in its usefulness. For this reason, each run of the model gives a different result, so in the following we will consider in this analysis the average results of the twenty runs that were conducted with the model.

The decision problem is similar to a classic game-theoretic economics problem, the prisoner's dilemma. Here, two criminals caught by the police decide whether to confess or deny the crimes they are said to have committed. Depending on whether one or the other criminal confesses or denies, the number of payments or years in prison varies (see Annex Table B.1). If both parties deny the crime, the two criminals can get off with a relatively light sentence due to lack of evidence, but if one of them confesses, the number of years to serve increases significantly. Since it is more profitable for both to confess than to deny, regardless of the other criminal's actions, in the end they will both confess and end up in prison for 5 years (Nash equilibrium), while if they persist in denying, they would both be better off (Pareto-efficient condition).[32]

32 Varian, H., (2010), *Intermediate Microeconomics – A modern approach*, (New York: W.W. Norton & Company).

Individual member states face a similar dilemma in the event of a cyber attack. If none of them attacks, there is no need to protect critical infrastructure and we are at a Pareto-efficient point. However, this is when it is more profitable for any of the states to pursue an offensive strategy because the enemy's infrastructure is not protected, so an easy target can yield significant results. However, other member states are thinking along the same lines, which will eventually lead to them launching major attacks on each other, while their defence spending will also increase significantly. This theoretical demonstration is supported by the results of our model, as the number of attacks increases exponentially between decision points (Figure 3). The growing number of infrastructures opens up new opportunities for member states to attack, which, as explained above, they will also exploit.

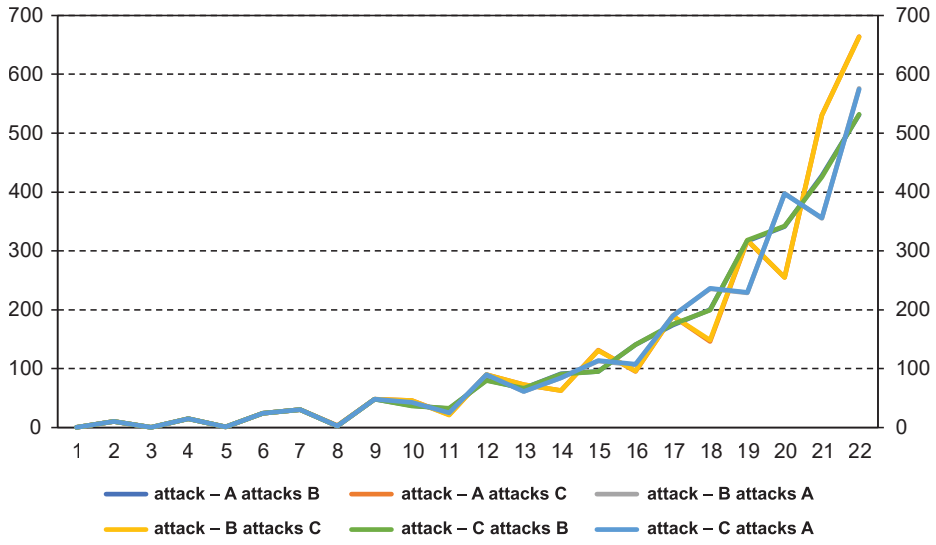


Figure 3. Evolution of the total attacks of each country averaged over 20 simulations.

This effect, similar to the *prisoner's dilemma* can certainly be detected in the simplest model setup (see Table 1). The agents do not have a clear, stable strategy, the utility gains from attacks encourage each country to attack, so the Pareto-efficient state of No Defence – No Attack is not achievable.

Table 1. Payoff functions for two countries for a period based on model parameters if they have 1-1 critical infrastructure (* denotes best response functions for a given strategy.)

		Country "B"			
		No defence – No attack	Defence – No attack	No defence – Attack	Defence – Attack
Country "A"	No defence – No attack	(0;0)	(0*; -10)	(-400; 90*)	(-400; 80)
	Defence – No attack	(-10; 0*)	(-10; -10)	(-10*; -10)	(-10*; -20)
	No defence – Attack	(90*; -400)	(-10; -10)	(-110; -110)	(-410; 80*)
	Defence – Attack	(80; -400)	(-20; -10*)	(80; -410)	(-20; -20)

The first important result of the basic model is that the average utility of countries decreases over time. The rate of loss is increasingly diverging from the course where states do not attack at all, but defend all their critical resources again at each decision point (see Figure 4). This is of course due to the increasing number of attacks, which in many cases have proved successful (see Figure B.1 in Annex). These results can thus be paralleled with the prisoner's dilemma with countries driving each other into more and more attacks due to the potential utility gains from attacks, which will eventually reduce their utility significantly, so that they move further and further away from the Pareto-efficient point over time.

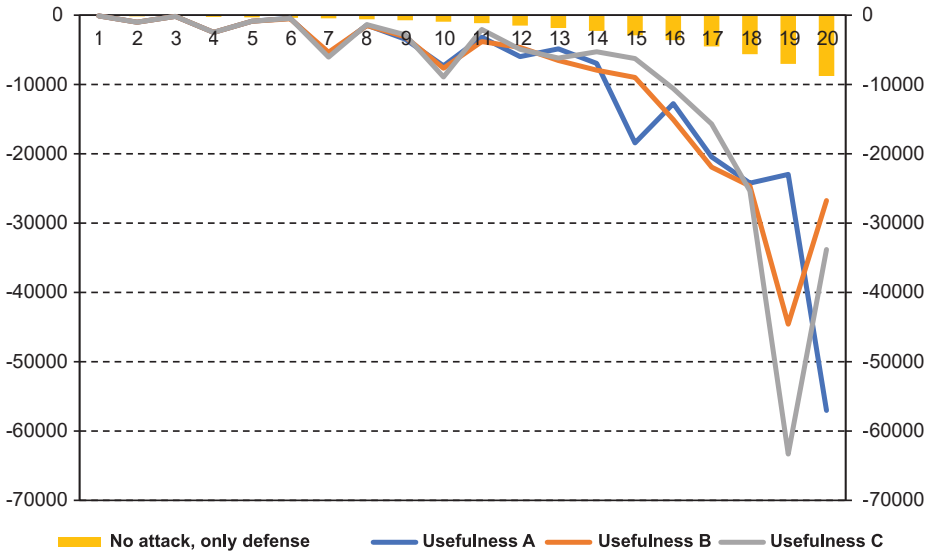


Figure 4. The evolution of the utility of each country averaged over 20 simulations, and the utility if all their critical infrastructure is protected and they never attack.

It is therefore worth considering whether the aggression of individual countries might be reduced if an external supranational organisation or some kind of *world government* can sanction countries that carry out cyber attacks. In the model, countries that have carried out a cyber attack are thus penalised (e) over the next two periods, reducing the usefulness of the country. With a sufficiently high penalty (e=1000), the number of cyber attacks decreases significantly, which implies a reduction in costs, so that the aggregate utility of the three countries improves significantly compared to the previous case (see Figure 5 and Figures B.2, B.3 in the Annex). The average number of attacks drops to roughly one hundredth of the number of attacks and the welfare loss decreases by more than 80 percent (utility function increases) compared to the previous case.

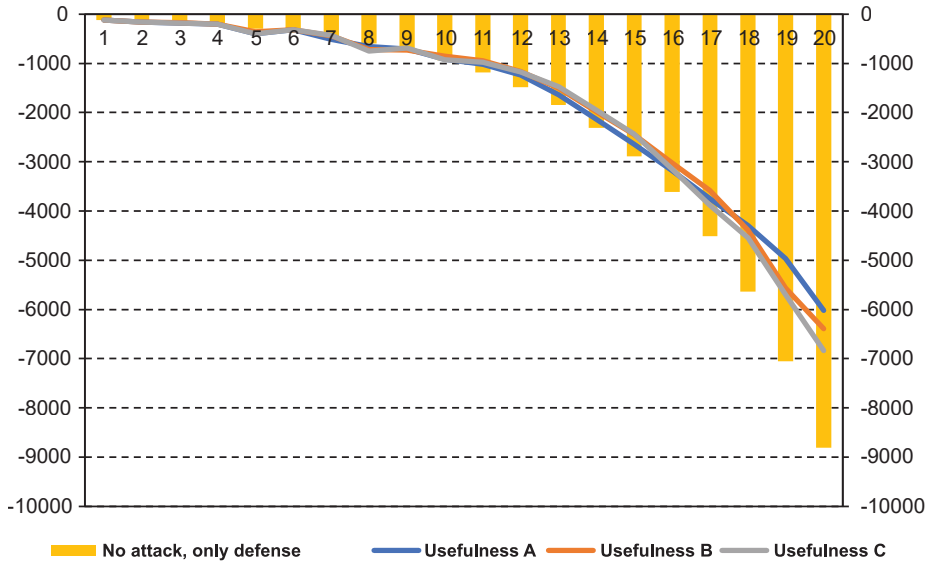


Figure 5. Evolution of the utility of each country averaged over 20 simulations, if e=1000 sanctions are imposed on the country that carried out the cyber attack.

However, deterrence is only effective if the penalty is really high: if the penalty is only 100 units, the number of attacks is reduced by 35% and the welfare loss by only 25%. For a high penalty, only the marginal cost of the attack becomes significant enough to turn the initial Pareto-efficient point into a Nash equilibrium point. By extending the simple model used before with sanctions, it is no longer worthwhile for any of the participants to attack, as the additional benefit is always less than the size of the sanction. Thus, in this structure, countries would never attempt to attack or defend their infrastructure, as this is the Nash equilibrium point of the game (see Table 2).

Table 2. Payoff functions for two countries for a period based on the model parameters if they have 1-1 critical infrastructure and face 1000 sanctions in case of attack (* denotes best response functions for a given strategy.)

		Country "B"			
		No defence – No attack	Defence – No attack	No defence – Attack	Defence – Attack
Country "A"	No defence – No attack	(0*;0*)	(0*; -10)	(-400; -910)	(-400; -920)
	Defence – No attack	(-10; 0*)	(-10; -10)	(-10*; -920)	(-10*; -1020)
	No defence – Attack	(-910; -400)	(-1010; -10*)	(-1110; -1110)	(-1410; -920)
	Defence – Attack	(-920; -400)	(-1020; -10*)	(-920; -1410)	(-1020; -1020)

Summary

One of the aims of this study was to show how technological developments and the digitalisation of the world could trigger processes in the future and how they should change the way societies and governments approach data protection. This analysis concludes that cyber attacks pose an increasing threat to the corporate, public and government sectors. Hacking into electronic devices and networks mostly affects national economic interests, so it is crucial for states to strengthen their presence in this area. The exact definition of infrastructures critical for cyber defence is not fully possible due to changing technology and the changing information technology industry, but the framework has by now been largely defined. This study also aimed to examine the future costs of government cyber attacks and cyber defence. Based on the results of our dynamic optimisation model, we conclude that it may be in the national economic interest of states to increase cyber attacks, as the costs of cyber attacks in the absence of sanctions are significantly below the potential gains. Thus, in the future, we may be moving further and further away from the global optimum, as without intervention the number of cyber attacks is likely to increase, which could induce increasing losses at the global level. In our further modelling, we then conclude that a supranational organisation with appropriate powers, if it sets a sufficiently high sanction, could significantly reduce the future number of cyber attacks and thus the welfare losses from cyber attacks and cyber defence. We therefore propose the establishment of common standards in the area of cyber governance, followed by compliance with the standards and common sanctions. However, we are aware that the practical realisation of the theoretical optimum faces significant limitations due to diverging geopolitical interests, changing technology and the impossibility of clearly identifying the attacking entity behind cyber attacks.

Annex A.

Structure of the model

Countries face the following utility function at each decision point:

$$\max u_i = \Sigma_{k=1}^{2} (av_i^k - bx_i^k - cy_i - dz_i^k) \quad (1)$$

If the country has carried out a cyber attack at the previous decision point (x_{i-1}^{k-1}), then its utility function changes as follows:

$$\max u_i = \Sigma_{k=1}^{2} (av_i^k - bx_i^k - cy_i - dz_i^k - e_i) \quad (2)$$

where "a" is the size of the reward for successful cyber attacks, "b" is the cost of a cyber attack, "c" is the cost of cybersecurity protection of a critical infrastructure, "d" is the cost of a hack into one of their critical infrastructures, and "e" is the size of the penalty. The *i-th* country thus decides how many cyber attacks it will launch against the *k-th* country (x_i^k) and how many of its critical infrastructures (I_i) it will gear with protection (y_i).

The number of successful attacks of the *i-th* country against the *k-th* country (v_i^k) is given by the ratio of all attacks against the k-th country (x_i^k) to the enemy's defended infrastructure (y_k) to total infrastructure (I_k): $v_i^k = x_i^{k*}(1-y_k/I_k)$. The number of hacked infrastructures of the *i-th* country (z_i^k) is calculated based on the number of attacks received (x_k^i) and the number of its own infrastructures (I_i) and defences (y_i): $z_i^k = x_k^{i*}(1-y_i/I_i)$. Thus, by definition, $v_i^k == z_k^i$, since the number of successful attacks by country *i* against all countries *k* must equal the number of infrastructures in country *k* that have been hacked by country *i*.

Countries look back over two periods and decide whether to attack more or less based on the changes in utility associated with attacking or defending. Overall, if more attacks at previous decision points generated more utility, they increase their number of attacks relatively, if less, they decrease their number of attacks. Similarly, if it has paid to defend in the past, the country continues to defend with greater force, if it has not paid to defend in the past two periods, the relative number of infrastructures protected decreases (see Annex C for exact calculations).

Initial parameters

a = 100; b = 10; c = 10; d = 400 throughout the simulation

It is modelled looking back over two periods, so the values for the first two periods are given, followed by twenty decision points after countries decide on their own strategy.

Period I values: $I_A = I_B = I_C = 5$; $y_A = y_B = y_C = 5$; $x_{AB} = x_{AC} = x_{BA} = x_{BC} = x_{CA} = x_{CB} = 0$

Period II values: $I_A = I_B = I_C = 10$; $y_A = y_B = y_C = 10$; $x_{AB} = x_{AC} = x_{BA} = x_{BC} = x_{CA} = x_{CB} = 10$

Annex B.

Calculation and tables

Table B.1. A possible payoff function of the prisoner's dilemma

		Robber "A"	
		Denies	Confesses
Robber "B"	Denies	(-1; -1)	(-10; 0)
	Confesses	(0;-10)	(-5;-5)

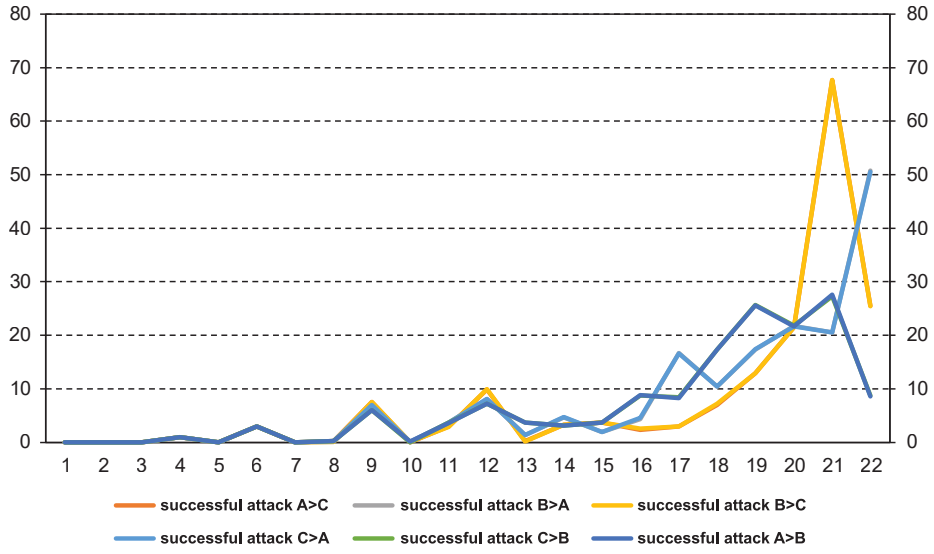


Figure B.1. Evolution of successful attacks for each country averaged over 20 simulations.

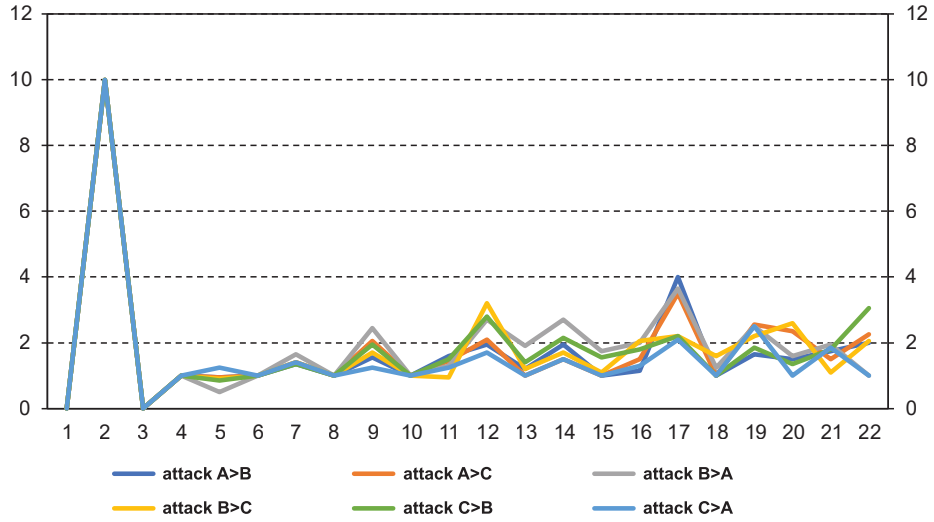


Figure B.2. The evolution of the total number of attacks by each country averaged over 20 simulations, where in case of a cyber attack the *world government* punishes the attacking member countries with e=1000 sanctions.

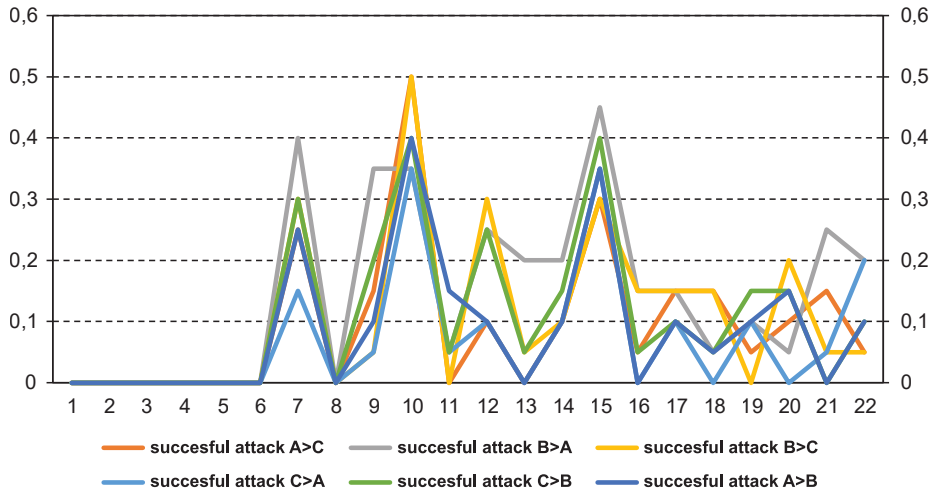


Figure B.3. The evolution of successful attacks of each country averaged over 20 simulations, if the *world government* punishes the attacking member countries with e=1000 sanctions in case of a cyber attack.

Annex C.

The spreadsheets and VBA code used in the calculation are available in the Dropbox folder below:
https://www.dropbox.com/sh/eg0guodzwu1gg6s/AACMPzQI0o446V4rxnLkSVsBa?dl=0

Bibliography

1. Government Decree 1139/2013. (III. 21.) on Hungary's National Cyber Security Strategy, https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf, accessed on 15.06.2020.
2. Government Decree 65/2013. (III. 8.) on the implementation of Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities, https://net.jogtar.hu/jogszabaly?docid=a1300065.kor, accessed on 15.06.2020.
3. Act CLXVI of 2012 on the identification, designation and protection of critical systems and installations, https://net.jogtar.hu/jogszabaly?docid=a1200166.tv, accessed on 15.06.2020.
4. Bodine-Baron, E., Helmus, T. C., Radin, A., Treyger, E., *Countering Russian Social Media Influence*, (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2740.html, accessed on 15.06.2020.
5. Bányi, B., 'Szemelvények a kiberhadviselés jelenéből' (Snippets from the present of cyber warfare), Part III, *Nemzetközi haditechnikai szemle*, (2019), http://real.mtak.hu/98525/1/HT_2019-1_cikk-04.pdf, accessed on 15.06.2020.
6. Business Insider (2019), 'IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers', https://www.businessinsider.com/internet-of-things-report, accessed on 15.06.2020.
7. Capgemini Research Institute, *Reinventing Cybersecurity with Artificial Intelligence – The new frontier in digital security*, (2019), https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf, accessed on 15.06.2020.
8. Columbus, L. '10 Predictions How AI Will Improve Cybersecurity In 2020', (2019), https://www.forbes.com/sites/louiscolumbus/2019/11/24/10-predictions-how-ai-will-improve-cybersecurity-in-2020/#56712eb96dd7, accessed on 15.06.2020.
9. Cyber Security Intelligence, 'The Future Of Cyber Security Is AI', (2019), https://www.cybersecurityintelligence.com/blog/the-future-of-cyber-security-is-ai-4550.html, accessed on 15.06.2020.
10. Dahlqvist, F., Mark Patel, M., Alexander Rajko, A., Shulman, J., 'Growing opportunities in the Internet of Things' (2019), https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things#, accessed on 15.06.2020.
11. Descartes Lab, (2020), https://www.descarteslabs.com/#overview, accessed on 15.06.2020.
12. Ericsson, *Ericsson Mobility Report (2016 November) – on the pulse of the networked society*, https://www.ericsson.com/en/mobility-report/reports, accessed on 15.06.2020.
13. European Commission, 'Cybersecurity industry' (2019), https://ec.europa.eu/digital-single-market/en/cybersecurity-industry?fbclid=IwAR27gK72s-_GNuMDBwwUYZ8rkQB5v2-_gl3I-pEKHysdimcu53SyEpJAknM, accessed on 15.06.2020.

14. Feledy, B., 'A kibertér mindent felfalhat' (Cyberspace can eat everything), (2018), https://index.hu/tech/2018/07/03/kiberter_cyber_kiberhadviseles/, accessed on 15.06.2020.
15. FT, 'India confirms cyber attack on nuclear power plant', (2019), https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6, accessed on 15.06.2020.
16. Gilmore, C. K. – Chaykowsky, M. – Thomas, B.: Autonomous Unmanned Aerial Vehicles for Blood Delivery: A UAV Fleet Design Tool and Case Study, (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR3047.html, accessed on 15.06.2020.
17. HelpNetSecurity (2019): European cybersecurity market to exceed $65 billion by 2025 https://www.helpnetsecurity.com/2019/12/03/european-cybersecurity-market/?fbclid=IwAR3GcwGwXvd_zA1OKgHvJ3hsDTSdKNileHefuDVCGl0X0nJ2etqd9xK9eWk, accessed on 15.06.2020.
18. IMF (2020) https://www.imf.org/external/index.htm, accessed on 15.06.2020.
19. ITU: X.1205: Overview of Cybersecurity (2008) https://www.itu.int/rec/T-REC-X.1205-200804-I, accessed on 15.06.2020.
20. Kovács, L., *A kibertér védelme* (Protecting cyberspace), (Dialóg Campus Kiadó, Budapest, 2018), https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf, accessed on 15.06.2020.
21. Lewis, J., *Economic impact of cybercrime*, (2018), https://www.csis.org/analysis/economic-impact-cybercrime, accessed on 15.06.2020.
22. Milkovich, D., '15 Alarming Cyber Security Facts and Stats' (2019), https://www.cybintsolutions.com/cyber-security-facts-stats/, accessed on 15.06.2020.
23. Our World in Data, 'Technological progress' (2020), https://ourworldindata.org/technological-progress, accessed on 15.06.2020.
24. Porche, I. R. III, 'Fighting and Winning the Undeclared Cyber War', (2019), https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html, accessed on 15.06.2020.
25. Ramachandran, R., 'How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks', (2019), https://www.entrepreneur.com/article/339509, accessed on 15.06.2020.
26. Szepesi, A., 'Holnaptól borul a fél világ? Mit jelent a kvantumfölény, mire számíthatunk ezután?', (Half the world will be upended from tomorrow? What does quantum supremacy mean and what can we expect next?), (2019), https://hvg.hu/tudomany/20191028_google_sycamore_kvantumfoleny_jelentese_hogyan_mukodik_kvantumszamitogep_mukodese_egyszeruen_qubit_kubit_ibm_summit_szuperszamitogep, accessed on 15.06.2020.
27. Takahashi, D., https://venturebeat.com/2017/03/28/intel-moores-law-isnt-slowing-down/, (2017), accessed on 15.06.2020.
28. Tálas, P., 'A varsói NATO-csúcs legfontosabb döntéseiről' (The main decisions of the Warsaw NATO Summit in Warsaw), (2016), http://www.nemzetesbiztonsag.hu/cikkek/nb_2016_2_09_talas_peter_-_a_varsoi_nato-csucs_legfontosabb_donteseirol.pdf, accessed on 15.06.2020.

29. WEF, *Global Risk 2015 – Insight Report (2015)*, http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf, accessed on 15.06.2020.
30. WEF, *Global Risk 2019 – Insight Report (2019)*, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf, accessed on 15.06.2020.
31. Varian, H., *Intermediate Microeconomics – A modern approach*, (New York: W.W. Norton & Company 2010).
32. Wired Magazine: 'Everything We Know About Ukraine's Power Plant Hack', (2016), https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/, accessed on 15.06.2020.

Henrietta Hegyi

Modernisation and industrial security after the COVID-19 pandemic in Hungary

Resume

The aim of this thesis is to look for evidence suggesting that the coronavirus crisis can have a positive long-term impact on the development of industrial technologies. In addition to reviewing various historical processes, the study seeks to support this hypothesis through a questionnaire survey involving industrial actors. Moreover, it provides an overview and analysis of the research findings, as well as attempting to make recommendations to support positive change and to draw attention to the challenges ahead.

Executive summary

The coronavirus pandemic has triggered a worldwide trend towards a new wave of industrial modernisation. Based on the questionnaire research reported in this paper, decision-makers of Hungarian industrial companies are aware of this trend, but their digital security preparedness is still limited. This is due to a lack of credible information on new technologies. The paper proposes a solution to this problem, emphasising the importance of public involvement.

Introduction

The general perception of crises is that they have a negative impact on the economy and create tensions in society, as their reorganising effect causes many people to lose their livelihoods or find themselves in difficult situations. While this is true, crises can also have long-term benefits, as they are beneficial for certain processes necessary for development.

The aim of this thesis is to prove that the SARS-COV (COVID-19) pandemic is expected to have a positive impact on the digitalisation processes in industry (especially in manufacturing) in the long run, and to draw attention to the security policy aspects of the current wave of modernisation and digitalisation in the Hungarian industry. From a methodological point of view, the analysis is carried out with a geopolitical perspective with the aim to create a framework for the local conditions. The author does not seek to explain the processes in detail, but she intends to review and summarise the overall structural changes and the threats they pose. All this will be complemented with Hungarian experience through exploratory empirical research, which can serve as pilot research, a guideline for future research activities that will mobilise further resources.

My first thesis: The recession caused by the coronavirus leads to a wave of modernisation in Hungarian industry. To support this thesis, I will examine whether there is a correlation between crises and innovation in general, and whether the impact of the crisis can be interpreted positively from a modernisation perspective. On the other hand, based on the news on the crisis triggered by the coronavirus pandemic, I will try to identify concrete signs that may point to a later wave of modernisation.

My second thesis: In the expected wave of digitalisation, or modernisation in general, Hungarian industry is exposed to certain security risks. I test this hypothesis using mainly empirical experience.

By the 2020s, the role of new technologies based on artificial intelligence, in particular, deep learning, has become unquestionable, and basic models will become more widely available, with a positive impact on the training of skilled professionals. Data markets are taking off around the world, fundamentally transforming the way states and international organisations operate. There is no doubt that we are currently witnessing a paradigm shift.

For the purposes of this paper, it is essential to distinguish between the words *modernisation* and *digitalisation*. Although modernisation is a broader concept, of which digitalisation is a part, and they do not mean the same thing, I use the two terms synonymously because these two processes are closely intertwined in this century: in the 4th (and the 5th) industrial revolution – some researchers are already talking about the existence of the 5th industrial revolution – digitalisation processes play a major role in modernisation.

In the analysis, I mostly use the word modernisation, because modernisation includes all kinds of transformations that are aimed at using the tools appropriate to the challenges of our present time and at achieving the goals in the most efficient way. However, these changes are not necessarily innovative, as they are often used only to bridge gaps.

The relationship between cyberspace and geopolitics

Before delving deeper into the information that supports or refutes the two theses formulated in the introduction, it is essential to review the geopolitical dimension of digital industrial security and cyberspace security, in order to better understand why it is so important to address the issue of digital protection of industrial companies and the cyber attacks that threaten them.

Geopolitics is a discipline that deals with the power position of the nations in the world and is strongly based on geography and spatiality. Geopolitical analyses are mostly aimed at identifying a dominant position, examining the processes that are changing it and making recommendations to governments. Analyses of cyberspace can be part of geopolitics because, on the one hand, cyberspace itself can be understood as a kind of fifth domain alongside the ones considered by classical geopolitics—land, sea, air, space[1]—and, on the other hand, cyberspace has specific physical infrastructures whose protection is of high priority for the state.

In addition to physical and theoretical spaces, the different levels of power competition therein, the *behaviour* of states and the dynamics of conflicts are all subjects of geopolitics, but there is still a tension between the geographical centricity of geopolitics and the study of cyberspace. It is therefore no coincidence that the geopolitical study of cyberspace raises a number of questions. The French geopolitical expert Frédérick Douzet asked whether cyberspace was really a new form of location definition. There are many definitions of cyberspace, although some states, including major powers such as China or Russia, do not even use the term, because it suggests that cyberspace is a specific *territory*, which would be subject to a different legal definition than if it were understood as an intellectual product. These states therefore simply refer to the *Internet* in their communications.[2] Geopolitics can help us to highlight the spatial elements of cyberspace—we need to think not only about the specific infrastructure needed for data storage and telecommunications, but also about the organisations and institutional systems that can be relevant to the analysis of different security policy issues. Such elements include, among others, the position of the great powers, their motivations, or the means to increase their influence. Geopolitics, as defined by Gearóid Ó Tuathail, can therefore be understood as the synthetic study of power, history, geography, present and future, with the aim of scientifically *predicting* change.[3]

Douzet points out that cyberspace can be broken down into layers.[4] This is important to highlight because several problems of definition can be avoided by not trying to interpret this complex concept as one whole, but by keeping in mind that it is a constructed concept that includes many different elements. At the same time, Douzet points out that the number of these layers is not clear and that there is no agreement on how to divide them. She highlights four areas for analysis: backbone (physical infrastructure), logistics (protocols and domains),

1 Szilágyi, 2018, pp. 184-185.
2 Douzet, 2016, p. 23.
3 Ó Tuathail, 2003. pp. 3-6.
4 Douzet, 2016, pp. 14-17.

user-friendly applications, and social and information network, also known as the cognitive or semantic layer.[5] The latter may seem at first sight to be far from geopolitics and closer to linguistics, so it may need some explanation as to why it is included in the segments to be examined. The information-social layer can be of interest to geopolitics because it helps to understand social conflicts, for example, why people in certain regions oppose local power, or what characterises pro- or anti-government groups in a given country.

On the other hand, geopolitics can also be powerful as it provides objective information about cyberspace that can influence the thinking and actions of governments or other actors in international politics. Classical geopolitics, which used to define geopolitical thinking until the Cold War, tended to follow a prescriptive line, while today's geopolitical analyses tend towards descriptive analyses as a result of the critical geopolitical approach, although their role in informing decision-making is not negligible.

Douzet does not specifically mention the institutional layer, which ensures the functioning and administration of the *backbone* in compliance with or in defiance of the regulations, but this can be an important aspect of an analysis. This institutional layer is somewhere between the *backbone* and the *logistics* or *applications*. It influences the way infrastructure is built and it has an impact on innovation processes and competitiveness. One example is the role of the General Data Protection Regulation (GDPR) in kick-starting the European data economy. The GDPR has generated controversy among EU members since its inception, and some views suggest that it will have a strong impact on the EU's global competitiveness in data trade.

The original definition of cyberspace comes from William Gibson's novel[6] in which Gibson describes a *space* where Internet users can access all the data on all the computer systems in the world. Although Gibson has written science fiction, but his work has brought the spatial understanding of Internet networks into the mainstream and it influenced Internet governance. His work led, for example, to the creation of the Electronic Frontier Foundation, the first international non-profit organisation dedicated to digital rights, in 1990.[7] The word *frontier* in the name of the foundation can be equated with the term *Wild West* in the Americas, describing the uncolonised parts of the country that is also the cradle of American democracy.

Industrial security, critical systems and geopolitical advocacy

The motivations of the perpetrators and implementers of cyber attacks are varied. The starting point of the attack can be an activist hacker group, a lone hacker seeking attention or even a government entity. In this chapter the author examines cyber attacks as a tool for geopolitical advocacy in order to get a broader picture of what can happen when a company or industry is attacked for reason related to foreign policy.

The European Commission published the EU-wide risk assessment report compiled by the European Cybersecurity Agency (ENISA) on 9 October 2019, on the basis of data from trusted bodies in the Member States. Among others, the report concludes that 5G networks in the

5 Douzet, 2016, pp. 15-26.
6 Neuromancer, 1984.
7 See: www.eff.org.

future can provide an ideal target for hackers and hacker groups with different interests, and that certain elements of the infrastructure can become more vulnerable to attacks than they are today. The study specifically highlights background and remote management functions that can provide remote access to critical network resources. Furthermore, the report also points out that the typical practice of mobile operators that buy network infrastructure from a single supplier may increase the exposure of that network.[8]

In a short publication the 5th Element Group, an organisation working to achieve the goals of the United Nations (UN) Agenda 2030, warned that the momentum of the 4th industrial revolution and the impetus of technology and trade is blinding humanity. This is why innovative businessmen such as Elon Musk publish a lot of information, the effects of which they do not have to take responsibility for later. They do this despite the fact that new technologies have the potential to become the *Orwellian enemy* of the people.[9]

The fact is that nowadays artificial intelligence, robotics and automation processes give many people the feeling that control is slipping out of humanity's hands, no wonder that one comes across so many utopian, threatening predictions, especially in the press. While the subjective layer of such highly influential statements is not worth much discussion, it is interesting to wonder why a global company working with sustainable development would make such a statement.

At a global level, the terrorist attacks against the United States on 11 September 2001 marked a turning point that has increased the role of information originating from cyberspace. After clarifying the circumstances of the terrorist attack, which had shocked the world, the United States slowly began its massive data collection programme, later revealed to the world from the data published by Edward Snowden. Snowden and other lesser-known activists and hacker groups have pointed to regulatory shortcomings in the overall programme.[10]

Industrial security has always been an important part of national security, but in Europe it was given special attention in 2007 when Estonia, a small but highly digitalised Baltic state, was hit by a DDoS attack of Russian origin which crippled its banking system, parliamentary and ministry websites and several media outlets.[11] Subsequently, the importance of cyber defence at a state and international level was further underlined by the Stuxnet attack in 2010, which revealed the virus to be more than a worm virus, but in fact a cyber weapon created in an international collaboration of state level organisations.[12] The next milestone was the damage caused by the NotPetya ransomware virus in Ukraine's vital systems during the conflict over Crimea in 2017. The attacks in Estonia and Crimea disabled critical infrastructures, the shutdown of which affected the whole country, and in the case of NotPetya, it had serious consequences for the whole world.[13] The virus has triggered a chain reaction in global cyberspace that spread beyond Ukrainian borders and caused disruption in the United States, as well as in several countries across Europe, particularly in Germany. One

8 EU coordinated risk assessment of the cybersecurity of 5G networks, ENISA, 2019
9 Gauri – Van Erdeem, 2019.
10 Deibert, 2020 and Snowden, 2019, pp. 96-103.
11 Kovács, 2018, pp. 145-148.
12 Kovács 2018, pp. 155-165.; Kovács-Sipos, 2010.
13 Kovács, 2018, pp. 131-140.

of the companies particularly hit hard by the virus was the shipping company A.P. Moller-Maersk, which is responsible for about one fifth of the world's maritime freight traffic and has accumulated several weeks of delay due to the breakdown of its system management communication devices. The attack was described by investigative journalist Andy Greenberg of Wired Magazine as "the world's first real cyber war", to be considered as the pinnacle of the ongoing conflict between Russia and Ukraine since 2014, which continued with the invasion of Crimea.[14]

The above conflicts and the lessons learned from them, as well as the increasing attention of national security services on cyberspace, are trends that will strongly influence the future development of international regulation and could all be subject to geopolitical monitoring. At the same time, these global events and the trends that emerge from them are very difficult to analyse due to the large number of unknown details. The increasing frequency of cyber attacks and the problems of countering them rightly raise the need for stricter regulation and control of digitisation processes.

After these examples, there is no question that the protection of cyberspace, and especially the cyberspace of industrial processes, is important from a national security and state protection point of view. To prepare for this, it has become necessary to set up specialised institutions (CSIRTs and information security authorities) at both national and international levels. Nevertheless, cybersecurity is a very complex task, involving national cybersecurity strategies, international and national legal frameworks and different security standards that serve as the basis for conducting vulnerability assessments and the preparation of regulations. Furthermore, a number of related services need to be set up, like the information required for the reports must be provided along with the organisational support necessary to receive reports. The provision of information and the promotion of cooperation are also important. Therefore, the task falls not within the exclusive competence of operational organisations, they are specifically created for incident management.[15]

What processes lead to a wave of modernisation?

In order to understand the impact of SARS-COV on industrial modernisation, it is worth first examining the circumstances in which previous industrial revolutions occurred and the link between industrial development and crises. The present chapter therefore deals with the first sub-thesis of the first thesis identified in the introduction, i.e. whether the recession caused by the coronavirus pandemic leads to a modernisation wave in Hungarian industry, whether there is a correlation between crises and innovation in general, and whether the impact of the crisis can be interpreted positively from a modernisation perspective. Firstly, I will look at the relationship between previous crises, security and industrial development, and secondly, I will try to draw conclusions from various national and international news reports on whether a wave of industrial modernisation is likely to emerge after the SARS-COV pandemic.

14 Rhysider, 2019, 30m35s.
15 Tikos, 2018, pp. 200-201.

Industrial revolutions are processes that take place over long years or decades, completely transforming first production itself (or the way services are made available) and then society as a consequence, which in itself has a destabilising effect on economic processes, but this effect is usually followed by a structural development in a positive direction. This is partly due to the fact that human society is constantly working to improve the quality of life, while industry is trying to keep up with these demands.

Industrial revolutions are points in economic history where rapid changes took place. The development of communication, energy use and mobility coincided that resulted in rising living standards and a lasting, deep structural change in business models.[16] Although advances in science and technology have steadily supported the development of industrialisation throughout the world, and the meaning of the term industrial revolution has been refined over the years, there is still no universal agreement on a definition. Therefore, the best way to understand what the term industrial revolution means is to interpret the process itself.

According to the traditional approach[17], industrial revolutions can be divided into three stages:

1. Change in a specific economic sector over a short period of time.
2. The change in the sector, which is due to the continuation of the first phase and which causes the sector as a whole to grow more dynamically than other industries, leading to a change in structural proportions. At this stage, the output and employment share of the sector concerned increases.
3. In the third stage, the effects of development spread to other sectors.

The first industrial revolution, which began in the late 18th century with the use of water and steam powered mechanical production equipment, is seen as an important turning point for mankind. At the beginning of the 20th century, the application of electrically powered mass production technologies by way of dividing labour, brought about the second industrial revolution. Later, with a continued automation of production, the third industrial revolution began in the mid-1970s, with the widespread use and promotion of electronics and information technology in factories and in everyday life.[18] All in all, these three earlier industrial revolutions took about two centuries to fully unfold, which provided enough time to protect industrial installations and maintain geopolitical stability. The fourth industrial revolution has been spreading at a rapid pace in recent years, with an increased attention on the Internet of Things (IoT)[19] and Cyber-physical systems (CPS)[20]. The Internet of Things means networked traditional devices that previously had no need or technology to communicate, for example, smart appliances such as the smart fridge, which allows you to order food instantly via a display. In the case of industrial devices, the term Industrial Internet of Things (IIoT) is increasingly being used instead of IoT, but this term is less common in the general literature.

16 Holodny, 2017.
17 Mokyr, 1985.
18 Klingenberg-do Vale Antunes, 2017.
19 Atzori et al., 2010.
20 Monostori, 2014.

The different types of innovation waves caused by crises have been studied by several academics and research institutes. On the oil crises of the 1970s, the Rapid Transition Alliance Institute for Climate Policy and Sustainable Energy Economics writes: *"Great innovation can emerge as a direct result of crisis. The oil crisis of the Organization of the Petroleum Exporting Countries (OPEC) shows how government led energy conservation and a whole new industry based on renewable energy can emerge as a result of a crisis. In the early 1970s, fossil fuel consumption soared and the industry boomed—until Middle Eastern oil producers turned off the supply tap in a shock manoeuvre. Despite the resulting deep recession, economies survived and industries adapted. Faced with a sudden lack of oil, energy conservation and efficiency became a top priority. Research into renewables was also stepped up. The 1973 oil crisis, with its loud echo in 1979, is a clear historical example of rapid transition and what people, communities and governments can do when mobilized to act."*[21]

A 2012 OECD study[22] reveals that the 2008 economic crisis had a negative impact on innovation and national R&D programmes. Furthermore, researchers point out that the crisis exposed pre-crisis weaknesses in some countries (such as Greece and countries in South-Eastern and Eastern Europe), certain sectors (such as the automotive industry) and specific types of innovation (such as financial innovation). Many countries implemented policies to support innovation during the time of crisis, putting innovation high on the political agenda. Government responses to the crisis focused on infrastructural investment for innovation and securing financial resources for businesses. With the onset of a crisis, many governments have recently started to cut spending on innovation.[23] However, researchers do not describe the fall in innovation as a direct consequence of the crisis, but rather as a result of poor crisis management due to misjudgement, rather than the financial situation itself. The study states that the policies introduced during the crisis had a positive impact on innovation. However, most countries relied on traditional infrastructure and financial instruments to accelerate the recovery process by reducing demand uncertainty. Recovery policies to support failing sectors proved misguided. Market forces continue to weaken them as the crisis exacerbated already prevailing trends and they ended up facing similar difficulties as before the crisis. Instead, the OECD study argues, resources should be allocated to sectors with growth potential, concurrently with industrial policies that promote the reallocation of resources, such as retraining programmes and R&D entrepreneurship programmes that reduce the costs of restructuring. Policy choices to avoid employment losses and to support training are essential to avoid a damage in the innovation systems. Researchers point out that such policies are important not only from a social point of view, but also because there are not enough new jobs to absorb the same skilled labour due to a lack of new business creation as well as to ensure that innovation can be carried out by attracting the right skilled labour.[24]

Savvy entrepreneurs and business leaders know that a crisis will not last forever and that it is necessary to manage the reserves until the recovery process starts. However, the new

21 Rapid Transition Alliance, 2019.
22 OECD, 2012.
23 OECD, 2012.
24 OECD, 2012.

economic cycle is also likely to bring structural changes in the composition of output and demand. In order to take advantage of the opportunities in a changing economic environment, successful companies need to be prepared to provide new and improved goods and services.

Building on the theory of Joseph Alois Schumpeter that crises do not just produce losers in the long run, Italian and British researchers have shown that in the long run, the firms that emerge from crises as winners are those that have not cut innovation spending. Their theoretical paper deals with two types of possibilities—the categories of creative destruction and creative accumulation. Creative destruction means that the most innovative companies emerge from the crisis as winners, while the rest ends up as failures. Creative accumulation leads to a slower and more stable innovation process. The researchers used the two categories to develop a model to analyse the strategies of European companies in terms of how they performed before, during and after the 2008 financial crisis.[25]

The first significant result of the analysis at an aggregate level is that the crisis has significantly reduced the number of companies that intend to increase their investment in innovation from 38% to 9%. There is no doubt that the crisis—at least in its early stages—destroyed investment in innovation. Contrary to expectations, towards the end of the crisis, it was not the firms with large reserves that continued their modernisation and R&D activities, but those that were flexible and able to find new customers and markets.[26]

Even though there are many different types of crises, they present opportunities as well as setbacks—regardless of what type they are. They will not destroy, rather transform existing structures and screen companies in such a way that they can survive beyond the trends, economic requirements and criteria of the time. This restructuring supports growth in the remaining firms. And by studying past industrial revolutions it can be concluded that the innovation activities of leading companies have an impact on their competitors and, by extension, on the sector and the industry as a whole. Seeing their success, some of the innovations are likely to be adopted in a sudden rush by an increasing number of players in the market.

It requires radical changes to transform a factory in a way that some or all of the workforce would be replaced by automated systems. The more technologically outdated the factory, the more challenging it can be to interrupt the maintenance and development processes already in place and build a completely new system, as all elements—IT systems, security, internal communications, company organisation—may need to be subordinated to and compliant with innovation. Crises are fundamentally good for automation because they create an environment conducive to a long-delayed or even uncompleted transformation through shutdowns, line clearances and high layoffs. Although the costs may be high, which is unfortunate in an incipient economic crisis, the short-term disadvantage of any conversion is a *necessary* evil that all manufacturers will have to face over time in order to adapt to the demands of modern industry. It means that the sooner one moves towards properly implemented modernisation, the greater long-term payback is expected.

It also seems increasingly likely that it is not only workers doing routine tasks who may fear the loss of their jobs, even if this idea runs counter to past experience. A much-cited

25 Archibugi et al., 2012, pp. 2-8.
26 Archibugi et al., 2012, pp. 26-28.

2017 study conducted by the McKinsey Institute found that while the automation of routine industrial tasks was the main reason for transition to new technologies in the past, many middle management workflows are now also under *threat* by these changes. Based on McKinsey's scenario modelling, it is estimated that automation could boost productivity by an annual 0.8-1.4 percent worldwide, thanks to generating a saving of $15 trillion in weekly labour cost for companies.[27] However, this estimate should be treated with caution. On the one hand, the automation of tasks—especially at management level—will take many years, and only certain subtasks can be expected to be automated at first, which will not mean that the work of managers will be lost, it will only be transformed. For instance, they will have more time to spend with customers. On the other hand, transformation involves many unforeseen factors. An important question is, for example, whether contributions will have to be paid for the robots. It may seem futuristic at first, but with the high-level of automation, it is likely that in the future there will be a need to replace the contributions paid for lost labour.

While the exact impact of crises is unpredictable, there is no doubt that they strongly influence industrial modernisation. The question is whether we should expect a sudden wave of modernisation or a prolonged, more stable process. This is strongly influenced by a number of external factors, such as the trends in place immediately before the crisis.

A somewhat bold but interesting analysis by Professor William I. Robinson at the University of California[28] suggests that the speed and comprehensiveness of the processes that are occurring today are unparalleled. Last time it was the industrial revolution of the eighteenth century that humanity saw such profound changes as we did in the 1980s, at the beginning of the capitalist global transformation. According to Professor Robinson, the consequence of this economic, structural transformation is what we now call the digital transformation. He argues that the main actors who have tried to convince the public that the 2008 economic crisis is over are those who benefit from the existing capitalist system. However, destabilisation processes are deeply rooted in the structure, so sooner or later another serious crisis can be expected. This suggests that the underlying structural conditions that triggered the 2008 crisis—most severe economic crisis since the 1930s—still persist and are likely to be exacerbated by the new restructuring of the global economy which is based on digitalisation and militarisation. According to the theory of growth it could advance because governments have fully exploited the monetary tools in order to maintain the system. However, this debt-driven consumption will trigger further waves of crisis in the long run.[29] If Robinson's theory proves to be correct, it will cause a fundamental shift in the international status quo.

Several studies suggest that the speed and complexity of the transition to the new digital era in this globalised environment does not yet allow for a harmonised approach. It is not yet possible to deeply understand the impact such measures have on different countries and regions. Most policies refer to the German *Industrie 4.0* policy, with the Made in China 2025 strategy in the second place with three references and the European Factories of the Future plan in the third place.[30]

27 McKinsey, 2017.
28 Robinson, 2018.
29 Robinson, 2018 pp. 78-80.
30 Liao et al., 2017.

The number of conferences and academic papers on Industry 4.0 has progressively increased 24-fold between 2013 and 2015. Given the growing global interest in the fourth industrial revolution, the question is to what extent cyber defence can keep up with this trend.

The digitalisation processes of the 2000s expanded cyberspace, both in physical (infrastructure) and info-communications terms, with new interconnected internal networks and digital tools for industry. From a geopolitical perspective, this is interesting for the following reasons:

4. The infrastructure is often not located in the country where the service is used. This used to be a problem even before, but now it poses a much greater risk due to the extension.
5. Rapid expansion is difficult to keep up with from a legal and security point of view, leaving newly implemented systems vulnerable.
6. Slowing down the process will help to build adequate protection, but will result in an economic backlog.
7. The most competitive technologies are under the partial or total control of the major powers, which can use them to their advantage.

The above considerations are important in making the right security policy choices. ENISA defines the Internet of Things in the first paragraph of the relevant webpage as *"a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision-making"*. The definition reveals that information plays a central role in the IoT networks, as part of a continuous cycle of sensing, processing and decision-making.[31]

The IoT is closely linked to cyber-physical systems and in this respect it enables the development of intelligent infrastructures (e.g. smart grids or intelligent transport). The threats and risks associated with IoT devices, systems and services are manifold and they evolve rapidly. The security risks affecting the Internet of Things, which have a major impact on the safety, security and privacy of citizens, cover a very broad area. It is therefore important to understand exactly what needs to be secured and what operational security measures need to be developed to help protect industrial assets from cyber threats. A major challenge in defining security measures for IoT is the complexity caused by the diversity of the technology's applications. It is essential to strike a balance between the specificities of each area, so it is important to take the differences in the distribution of risks in different environments into account.[32]

After the economic crisis of 2008, many wondered whether one could create the conditions where humanity would no longer have to fear a similar situation again. However, the current epidemiological situation has once again created an environment in which the economy is faltering. Although the exact chain of events was unpredictable, several experts warned about the development, the spread and the devastating effect of the pandemic. Nouriel Roubini, economist and geostrategy researcher at New York University's Stern School of Business, explains in an article in The Guardian that while previous crises took years to unfold, the

31 ENISA, 2020.
32 Id.

SARS-COV crisis took only a month and shook the global economy much more deeply.[33] This is why banks are already having to make concessions to slow the economic meltdown. This transformation favours the unfolding of the 4th (and 5th) industrial revolution, as the epidemiological situation has shown the need for a robotic workforce in a health crisis.

What kind of life can we expect once the SARS-COV pandemic is over? Will robots take over the jobs related to production? Workers and employers are rightly concerned with these issues, as any economic downturn favours the introduction of automated equipment, and observations so far suggest that this will be particularly true of the recession caused by SARS-COV.

The new coronavirus pandemic damages the labour market in many ways. In recent weeks, the number of applications for unemployment benefit around the world has hit record highs, as entire industries have been forced to close down in order to stop the spread of SARS-COV or switch to manufacturing the tools needed to deal with the crisis.[34] As a result, the economy took a big tumble, with the Dow Jones Industrial Average and the S&P 500 down more than 20% from their February highs.

Although the quarantine measures are temporary, the impact of this economic downturn on the labour market will be long-lasting. Mark Muro, senior fellow and policy director at the Brookings Institution's Metropolitan Policy Program, recently wrote, citing[35] analysis by colleagues[36] that the downturns caused by the coronavirus will provide the same long-term boost to the uptake of automated equipment as did previous crises.

Two analysts from the US National Bureau of Economic Research, Nir Jaimovich and Henry Siu, concluded in a study[37] that 88% of job losses in the three crises studied over the past 30 years fell into the category of jobs that can be automated. And another study by Brad Hershbein and Lisa Kahn, researchers at the University of Rochester—in which they looked at more than 100 million job advertisements—shows that firms have been able to effectively replace the low-skilled workers they have lost with various combinations of new technologies.[38]

In February, several articles appeared in the online press describing the phenomenon as the so-called *black swan*, referring to the world-famous book by Nassim Taleb.[39] However, Taleb later said in an interview that there was no similarity, as the pandemic and its consequences were foreseeable.[40] The author will support this statement by presenting the recent news stories described below.

Chris Hansen, head of Valiant Capital Management, reacted to the predictions of a coronavirus outbreak back in January, and adjusted his strategy to the expectations to generate high returns by shorting certain stocks. Valiant started shorting shipping companies, airlines and travel companies in February, which resulted in a 36% year-to-date return by the end of March. The performance is striking because, meanwhile, the S&P 500 fell by 19.6% and the MSCI All World Index by 21.3%.[41]

33 Roubini, 2020.
34 Taylor-Schwartz, 2020.
35 Muro-Maxim-Whiton, 2020.
36 Muro, 2020.
37 Jaimovich-Siu, 2012.
38 Hershbein-Kahn, 2016.
39 Origin: The Black Swan, 2007.
40 Avishai, 2020.
41 Chung, 2020.

In 2015, a team of Chinese and American researchers (including Zheng-Li Shi, also known in the tabloid media as the Wuhan Bat Lady) published the research in Nature describing how the previous SARS-CoV outbreak was a milestone in the study of interspecies virus transmission and stating that more similar outbreaks could be expected in the future.[42]

The possibility of a pandemic and the way it spread was addressed by a number of experts in the field of network science,[43] including Alessandro Vespignani and his colleagues.[44] Albert-László Barabási made the following statement in a Spektrum programme in 2015: *I don't think we have seen everything yet. The question in the 21st century is not whether there will be a pandemic, but when and how devastating it will be.*[45]

Kamran Khan, a physician specialising in infectious diseases and public health, had a first-hand experience of the SARS epidemic in 2002-2004. Khan had watched the virus sweeping the city paralyse hospitals, and it had left such a deep impression on him that he decided to find a way to track diseases more effectively. As a result, in 2008, he set up a scientific research programme called BioDiaspora, and began to investigate how commercial aviation connects the world's population. Within the project, he managed to anticipate the spread of the first major influenza pandemic of the 21st century, and in 2012, together with the UK authorities, they searched for and identified the epidemiological risks of the London Olympics.[46]

The real breakthrough came in 2014, when the company took on the name BlueDot after a major capital injection, and soon afterwards successfully predicted how and when the Ebola virus could leave West Africa by analysing billions of roadmaps. Later, in the case of the Zika virus from Brazil, they did not miss the mark and used their risk analysis models to warn of an outbreak in Florida six months before it occurred.

Epidemiologist Larry Brilliant spoke 14 years ago at the TED Global Conference series about the consequences of a pandemic. Although he seems to have overestimated the scale of the outbreak, predicting 100 million victims, he was probably not wrong about the economic impact: recession and unemployment will follow the epidemic emergency that the virus causes.[47]

The research cited above also highlights the fact that the SARS-COV pandemic is not an isolated case, but one of a growing number of new diseases that will be followed by more in the future. These findings do not mean that the emergence and spread of the epidemic was entirely predictable, but that the possibility of a pandemic, alongside other types of crises, has long been anticipated by researchers. With this in mind, it is no wonder that some business owners started preparing for the more difficult economic period already at the early stages of the breakout.

42 Menachery-Yount-Debbink, 2015.
43 Carey, 2020.
44 Chinazzi-Davis-Ajelli, 2020.
45 Portfolio, 2020.
46 Niiler, 2020.
47 Levy, 2020.

Table 1. Processes reinforcing the modernisation wave
Source: own research

Processes in place before SARS-COV	Developments due to SARS-COV
The 4th Industrial Revolution is an ongoing process that requires the creation of an ever more extensive digitalisation ecosystem across industries.	SARS-COV has shown that industry needs a higher degree of robotisation in addition to or instead of a human workforce that is less resistant to health crises.
Stronger defences and stronger action are needed to counter the growing threat of terrorism and the increasing frequency of cyber attacks on critical infrastructure in recent decades.	There is a greater role for national security in the SARS-COV crisis, which means tighter controls.
Over the past two decades, developed economies have begun to digitise at the state level, and with this cyber defence has been given a greater role.	A SARS-COV járvány okot adott arra, hogy a globális technológiai vállalatok, mint a Facebook, a Google, az Alibaba vagy a Tencent a nagyhatalmak kormányaival együttműködve több adatot gyűjthessenek a felhasználók készülékein keresztül (például tartózkodási helyüket illetően).
(Mass surveillance in the United States, and the increasing use of camera systems in China, are warning signs of this).	The SARS-COV outbreak has given rise to global technology companies such as Facebook, Google, Alibaba and Tencent working with the governments of major powers to collect more data on users' devices (for example, their location).

Reading the news about the outbreak, one might get the impression that there are a relatively high number of professionals who have in some way anticipated a possible crisis. To determine exactly how much more predictable the current crisis was than the previous ones would require a much deeper analysis than the present observations, but in our case, this information is sufficient to conclude that some professionals, consultants and therefore some companies were aware that another crisis was coming in the near future. Assuming this was the case, it can be concluded that these economic agents, albeit at different levels, may have been prepared for the downturn.

Post COVID-19 modernisation processes and their risks in Hungary

In this chapter, I will attempt to support both theses, but from different perspectives than in previous chapters. On the one hand, the author focuses specifically on the Hungarian industry, and on the other, she makes her arguments based on primary research, with the exception of the introductory, outlining paragraphs.

According to a study published by the Research and Development Observatory of the National Innovation Office, based on data provided by the Hungarian Central Statistical Office (HCSO), the majority of R&D expenditure as a share of GDP is linked to manufacturing, while professional, scientific and technical activities and education also make a significant contribution. The founding document of the Hungarian Industry 4.0 National Technology Platform was signed on 6 May 2016 by Hungarian research institutes, educational institutions,

companies and professional associations located in Hungary, to lay the foundations for the regulation of production and R&D processes, and to fulfil their mission as defined in their operational rules, the working groups were appointed to carry out the tasks.[48]

The Digitising European Industry Strategy aims to reinforce the competitiveness of the EU in digital technologies, which is a key part of the EU's Digital Single Market' strategy. The success of the strategy requires the integration of digital innovation across the whole cross-section of the economy.[49]

According to HCSO data *in 2018, Hungary's GDP per capita at purchasing power parity was 71% of the EU-28 average, three percentage points higher than a year earlier. In 2018, GDP at current prices in Hungary grew faster than the EU average, by 9.9%.*[50] The following findings can provide information on the Hungarian manufacturing industry: *Manufacturing expanded by 3.7% in 2018. Of the three largest subsectors, output in the most important one, transport equipment, was virtually flat, while the output of computer, electronic and optical products increased by 6.8% and food, beverages and tobacco by 4.9%.*[51] GDP volume expanded by 4.9% in 2019. Services contributed 2.3 percentage points to GDP growth this year, while industry and construction contributed one percentage point each.[52]

Data shows that industrial production increased in all regions, with the highest growth recorded in the Pest region. The value of industrial investment in 2018 was HUF 2,607 billion, up 10% year-on-year at comparable prices, according to the Hungarian Central Statistical Office.[53] In both years, the services sector was the main driver of the GDP growth, with investment in electricity, gas, steam and air conditioning increasing by 39%[54] in 2018. Within the energy sector, significant investments were made in electricity generation.[55]

The data from the HCSO therefore shows that in the years immediately preceding the outbreak of the pandemic, Hungarian industrial production—and in some areas investment in industry—increased. For the purposes of this paper, the priority sectors within manufacturing are automotive, computers, electronics and optical products, food, industrial and tobacco products, metal manufacturing and processing, rubber, plastics as well as non-metallic mineral products. In addition, the services industry may also be covered, although this is a very complex category, involving many different services.

Beside the presentation of statistical data, it is worth mentioning the work of Andrea Szalavecz on the Hungarian context of post-crisis modernisation, in which she examined the impact of the reorganisation of global organisations on Hungarian subsidiaries in 2016. Based on the interviews with thirteen firms in the automotive, electronics and other mechanical engineering industries, she concludes that the reorganisation measures implemented during and after the 2008 crisis clearly had a positive impact on the interviewees (with the exception of one firm). Parent companies have transferred additional production functions from their

48 Lazaro, 2017.
49 Redaktor, 2018.
50 KSH (HCSO), 2019 p. 1.
51 KSH (HCSO), 2018a p. 3.
52 KSH (HCSO), 2020.
53 KSH (HCSO), 2018a p. 3.
54 KSH (HCSO), 2018a p. 8.
55 KSH (HCSO), 2018a p. 8.

subsidiaries in developed countries to Hungary. Szalavecz also points out that knowledge-intensive support functions have also been given local or regional responsibility, broadening and deepening the scope of development tasks for the subsidiaries.[56]

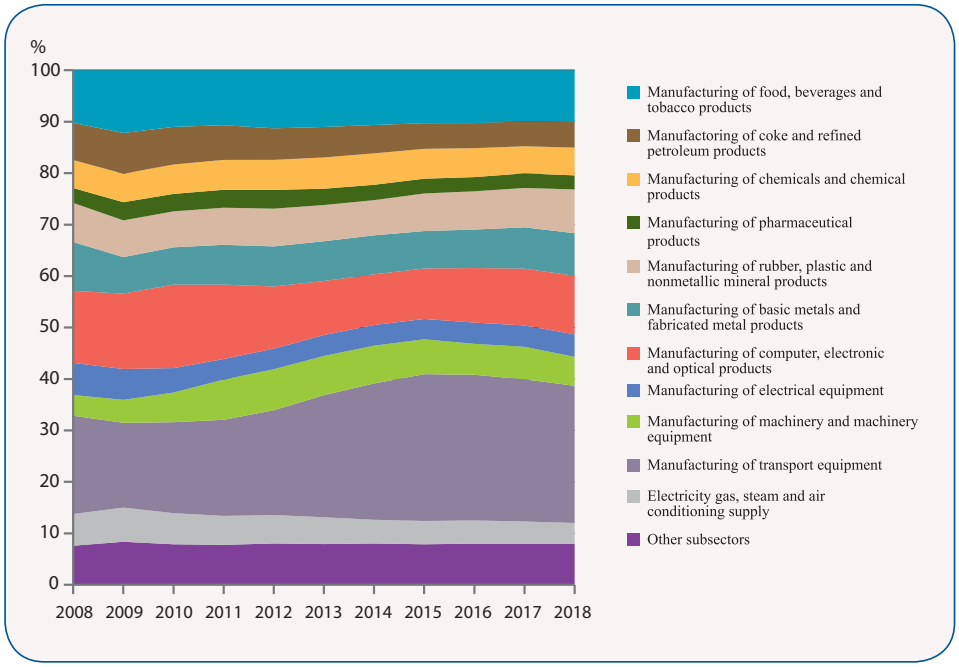


Figure 1. Breakdown of industry's production value by major subsectors
Source: KSH (HCSO), 2018a, p. 14

In 2019, Hungary is ranked 6th from the bottom in the Digital Economy and Society Index (DESI), a measure of the digitalisation process and its elements. This suggests not only that further development is needed, but also that the Hungarian market is still unsaturated, which could be a positive factor in attracting investors. As with any new IT modernisation, if the implementation period is too short, the chances of a system being exposed to threats from malicious intruders are much higher.

Modernisation and industrial security – questionnaire survey

I conducted my own questionnaire survey in order to investigate what business leaders in Hungary thought about the digitalisation of industry and the modernisation of their own companies during the pandemic emergency of 2020. The questionnaire contained 30 questions and consisted of two main sections. The first section was designed to gauge respondents' views

56 Szalavecz, 2016. p. 2.

on whether they expected a wave of development within their industry in the coming years, and also included questions on their plans, such as whether they themselves plan to invest in major modernisation in the next 5-10 years. The second section covered security related issues.

Answers were submitted between 21 and 27 April 2020. According to the report by GKI Digital, which focuses mainly on e-commerce, this period has fallen into phase 4 of the epidemic emergency, characterised by the normalisation of supply chains and the elimination of stock shortages.[57] In terms of protection, the late April period marked the end of the 1st wave of the pandemic, as the government introduced the new rules effective of 1 May.[58] This means that the first effects of the pandemic were already visible during this period, and the first industry management changes for 2020 could already be in place. However, it should also be remembered that the short period only allows for a snapshot.

The questionnaire was distributed to respondents through a well-known industry magazine and a national research centre on the fourth industrial revolution. In terms of platforms, the questionnaire was also available by email (newsletter, internal email) and Facebook, and altogether 86 responses were received. After the questionnaire was filled out, only respondents at middle management level and above were selected, as the answers revealed that there is a lot of misunderstanding in lower positions about technologies such as cloud services, IoT, artificial intelligence or 5G. In addition, lower-ranking professionals do not have a complete overview of the company's plans.

Table 2. Respondents of the questionnaire survey
Source: own research

Position	Field of expertise
Manager, Owner	Logistics, Transport
Manager, Owner	Business service
Manager, Owner	Industrial IT service
Manager, Owner	Construction industry
Manager, Owner	Business service
Manager, Owner	Food industry
Manager, Owner	Industrial IT service
Manager, Owner	Robotics
Manager, Owner	Metalworking
Manager, Owner	Other manufacturing industry
Middle manager	Metalworking
Middle manager	Other manufacturing industry
Middle manager	Industrial IT service
Middle manager	Other manufacturing industry
Middle manager	Metalworking
Middle manager	Construction industry

57 GKI Digital, 2020.
58 MTI, 2020.

Three of the experts surveyed did not know what IoT meant (they did not understand the English or the Hungarian phrase), the other respondents could specify what they meant by IoT devices in a free text box at the next point of the questionnaire. Most respondents highlighted network, instant accessibility and controllability in their definition. One respondent defined IoT as "searching for the unknown".

Six of the respondents said that their company uses some kind of IoT-based device, but when asked what form of device they use, one respondent said that 'phone and printer' was what they had in mind. As these do not fall into the IoT category according to the definition used for the questionnaire, I accepted a total of five positive answers. The IoT devices mentioned included smart meters, RFID devices, devices for monitoring work areas, asset protection devices linked to video systems, and devices used to control and monitor the operation of machines used in manufacturing.

There were two positive responses on the use of AI, but as there was also the problem that one respondent mentioned non "real" AI-based systems, only one response is acceptable. In the case of a positive answer, the company uses the technology to make predictions and optimise machines.

The next part of the questionnaire asked what changes Hungarian industry leaders expect to see in their industry over the next 5-10 years. In response to the question "Do you think your industry is likely to experience a wave of modernisation in the next 5 years?" There were twelve positive answers (yes, almost certainly), two answers were "Possible" and one answer was "No" – the respondent works in metalworking.

The same question was asked, but for the next 10 years. The only difference in the answers was that the respondent who answered "No" to the previous question chose "Possible" for this point.

Table 3. To what extent do you expect a wave of modernisation in the industry concerned?
Source: Own research

Possible answers	Do you expect a wave of modernisation in your industry in the next 5 years?	Do you expect a wave of modernisation in your industry in the next 10 years?
Possible	2	3
Yes, almost certainly	13	13
No	1	0

It is interesting to compare these ideas with the next two questions, which were designed to assess whether the company was planning to modernise over the course of 5 to 10 years. While there were almost no negative responses regarding industries, in this case only eight respondents answered with a clear "Yes" for the 5-year time frame and only ten for the 10-year time frame.

Table 4. Can modernisation be expected in the company?
Source: own research

Possible answers	To your knowledge, is your company planning any modernisation within the next 5 years?	To your knowledge, is your company planning any modernisation within the next 10 years?
Possible	6	5
Yes, almost certainly	8	10
No	2	1

A separate question was asked in case there is already some modernisation going on within the company, which has recently started. The responses are shown in the table below.

Table 5. Modernisation process in the companies concerned
Source: own research

Possible answers	Has your company started any modernisation in the last ONE year?
Yes, in several areas	6
Yes, but only to a lesser extent	7
Not at all	3

In the next part of the questionnaire, respondents were also given the opportunity to elaborate on these processes. The questionnaire was designed to map out exactly where business leaders and middle managers expect modernisation to take place in their industry and in their company in the next five to ten years. In the tables below I used a scale of 1 to 4, with 1 indicating no modernisation expected at all, and 4 indicating that it is planned and will definitely happen.

Table 6. Summary of responses regarding industrial modernisation
Source: own research

In which areas of your industry do you expect to see a significant amount of modernisation in the next 5-10 years?																
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16
a. modernisation of production lines	3	3	4	2	1	3	2	3	4	4	3	3	4	4	3	3
b. replacement of factory workers by machines	3	3	4	1	1	3	2	3	4	3	2	4	3	3	3	3
c. replacement of security personnel with machines/ IT systems	2	2	3	2	2	4	3	4	4	3	2	3	1	3	2	2
d. modernisation of security systems	3	3	3	3	2	4	3	4	4	4	2	3	3	3	2	3
e. modernisation of small electronic devices	3	3	4	3	3	3	4	2	4	3	4	2	2	3	3	3
f. modernisation of production equipment, production units	3	3	4	2	2	3	4	4	4	4	3	2	3	4	3	3
g. modernisation of transport equipment	3	3	4	3	2	2	3	3	4	3	3	2	4	3	3	3
h. modernisation of transport IT and communication systems	3	3	4	3	3	3	4	3	4	4	3	3	3	4	3	4
i. repetitive tasks related to office administration	2	3	3	3	3	2	3	4	4	3	4	2	1	3	3	4
j. modernisation of office IT systems and software	2	3	3	3	3	2	4	3	4	4	3	1	3	3	3	4
k. IoT equipment purchase and modernisation	3	2	3	3	3	3	3	3	4	3	3	1	2	3	1	3
l. Acquisition and modernisation of AI-based tools	2	2	3	2	2	3	3	4	4	3	3	1	4	3	2	3
m. Building / developing a cloud-based system	3	3	3	3	2	4	4	4	4	4	3	2	2	3	2	4

According to the responses, respondents expect their industry to modernise mainly the following areas: production equipment, production units, communication systems, and the introduction and development of cloud-based systems.

Table 7. Areas of modernisation for the company over the next five years
Source: own research

In which areas do you expect your company to modernise in the next 5 years?																
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16
a. modernisation of production lines	1	3	1	2	1	2	3	2	1	4	2	2	1	3	3	2
b. replacement of factory workers by machines	2	2	1	1	2	2	3	3	1	3	2	1	1	3	2	3
c. replacement of security personnel with machines/ IT systems	2	2	1	2	2	4	3	3	1	3	2	1	1	2	1	2
d. modernisation of security systems	2	3	1	3	2	4	3	3	1	4	3	1	1	3	1	3
e. modernisation of small electronic devices	3	3	2	3	3	4	4	2	4	4	4	3	1	3	2	3
f. modernisation of production equipment, production units	3	3	1	2	3	2	4	3	1	4	3	2	1	3	3	3
g. modernisation of transport equipment	3	3	1	3	3	2	3	3	1	4	2	1	1	2	3	4
h. modernisation of transport IT and communication systems	3	3	2	3	2	2	3	3	4	4	3	1	1	3	3	3
i. repetitive tasks related to office administration	2	3	2	3	2	4	3	4	4	4	3	1	1	3	3	3
j. modernisation of office IT systems and software	2	3	2	3	2	4	3	3	4	4	3	2	1	3	3	3
k. IoT equipment purchase and modernisation	2	2	2	3	2	4	4	3	4	4	3	1	1	3	1	3
l. Acquisition and modernisation of AI-based tools	3	2	3	2	1	4	3	3	4	4	3	1	1	3	1	3
m. Building / developing a cloud-based system	3	3	2	3	3	4	3	3	4	4	2	2	1	3	1	3

Regarding their own company, respondents gave more conservative answers. It was interesting to see that one respondent does not expect any modernisation at all in his company. The others mostly expected the modernisation of small electronic devices, the replacement of repetitive tasks related to office administration, the purchase and modernisation of IoT devices. This means that although the majority have a strong opinion on trends affecting

their industry, for some reason they did not wish to follow these trends with regard to the modernisation of their own company. To explore these reasons more in-depth, the next series of questions asked respondents to weigh up the issues that they would consider when investing in modernisation.

Table 8. Key considerations when planning modernisation investments
Source: own research

If you were leading your company's modernisation programme, how much weight would you give to the following aspects in your investment?																
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16
a. expected costs	4	3	3	3	3	3	3	4	3	3	3	3	1	4	3	3
b. make the process as quick as possible	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2
c. information security (software, training, etc.)	4	3	4	4	3	4	3	4	4	4	3	3	3	4	4	3
d. infrastructure security (proper implementation, reliability of suppliers, etc.)	4	3	4	3	3	4	4	3	4	4	3	3	3	4	4	3
e. replacing and renovating old equipment as much as possible	3	3	2	3	2	3	3	3	3	3	3	3	3	4	4	3
f. replacing as much of the live workforce as possible with automated or software-based solutions	2	3	3	3	3	3	3	3	4	2	3	1	1	3	3	3
g. supporting the work of the existing live workforce as much as possible with machines or software solutions	3	3	3	3	4	3	3	3	4	4	3	4	1	3	3	4

It is interesting to note that most respondents would give similar weight to all aspects, and it is striking that only three respondents identified *expected costs* as a high priority. However, the answers also indicate that information security and infrastructure security are also a priority for quite a few respondents. For five of them, supporting the human workforce with machines or software is also a top priority, and its effective implementation would be an important step in the context of existing global innovation trends. The other part of the questionnaire covered security related issues.

Table 9. Answers to questions related to company security
Source: own research

Are the following statements true for your company?																
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16
a. It has a well-functioning access control system	Y	Y	N	Y	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
b. It has adequate software protection (unified system, antivirus, etc.)	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N
c. The office infrastructure is adequately protected	Y	Y	N	Y	Y	Y	Y	N	N	Y	Y	Y	N	Y	Y	Y
d. The production line or the equipment used for production or service are safe	N	Y	N	N	Y	N	Y	N	N	Y	Y	Y	N	Y	Y	N
e. Work can be done safely on your personal work equipment	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	N
f. IT equipment (laptop, mobile phone, etc.) can be taken home by employees	Y	Y	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N
g. On IT devices, employees also carry out (personal) activities unrelated to their tasks (storing personal files on the devices, use Facebook and their own email address, leisure activities, etc.)	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	Y	Y

Although the previous questions suggest that security is a high priority for company managers, the following series of questions leads to the following conclusions:

- Half of those surveyed do not consider the production line or the equipment used for production and services to be safe.
- Three respondents said that work on company equipment cannot be done in a secure manner.
- In sixteen out of ten companies, employees can take their IT devices home and in eleven cases it is common for them to use the equipment for personal communication, including social media and email.

The next series of questions also covered a narrower scope of security related issues, such as concerns and ideas about the deployment of 5G networks. From an IT security point of view, it is mainly relevant because devices can only connect to the 5G network if they have the appropriate chips. In terms of the development level of 5G technology, China's Huawei is leading the way alongside some other Chinese, Korean and US competitors, so market acquisition also has its geopolitical and security policy implications.

America has banned Huawei in its territory. The Chinese company grew by 33% in 2017, which is a huge market growth. For America, maintaining the position of Apple is an important economic issue. But what is 5G and why is it interesting? There are two main factors that make 5G special. One is its speed and the other is that it requires a completely new infrastructure, new devices with new chips.[59] Three factors have had a significant impact on the industry in recent years, which are summarised in the table below.

Table 10. The impact of individual technologies on the industry
Source: own research

Technology	Impact on industry
IoT devices	The emergence of devices capable of 5G communication
Artificial intelligence, machine learning	Fast and efficient data processing
Cloud-based systems	Cheap and efficient data storage
5G	Fast transfer of large data

These developments predict that in the future, it will not only be easy and cheap to work with data that can be detected by simple sensors in microelectronic devices (such as humidity, vibration or light intensity), but video images can be quickly and efficiently transmitted in a high resolution format.

The switchover cannot happen immediately, of course, as the necessary infrastructure needs to be in place to achieve sufficient coverage to transmit data over long distances. However, during the transition period, there are increased risks in installations where the safety system is not yet at a level that would be appropriate for the technology.

59 Index, 2020.

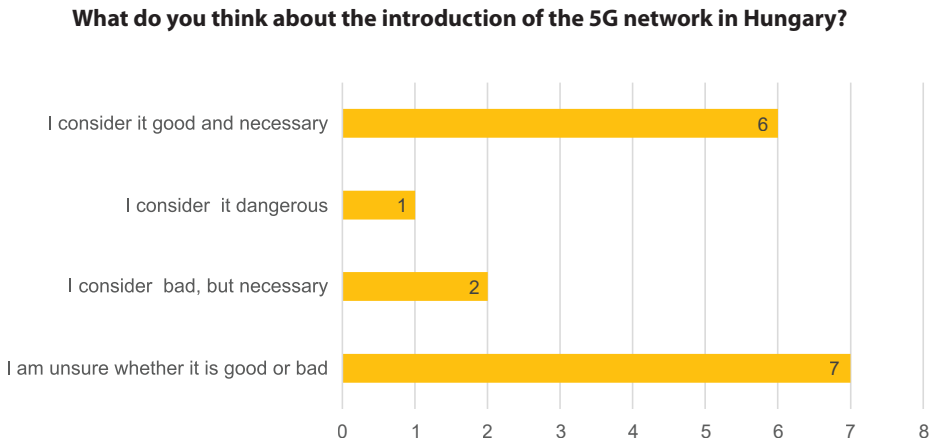


Figure 2. Summary of responses received on the introduction of 5G network in Hungary

The overall opinion on the 5G network is mixed, but the majority of respondents is positive about the change. The respondents could express the opinion by answering an open question that was aimed at exploring the underlying reasons. Five of the respondents highlighted the fact that they could not find "convincing information, descriptions" or "objective sources" on the exact natural and health-related risks of the 5G network. Seven respondents answered that 5G deployment is essential for development, as "modernisation requires the deployment of high-capacity, fast and congestion-free connections". Three respondents mentioned a specific negative impact, namely "increased exposure of the environment to radiation", "natural destruction" or "long-term health effects on humans". One respondent said that the current speed would be sufficient for the needs of their business. Only two respondents expressed an opinion regarding which company builds the 5G infrastructure.

In the next question, respondents had to select the company they would prefer to deploy the 5G network. The choices were: a) Huawei (China), b) ZTE (China), c) Qualcomm (USA), f) Samsung Electronics (South Korea), g) HPE (Germany), h) Ericsson (Sweden), i) Nokia (Finland), j) Makes no difference.

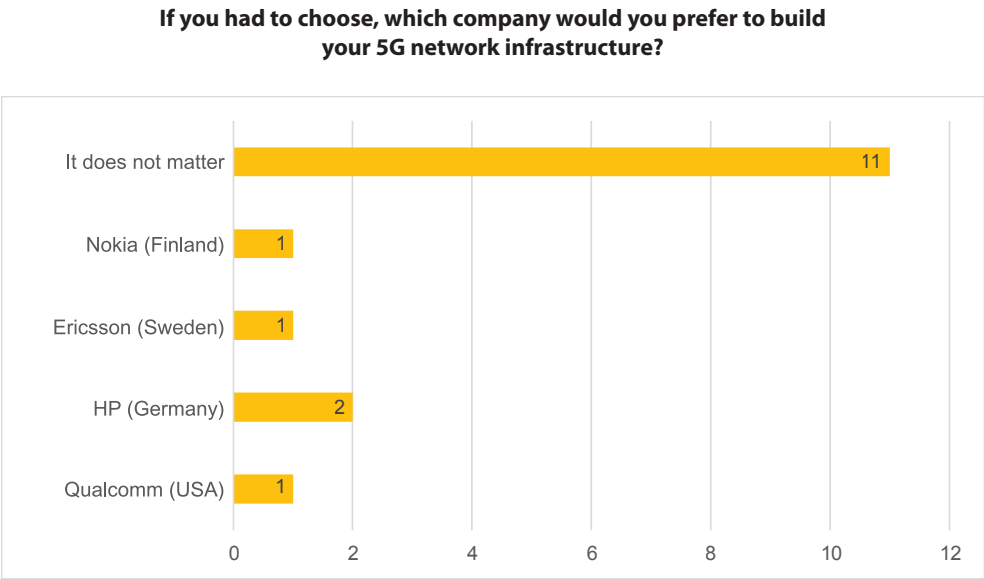


Figure 3. Summary of responses received on the deployment of the 5G network infrastructure

Based on the responses received, eleven out of sixteen respondents expressed no specific commitment regarding the deployment of the 5G network infrastructure. There could be several reasons for this, for example they do not have enough information about the providers or it does not matter to them who the actual provider is.

Afterwards, respondents were asked to explain why they had chosen the option they had. Those who answered that it made no difference which company builds the 5G infrastructure mostly said they had little knowledge of the technology. As none of the companies listed was a Hungarian company, respondents would prefer to make a decision based on the content of the price quotes. Those who chose European companies typically did so for security reasons, or because the company is embedded in a society where "stability and transparency" are a priority and this nation has "the right checks and balances and sense of responsibility". The only reason why the respondent who voted for the US company chose Qualcomm was because he thought it was the lesser evil.

The next two questions were also related to 5G, but they sought to explore the answers from a different perspective. Since emphasising the health risks associated with 5G has a geopolitical relevance (this is the reason why the network deployment is obstructed in Switzerland[60]), it is important to understand what Hungarian leaders think of this issue.

60 E&T, 2020.; Reuters, 2020.

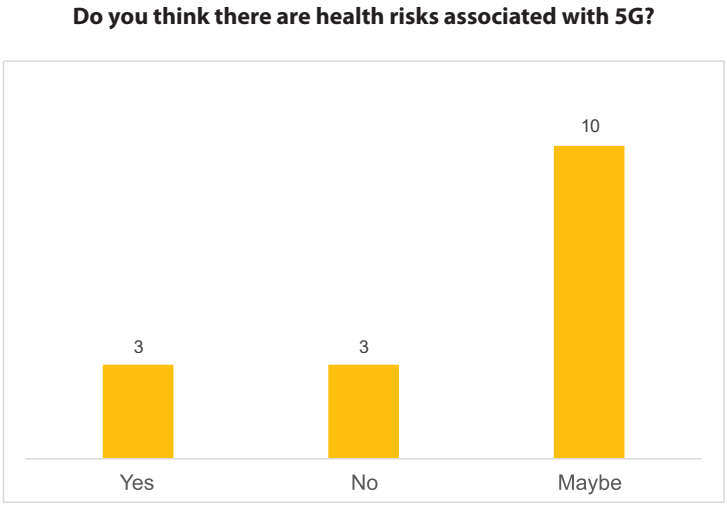


Figure 4. Opinions on health risks associated with 5G

The above chart shows that most respondents are uncertain about the health risks, while some people hold very certain opinion on the harmfulness or harmlessness of the technology (3 and 3 of each, respectively).

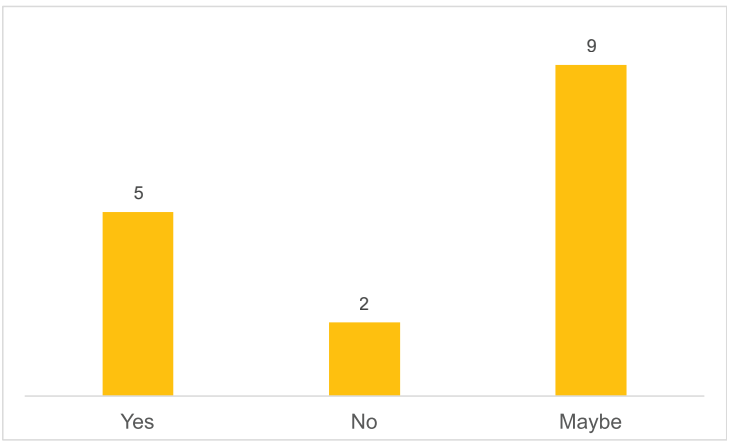


Figure 5. Issues related to 5G information security risks

It is interesting to note that nine respondents were uncertain about the security risks regarding the 5G network deployment, and five respondents were convinced and confident that the new technology does pose such a risk. Furthermore, respondents said that information security is important, but that managers do not want to choose a 5G network company based on this, but on other criteria, such as price quotes.

The final question examined the subjective perception of company managers and middle managers regarding the safety within their own company in a comprehensive way.

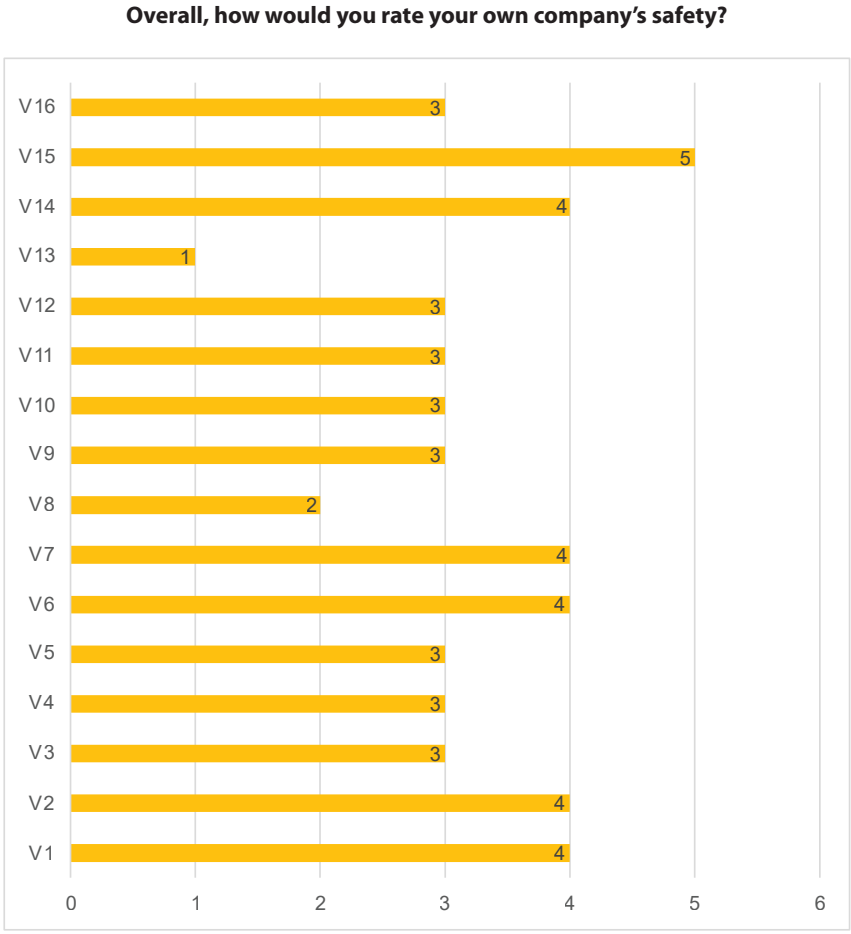


Figure 6. Summary of responses

It is striking that only one respondent gave the highest score to his company's security system, while most of them chose a medium score. It is important to note that these values represent the respondents' opinions, not the actual strength of their company's security systems. This is worth highlighting because the number of medium scores in this respect can be positive, as it suggests that most respondents are aware of the potential risks and may therefore be more persuaded by a possible offer to improve the security of the company.

Possible future scenarios and threats to industrial modernisation in Hungary

Following the detailed description of the questionnaire, in this chapter the author will briefly summarise the results obtained, with a particular focus on the points that could be risk factors.

The results presented in the previous chapter confirm that from a business perspective Hungary ranks among the relatively under-digitalised countries.[61] Given the trends already in place, an increase in the level of digitalisation can be expected in the future, especially if foreign investors include companies that emerge from the crisis as winners. However, if companies and governments do not place enough emphasis on supporting innovation, modernisation and closely related educational programmes, this could lead to a larger backlog in the future, as data suggest such trends shall persist and become even stronger in the long-term.

Based on the theoretical analysis and empirical research, the following geopolitical and economic risk factors can be identified in relation to the digitalisation of Hungarian industry:

- The slow pace of digitisation could result in an economic backlog.
- Huawei may be the most promising candidate for 5G deployment because of the European regulations, the company's approval rating among business leaders and its competitiveness.
- The risk of potential attack (intrusion) is increased due to the way employees use devices (especially due to shadow IT).
- The lack of objective information on security and the 5G network means that there is a higher probability of making wrong decisions.
- The sudden surge of modernisation may create conditions that make it even more difficult to perform complex cyber defence tasks and to investigate vulnerabilities and prevent problems.

Since according to the questionnaire some business leaders have unrealistic perceptions about the level of IT within their companies (for example, because there is mismatch between face-to-face communication on devices and the perception of security, or due to a lack of resources allocated for 5G communication networks), information and awareness-raising can be key to building security perceptions.

61 DESI, 2020.

In the light of the above information, it could be useful to create an information sharing platform where Hungarian industrial players can receive filtered, credible and reliable information in the Hungarian language regarding the latest technologies, even from different sources.

There are initiatives in Hungary that provide information on how to introduce modern technological solutions and what factors are required for it, but they are either profit-oriented (magazines, company news sites, blogs) or they only focus on a specific technology (e.g. an information site for Hungarian companies that use artificial intelligence).

Furthermore, the differences should be examined between the SME sector and large companies as well as their significant interlinkages in terms of cybersecurity. This mapping process this will provide a clearer picture on risk factors that cannot be inferred from the general responses of industrial decision-makers alone.

From a practical point of view, the dissemination of credible information deserves particular attention. It requires the mapping of where industry decision-makers get their information from, the reason why they choose those sources as well as the most appropriate way for them to acquire it. There could be stark differences in this area, where a busy senior executive is probably more easily available to attend an industry conference to give a presentation or join a networking event than a middle manager who reads the most important industry news over lunch or gets up-to-date information by reading the newsletters of their partner companies.

Summary

Studies on the nature of previous crises and industrial revolutions suggest that there is a strong possibility that the post-corona crisis will amplify certain innovation trends in the long run. Based on this assumption, it may be worthwhile to examine which industries, countries and technologies are more likely to experience a wave of innovation, and paying particular attention to these, develop appropriate policy decisions for the future.

The questionnaire-based research in this paper only reflects the opinions and preparedness of a handful of company managers. It does not give a complete picture of the market situation, so it may be worthwhile to extend the research to a larger sample, especially in view of the controversial answers.

The state, industrial actors and the European Union must cooperate in order to ensure that industrial digitalisation is safe and secure. Given the complexity of the task and the situation created by the crisis, the solution cannot be left to one party or the other.

In addition to the above research on 5G networks, a content analysis may provide a more comprehensive and specific answer as to what health care and information security related risks have disseminated in the Hungarian media. It would give a clearer picture on the information strategies that companies should develop to help them make a safe transition to new technologies.

From a geopolitical point of view, one of the most important issues for Hungary is to find a balance in its foreign policy and to allow technological standards as well as foreign companies to enter the market. This is how Hungary can assert its own interests within the

Central and Eastern European region. While Hungary should pay attention to the appropriate security measures in the development of its cyber defence policy, it must also comply with EU requirements, prevent the technological lagging behind as well as seek and grab new opportunities. Maintaining this balance becomes particularly important if the scenario presented in this research materialises, i.e. if the post-SARS-COV crisis also leads to deeper transformation that accelerates geopolitical realignment and results in tighter controls.

Bibliography

1. Archibugi, D., Filippetti, A. Frenz, M., (2012), *The Impact of the Economic Crisis on Innovation: Evidence from Europe. Technological Forecasting and Social Change*, https://www.researchgate.net/publication/238048698_The_Impact_of_the_Economic_Crisis_on_Innovation_Evidence_from_Europe, accessed on 28.04.2020.
2. Avishai, Bernard, (2020), 'The pandemic isn't a black swan but a portent of a more fragile global system', *New Yorker*, (21.04.2020), https://www.newyorker.com/news/daily-comment/the-pandemic-isnt-a-black-swan-but-a-portent-of-a-more-fragile-global-system, accessed on 28.04.2020.
3. Carey, Benedict, (2020), 'Mapping the Social Network of Coronavirus', *New York Times*, (13.03.2020), https://www.nytimes.com/2020/03/13/science/coronavirus-social-networks-data.html, accessed on 28.04.2020.
4. Chinazzi, M., Davis, Jessica T., Ajelli, M., et al., (2020), 'The effect of travel restrictions on the spread of the 2019 novel coronavirus (SARS-COV) outbreak', *Science*, Vol 368, Issue 6489, (24.04.2020), https://science.sciencemag.org/content/368/6489/395, accessed on 29.04.2020.
5. Chung, Juliet, (2020), 'This Hedge Fund Saw Risks of Coronavirus Early. Now It's Up 36%', *Wall Street Journal*, (02.04.2020), https://www.wsj.com/articles/this-hedge-fund-saw-risks-of-coronavirus-early-now-its-up-36-11585819802, accessed on 28.04.2020.
6. Deák, Veronika (ed.), (2018), *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára*. (Targeted cyber attacks. Annual training for the person responsible for electronic information system security), Hungarian University of Public Service (NKE), http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/11181/EIB2018_50_C%C3%A9lzott%20kibert%C3%A1mad%C3%A1sok_imprim%C3%A1lt.pdf?sequence=1&isAllowed=y, accessed on 28.04.2020.
7. Deibert, Ron, 'The Geopolitics of Cyberspace after Snowden', http://currenthistory.com/Deibert_CurrentHistory.pdf, accessed on 28.04.2020.
8. DESI, (2020), Europe.ec Connectivity – Broadband market developments in the EU, Digital Economy and Society Index Report 2019, https://ec.europa.eu/digital-single-market/desi, accessed on 29.04.2020.
9. Douzet, Frédérick (2016): 'Geopolitika a kibertér megértéséhez' (Geopolitics to understand cyberspace), *Műhelymunkák, A virtuális tér geopolitikája* (Workshop, Geopolitics of Virtual Space), 2016/I., http://mek.oszk.hu/16100/16182/16182.pdf, accessed on 27.04.2020.

10. E&T (2020), 'Swiss refuse to back down on 5G radiation standards, hampering rollout', (23.04.2020), https://eandt.theiet.org/content/articles/2020/04/swiss-refuse-to-back-down-on-5g-radiation-standards-hampering-rollout/, accessed on 29.04.2020.
11. ENISA (2019), 'EU coordinated risk assessment of the cybersecurity of 5G networks', https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049, accessed on 14.06.2020.
12. ENISA (2020), 'IoT', https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot, accessed on 29.04.2020.
13. Gauri, P., Van Erdeen, J., (2019), *A 5th Industrial revolution? What it is, and why it matters*, https://5thelement.group/wp-content/uploads/2019/05/A-5th-Industrial-Revolution_-What-It-Is-And-Why-It-Matters_05.03.19_vX.pdf, accessed on 29.04.2020.
14. Gibson, William, (1984), *Neuromancer*, (Ace Science Fiction Books, New York), ISBN: 9780441569595.
15. GKI Digital, (2020), 'A koronavírus nyertese?! – lendületben az e-kereskedelem' (The winner of the coronavirus – e-commerce is on the rise), (07.05.2020), https://gkidigital.hu/2020/05/07/koronavirus/, accessed on 21.06.2020.
16. Hershbein, Brad J., Kahn, Lisa B., (2016): 'Do recessions accelerate routine-biased technological change? Evidence from Vacancy Postings', (Upjohn Institute, 17.10.2016), https://research.upjohn.org/cgi/viewcontent.cgi?article=1272&context=up_workingpapers, accessed on 29.06.2020.
17. Holodny, E., (2017), 'A keyplayer in China and the EU's 'third industrial revolution' decribes the economy of tomorrow', *Business Insider*, (16.07.2017), http://www.businessinsider.com/jeremy-rifkin-interview-2017-6, accessed on 29.04.2020.
18. Index, (2020), 'America bans Huawei', https://index.hu/aktak/huawei_kitiltas_egyesult_allamok_kina_kereskedelmi_haboru_kemkedes_nemzetbiztonsagi_kockazat_szankciok_android/, accessed on 09.03.2021.
19. Jaimovich, Nir, Siu, Henry E., (2012), 'Job Polarization and Jobless Recoveries', NBER Paper Series, https://www.nber.org/system/files/working_papers/w18334/w18334.pdf, accessed on 09.03.2021.
20. Klingenberg, Cristina Orsolin, do Vale Antunes, José Antônio Jr., (2017), 'Industry 4.0: what makes it a revolution?', https://www.researchgate.net/profile/Cristina-Klingenberg/publication/319127784_Industry_40_what_makes_it_a_revolution/links/5993035e458515c0ce61eb5e/Industry-40-what-makes-it-a-revolution.pdf, accessed on 09.03.2021.
21. Kovács, László (2018): *A kibertér védelme* (Protecting cyberspace), National University of Public Service (NKE), https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf, accessed on 29.04.2020.
22. Kovács L., Sipos M., (2010),: 'A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala' (Stuxnet and what's behind it: Facts and the dawn of cyberwar), *Hadmérnök Journal*, Volume 5, Number 4., http://hadmernok.hu/2010_4_kovacs_sipos.pdf, accessed on 29.04.2020.

23. Kralovánszky, Kristóf, (2019), 'A kibertér fejlődése' (The evolution of cyberspace), *Hadmérnök Journal*, Vol. 14, No. 4, http://real.mtak.hu/108269/1/HM_2019_4_Kralovanszky_Kristof.pdf, accessed on 29.04.2020.
24. KSH (HCSO), (2018a), 'Helyzetkép az iparról' (A snapshot of the industry), http://www.ksh.hu/docs/hun/xftp/idoszaki/jelipar/jelipar18.pdf, accessed on 29.04.2020.
25. KSH (HCSO), (2018b), 'Digitális gazdaság és társadalom' (Digital economy and society), http://www.ksh.hu/docs/hun/xftp/idoszaki/ikt/ikt18.pdf, accessed on 29.04.2020.
26. KSH (HCSO), (2019), 'Statisztikai tükör' (Statistical mirror), http://www.ksh.hu/docs/hun/xftp/stattukor/gdp_eu/gdp_eu18.pdf, accessed on 29.04.2020.
27. KSH (HCSO), (2020): 'Gyorstájékoztató. Bruttó hazai termék (GDP), 2019. IV. negyedév (második becslés)' (Information on the Gross Domestic Product for Q2, second estimate), http://www.ksh.hu/docs/hun/xftp/gyor/gdp/gdp1912.html, accessed on 21.06.2020.
28. Lazaro, O., (2017), 'Analysis of National Initiatives for Digitising Industry. Hungary: IPAR 4.0.', https://ec.europa.eu/futurium/en/system/files/ged/hu_country_analysis.pdf, accessed on 29.04.2020.
29. Levy, Steven, (2020), 'The Doctor Who Helped Defeat Smallpox Explains What's Coming', *Wired*, (19.03.2020), https://www.wired.com/story/coronavirus-interview-larry-brilliant-smallpox-epidemiologist, accessed on 29.04.2020.
30. Liao, Y., Loures, E. R., Deschamps, F., Brezinski, G., & Venâncio, A., (2018), 'The impact of the fourth industrial revolution: a cross-country/region comparison', (28.01.2018), https://www.researchgate.net/publication/322507266_The_impact_of_the_fourth_industrial_revolution_A_cross-countryregion_comparison, accessed on 28.04.2020.
31. McKinsey Institute, (2017), 'A future that works: automation, employment and productivity', https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Digital%20Disruption/Harnessing%20automation%20for%20a%20future%20that%20works/MGI-A-future-that-works_Full-report.ashx, accessed on 29.04.2020.
32. Menachery, V., Yount, B., Debbink, K. et al., (2015), 'A SARS-like cluster of circulating bat coronaviruses shows potential for human emergence', (09.11.2015), https://www.nature.com/articles/nm.3985, accessed on 29.04.2020.
33. Monostori, L., (2014), 'Cyber-physical production systems: Roots, expectations and R&D challenges', https://www.researchgate.net/publication/263857376_Cyber-physical_Production_Systems_Roots_Expectations_and_RD_Challenges, accessed on 27.04.2020.
34. Mokyr, J.I. (ed.), (1985), *The Economics of the Industrial Revolution*, (Rowman & Littlefield Publishers Inc, USA).
35. MTI, (2020), 'Hétfőtől kezdődik a védekezés új szakasza' (A new phase of protection begins on Monday), (01.05.2020), https://koronavirus.gov.hu/cikkek/hetfotol-kezdodik-vedekezes-uj-szakasza, accessed on 21.06.2020.

36. Muro, Mark, (2020), 'How COVID-19 will change the nation's long-term economic trends, according to Brookings Metro scholars', https://www.brookings.edu/research/how-covid-19-will-change-the-nations-long-term-economic-trends-brookings-metro/, accessed on 09.03.2021.
37. Muro, Mark, Maxim, Robert, Whiton, Jacob, (2020), 'The robots are ready as the COVID-19 recession spreads', https://www.brookings.edu/blog/the-avenue/2020/03/24/the-robots-are-ready-as-the-covid-19-recession-spreads/, accessed on 09.03.2021.
38. Niiler, Eric, (2020), 'An AI Epidemiologist Sent the First Warnings of the Wuhan Virus', (25.01.2020), https://www.wired.com/story/ai-epidemiologist-wuhan-public-health-warnings/, accessed on 29.04.2020.
39. OECD, (2012), 'OECD Science, Technology and Industry Outlook 2012', https://www.oecd.org/sti/sti-outlook-2012-chapter-1-innovation-in-the-crisis-and-beyond.pdf, accessed on 29.04.2020.
40. Ó Tuathail, Gearóid, (2003), 'Introduction XI-XXXI' in 'Thinking critically about geopolitics', *The Geopolitics Reader*, (Routledge, London and New York), ISBN: 0203444930, https://frenndw.files.wordpress.com/2011/03/geopol-the-geopolitics-reader.pdf, accessed on 09.03.2021.
41. Portfolio (2020), 'Itt egy videó arról, amikor a világhírű magyar tudós 5 évvel ezelőtt megjósolja a világjárványt' (Here is a video of the world-famous Hungarian scientist predicting the pandemic 5 years ago), *Portfolio*, (22.03.2020), https://www.portfolio.hu/gazdasag/20200322/itt-egy-video-arrol-amikor-a-vilaghiru-magyar-tudos-5-evvel-ezelott-megjosolja-a-vilagjarvanyt-421126, accessed 29.04.2020.
42. Rapid Transition Alliance, (2019), 'From oil crisis to energy revolution. How nations once before planned to kick the oil habit', (26.04.2019), https://www.rapidtransition.org/stories/from-oil-crisis-to-energy-revolution-how-nations-once-before-planned-to-kick-the-oil-habit/, accessed on 29.04.2020.
43. Redaktor, (2018), 'Digitális Egységes Piac: a Digitális Innovációs Központok Munkacsoportjának harmadik találkozója az európai ipar digitális átalakításáért' (Digital Single Market: third meeting of the Digital Innovation Centres Task Force for the digital transformation of European industry), *eGov Hírlevél*, https://hirlevel.egov.hu/2018/06/03/digitalis-egyseges-piac-a-digitalis-innovacios-kozpontok-munkacsoportjanak-harmadik-talalkozoja-az-europai-ipar-digitalis-atalakitasaert/, accessed on 09.03.2021.
44. Reuters, (2020), 'Swiss maintain 5G emission standards amid safety concerns', (22.04.2020), https://www.reuters.com/article/us-swiss-5g/swiss-maintain-5g-emission-standards-amid-safety-concerns-idUSKCN22420H, accessed on 29.04.2020.
45. Robinson, I. William, (2018), 'The next economic crisis: digital capitalism and global police state', *Sage*, https://journals.sagepub.com/doi/pdf/10.1177/0306396818769016, accessed on 29.04.2020.

46. Roubini, Nouriel, (2020), 'Coronavirus pandemic has delivered the fastest, deepest economic shock in history', *The Guardian*, (25.03.2020), https://www.theguardian.com/business/2020/mar/25/coronavirus-pandemic-has-delivered-the-fastest-deepest-economic-shock-in-history?CMP=Share_iOSApp_Other&fbclid=IwAR1xiYWqB0xx3antvltQ_G0BhavbU2bbmF0guVhjQNtvhqxBwoku1KWWmc4, accessed on 29.04.2020.
47. Rhysider, Jack, (2019), 'NotPetya', EP 54, https://darknetdiaries.com/episode/54/, accessed on 09.03.2021.
48. Schwab, Klaus, (2015), 'The Fourth Industrial Revolution. What It Means and How to Respond' *Foreign Affairs*, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution, accessed on 09.03.2021.
49. Snowden, Edward, (2019), *Rendszerhiba*, (XXI. Század Kiadó, Budapest), ISBN 978 615 5955 69 3.
50. Szalavetz, Andrea, (2016), 'Az ipar 4.0 technológiák gazdasági hatásai –Egy induló kutatás kérdései' (The economic impact of Industry 4.0 technologies - Initial research issues), *Külgazdaság*, 60, http://real.mtak.hu/39363/1/Ipar40.pdf, accessed on 29.04.2020.
51. Szilágyi, István, (2018), *A geopolitika elmélete* (Theory of geopolitics), Second ed., (PAIGEO Alapítvány, Budapest), ISBN 978 615 80951 0 5.
52. Taylor, Edward, Schwartz, Jan, (2020), 'Volkswagen suspends production as coronavirus hits sales', Reuters, https://www.reuters.com/article/us-volkswagen-results-2019-idUSKBN2140OF, accessed on 09.03.2021.
53. Tikos, Anita, (2018), 'Információmegosztás szervezetek és államok között célzott kiberbiztonsági incidensek esetén' (Information sharing between organisations and states in the event of targeted cybersecurity incidents), Deák, Veronika (ed.), (2018), 'Célzott kibertámadások Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára' (Targeted cyber attacks Annual training for the person responsible for the security of electronic information systems), Hungarian University of Public Service (NKE), http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/11181/EIB2018_50_C%C3%A9lzott%20kibert%C3%A1mad%C3%A1sok_imprim%C3%A1lt.pdf?sequence=1&isAllowed=y, accessed on 28.04.2020.

István Paráda

Military cyber exercises to achieve security strategies and digitalisation objectives

Resume

The development and management of NATO and US cyber strategy clearly shows the significant impact of technological and IT developments on security policy. At international level one of the important tools to achieve the objectives set out in security policy strategies is the conduct of military cyber exercises. To this end, I recommend that technical cybersecurity exercises are organised and implemented in Hungary, both at the security policy level, at the administrative level and in the military context.

Executive summary

Thanks to technological and information developments and revolutions, security policy has also undergone significant changes over the past years. Aspects of cyberspace and cyber operations have emerged in security policy strategies. One way to accomplish these aspirations is to conduct military cyber exercises. In both security policy and military contexts, I recommend organizing and implementing technical cyber operation exercises in Hungary.

Introduction

As technology continues to evolve and new security challenges and threats emerge, cyber operations have become a common part of military activities. The North Atlantic Treaty Organisation (hereinafter referred to as NATO), the United States of America and Hungary have recognised the raison d'être of such a skill. It is clear that almost every country is seeking to address cyberspace security issues at national level. Cyberspace is a collective term for "users, devices, software, processes, stored or in-transit information, services and systems that are directly or indirectly connected to a computer network".[1]

If we talk about security itself or about managing cyber operations on a national scale, it means that it has to be interpreted at a strategic level. The question arises as to how national strategies are addressing the information revolution and the rapid pace of information and technological development that it entails. Are they ignored, do they become part of the process, or do they exploit their potential?

From the perspective of national security and national military strategies, both Hungary and the Hungarian Defence Forces face significant challenges in the development of cyber operational capabilities. There are many results of the work in this field, such as the establishment of the Cyber Defence Academy of the Hungarian Defence Forces[2] in Szentendre. The Hungarian Defence Forces aim to meet a number of cyber defence requirements from the state, national and military sides, in line with the current National Security Strategy of our country[3], its National Military Strategy[4] and National Cyber Security Strategy[5] as well. In addition, it can be determined that in Hungary, security policy and military cyber operations efforts are carried out in accordance with Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies[6].

Many allied and neighbouring nations are also placing significant emphasis on practical training and education in information security and cyber operations to develop, improve and achieve the capabilities identified in the strategies. One way to do this is to plan and conduct military cyber exercises to help acquire the relevant knowledge and skills. These exercises take place at several levels, including strategic, i.e. managerial and decision-making levels as well as technical and professional levels. Military cyber exercises are a major contribution to achieving the objectives of the national security, national military and national cybersecurity agendas.

For this reason, the author believes that the role of cyber strategies within national security, military and national security strategies and their linkage with military cyber exercises is of utmost importance, as they result in a militarily and security-politically advantageous situation and a continuous development and advantageous digital position for nations able to organise and conduct such exercises.

---

1 László Kovács, *A kibertér védelme* (Protecting cyberspace), (Budapest, Dialóg Campus Kiadó, 2018), https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf, accessed on 30.03.2020.

2 Ádám Draveczki-Ury, 'Átadták a Magyar Honvédség Kiber Képzési Központját' (The Cyber Training Centre of the Hungarian Defence Forces was inaugurated), (13.06.2019 12:00), https://honvedelem.hu/galeriak/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat/, accessed on 30.03.2020.

3 Government Decree 1035/2012. (II. 21.) on the National Security Strategy of Hungary.

4 Government Decree 1656/2012. (XII. 20.) On the National Military Strategy of Hungary.

5 Government Decree 1139/2013. (III. 21.) Government Decree.

6 Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies.

Evolution of NATO cyber defence guidelines

Today, the use of information and info-communication technology is considered a basic service. It impacts almost every aspect of our lives, from financial transactions to obligations at work and other daily activities. If we look at the issue from a military perspective, it is clear that the rapid development of information, telecommunications and electronics technology has inevitably reached the field of security policy. This development and the consequent emergence of cyber operations have an impact on the political and economic sectors, as well as on the armed forces.[7] As a member state, Hungary abides by and complies with the provisions set out in the North Atlantic Treaty.

Before describing the processes related to cyber policies, it is important to formulate the definition of cybersecurity. The definition of cybersecurity based on document ITU-T X.1205 of the International Telecommunication Union is as follows: *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment, the organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of information transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment."*[8]

Since 2007, NATO has prioritised cyber defence and cyber warfare. There are many records of the cyber operations launched against Estonia in 2007, when a series of attacks triggering a major Denial of Service (DoS) occurred. In April 2007, the removal of a Soviet World War II memorial in Tallinn met with great indignation from the Russian population in Estonia. At the same time, Estonia's IT and telecommunications infrastructure was under cyber attack, mainly from outside the country. The attacks launched probably from Russia are due to disagreements between Estonia and Russia. The incident drew the attention to entirely new forms of warfare. The event is a significant example of the important role that info-communications play in society. The event made it clear that NATO must respond to new challenges and recognise the need to develop appropriate capabilities. Particularly, because—under Article 5 of the Treaty of the North Atlantic Treaty Organisation that was signed in Washington on 4 April 1949—collective defence means that an attack on a NATO member state is considered an attack on the organisation. Article 5 of the NATO Treaty provides as follows: *"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will*

7 Szabolcs Jobbágy, 'Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő' (The convergence of the information society, information technology and telecommunications. Past, present, future), *Hadmérnök Journal*, Vol. IV No. 1, (March 2009), pp. 185-188, http://www.hadmernok.hu/2009_1_ jobbagy.pdf, accessed on 30.03.2020.

8 ITU-T X.1205 telecommunication standardisation sector of ITU (04/2008) series x: data networks, open system communications and security telecommunication security overview of cybersecurity. 8., https://www.itu.int/rec/T-REC-X.1205-200804-I, accessed on 30.03.2020.

assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area."[9] Recognising the attack that crippled Estonia's IT and telecommunications infrastructure, NATO saw the need to introduce measures on cybersecurity and cyber operations.

In 2008, the Alliance established the Cooperative Cyber Defence Centre of Excellence (hereinafter referred to as: CCDCOE). It is dedicated to education, research and development of cyber operations and cybersecurity, and also examines moral and legal issues, in addition to technical and technological perspectives. The idea of creating the CCDCOE was approved by the Supreme Allied Commander Transformation in 2006. Negotiations with the sponsoring nations started in 2007 and the Memorandum of Understanding was signed in 2008. In addition to the founding members, NATO member states are joined by a steady stream of sponsoring nations, including Hungary in 2010.[10] As a consequence of the events of 2007, the declarations have also increasingly focused on cybersecurity and cyber operations, as can be seen in the 2008 Bucharest Summit Declaration.[11]

At the Lisbon Summit in 2010, a new strategic blueprint was adopted, tasking the North Atlantic Council (NAC) with the development of a thorough new NATO cyber defence policy and an implementation plan. The scope of armed attacks has been broadened in the context of collective defence under Article 5 of the Treaty.[12] The Lisbon Summit Declaration provided more detailed information on cybersecurity than previous ones. The concept of cyberspace has emerged and cyber defence has become important in conflict management. The need to accelerate the achievement of capabilities and the need for planning processes to assist allies has been given a prominent role.[13]

At the Chicago Summit in May 2012, Allied leaders reaffirmed their commitment to improve the Alliance's cyber defences by centralising the protection of all NATO networks and making significant improvements to the NATO Computer Incident Response Capability (NCIRC). With the adoption of the post-Lisbon cyber defence vision, policy and action plan, new cyber defence measures have been integrated into the Alliance's systems and procedures.

In May 2014, NCIRC reached full operational capability, providing enhanced protection for NATO networks and users. At the Wales Summit in September 2016, the Allies endorsed the new cyber defence policy and approved a new action plan which, together with the policy, will contribute to the Alliance's core tasks. The policy and its implementation within the Alliance have been kept under close review at both political and technical levels

9 North Atlantic Treaty, Washington DC, 4 (April 1949), Articles 1, 5, https://www.nato.int/cps/ic/natohq/official_texts_17120.htm?Selectedlocale=hu, accessed on 30.03.2020.

10 László Kovács, Gergely Szentgáli, 'National Cyber Security Organization: Hungary'. 11. (Tallinn, 2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_HUNGARY_2015-10-12.pdf, accessed on 30.03.2020.

11 Bucharest Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008, https://www.nato.int/cps/en/natolive/official_texts_8443.htm, accessed on 30.03.2020.

12 Gergely Szentgáli, 'A NATO kibervédelmi politikájának fejlődése' (The Evolution of NATO's Cyber Defence Policy), *Bolyai Szemle*, volume XXI. Issue 2, (2012), pp 80-85, http://archiv.uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf, accessed on 30.03.2020.

13 Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010, https://www.nato.int/cps/ua/natohq/official_texts_68580.htm, accessed on 30.03.2020.

and updated in response to the cyber threat. NATO and the European Union concluded a technical agreement on cyber defence on 10 February 2016, whereby both organisations will provide appropriate assistance to prevent and respond to cyber attacks. This technical agreement between the NCIRC and the Computer Emergency Response Team of European Union (CERT-EU) provides a framework for the exchange of information and sharing of best practices between the crisis response teams.

The defence ministers agreed on 14 June 2016 to recognise cyberspace as a new dimension at the Warsaw summit. This is an addition to the Alliance's current areas of operation—air, water, land and space. There are many definitions of cyberspace, but I would like to highlight one of them. According to the official dictionary of the US Department of Defense, cyberspace is *"A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"*.[14] This recognition does not change NATO's mission or mandate, which is clearly defensive. As in all areas of action, NATO acts in accordance with international law. The Alliance also acknowledged efforts in other international forums to develop standards of responsible, good governance and confidence-building measures, and to help create a more transparent and stable cyberspace for the international community. At the Warsaw Summit in July 2016, heads of state and government of the allied nations reaffirmed NATO's defensive mandate and the already recognised cyberspace as an area of operations in which NATO must defend itself effectively, as it does in the other four dimensions. The Allies have also committed to prioritise the cyber protection of their national networks and infrastructures. On 6 December 2016, NATO and the EU adopted more than 40 measures to promote cooperation between the two organisations, including to counter hybrid threats[15], cyber defence and to make their common neighbourhood more stable and secure. In the field of cyber defence, NATO and the EU hold joint exercises to promote research, training and information sharing.

"(70) Cyber attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success. Furthermore, it will ensure more effective organisation of NATO's cyber defence and better management of resources, skills, and capabilities. This forms part of NATO's long-term adaptation. We continue to implement NATO's Enhanced Policy on Cyber Defence and strengthen NATO's cyber defence capabilities,

14 Joint Publication 3-12 (R), Cyberspace Operations, (5 Feb 2013), 69, http://www.dtic.mil/doctrine/new_ pubs/jp3_12R.pdf, accessed on 30.03.2020.

15 Tibor Babos, 'Hibrid hadviselés a NATO-ban' (Hybrid Warfare in NATO), *Honvédségi Szemle*, Volume 6 Issue 6, (November 2010), HU ISSN 2060-1506, http://193.22Ő.76.Ő/download/konyvtar/digitgy/tartalomjegyz/honv_szemle_2010_6.pdf, accessed on 30.03.2020.
("Hybrid threats are those capabilities whereby adversaries can adaptively employ both conventional and non-traditional means simultaneously to achieve their own purposes.")

benefiting from the latest cutting edge technologies. (71) We will ensure that Allies are equipped for, and meet requirements tailored to, the 21st century. Today, through our Cyber Defence Pledge, we have committed to enhance the cyber defences of our national networks and infrastructures, as a matter of priority. We are expanding the capabilities and scope of the NATO Cyber Range, where Allies can build skills, enhance expertise, and exchange best practices."[16]

Defence Ministers adopted an updated cyber defence and action plan on 16 February 2017 to recognise cyberspace as an operational area. This will increase the ability of allies to cooperate, develop capabilities and share information. On 8 November 2017, defence ministers agreed in principle to establish a new Cyber Operations Centre as part of the plan for an adapted NATO command structure. This will strengthen NATO's cyber defences and help cyber integration planning and operations. The ministers also agreed to integrate the allies' national cyber capabilities into NATO missions and operations. The Allies retain full ownership of the contributions, just as they retain ownership of tanks, ships and aircraft in NATO missions.

Summary

NATO has always protected its communications and information systems, but it addressed cyber defence for the first time at the Prague Summit in 2002. At the Riga Summit in 2006, the allied leaders recognised the need to further protect these information systems. In the wake of the 2007 cyber attacks on public and private institutions in Estonia, the allied defence ministers agreed in June that significant work was needed in this area.

It is clear that NATO has recognised the new security challenges and is taking action in response to the events that have taken place as well as the continuously evolving situation. Furthermore, it wants to develop its existing and applied capabilities in this field and support educational, practice-oriented dissemination, scientific and research activities. The defensive nature of NATO remains fundamental, and cyberspace has been recognised as a dimension of operations in which NATO must defend itself as effectively as in the air, on land and at sea. NATO is strengthening its capabilities for cyber education, training and exercises. NATO also organises and conducts cyber exercises, such as Locked Shields, with the involvement of the member states. This exercise is described in detail in the chapter on International Military Cyber Exercises.

I believe that NATO has recognised the importance of cyber defence and cyber operations in due time. It has made and will continue to make significant efforts to develop and improve the related capabilities, and Hungary and the Hungarian Defence Forces should follow suit. In line with the cybersecurity strategy, the development of cybersecurity capabilities within the Hungarian Defence Forces could be vital for future tasks, where one of the pillars should rest on a domestic military cybersecurity exercise.

16 NATO, 'Summit Guide Warsaw', 8-9 July 2016, pp. 124-128, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf, accessed on 30.03.2020.

Evolution of the US cyber defence policy

The United States of America is at the forefront in implementing cybersecurity policies and strategies worldwide. The federal government issued the first national cybersecurity strategy back in 2003.[17] The document set out three strategic objectives:

- prevent cyber attacks against critical infrastructure;
- minimise vulnerabilities to cyber attacks;
- reduce the damage and recovery time caused by cyber attacks.
- Five national priorities have been identified to achieve these goals:
- the securing of federal computer systems and networks;
- the development of responsiveness;
- the establishment of a threat and vulnerability mitigation programme;
- an awareness-raising and training programme on cybersecurity;
- the system of international cooperation.

In the following section, the author reviews the most important strategic documents and federal laws, including executive orders on cybersecurity issued by US presidents, in chronological order. These documents include:

- the protection of national critical infrastructure and the security of federal computer systems and networks;
- the definition of roles and responsibilities of federal, state, local, regional and private partners;
- the international, national security, defence and counter-intelligence aspects of cybersecurity.

Cybersecurity in the early nineties became a vexing problem for national security. The US cybersecurity policy is rooted in the efforts to protect critical infrastructure. In 1996, President Bill Clinton issued Executive Order no 13010 on the Protection of Critical Infrastructure.[18] The decision established the President's Commission on Critical Infrastructure Protection, which raised awareness of cyber attacks and threats to national security. Presidential Decision Directive 63 of 1998 (hereinafter: PDD)[19] established a structure under the White House to coordinate the federal government's efforts to protect critical infrastructure from Internet attacks. PDD 63 established a number of cybersecurity-related organisations within the government, including the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, with the Office of Critical Infrastructure supporting the Coordinator and the National Infrastructure Protection Center.[20]

17 The White House, The National Strategy to Secure Cyberspace, (2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, accessed on 30.03.2020.

18 Executive Order 13025 – Amendment to Executive Order 13010, the President's Commission on Critical Infrastructure Protection, (November 13, 1996), https://www.gpo.gov/fdsys/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2390-3.pdf, accessed on 30.03.2020.

19 Presidential Decision Directive/NSC-63, The White House, (Washington, 22 May 1998), https://fas.org/irp/offdocs/pdd/pdd-63.pdf, accessed on 30.03.2020.

20 Kevin P.Newmeyer, 'Who Should Lead U.S. Cybersecurity Efforts?', (2012), pp 118-119, http://cco.ndu.edu/Portals/96/Documents/prism/prism_3-2/prism115-126_newmeyer.pdf, accessed on 30.03.2020.

The Federal Information Security Management Act (hereafter: FISMA),[21] used the risk management framework developed by the National Institute of Standards and Technology (NIST) as part of the e-Government Act 2002 to standardise cybersecurity processes among US government organisations. As a result of this event, the Federal Chief Information Officer (FCIO) is responsible for overseeing the government's use of technology, both in terms of spending and strategy. It clarified and strengthened NIST's responsibility for developing security standards for federal computer systems (excluding defence and intelligence systems), created a central federal incident center, and made the Office of Management and Budget (OMB) responsible for publishing federal cybersecurity standards.

In 2002, the Department of Homeland Security was created under the Homeland Security Act (DHS), inter alia to coordinate the national infrastructure for critical infrastructure protection in the information and communications sectors.

Presidential Directive No 7 of 2003 on land security[22] defined the identification and prioritisation of critical infrastructure in the physical world and in cyberspace to protect against terrorist attacks. It updated the roles and responsibilities of the various agencies in the Homeland Security Act of 2002 and other instruments. It reaffirmed the DHS's responsibility to lead efforts to protect the entire critical infrastructure and designated the department as the lead agency for the information and communications industry to share information on threats, assess vulnerabilities, and prepare appropriate security and emergency response measures and plans. It also directed the DHS to create a National Infrastructure Protection Plan (NIPP), which was prepared and published in 2006.[23]

Under the Bush administration, cybersecurity was a complex matter, with limited leadership and shared responsibility between the White House and the Department of Defense (DoD). Homeland Security was given an overall coordination role, but the responsibility remained with the individual agencies. The National Military Strategy for Cyberspace Operations, issued by the Supreme Command in 2006, is the first comprehensive document[24] that describes the US military's approach to cyberspace operations. The document outlined the role of the US Armed Forces in conducting military operations in cyberspace to protect US interests. According to the strategy, "the Department of Defense (DoD) relies on cyberspace to achieve national military objectives in the areas of military, intelligence, and business operations."

In January 2008, President George W. Bush signed National Security Presidential Directive and Homeland Security Presidential Directive 23[25] for DHS and OMB to set minimum operating standards for the federal government's civilian networks. Both directives emphasised comprehensive control, which is supported by the Comprehensive National Cybersecurity

21 The United States Congress, H.R.2458 -E-Government Act of 2002. 107th Congress (2001-2002), (2002), https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf, accessed 30.03.2020.

22 U.S. Department of Homeland Security, Homeland Security Presidential Directive 7: Critical Infra-structure Identification, Prioritization, and Protection, (2003), http://www.dhs.gov/homeland-security-presidential-directive-7, accessed on 30.03.2020.

23 National Infrastructure Protection Plan 2006, https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf, accessed on 30.03.2020.

24 National Military Strategy for Cyberspace Operations, Chairman of the Joint Chiefs of Staff, Washington, (December 2006), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf, accessed on 30.03.2020.

25 National Security Presidential Directive 54/Homeland Security Presidential Directive 23, The White House, Washington, (2008), https://fas.org/irp/offdocs/nspd/nspd-54.pdf, accessed on 30.03.2020.

Initiative (CNCI)[26] with guidelines. The CNCI states that it will provide protection against the most direct and complete spectrum of threats and strengthen the future security environment by providing a comprehensive approach that includes law enforcement, intelligence and military capabilities. In 2009, President Obama launched the Cyberspace Policy Review, a 60-day government review of the cyberspace, to ensure proper integration, funding, and coordination of the CNCI with Congress and the private sector.[27] The review proposed a stronger White House and stronger accountability for federal leadership and cybersecurity. It also identified ten short-term and fourteen medium-term actions to support the general objectives of the CNCI.

Broader national security and defence strategies also outline cybersecurity objectives. The 2010 National Security Strategy[28] was the first US national security strategy to address cyber threats. The 2010 Quadrennial Homeland Security Review highlighted "cyberspace safety and security" as one of the five key national security missions.[29] Based on military defence considerations approaching cybersecurity, the Cyber Command of the US (: USCYBERCOM) was created in 2010 and became operational in the same year.[30] To implement the National Security Strategy and achieve the goals set by the Quadrennial Homeland Security Review[31], DHS developed an action plan, titled the Blueprint for Secure Cyber Future[32] in 2011. The action plan covers two areas—critical information infrastructure and the cyber environment. In May 2011, the White House released its international cyberspace strategy,[33], which reflects the approach of United States to international relations and communicating national priorities. The overall goal of the strategy is that the United States will operate an international, open, interoperable, secure, and reliable information and communications infrastructure that supports international trade, enhances international security, and promotes free expression and innovation. To achieve this goal, they will build and maintain an environment in which standards of responsible conduct govern the state actions, sustain partnerships and support the rule of law in cyberspace. As a result of the international strategy for cyberspace, the US National Strategy (2011) recognised that cyberspace has become a theatre of war in its own right and that the United States will increase deterrence in air, space, and cyberspace and improve its ability to defeat attacks against systems or infrastructure.

In 2012, the Obama administration supported legislation that would give DHS the authority to protect critical infrastructure networks; however, the bill failed to pass Congress twice. In response, Obama issued Improving Critical Infrastructure Cybersecurity (EO 13636)[34].

26 Comprehensive National Cybersecurity Initiative (CNCI), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf, accessed on 30.03.2020.
27 Cyberspace Policy Review, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-028.pdf, accessed on 30.03.2020.
28 National Security Strategy, http://nssarchive.us/NSSR/2010.pdf, accessed on 30.03.2020.
29 Quadrennial Homeland Security Review, https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf, accessed on 30.03.2020.
30 US Department of Defense, 'U.S. Cyber Command Fact Sheet', https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf, accessed on 30.03.2020.
31 The Quadrennial Homeland Security Review, https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf, accessed on 30.03.2020.
32 Blueprint for Secure Cyber Future, https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf, accessed on 30.03.2020.
33 International Strategy for Cyberspace, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, accessed on 30.03.2020.
34 Improving Critical Infrastructure CyberSecurity (EO 13636), https://www.dhs.gov/sites/default/files/publications/EO-13636-Improving-Critical-Infrastructure-Cybersecurity-508.pdf, accessed on 30.03.2020.

This binding document for the President complements all previous ones and ensures a better exchange of information between the federal government and the private sector. It also sets minimum criteria to improve the security of critical infrastructures. The Presidential Directive on Critical Infrastructure Security and Resilience (PPD-21)[35] issued under no. EO 13636 did not make significant changes to policy, roles, responsibilities, and programs. However, it did call for existing public and private sector actors to assess the data and system requirements underlying effective information sharing and to improve situational awareness.[36] It drew attention to the review of the National Infrastructure Protection Plan and finally to the revision of the third review of the plan in 2013. The 2013 National Cybersecurity and Critical Infrastructure Protection (hereafter: NCCIP)[37] ensures DHS's role in cybersecurity prevention and response and establishes an information sharing partnership between DHS and critical infrastructure owners and operators. The Quadrennial Homeland Security Review was revised in 2014. The investigation revealed the DoD's responsibility to develop new and expanded full-spectrum cyberspace capabilities to defend the country and support military missions around the world. The 2014 DoD Quarterly Defense Review defines the key role of DoD in cyberspace as follows: "...we must be able to defend the integrity of our own networks, protect our key systems and networks, conduct effective cyber operations overseas when directed, and defend the Nation from an imminent, destructive cyberattack on vital US interests." The Cyber Electromagnetic Activities (FM 3-38)[38], published by the United States Army in 2014, provides guidance for cyber electromagnetic activities and provides tactics and procedures for planning, integrating, and synchronizing. The doctrine compares army operations with electronic warfare. In addition, Joint Cyberspace Operations (JP 3-12)[39] addresses the uniqueness of military operations in cyberspace and clarifies cyberspace operations. In 2014, the federal government created the Critical Infrastructure Development Framework[40], a voluntary cybersecurity framework, which provides guidelines, practices and voluntary standards for the private sector to ensure critical infrastructure is protected.

From a military perspective, the current National Security Strategy, adopted in early 2015, is an updated version of the previous 2011 edition, it recognises the growing threat of devastating cyber attacks and announces the US intention to strengthen cybersecurity of critical infrastructure. The document focuses primarily on the intention of the United States to promote international standards in cyberspace. The new strategy will provide greater transparency regarding the own offensive and operational capabilities of the DoD.

35 Presidential Policy Directive The Critical Infrastructure Security and Resilience 55, https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf, accessed on 30.03.2020.

36 Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience, https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf, accessed on 30.03.2020.

37 National Cybersecurity and Critical Infrastructure Protection (NCCIP), https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf, accessed on 30.03.2020.

38 U.S. Department of Army, 'Cyber Electromagnetic Activities', No. 3-38, Washington, (2014), http://fas.org/irp/doddir/army/fm3-38.pdf, accessed on 30.03.2020.

39 Joint Cyberspace Operations Cyberspace Operations, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf, accessed on 30.03.2020.

40 Framework for Improving Critical Infrastructure, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, accessed on 30.03.2020.

Summary

In the United States, cybersecurity policy now consists of partial measures, similarly to legislation, which is less comprehensive and are of a more local character. More than 50 statutes cover various aspects of cybersecurity. As there is no overarching framework that synthesises these documents or provides a comprehensive description of the current strategy, a clear understanding and definition of overall strategic objectives and priorities is a complex task. Most of the existing documents refer to national priorities in the narrower cybersecurity domains, but they facilitate a departure from the priorities and structure and do not specify whether they link to or override other policy documents. Most of these documents do not describe how they fit into the overall national cybersecurity strategy.[41]

For the US government, cybersecurity policies go back the 1990s through its security policy, and the government clearly recognised the new security challenges and wanted to respond to the events and situations that arose. Many of its directives, guidelines and presidential decrees refer to strategic regulation and guidance, which is treated with the utmost priority and kept up-to-date. In addition, it points out that the skills and competences already achieved are further developed, and supports the educational, scientific and research directions. It also aims to provide technical support to Member States and their own organisations by providing them with the appropriate skills. These technical assistances include several military exercises, with cybersecurity exercises such as Cyber Shield among them. This exercise is explained in more detail in the next chapter.

41 National Cyber Security Organization, United States (2016), https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf, accessed on 30.03.2020.

International military cyber exercises

IT security is already part of several military exercises, and cyberspace has been adopted by NATO as a theatre of operations. It is also an alert to threats from cyberspace, dangers and eventual attacks, and a preparation for testing the reliability of C4ISR (Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance) systems.

Exercises are organised and run specifically for IT systems professionals, often involving civilian experts. Such exercises include:

- Cyber defence exercise (CDX)[42]
- Cross swords[43]
- Cyber coalition[44] [45]
- Cyber perseu[46]
- Cyber czech[47]
- Cyber tesla[48]

In addition to those listed above, I would like to highlight two practices which, in my opinion and experience, have a significant track record, good organisation and professional, technological and technical characteristics. These two are an excellent example of the multi-faceted and complex nature of cyber exercises. In addition, they are flagships of the educational objective set out in the Cybersecurity Strategies, which is to provide practical and skills-based knowledge. These two exercises were named Locked Shields and Cyber Shield.

Locked Shields

The Locked Shields exercise series is available to the specialist pool of military intelligence information systems of NATO member states[49], organised annually by the NATO Centre of Excellence in Cyber Defence. Following on from the first exercise in 2010, the number

42 Cyber Research Center - CDX Network, https://www.usma.edu/centers-and-research/cyber-research-center/data-sets, accessed on 30.03.2020)

43 Cymmetria, 'The Crossed Swords wargame: Catching NATO red teams with cyber deception', (25 May 2017), https://cymmetria.com/blog/nato-crossed-swords-exercise/, accessed on 30.03.2020.

44 NATO, 'NATO's flagship cyber exercise begins in Estonia', (2017), https://www.nato.int/cps/ic/natohq/news_149233.htm, accessed on 30.03.2020.

45 László Szűcs, 'The cyber defence exercise was successful', (2011) https://honvedelem.hu/cikk/29471/sikeres-volt-a-kibervedelmi-gyakorlat, accessed on 30.03.2020.

46 INDRA, 'The Portuguese Armed Forces complete Cyber Perseu, the National Cyberdefense exercise, using Indra's Minsait Cyber Range platform', https://www.indracompany.com/en/noticia/portuguese-armed-forces-complete-cyber-perseu-national-cyberdefense-exercise-using-indras, accessed on 30.03.2020.

47 Jan Vykopal, Ondřej Mokoš, 'Czech cyber defence exercise', https://www.terena.org/activities/tf-csirt/meeting47/J.Vykopal-O.Mokos-Czech-lessons.pdf, accessed on 30.03.2020.

48 'Multinational Exercise Cyber Tesla', (13 November 2019), http://www.vs.rs/en/news/BA5E2A5D062D11EAAC980050568F5424/multinational-exercise-cyber-tesla-2019, accessed on 30.03.2020.

49 NATO Cooperative Cyber Defence Centre of Excellence, 'Cyber Defence Exercise Locked Shields 2012. After Action Report', https://ccdcoe.org/library/publications/cyber-defence-exercise-locked-shields-2012-after-action-report/, accessed on 30.03.2020; NATO Cooperative Cyber Defence Centre of Excellence, 'Cyber Defence Exercise Locked Shields 2013. After Action Report', https://ccdcoe.org/library/publications/cyber-defence-exercise-locked-shields-2013-after-action-report/, accessed on 30.03.2020; NATO Cooperative Cyber Defence Centre of Excellence, 'Locked Shields 2014 After Action Report: Executive summary', https://ccdcoe.org/library/publications/locked-shields-2014-after-action-report-executive-summary/, accessed on 30.03.2020.

of participants and the complexity of the tasks increase every year. The Hungarian Defence Forces have been participating in the exercise since 2014. The exercise staff is under constant strain, as participants are required to monitor an unknown, poorly documented, large-scale network with little time to prepare and execute. In addition, some system components have been infected on purpose and certain defence roles have been deliberately disabled. The network environment is inhomogeneous, typically using outdated or unpatched operating systems, and in many cases old, vulnerable or misconfigured services. In parallel with countering attacks, participants need to use effective communication within the team, which includes sharing information about the attacker and the attack method, prioritising tasks and managing concurrent events. In addition, there may be a variety of test cases, including operational and user support, new server feature installation and configuration changes, as well as legal, media and strategic decision tasks. Apart from the right solutions, deadlines, presentation and professional credibility are also taken into account. The participants are also required to write reports, which are designed to make one's point effectively and use specialist language.[50]

From an education and security policy perspective, the exercise highlights the need for professionals facing technical barriers to work in teams and share information both horizontally and vertically. It contributes to the development of both technical and decision-making security awareness and knowledge.

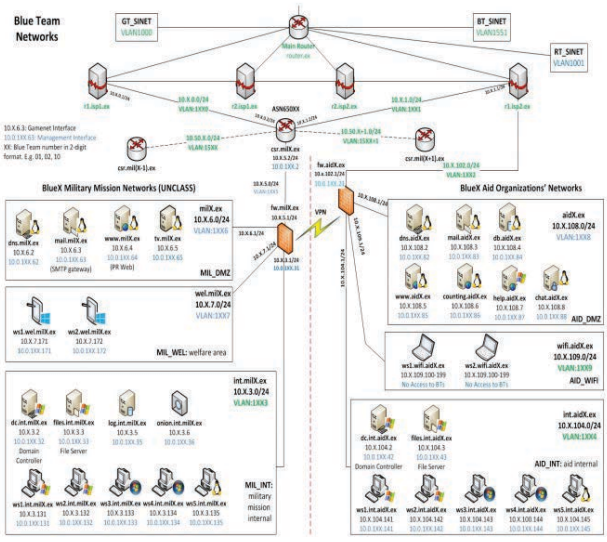


Figure 1. NATO Locked Shields 2013 exercise virtual infrastructure
(Source: Cyber Defence Exercise Locked Shields 2013. After Action Report https://ccdcoe.org/library/publications/cyber-defence-exercise-locked-shields-2013-after-action-report/)

50 András Szabó, 'Technikai kiberbiztonsági gyakorlatok – nemzetközi kitekintés' (Technical cybersecurity practices – an international perspective), Hadmérnök Journal, ISSN 1788-1929, Volume XIII, Issue 1, (March 2018), http://hadmernok.hu/181_23_szabo.pdf, accessed on 30.03.2020.

Cyber Shield

Cyber Shield is a defensive cyberspace operation training program that brings together the capabilities of the Unites States Army, the National Guard, the Air National Guard, the Coast Guard, industry partners and civilians to exercise and test their skills in response to cyber incidents. The aim is to train the first line of defence of states quickly and effectively, to prevent cyber attacks against their nations' vulnerable critical infrastructure and sensitive public services.[51]

The exercise known as Cyber Shield began in 2012 as a simple red and blue team exercise, but has grown to an 800-strong event that reflects the Guard's larger role in the cyber defence of the United States. In 2019, National Guard units from 40 states participated in the exercise, as well as personnel from the private sector and federal agencies such as the FBI and the National Security Agency. Among other things, participants test their ability to detect suspicious activity on the network and block unauthorised access to the system. "It's a collective training event for us, so it will enhance our warfighting skills. And that's very important to us," said General Jeffrey Burkett, Chief of Internal Operations for the National Guard Bureau, about the exercise.[52] The first week of the exercise consisted of training hours during which participants received re-certification or refresher courses to maintain their existing qualifications. The second week consisted of an actual training exercise, during which teams used their technical skills to defend their networks without a digital war event.

The training scenarios used during the week of teaching or learning are designed to mimic real life using a team system. The Red Team is the Opposite Force (OPFOR), who operate on virtual infrastructure against the defensive Blue Team. The team system allows participants to react in real-time to cyber attacks and execute defensive manoeuvres. They conduct real operations to penetrate the network of defending troops to maintain a continuous presence, steal data and disrupt the network. The aim is not to destroy the network of defence teams, but to raise awareness of the various cyber risks. Once these scenarios are completed, a collaborative in-depth analysis of what happened from the perspective of both OPFOR and the defending troops will be shared. While the real world does not provide the ability to provide a complete analysis of what each party is doing, a quick overview provides invaluable information for all teams to learn from, in order to detect threats more effectively.[53]

51 Defense visual information distribution service: Cyber shield 19, https://www.dvidshub.net/feature/cybershield19, accessed on 30.03.2020.

52 Sean Lyngaas, 'Inside the National Guard's annual Cyber Shield drill', (16 April 2019), https://www.fedscoop.com/inside-national-guards-annual-cyber-shield-drill/, accessed on 30.03.2020.

53 Master Sgt. Brad Staggs, 'Indiana National Guard participates in Cyber Shield', (29 April 2016), https://www.army.mil/article/167051/indiana_national_guard_participates_in_cyber_shield_2016, accessed on 30.03.2020.

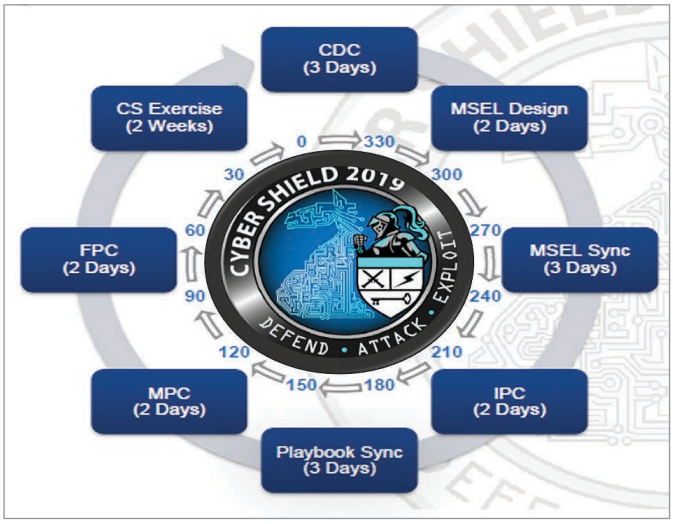


Figure 2. Exercise Cyber Shield 2019, Lifecycle events
(Source: Cyber Shield 2019 unclassified COL Teri D. Williams)

The events in the life cycle model shown in Figure 2 include the following activities and decisions:

- Concept Design Conference (CDC): It defines the objectives of the exercise, assigns initial tasks and reduces previous shortcomings.
- MSEL planning (Develop the Master Scenario Events List): develops the Master Scenario Events List (MSEL) and identifies the inputs needed to develop the scenario.
- MSEL Sync (MSEL2): further develops and refines the MSEL exercise, scenario injects and threat actor activities.
- Initial Planning Conference (IPC): It defines the staffing, equipment and training requirements and develops the operational concept.
- Playbook Sync (MSEL3): It prepares the training schedule, the MSEL and the playbook.
- Main Planning Conference (MPC): It consolidates initial funding requirements, finalises the field environment and refines the exercise schedule.
- Final Planning Conference (FPC): It develops support requirements, field environment and practical events.
- Cyber Shield Exercise (CS) provides a collective practical event and creates the conditions for the evaluation of the RC Cyber forces.

The exercise covers topics such as intrusion detection, the law of data security and threat analysis. From an education and security policy perspective, the exercise highlights the scale of the technical cyber challenges facing nations and the ongoing work that is being done in this area. Hungary, Ukraine and Serbia, among others, were invited as observers to the 2019 exercise. This is a major step forward in the sharing of experience and information.

Conclusion

The cyberspace was defined as an operational space at the 2016 NATO Summit in Warsaw, where member states committed to improving their cyber defence capabilities and agreed to improve information sharing, organise joint education, training and exercises. By examining the policies of the NATO and the United States of America, I came to the conclusion that the international examples are not fully transferable to the Hungarian context. In addition to joint exercises, Hungary should independently define and develop a military cyber exercise, which will provide a basis for testing the IT network and for the proper training of the specialised personnel and the practical acquisition of knowledge.

Such exercises strengthen the links between professionals working in different fields and raise awareness to the security, national security and military implications of cybersecurity, in addition to its technical aspects. They can help raise security awareness among people working with IT systems. In addition, the exercises provide a traceable framework, which can be one way of achieving the objectives of the strategies detailed in the application, thus provide evidence for the effective military implementation and fulfilment of the objectives of the National Strategies.

In the professional view of the author the IT and information protection specialists of the Hungarian Defence Forces perform their operational tasks with the utmost expertise. However, the organisation and development of an exercise, as defined in the National Security, National Military and National Cyber Security Strategies, contribute significantly to achieving and maintaining an advantageous position in the international security arena, for which operational roles are not necessarily sufficient.

Technical task implementation requires decisive and outstanding knowledge, preparation and training, but the training of the staff performing technical tasks cannot be thorough and complete without practice. These cyber exercises will enhance communication skills, teamwork and task management skills, alongside technology and technical skills.

It is also important to see that the new warfare dimension has links with physical infrastructures (land, sea, air and space), so their interaction must be taken into account. These dependencies increase the number of threats. There is a need for experienced staff who are prepared for the challenges in cyberspace, in line with the digitalisation of security policy.

The author proposes that, in keeping with the activities of other states in security policy and cyber operations exercises, Hungary should also organise and conduct technical cybersecurity exercises, both at the security policy and administrative level, as well as in the military context. This would prepare professionals in the Hungarian legal and technological environment and adapt their skills to current international challenges.

Bibliography

1. Kovács, László, A kibertér védelme (Protecting cyberspace), (Budapest: Dialóg Campus Kiadó, 2018), https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf, accessed on 30.03.2020.
2. Draveczki-Ury, Ádám, 'Átadták a Hungarian Honvédség Kiber Képzési Központját', (The Cyber Training Centre of the Hungarian Defence Forces was inaugurated) (13.06.2019 12:00), https://honvedelem.hu/galeriak/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat/, accessed on 30.03.2020.
3. Government Decree No 1035 of 2012. (II. 21.) on the National Security Strategy of Hungary
4. Government Decree No 1656 of 2012. (XII. 20.) on the National Military Strategy of Hungary
5. Government Decree No 1139 of 2013. (III. 21.)
6. Act L of 2013 on the electronic information security of state and local government bodies
7. Jobbágy, Szabolcs, 'Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő', (The convergence of the information society, information technology and telecommunications. Past, present, future.), *Hadmérnök Journal*, Vol. IV No. 1, (March 2009), pp. 185-188, http://www.hadmernok.hu/2009_1_jobbagy.pdf, accessed on 30.03.2020.
8. ITU-T X.1205 telecommunication standardization sector of ITU (04/2008) series x: data networks, open system communications and security telecommunication security overview of cybersecurity. 8., https://www.itu.int/rec/T-REC-X.1205-200804-I, accessed on 30.03.2020.
9. The North Atlantic Treaty, Washington DC, 4 April 1949, 1. 5., https://www.nato.int/cps/ic/natohq/official_texts_17120.htm?Selectedlocale=hu, accessed on 30.03.2020.
10. Kovács, László, Szentgáli, Gergely, 'National Cyber Security Organization: Hungary'. 11. (Tallinn, 2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_HUNGARY_2015-10-12.pdf, accessed on 30.03.2020.
11. Bucharest Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008, https://www.nato.int/cps/en/natolive/official_texts_8443.htm, accessed on 30.03.2020.
12. Szentgáli, Gergely, 'A NATO kibervédelmi politikájának fejlődése' (The Evolution of NATO's Cyber Defence Policy), *Bolyai Szemle*, volume XXI. Issue 2, (2012), 80-85, http://archiv.uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf, accessed on 30.03.2020.
13. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010, https://www.nato.int/cps/ua/natohq/official_texts_68580.htm, accessed on 30.03.2020.
14. Joint Publication 3-12 (R), 'Cyberspace Operations', (5 Feb 2013), p. 69, http://www.dtic.mil/doctrine/new_ pubs/jp3_12R.pdf, accessed on 30.03.2020.

15. NATO Summit Guide Warsaw, pp. 8-9. July 2016, 124-128 https://www.nato.int/nato_static_f l2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf, accessed on 30.03.2020.
16. The White House, The National Strategy to Secure Cyberspace, (2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, accessed on 30.03.2020.
17. Executive Order 13025 – Amendment to Executive Order 13010, the President's Commission on Critical Infrastructure Protection, (November 13, 1996), https://www.gpo.gov/fdsys/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2390-3.pdf, accessed on 30.03.2020.
18. Presidential Decision Directive/NSC-63, The White House, Washington, (May 22, 1998), https://fas.org/irp/offdocs/pdd/pdd-63.pdf, accessed on 30.03.2020.
19. Newmeyer, Kevin P., 'Who Should Lead U.S. Cybersecurity Efforts?', (2012), 118-119, http://cco.ndu.edu/Portals/96/Documents/prism/prism_3-2/prism115-126_newmeyer.pdf, accessed on 30.03.2020.
20. The United States Congress, H.R.2458 -E-Government Act of 2002. 107th Congress (2001-2002), (2002), https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf, accessed on 30.03.2020.
21. Public Law 107-296, 25 Nov 2002, 107th Congress an Act To establish the Department of Homeland Security, and for other purposes, https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf, accessed on 30.03.2020.
22. U.S. Department of Homeland Security, Homeland Security Presidential Directive 7: Critical Infra-structure Identification, Prioritization, and Protection, (2003), http://www.dhs.gov/homeland-security-presidential-directive-7, accessed on 30.03.2020.
23. National Infrastructure Protection Plan 2006, https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf, accessed on 30.03.2020.
24. National Military Strategy for Cyberspace Operations, Chairman of the Joint Chiefs of Staff, Washington, (December 2006), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf, accessed on 30.03.2020.
25. National Security Presidential Directive 54/ Homeland Security Presidential Directive 23, The White House, Washington, (2008), https://fas.org/irp/offdocs/nspd/nspd-54.pdf, accessed on 30.03.2020.
26. Comprehensive National Cybersecurity Initiative (CNCI), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf, accessed on 30.03.2020.
27. Cyberspace Policy Review, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-028.pdf, accessed on 30.03.2020)
28. National Security Strategy http://nssarchive.us/NSSR/2010.pdf, accessed on 30.03.2020.
29. Quadrennial Homeland Security Review, https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf, accessed on 30.03.2020.
30. US Department of Defense, 'U.S. Cyber Command Fact Sheet', https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf, accessed on 30.03.2020.

31. Blueprint for Secure Cyber Future, https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf, accessed on 30.03.2020.
32. International Strategy for Cyberspace, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, accessed on 30.03.2020)
33. Improving Critical Infrastructure Cybersecurity (EO 13636), https://www.dhs.gov/sites/default/files/publications/EO-13636-Improving-Critical-Infrastructure-Cybersecurity-508.pdf, accessed on 30.03.2020.
34. Presidential Policy Directive The Critical Infrastructure Security and Resilience 55, https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf, accessed on 30.03.2020.
35. Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience, https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf, accessed on 30.03.2020.
36. National Cybersecurity and Critical Infrastructure Protection (NCCIP), https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf, accessed on 30.03.2020.
37. The Quadrennial Homeland Security Review https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf, accessed on 30.03.2020.
38. U.S. Department of Army, 'Cyber Electromagnetic Activities', No. 3-38, Washington, (2014), http://fas.org/irp/doddir/army/fm3-38.pdf, accessed on 30.03.2020.
39. Joint Cyberspace Operations Cyberspace Operations http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf, accessed on 30.03.2020.
40. Framework for Improving Critical Infrastructure https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, accessed on 30.03.2020.
41. A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats 2018 https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf, accessed on 30.03.2020.
42. National Cyber Security Organization: United States 2016 https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf, accessed on 30.03.2020.
43. Cyber Research Center – CDX Network https://www.usma.edu/centers-and-research/cyber-research-center/data-sets, accessed on 30.03.2020.
44. Cymmetria, 'The Crossed Swords wargame: Catching NATO red teams with cyber deception', (25 May 2017), https://cymmetria.com/blog/nato-crossed-swords-exercise/, accessed on 30.03.2020.
45. NATO, 'NATO's flagship cyber exercise begins in Estonia', (2017), https://www.nato.int/cps/ic/natohq/news_149233.htm, accessed on 30.03.2020.

46. Szűcs, László, 'Sikeres volt a kibervédelmi gyakorlat' (The cyber defence exercise was successful), (2011), https://honvedelem.hu/cikk/29471/sikeres-volt-a-kibervedelmi-gyakorlat, accessed on 30.03.2020.
47. INDRA, 'The Portuguese Armed Forces complete Cyber Perseu, the National Cyberdefense exercise, using Indra's Minsait Cyber Range platform', https://www.indracompany.com/en/noticia/portuguese-armed-forces-complete-cyber-perseu-national-cyberdefense-exercise-using-indras, accessed on 30.03.2020.
48. Vykopal, Jan, & Mokoš, Ondřej, 'Czech cyber defence exercise', https://www.terena.org/activities/tf-csirt/meeting47/J.Vykopal-O.Mokos-Czech-lessons.pdf, accessed on 30.03.2020.
49. 'Multinational Exercise Cyber Tesla', (13 November 2019), http://www.vs.rs/en/news/BA5E2A5D062D11EAAC980050568F5424/multinational-exercise-cyber-tesla-2019, accessed on 30.03.2020.
50. NATO Cooperative Cyber Defence Centre of Excellence, 'Cyber Defence Exercise Locked Shields 2012. After Action Report', https://ccdcoe.org/library/publications/cyber-defence-exercise-locked-shields-2012-after-action-report/, accessed on 30.03.2020.
51. NATO Cooperative Cyber Defence Centre of Excellence, 'Cyber Defence Exercise Locked Shields 2013. After Action Report', https://ccdcoe.org/library/publications/cyber-defence-exercise-locked-shields-2013-after-action-report/, accessed on 30.03.2020.
52. NATO Cooperative Cyber Defence Centre of Excellence, 'Locked Shields 2014 After Action Report: Executive summary', https://ccdcoe.org/library/publications/locked-shields-2014-after-action-report-executive-summary/, accessed on 30.03.2020.
53. Szabó, András, 'Technikai kiberbiztonsági gyakorlatok – nemzetközi kitekintés' (Technical cybersecurity practices – an international perspective), *Hadmérnök Journal*, ISSN 1788-1929, Volume XIII, Issue 1, (March 2018), http://hadmernok.hu/181_23_szabo.pdf, accessed on 30.03.2020)
54. Defense visual information distribution service: Cyber shield 19, https://www.dvidshub.net/feature/cybershield19, accessed on 30.03.2020.
55. Lyngaas, Sean, 'Inside the National Guard's annual *Cyber Shield* drill', (16 April 2019), https://www.fedscoop.com/inside-national-guards-annual-cyber-shield-drill/, accessed on 30.03.2020.
56. Master Sgt. Staggs, Brad, 'Indiana National Guard participates in Cyber Shield', (29 April 2016), https://www.army.mil/article/167051/indiana_national_guard_participates_in_cyber_shield_2016, accessed on 30.03.2020.

HUNEXPERT

digital success programme

MATE
HUNGARIAN UNIVERSITY OF AGRICULTURE AND LIFE SCIENCE

SZENT ISTVÁN SECURITY RESEARCH CENTER

HUNGARIAN ATLANTIC COUNCIL

NATIONAL COUNCIL OF STUDENT RESEARCH SOCIETIES

DOSZ
Association of Hungarian PhD and DLA Candidates