LUDOVIKA
UNIVERSITY PRESS

AARMS

ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE

Volume 22 (2023)
Issue 3

ISSN 2498-5392 (print)
ISSN 2786-0744 (online)

AARMS is a peer-reviewed international scientific journal devoted to reporting original research articles and comprehensive reviews within its scope that encompasses the military, political, economic, environmental and social dimensions of security and public management.

AARMS is published in one volume of three issues per year by the University of Public Service, Budapest, Hungary, under the auspices of the Rector of the University.

All correspondence should be addressed to Prof. József PADÁNYI, DSc, Editor-in-Chief,
University of Public Service
P. O. Box 15, H-1581 Budapest 146 Hungary
aarms@uni-nke hu

AARMS
ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE
Volume 22
Issue 3
2023

An International Journal of Security, Strategy, Defence Studies,
Military Technology and Public Management
Published by the University of Public Service
József PADÁNYI (Chair of the Editorial Board)
József SOLYMOSI (Honorary Chair of the Editorial Board)

Publisher:

University of Public Service, Ludovika University Publishing House
Responsible for Publishing:
Gergely DELI Rector

Copy editor:

Zsuzsánna GERGELY

Typeset and print by the University of Public Service
ISSN 2498-5392 (print)
ISSN 2786-0744 (online)

Contents

AARMS Vol. 22, No. 3 (2023) 5–18.

10.32565/aarms.2023.3.1

Assessing Offensive Cyber Capabilities

Exploring the Talent Behind Cybersecurity

Gábor SELJÁN[1]

The recent emergence of mercenary spyware like Pegasus or Russia's ongoing conventional warfare in Ukraine, supplemented by a cyber offensive we never experienced before, made cybersecurity even more critical. Despite the considerable research in the field, it seems that academia and the private sector have not been able to keep up with the growing importance of security and privacy resulting from the significant increase in cyber threats to critical services, infrastructure and human rights. Research on cyber capabilities tends to focus on the general understanding of the field and pays less attention to the rapid spread of increasingly advanced offensive cyber capabilities. Correctly assessing the capabilities of others and recognising the steps necessary to develop their own capabilities are essential for any country in combating future cybersecurity challenges. However, since there is no consensus on describing even basic cyber capabilities, current research uses different interpretations and usually lacks offensive capabilities altogether. In this article, I discuss the problem of assessing, measuring and evaluating offensive cyber capabilities, starting from the different definitions of some related terms through the various cyber power indices, right down to the talent behind cybersecurity, and perhaps the most promising indicators for assessing offensive capabilities.

Keywords: *cyber power, cyber capabilities, offensive security, cybersecurity indices*

Defining offensive cyber capabilities

To date, there is no well-defined or generally agreed-upon definition of the term *cyber power.* Even the term *vulnerability* has more than a dozen definitions and formulations in the glossary compiled by the Computer Security Resource Center (*CSRC*) at the National Institute of Standards and Technology (*NIST*)[2], hence what constitutes *offensive cyber capability* (*OCC*) is even more heavily debated both in academia and among policy-makers. It is cumbersome to agree on a universal definition of offensive cyber

[1] PhD candidate, Corvinus University of Budapest, e-mail: gabor.seljan@stud.uni-corvinus.hu

[2] CSRC 2021.

capabilities for several reasons. As explained by Miralis (2019), a narrow definition may exclude so many potentially malicious offensive cyber activities that policy-making efforts based on that definition will be futile. However, a broader definition may also capture legitimate activities, for example, research and development, aiming to create the necessary cybersecurity tools to defend against cyberattacks and any limitation on those activities could harm cyber incident responders and network defenders more than threat actors.[3] In the following paragraphs, I briefly overview some of the related terms and their interpretations.

In his proposed definition, Kuehl (2009) outlined the fundamental ideas of cyber power: "*The ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.*"[4] According to this early interpretation, cyberspace was already considered to be a domain of warfare, although NATO officially recognised it as the fifth domain of operations much later at the Warsaw Summit, as further explained by Minárik (2016).[5] Meanwhile, in the view of the Economist Intelligence Unit (*EIU*) and Booz Allen Hamilton (*Booz*), cyber power is "*the ability of a country to withstand cyberattacks and to deploy the digital infrastructure needed for a productive and secure economy*",[6] which interpretation feels somewhat controversial.

Considering the military approach to offensive cyber capabilities, for example, the military doctrine of the United States defines a cyberspace capability as *"a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace"*,[7] while the military doctrine of both the United States and the United Kingdom defines *offensive cyber operations (OCO)* very similarly as *"activities that project power to achieve military objectives in, or through, cyberspace"*.[8] The Allied Joint Doctrine for Cyberspace Operations further discusses the military context, emphasising that, besides supporting operations in the physical domains, offensive cyber capabilities may also aid information operations *"to influence, disrupt, corrupt or usurp the decision-making of adversaries"*.[9] However, the document does not explain the term *"capabilities"* in detail. Uren et al. (2018) from the Australian Strategic Policy Institute (*ASPI*) proposed another definition, explaining that *"in the context of cyber operations, having a capability means possessing the resources, skills, knowledge, operational concepts and procedures to be able to have an effect in cyberspace"*.[10]

From these various definitions and formulations, Gunjan Chawla and Vagisha Srivastava (2020) from the Centre for Communication Governance at the National Law University Delhi (*CCG NLU*) concluded that *"cyber capabilities and cyber operations are not synonymous, but cyber capabilities are a prerequisite to conducting offensive cyber operations"*.[11] This view is further corroborated by DeSombre et al. (2021) from the

3 Miralis 2019.
4 Kuehl2009: 24–42.
5 Minárik 2016.
6 Economist Intelligence Unit 2011: 7.
7 Joint Chiefs of Staff 2018: 100.
8 Ministry of Defence 2018: 32.
9 NATO Standardization Office 2020: 25.
10 Uren et al. 2018.
11 Chawla–Srivastava 2020.

Atlantic Council's Cyber Statecraft Initiative, which defines offensive cyber capabilities as *"the combination of tools; vulnerabilities; and skills, including technical, organizational, and individual capacities used to conduct offensive cyber operations".*[12]

As explained by Christopher S. Chivvis and Cynthia Dion-Schwarz (2017), compared to the conventional methods used by nation states, offensive cyber capabilities are less expensive, more difficult to detect and attribute (or at least easier to deny), and more effective to cause the target serious harm by exploiting security flaws. Due to the asymmetrical nature of cyber capabilities, smaller or simply resource poor countries can outperform large, resource rich nations and have a greater impact in cyberspace than they would otherwise have in the physical space.[13]

Measuring offensive cyber capabilities

> *"Achievements are made by talent, and industries are expanded by talent. In all things in this world, people are the most precious; and all innovative achievements are produced by people. Hard power or soft power, when it comes down to it, it all depends on the power of talent."* – Xi Jinping, 2018[14]

How can we assess and measure something that is not clearly defined? Though notable research was published by military- and defence-related organisations, studies on cyber power are much less common than studies on cybersecurity. There are also visible attempts to evaluate a nation's cyber power capability among the studies. For example, the National Capabilities Assessment Framework (*NCAF*) proposed by Sarri et al. (2020) from the European Union Agency for Cybersecurity (*ENISA*) provides a self-assessment of the level of maturity by assessing specific objectives to help enhance and build cybersecurity capabilities.[15]

Still, comprehensive comparisons of cyber power indices and associated studies focusing on offensive cyber capabilities are lacking in the literature. To fill this void, in a recent study, Çifci (2022) analysed global indices and studies for assessing cybersecurity and cyber power and compared them in terms of their comprehensiveness and strength for measuring country-level capabilities. For this purpose, Çifci proposed a conceptual framework that classified ninety indicators into fourteen categories, one of which is offensive capabilities. The framework offers only two indicators for cyber workforce and five each for cybersecurity research and offensive capabilities. However, the comparison excludes the latter category to maintain accurate calculations.[16]

Over the past decade, several organisations have worked on creating methods to assess the cyber power of countries, according to their interpretations. Many of them have been based on data collected by self-assessment via surveys with questionnaires, often resulting

[12] DeSombre et al. 2021b: 1.
[13] Chivvis–Dion-Schwarz 2017.
[14] Murphy et al. 2021.
[15] Sarri et al. 2020.
[16] Çifci 2022.

in composite weighted indices that produce a final ranking of countries. One of the various drawbacks of such indices is that the results can only be interpreted in relation to each other and if many countries are close in score, their rankings must be interpreted with special care. Composite indices are mostly focused on cybersecurity in general, covering various aspects of the information and communication technology (*ICT*) sector, including cyber incident response and recovery. Another difficulty is that the various organisations define the concept of cyber capabilities differently and therefore also measure them differently. In the following paragraphs, I briefly summarise some of the reports associated with measuring cyber capabilities.

A study on Cyber Warfare (*CW*) created by the Institute for Security Technology Studies (*ISTS*) at Dartmouth in 2004 was one of the first and most extensive research in determining the cyber warfare capability of countries. As Çifci (2022) summarised this study in a recent paper, Dartmouth researchers used an interdisciplinary method to combine strategic, technological and political analysis to provide an evaluation of the offensive cyber capabilities of chosen nation states and the possible consequences of cyberattacks on United States computer networks. Instead of quantitative measurements or rankings, the study measures government and private sector capabilities and provides qualitative statements about the selected nations.[17]

The Cyber Power Index (*CPI*), created in 2011 by the Economist Intelligence Unit (*EIU*) and Booz Allen Hamilton (*Booz*), ranked nineteen of the G20 nations in four areas: legal and regulatory framework; social-economic context; technology infrastructure; and industry application. The *CPI* claims to provide a broad measure of cyber power because it does not solely assess cybersecurity-related capabilities. However, with little focus on defence, it emphasises the economic and resource indicators, which do not fully depict cyber power, and it does not measure or even mention offensive cyber capabilities.[18]

The International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) first published in 2015 is based on the weighted scoring of questionnaire responses received from countries participating in the survey. The GCI is a composite index of several indicators that monitor and compare the level of the cybersecurity commitment of countries regarding the five pillars of the Global Cybersecurity Agenda (GCA), including the legal, technical, organisational and capacity-building measures and the cooperation aspects of national cybersecurity cultures of different countries. The GCI is published for over one hundred seventy countries and is one of the most comprehensive measures of cybersecurity commitment of countries; however, the five pillars of the cybersecurity agenda do not cover offensive capabilities.[19]

The Cyber Readiness Index (CRI) 2.0 also published in 2015 by Demchak et al. from the Potomac Institute evaluates and measures a country's preparedness levels for certain cybersecurity risks, paying particular attention to the economic importance of cybersecurity or in other words the "economic erosion caused by cyber insecurity". Although the CRI

[17] Billo–Chang 2004.
[18] Economist Intelligence Unit 2011: 7.
[19] ITU 2021.

2.0 analyses one hundred twenty-five nations, it does not rank or score them and only briefly mentions offensive capabilities as part of defence and crisis response.[20]

The report entitled "Cyber Capabilities and National Power: A Net Assessment" published in 2019 by the International Institute of Strategic Studies (IISS) follows a qualitative methodology and analyses the wider cyber ecosystem. The CCNP represents a snapshot in time and assesses the capabilities of fifteen countries in seven categories, including offensive cyber defined as "cyber operations that are principally intended to deliver an effect rather than those principally intended to gather intelligence". Furthermore, the report considers cyber espionage and network exploitation as intelligence gathering and covers them as core cyber intelligence capabilities. The CCNP divides the actors into three tiers based on their world-leading strengths in the various categories, but it does not rank the countries under investigation numerically within the tiers, because that would depend on the degree of importance attributed to each category.[21]

Voo et al. from the Belfer Center published the National Cyber Power Index (NCPI) in 2020. This index measures thirty countries' cyber capabilities in the context of seven broad categories called national objectives. The authors compiled and developed twenty-seven unique indicators to measure a state's cyber capabilities. The NCPI provides a comprehensive overall measurement of a country's aptitude as a cyber power with a combination of two standalone measures, the Cyber Capability Index (CCI) and the Cyber Intent Index (CII). The latter reflects the different prioritisation that some countries place on developing specific objectives, hence it can be considered equivalent to a weight.[22]

As Çifci (2022) also highlights the difficulties of measuring offensive cyber capabilities, one common limitation of these indices is the high level of secrecy on the related topics,[23] hence offensive cyber capabilities have also proven especially hard to measure objectively, given the lack of publicly available information. However, the continuing proliferation of offensive cyber capabilities also increases the visibility of an otherwise covert area of cybersecurity.

Additionally, the scope of these studies also seems to fall short, considering the unprecedented pace of proliferation. According to Marczak et al. (2018) from the Citizen Lab, while most cyber capability indices cover about thirty countries or less, the notorious Israeli cyber intelligence firm NSO Group provides services to operations in forty-five countries.[24] Furthermore, based on a document that surfaced during a lawsuit, another Israeli spyware firm, Candiru was negotiating deals with clients from over sixty countries.[25]

---

20 Demchak et al. 2015.
21 IISS 2021.
22 Voo et al. 2020.
23 Voo et al. 2020: 10.
24 Marczak et al. 2018.
25 Ziv 2020.

Indicators of offensive cyber capabilities

> "*Imagine that you are a chef. If you are a chef and you've got an empty kitchen, you will not be cooking anything. But if you are a chef and you've got some ingredients, then you can make some things. If I saw those ingredients, then I can kind of guess what you can make. But there comes a point where you don't know what is going to come out of the kitchen until you know who the chef is.*" – Julia Voo, 2020[26]

What indicators can we identify to assess offensive cyber capabilities without a clear definition to understand and scarce public information to measure? As explained by Liff (2012), although it may be simple to acquire a basic level of attack capability against computer networks, successfully attacking more secure systems or a more sophisticated adversary would require resources well beyond the means of conventionally weak actors.[27] At the same time, as highlighted by the Atlantic Council's Cyber Statecraft Initiative, the proliferation of offensive cyber capabilities shows that many governments are willing and able to pay the price to purchase the capabilities necessary for their various objectives. Even so, they cannot find the talent they need or cannot afford the expenses of in-house capability development lasting even decades. Meanwhile, Access-as-a-Service (AaaS) firms offer government-level capabilities at private sector speeds.[28] The continuous proliferation of cyber capabilities also increases the risk of incidents that draw public attention to otherwise concealed capabilities.

However, offensive cyber capabilities flow into all other aspects of society. Including, but not limited to, the digital economy as the Internet and technology transforms the way we do business, the national skill base needed for future economic development, or the university education required by today's information and knowledge-based society. Based on the International Institute for Strategic Studies (IISS), cyber capable countries also identify skills shortage as a significant risk, hence have embarked on upskilling and training initiatives. The cybersecurity skills shortage impacts the national labour markets worldwide, and the problem seems to persist, despite the proposed initiatives and launched actions.[29] It seems the skills shortage sets a common ground for understanding the importance of talent identification, development and management, which are all essential for both cyber capability development and cyber capacity building. Since zero-day vulnerabilities, crucial components of offensive cyber capabilities cannot be reused, the various actors in cyberspace need to develop their vulnerability research capabilities to identify new, previously unknown security flaws.

The question arises, why some states are incapable of producing the required cyber capabilities organically? It seems that research and education appear to be stronger in the liberal-democratic states, while the education systems of authoritarian countries

[26] AttackIQ 2020.
[27] Liff 2012: 401–428.
[28] DeSombre et al. 2021a.
[29] DeSombre et al. 2021a: 8.

remain underdeveloped. Similarly, Sanborn and Thyne (2013) highlight that authoritarian regimes typically underinvest in education, as education promotes democratisation. Hence, they misappropriate resources elsewhere.[30] Nevertheless, cyber-related research and education are difficult to implement without adequate public and higher education systems. The recently updated global inventory of commercial spyware initially compiled and released by Feldstein and Kot (2023) incorporates incidents from 2011 to 2023 and suggests a connection between the education system and the cyber power of a country, because "the data shows that autocratic regimes are far likelier to purchase commercial spyware or digital forensics than democracies".[31]

However, while defining and measuring cyber capabilities is difficult, assessing the educational capacities required for cyber talent identification, development and management may be a more straightforward approach. The different levels of the educational system, including elementary education, higher education and universities, are the core of cybersecurity competence. We can measure the availability of educational and training resources by indicators such as those described by Šendelj and Ognjanović (2015) and used by the Enhancement of Cyber Educational System of Montenegro (*ECESM*) project: organisational capacities; the number of courses, departments and study programs addressing cybersecurity issues; the number of organised training and workshops.[32] Aiming to attract students, the information behind these indicators is traditionally part of some publicly available curricula. The previously mentioned indicators can be further supplemented, for example, by the number of academic or professional security researchers, publicly disclosed security vulnerabilities, and online published technical analysis reports or custom-developed security tools.

One such resource is the Cybersecurity Higher Education Database (CyberHEAD), the largest validated cybersecurity higher education database in the European Union. Additionally, in their report about the European cybersecurity skills framework, Nurse et al. (2022) provide an overview of the current supply of advanced cybersecurity skills in Europe through an analysis of CyberHEAD. They collected the data via a questionnaire and supplemented the provided answers with publicly available information. The report includes the complete replies to questions that need to be answered by European academic institutions when listing their programs in CyberHEAD.[33]

Such raw data and information could serve as an appropriate basis for a more accurate assessment of cyber power, including offensive cyber capabilities. For example, Figure 1 below shows the distribution of cybersecurity education programs between European countries. Although these are only quantitative indicators, based on just the number of programs available, it seems that Spain (23), Italy (18), France (11) and Poland (11) are currently leading the way in cybersecurity upskilling. Their current educational advantage over other EU countries may be reflected in their future progress in offensive cyber capability development.

---

30 Sanborn–Thyne 2013: 773–797.
31 Feldstein–Kot 2023.
32 Šendelj–Ognjanović 2015.
33 Nurse et al. 2022.

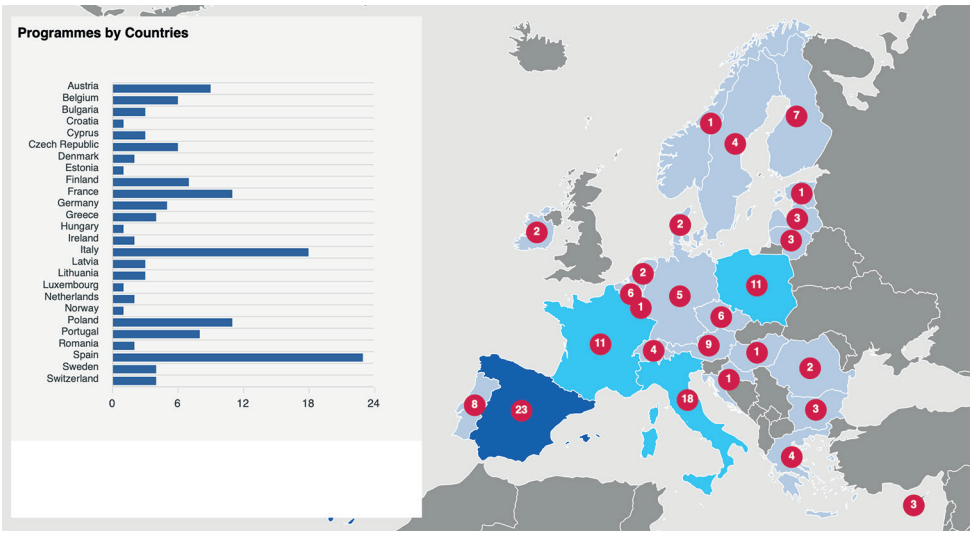


Figure 1: EU-wide distribution of cybersecurity programs registered in the CyberHEAD database in 2022

Source: ENISA 2023.

As also recognised by Xiangzhan et al. (2016), "competition between talented people […] is fundamental to international cyberspace security".[34] Given a supportive environment, cyber talents tend to stand out like islands in the sea through various individual or independent contributions during various hacker competitions. For example, the United States aims to reduce the skills shortage with the Cyber Challenge (USCC) program, launched to identify, attract and recruit the next generation of cybersecurity professionals. Young cybersecurity enthusiasts compete against each other online, and the top performers are invited for an in-person training program the following summer. Additionally, in 2019 former American president Donald J. Trump established the President's Cup Cybersecurity Competition (PCCC) for federal employees to identify cybersecurity talents inside the federal workforce.[35]

Hacking contests are also great places to scout for talented people. The number of participants and their results could be indicators of the offensive cyber capabilities of their indirectly represented nations. Mainly enterprises sponsor hacking competitions to publicise the security of a product and to use the security community to learn about new and innovative research techniques. They usually provide a commercially sold product and encourage the participants to find and exploit its vulnerabilities. Although Pwn2Own is the most famous hacking contest and offers the highest prizes in the world, Tianfu

[34] Xiangzhan et al. 2016: 49–52.
[35] Trump 2019.

Cup also became a notable contest in recent years after China banned its former winner security researchers from participating in Pwn2Own.[36]

Security researchers commonly share information on new vulnerabilities, methodologies, or techniques in the cybersecurity community. In the same way, it is also a common practice to share custom-developed software tools on collaborative coding platforms like GitHub or GitLab. Public technical analysis reports of notorious vulnerabilities, proof-of-concept exploits, or security software tools may draw attention to their author as a skilled professional or high-potential cybersecurity talent.

Hack the Box and TryHackMe are just a few of the well-known cybersecurity training and game platforms that are great for learning and testing a candidate's knowledge. Users in these Capture the Flag (CTF) games must find their way through vulnerable systems that are purposefully made insecure and collect flags to keep track of their progress. Users advance in the ranks by completing the challenges, and we can track their success on their public profiles, which makes their talent visible to everyone.

Vendors initiated bug bounty programs in the 1980s to allow security researchers to report vulnerabilities. In the ideal case, they incentivise hackers to do the right thing and report flaws to the developer. Current bug bounty programs are either managed internally by the vendor or by a third party like HackerOne or Bugcrowd. However, many programs offer public thanks and acknowledgment to the researchers, who can earn points for their reports and appear on public leader boards. As Miyashita and Eckert summarised in the year-end review of their 2022 bug bounty program, Microsoft awarded three hundred thirty-five security researchers across forty-six countries, supported by the below world map in Figure 2, showing the distribution of researchers based on their location. Based on the grey scale from one to seventy-seven, the order of countries with the most awarded researchers seems to be China, USA, India, the U.K., Germany and Eastern Europe also participated.[37]

Even though employers usually prohibit their staff from participating in hacking contests or bug bounty programs,[38] their employees still compete with others in the labour market, often with a publicly available resume highlighting key work achievements, skills and experience. Thereby the labour market can serve as indirect feedback to measure the overall performance of a cybersecurity educational system and the cyber capability of a country. The cybersecurity sector is always looking for skilled workers and will find them where the educational system can produce them.

Furthermore, the nature of the positions available in the labour market also plays a decisive role regarding cyber capabilities. Distinguishing between the added value of the various job roles is essential. For example, while an analyst has an important role in defence against cyberattacks, an exploit developer has a crucial impact on building offensive capabilities.

---

36 Blue 2018.
37 Miyashita–Eckert 2022.
38 Laszka et al. 2018: 138–159.

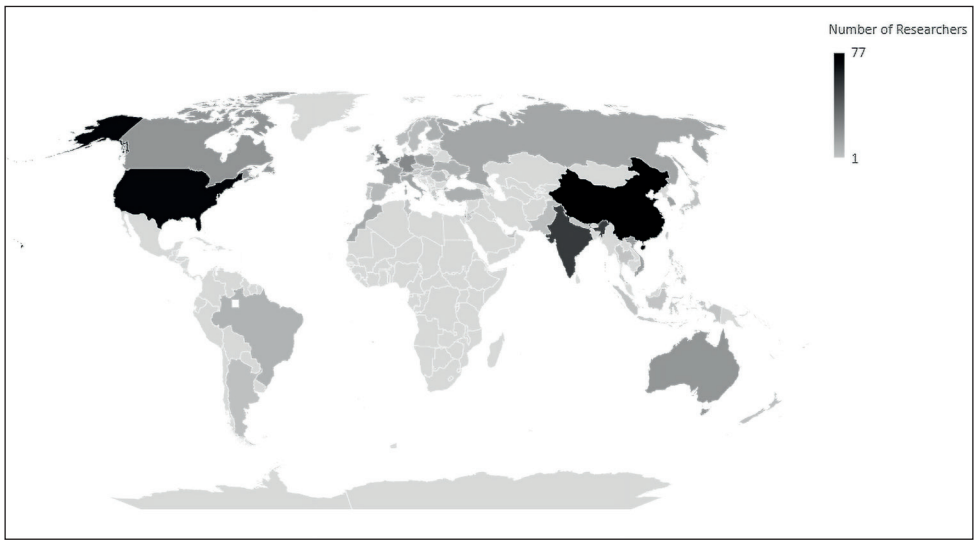


Figure 2: Worldwide distribution of security researchers awarded by Microsoft in 2022
Source: Miyashita–Eckert 2022.

The main advantage of the previously discussed indicators is that the necessary information is publicly accessible on the Internet. The data can be collected in an automated way, without questionnaires or interviews. The security community may ensure the authenticity and correctness of public information by early exposing false claims, especially regarding offensive security. After verification and validation, the data can be evaluated objectively.

Conclusion

Secrecy is the basis of offensive security. Assessing and measuring something that nation states want to keep secret and hidden is difficult, to say the least. Yet, if we take a holistic view of offensive security, we may find the signs by which otherwise hidden cyber capabilities can become investigable.

Offensive security requires human ingenuity and creativity, hence it is often more of an art than a science, and as such, it requires artists to do it. Allowing people to tackle challenges without constraints is the best way to bring out the best in them. Thereby, their shining talent will be something we can look for when assessing cyber capabilities. As young people hone their skills, they show their talent to the public. During this time, the secrecy that traditionally characterises the cybersecurity profession does not yet cover their activities. As a result, important information (blog posts, code repositories, competition results and resumes) is publicly available from this period, based on which cyber capabilities could be assessed and measured by a better approximation.

In this sense, the key to successful offensive cyber capability development is the size and quality of the available workforce, while the labour shortage affects all actors.

Whoever can first meet the challenge of the cybersecurity skills shortage, may win the cyber race. Though China has demonstrated its cyber power with its outstanding performance in the indicators mentioned earlier, due to its massive population scale and political establishment, the talent shortage may have a particularly negative impact on the country. According to a ministry report, China will have a more than three-million-person talent gap in cybersecurity by 2027, while its higher education institutions can only produce thirty thousand new professionals annually.[39]

Meanwhile, as Harvard University scholar Graham Allison and former Google CEO Eric Schmidt argued, though the United States faces the same problem, its immigration policy could offer a significant advantage in the race for talent.[40] Cybersecurity-specific agency actions, similar to those announced by the Biden–Harris Administration to attract international STEM talent,[41] would allow the U.S. to recruit and retain qualified foreign nationals who already possess the requisite skills, education and expertise, without investing the time and resources needed to train them. In contrast, China's great weakness is its inability to attract foreign talent, because it has limited itself to its own population, while the U.S. can recruit from all over the world.

References

Allison, Graham – Schmidt, Eric (2022): The US Needs a Million Talents Program to Retain Technology Leadership. Immigration is the United States' Secret Sauce – Including in Its Competition with China. *Foreign Policy*, 16 July 2022. Online: https://foreignpolicy.com/2022/07/16/immigration-us-technology-companies-work-visas-china-talent-competition-universities/

AttackIQ [@AttackIQ] (2020): Think Bad, Do Good: Julia Voo and the National Cyber Power Index. *YouTube*, 05 October 2020. Online: www.youtube.com/watch?v=OESUV5qRfdY

Billo, Charles – Chang, Welton (2004): Cyber Warfare – An Analysis of the Means and Motivations of Selected Nation States. *Institute for Security Technology Studies at Dartmouth College*, 01 November 2004. Online: www.researchgate.net/publication/230687826

Blue, Violet (2018): When China Hoards Its Hackers Everyone Loses. *Engadget*, 16 March 2018. Online: www.engadget.com/2018-03-16-chinese-hackers-pwn2own-no-go.html

Chawla, Gunjan – Srivastava, Vagisha (2020): What Are 'Offensive Cyber Capabilities'? *The CCG Blog*, 07 August 2020. Online: https://ccgnludelhi.wordpress.com/2020/08/07/what-are-offensive-cyber-capabilities/

Chivvis, Christopher S. – Dion-Schwarz, Cynthia: Why It's So Hard to Stop a Cyberattack – And Even Harder to Fight Back. *The RAND Blog*, 30 March 2017. Online: www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html

[39] Shen 2022.
[40] Allison–Schmidt 2022.
[41] The White House 2022.

Çıfcı, Hasan (2022): Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework. *Research Square,* 17 October 2022. Online: https://doi.org/10.21203/rs.3.rs-2159915/v1

CSRC (2021): Vulnerability – Glossary. *NIST,* 2021. Online: https://csrc.nist.gov/glossary/term/vulnerability

Demchak, Chris – Kerben, Jason – McArdle, Jennifer – Spidalieri, Francesca (2015): Cyber Readiness Index 2.0. *Potomac Institute for Policy Studies,* November 2015. Online: https://potomacinstitute.org/images/CRIndex2.0.pdf

DeSombre, Winnona – Campobasso, Michele – Allodi, Luca – Shires, James – Work, JD – Morgus, Robert – O'Neill, Patrick Howell – Herr, Trey (2021a): A Primer on the Proliferation of Offensive Cyber Capabilities. *Atlantic Council,* 01 March 2021. Online: www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/

DeSombre, Winnona – Shires, James – Work, JD – Morgus, Robert – O'Neill, Patrick Howell – Allodi, Luca – Herr, Trey (2021b): Countering Cyber Proliferation: Zeroing in on Access-as-a-Service. *Atlantic Council,* 01 March 2021. Online: www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/

Economist Intelligence Unit (2011): Cyber Power Index. Findings and Methodology. *Booz Allen Hamilton,* August 2011. Online: https://web.archive.org/web/20151017081309/www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

ENISA (2023): *Cybersecurity Higher Education Database: Programmes Location.* Online: www.enisa.europa.eu/topics/education/cyberhead/#/statistics

Feldstein, Steven – Kot, Brian (2023): Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. *Carnegie Endowment for International Peace,* 14 March 2023. Online: https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

IISS (2021): Cyber Capabilities and National Power: A Net Assessment. *International Institute for Strategic Studies,* 28 June 2021. Online: www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

ITU (2021): Global Cybersecurity Index 2020. *International Telecommunication Union,* 29 June 2021. Online: www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Joint Chiefs of Staff (2018): *Joint Publication 3-12. Cyberspace Operations.* Online: https://irp.fas.org/doddir/dod/jp3_12.pdf

Kuehl, Daniel T. (2009): From Cyberspace to Cyberpower: Defining the Problem. In Kramer, Franklin D. – Starr, Stuart H. – Wentz, Larry K. (eds.): *Cyberpower and National Security.* University of Nebraska Press. 24–42. Online: https://doi.org/10.2307/j.ctt1djmhj1.7

Laszka, Aron – Zhao, Mingyi – Malbari, Akash – Grossklags, Jens (2018): The Rules of Engagement for Bug Bounty Programs. In Meiklejohn, Sarah – Sako, Kazue (eds.): *Financial Cryptography and Data Security.* Berlin–Heidelberg: Springer. 138–159. Online: https://doi.org/10.1007/978-3-662-58387-6_8

Liff, Adam P. (2012): Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, 35(3), 401–428. Online: https://doi.org/10.1080/01402390.2012.663252

Marczak, Bill – Scott-Railton, John – McKune, Sarah – Razzak, Bahr Abdul – Deibert, Ron (2018): Hide and seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. *Citizen Lab*, 18 September 2018. Online: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Minárik, Tomáš (2016): NATO Recognises Cyberspace as a "Domain of Operations" at Warsaw Summit. *NATO CCDCOE*, 21 July 2016. Online: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

Ministry of Defence (2018): *Joint Doctrine Note 1/18. Cyber and Electromagnetic Activities.* Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf

Miralis, Dennis (2019): Defining Offensive Cyber Capabilities. *NGM Lawyers*, 19 March 2019. Online: https://ngm.com.au/defining-offensive-cyber-capabilities/

Miyashita, Lynn – Eckert, Madeline (2022): Microsoft Bug Bounty Programs Year in Review: $13.7M in Rewards. *Microsoft Security Response Center*, 11 August 2022. Online: https://msrc.microsoft.com/blog/2022/08/microsoft-bug-bounty-programs-year-in-review-13-7-in-rewards/

Murphy, Ben – Creemers, Rogier – Kania, Elsa – Triolo, Paul – Neville, Kevin – Webster, Graham (2021): Xi Jinping: 'Strive to Become the World's Primary Center for Science and High Ground for Innovation'. *DigiChina at Stanford University*, 18 March 2021. Online: https://digichina.stanford.edu/work/xi-jinping-strive-to-become-the-worlds-primary-center-for-science-and-high-ground-for-innovation/

NATO Standardization Office (2020): *Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations.* Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Nurse, Jason R. C. – Adamos, Konstantinos – Grammatopoulos, Athanasios – Di Franco, Fabio (2022): Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education. *Publications Office of the European Union*, 03 January 2022. Online: https://doi.org/10.2824/033355

Sanborn, Howard – Thyne, Clayton L. (2013): Learning Democracy: Education and the Fall of Authoritarian Regimes. *British Journal of Political Science*, 44(4), 773–797. Online: https://doi.org/10.1017/S0007123413000082

Sarri, Anna – Kyranoudi, Pinelopi – Thirriot, Aude – Charelli, Federico – Dominique, Yang (2020): National Capabilities Assessment Framework. *Publications Office of the European Union*, December 2020. Online: https://doi.org/10.2824/590072

Šendelj, Ramo – Ognjanović, Ivana (2015): Cyber Security Education in Montenegro: Current Trends, Challenges, and Open Perspectives. *7th Annual International Conference on Education and New Learning Technologies (EDULEARN15)*, 08 July 2015. Online: https://ecesm.net/sites/default/files/EDULEARN_Sendlej.Ognjanovic.pdf

Shen, Xinmei (2022): China's Demand for Cybersecurity Talent Will Exceed Supply by over 3 Million in Five Years, Says Education Ministry Report. *SCMP,* 08 September 2022. Online: www.scmp.com/tech/tech-trends/article/3191781/chinas-demand-cybersecurity-talent-will-exceed-supply-over-3

The White House (2022): Fact Sheet: Biden–Harris Administration Actions to Attract STEM Talent and Strengthen our Economy and Competitiveness. *The White House,* 21 January 2022. Online: www.whitehouse.gov/briefing-room/statements-releases/2022/01/21/fact-sheet-biden-harris-administration-actions-to-attract-stem-talent-and-strengthen-our-economy-and-competitiveness/

Trump, Donald J. (2019): America's Cybersecurity Workforce. *The White House,* 02 May 2019. Online: www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce

Uren, Tom – Hogeveen, Bart – Hanson, Fergus (2018): Defining Offensive Cyber Capabilities. *Australian Strategic Policy Institute, 0*4 July 2018. Online: www.aspi.org.au/report/defining-offensive-cyber-capabilities

Voo, Julia – Hemani, Irfan – Jones, Simon – DeSombre, Winnona – Cassidy, Dan – Schwarzenbach, Anina (2020): National Cyber Power Index 2020. *Belfer Center for Science and International Affairs,* September 2020. Online: www.belfercenter.org/publication/national-cyber-power-index-2020

Xiangzhan, Yu – Hongli, Zhang – Haining, Yu – Zhihong, Tian – Jianhong, Zhai – Zhuting, Pan (2016): Cyberspace Security Competition and Talent Management. *Strategic Study of Chinese Academy of Engineering,* 18(6), 49–52. Online: https://doi.org/10.15302/J-SSCAE-2016.06.010

Ziv, Amitai (2020): Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed. *Haaretz,* 07 September 2020. Online: www.haaretz.com/israel-news/tech-news/.premium-mobile-spytech-millions-in-gulf-deals-top-secret-israeli-cyberattack-firm-reve-1.9125915

AARMS Vol. 22, No. 3 (2023) 19–41.

10.32565/aarms.2023.3.2

Quantitative Analysis of the Possible Sites of a New Danube Bridge to Bypass Budapest on Rail – Part 1[1]

Bence TÓTH,[2] Zsolt LÉVAI[3]

Since 1920, almost all the traffic on rail crossing the Danube in Hungary, crosses it in Budapest via the Southern Railway Bridge which makes it heavily overloaded. This is a very disadvantageous situation not only for commercial shipping but also for military uses as there is certain heavy military equipment that can only be transported via rail.

In our two-part article, we examine the locations of new bridges that could be alternatives to bypass Budapest and thus to reduce the traffic load on the railway lines of the capital. In this first part of our paper, we present the effect of a new Danube bridge as an alternative to the V0 railway line. We examine the possible sites of the bridge with several different route alternatives connecting it to the existing railway lines by using traffic simulation.

Keywords: *railway, bridge, graph theory, traffic, military engineering*

Introduction

The research priorities in military sciences and especially in military engineering,[4] are changing over time according to the international defence situation. Eight main research areas have been identified by a recent research, namely military theory and warfare, strategy and defence planning, Vision of the Hungarian Armed Forces, defence and good governance, country defence, HR and personnel work, international crisis management and peacekeeping, and military history, preservation of tradition and civil–military relations.[5] From these areas both country defence and defence planning are strongly related to the logistic capacities of the armed forces. A vital part of the logistic network of an army is the transportation sector. Both the railway and the road sector are mainly operated by the

[1] This publication was prepared with the professional support of the Doctoral Student Scholarship Program of the Co-operative Doctoral Program of the Ministry of Innovation and Technology financed from the National Research, Development and Innovation Fund.

[2] Assistant Professor, University of Public Service, e-mail: toth.bence@uni-nke.hu

[3] PhD student, University of Public Service, Faculty of Military Science and Officer Training, Doctoral School of Military Engineering, e-mail: levai.zsolt@kti.hu

[4] Haig 2016: 115–116.

[5] Boda et al. 2016: 2–23.

civil sector and the armed forces own a relatively small part of the infrastructure as the national network is used for everyday civil transportation purposes.

Therefore, the defence preparations of a country requires the transport network to be available in sufficient quantity and quality to perform the necessary military movements and transportation tasks when needed. Therefore, during this defence preparation, the network elements on which the military transportation actions will take place, should be identified. These elements then must be properly maintained and protected to be ready for the transportation tasks at all times. After any damage, they must be rebuilt immediately so traffic can be picked up as soon as possible. This is not only the interest of Hungary but is also an allied obligation and one of the basic conditions for the feasibility of NATO's[6] Host Nation Support tasks.

But not only because of the military applications but also because of the everyday freight traffic share of the railway should the network be developed. The share of rail in the freight traffic of the country in 2021 was 16.48% of the total weight of goods transported, which is 22.04% of freight tonne-kilometres.[7] One-sixth of goods therefore reach their destination by rail, which is quite a small proportion compared to the 55% level in 1985,[8] despite the aim of maintaining the share of rail transport at a higher level than in Western Europe.[9] Furthermore, there is a political will in the European Union (EU) to shift freight traffic from road to rail as much as possible, not only for reasons of economy but also because railway transport is much more environmental friendly due to its lower emissions and lower noise pollution.[10]

One of the critical points in the railway network of Hungary is the crossing of the Danube.[11] The railway infrastructure of the capital is already congested due to the significant passenger traffic, and the additional train paths booked for freight trains reduce the free capacity of the railway tracks further. The overloaded infrastructure raises questions about the solvability of security tasks. This is primarily a question of the feasibility of military rail transportation tasks.[12]

In our two-part article, we examine the locations of new bridges that could be alternatives to bypass Budapest and thus to reduce the traffic load on the railway lines of the capital. In the first part of our paper, we present the effect of a new Danube bridge as an alternative to the V0 railway line. In the second part, we examine the situation on the river Tisza and suggest a combined way of development to treat the capacity changes in the context of the whole network.

---

6 NATO – North Atlantic Treaty Organization.
7 For more information see www.ksh.hu/stadat_files/sza/hu/sza0002.html
8 Szászi 2010: 101–118.
9 Szászi 2007: 32–59.
10 Berényi–Lévai 2020.
11 Horváth 2006: 321–336.
12 Szászi 2013b: 98–107.

PART 1

The railway infrastructure of Hungary

The density of the railway network of Hungary is relatively high. Its 7,441 km total length[13] means 8.00 km/100 km^2 density which is the sixth highest in the world after Switzerland (12.63), the Czech Republic (12.12), Belgium (11.72), Germany (10.75) and Luxembourg (10.48).[14] However, other parameters are not that good, for example the ratio of electrified lines is only 37.7% and the ratio of double-tracked lines is only 16.6%.[15]

When the border was drawn after World War I, on the Subotica – Timișoara – Arad – Oradea – Satu Mare – Korolevo – Chop – Košice – Rožňava – Lučenec line, i.e. within the railway ring of the Kingdom of Hungary built at the end of the 19th century, the railway network of the remaining part of Hungary became transversally blocked. The remaining connections between the radial main lines were single-tracked lines with low capacity and therefore could not be used as real alternatives in case of disruptions of the main lines. The only connection point was Budapest and still is today.

Bottlenecks

After the Treaty of Trianon, only three railway bridges remained in the country. The northernmost was the Újpest Railway Bridge, a single-tracked bridge in the northern part of Budapest. The second, also in Budapest, was the Southern Railway Bridge, a double-tracked crossing. The third was the Türr István Bridge at Baja, 144 km south of Budapest, a single-tracked bridge. To date, these are still the only bridges that provide the possibility of crossing the Danube within Hungary. In the meantime, the Újpest bridge and Southern bridge were electrified, but the railway line that connects the line of the Újpest bridge back to the core network was not, therefore in the view of electrification, it lies on a branch line. A third track of the Southern bridge is currently being built, but this does not solve the substitutability of this bridge.

There is one more railway bridge that connects Komárom in Hungary with Komárno in Slovakia, but it is also a border crossing. This bridge cannot be taken into account in the defence preparations.

Therefore, one of the most neuralgic points of the Hungarian railway infrastructure is the crossing of Budapest. This means two things: passing through the capital and crossing the Danube. The east–west railway lines run long in the city, causing much noise pollution for the residents. International freight trains crossing the Danube in Hungary pass almost exclusively over the Southern Railway Bridge, which is also located in the capital, on the southern edge of the city centre. The problem is most pronounced in the congestion of the

[13] For more information see www.ksh.hu/stadat_files/sza/hu/sza0041.html
[14] Further details at https://w3.unece.org/PXWeb/en/PDFCountryProfiles
[15] See www.mavcsoport.hu/mav/bemutatkozas

Ferencváros–Kelenföld line section, which includes the bridge and as a result, the bridge is on the edge of its capacity.[16]

It is therefore necessary to ensure the possibility of providing an alternative route for the Southern bridge as a critical infrastructure element in case of its disruption (which can also mean the disruption of the Ferencváros–Kelenföld line section that contains it). In the current network, due to the previously described state of the two remaining bridges, neither the Újpest nor the Baja bridge is an alternative to the Southern bridge.

The distance between Budapest and Almásfüzitő via the Újpest bridge is only 8 km longer than the route leading through the Southern bridge, however, it does not provide a direct connection to Kelenföld on the right bank of the Danube. The trains have to pass through the hilly and partly single-tracked Budapest–Esztergom line and the single-tracked Esztergom–Almásfüzitő line which is not electrified, and this causes a significant increase in the travel time. In addition, the capacity of the lines is insufficient to handle the traffic of the Southern bridge. The Baja Bridge is located 144 km south of the Southern bridge, so the length of the route bypassing Budapest would increase so much that it makes this bridge an unrealistic alternative.[17] The Baja bridge is also located on a single-track, non-electrified line, which further increases the travel time and reduces its capacity.

The railway infrastructure of Budapest

Budapest is the most important railway junction in the country. The railway lines to and through the city are used by tens of thousands of people a day, and the freight traffic passing through them also means tens of thousands of tons of goods a day. Most of the railway lines were built in their present form by the beginning of the 20th century, which means that the structure of the network reflects the conditions of the beginning of the last century as it was designed to satisfy the needs of that time (passenger and freight, too). A significant part of the railway developments was and is still carried out on lines outside of Budapest, therefore the railway network of the capital has now become a barrier rather than a facilitator of the spread of modern modes of transport. The capacity of the system did not change over time as no capacity-enhancing developments were implemented and thus Budapest became a bottleneck in the railway network of Hungary.

Budapest is the starting point of 11 main national railway lines and three suburban railway lines (HÉV), which, though operated by the same corporation, uses different voltage system and therefore is not compatible with the railway network. One HÉV line, the one that connects the district of Csepel, runs entirely within the city. The main railway lines start from three main termini, Keleti pályaudvar, Nyugati pályaudvar and Déli pályaudvar (literally, Eastern, Western and Southern Railway Station) but the lines of local interest also start from two different terminals, Kőbánya-Kispest and Rákospalota-Újpest.

A significant part of the railway infrastructure of Budapest is composed of the elements of the so-called Circular Railroad (Figure 1). These are the line network

[16] Lévai 2020: 198–223.
[17] Szászi 2014: 25–48.

elements that make the connection between each radial line inside the city. The most important element is the Outer Circular Railroad, the railway line between Kőbánya-Felső–Rákos and Rákosrendező–Rákospalota-Újpest stations, which connects railway lines No. 1 (Budapest–Hegyeshalom), 80 (Budapest–Hatvan–Miskolc–Nyíregyháza), 120 (Budapest–Újszász–Szolnok–Békéscsaba–Lőkösháza) and 150 (Budapest–Kelebia) with lines No. 2 (Budapest–Esztergom) and 70 (Budapest–Vác–Szob), thus allowing the north–south passage through the city without entering a terminal station. The significance of the Outer Circular Railroad is shown by the fact that it was built as a double-tracked line, it is electrified and is equipped with automatic block signalling (ABS). At the same time, one of the most important sections, the Angyalföld junction and Rákospalota-Újpest section is only single-tracked and is in poor condition. Between Angyalföld junction and Rákosrendező station, the line speed is only 40 km/h. Though this section provides the north–south connection, its limited capacity significantly reduces the capacity of the entire network. In addition, the so-called "Marchegg Bridge" over lines 70 and 71 (Budapest–Vácrátót–Vác) that connects the Outer Railroad Circular with Angyalföld station and thus with lines No. 2 and 4 (Esztergom–Almásfüzitő), is electrified, but single-tracked.

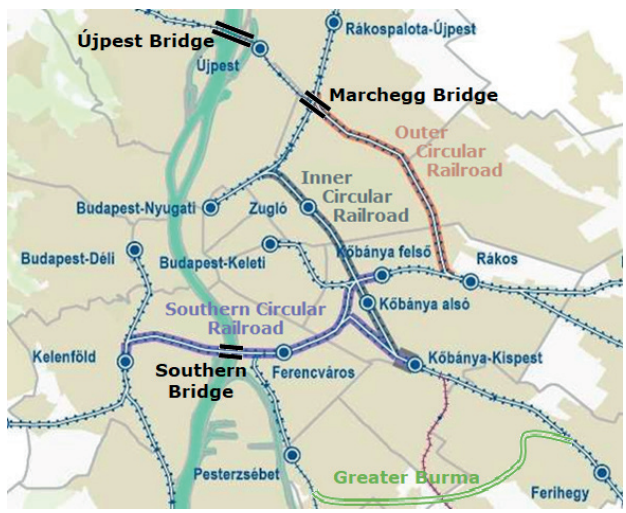


Figure 1: Elements of the Budapest Circular Railroad

Source: Compiled by the authors based on BRNS 2019.

The Inner Circular Railroad is the line Városliget junction – Kőbánya-Teher – Kőbánya-Kispest, which coincides the Budapest section of line No. 100 (Budapest–Cegléd–Szolnok–Debrecen–Nyíregyháza–Záhony).

The third significant section of the Circular Railroad is the Southern Circular Railroad, the Kőbánya-Kispest – Kőbánya felső – Ferencváros – Kelenföld line, which is also double-tracked, electrified and equipped with ABS. This line provides the east–west connection without the need of entering a terminus.

One peculiar element of the Circular Railroad is a short section, a wye, the so-called Királyvágány (literally, "King's track"), which connects the stations Kőbánya felső and

Kőbánya-Teher and thus provides a direct connection between lines No. 80, 120, 100 and 70. Its length is 1.3 km, it is single-tracked, electrified with a line speed of 30 km/h. Its name originates from the person to whom it was specifically built for: Franz Joseph I, emperor of Austria and king of Hungary. By using this wye, the royal train from Nyugati Railway Station could easily turn in the direction of Gödöllő, where the royal summer palace was situated. The track is rarely used but if developed to two tracks with much higher line speed it could have a role in substituting the Outer Circular Railroad.

The so-called Greater Burma line can also be considered part of the Circular Railroad (the Lesser Burma line that connected Ferencváros and Soroksár stations was completely dismantled in 2006). The Greater Burma was once double-tracked, but today it is only single-tracked. It connects Soroksár station on line No. 150 with Pestszentimre station on line No. 142 (Budapest–Lajosmizse–Kecskemét) and Szemeretelep station on line No. 100. The line is out of operation, it was last used in 2001, during the reconstruction of line No. 150 as a bypass route between Soroksár and Pestszentimre.[18] Its condition has significantly deteriorated since, the speed limit is currently 0 km/h. The other part of the line between stations Pestszentimre and Szemeretelep is no longer intact, the tracks are missing in several places.

Brownfield developments

The basic thought behind the studies to be presented is to analyse sites where there are railway lines on both banks of the Danube. Thus, only the most necessary construction costs have to be taken into account as only the building of the bridge is a greenfield development, the connecting railway lines already have the infrastructure which reduces the costs being a brownfield development.[19]

Each path was analysed using a mathematical model and we looked for the alternative with the best properties. These properties included the traffic passing through the new bridge in normal operating circumstances,[20] the ratio with which they can decrease the traffic passing through Budapest and the redundancy they provide in case of disruption of other bridges.

Our study covers several possible sites and route variants. Of course, it is necessary to build new network elements for all variants, but since we are basically looking for brownfield solutions, they always mean significantly less greenfield investment than the construction of a fully greenfield V0.[21]

[18] Kristóf–Lévai 2002: 3–6.
[19] Lakatos et al. 2016: 181–288.
[20] Tóth 2018: 505–519.
[21] Tóth–Horváth 2019: 109–129.

The graph model of the railway network of Hungary

The mathematical model used for the calculations has been presented in detail earlier, so we will only discuss it here as much as it is necessary for understanding.[22]

A weighted directed graph is used to model the railway network of Hungary. The nodes of the graph corresponds to stations where a change in the direction is possible. The sidings of the Hungarian Army were also included.[23] Stops with no switches were not included in the model. Also, the stations with exactly two neighbouring stations, the so-called joint nodes, were transformed out: each joint node and its two connecting edges were substituted with a single edge with a weight of the sum of the two edges replaced.[24]

The edges of the graph represented the line sections between these stations. Two weights were assigned to an edge: to calculate the shortest path, the length of the corresponding line section, and to determine the fastest path, the ratio of the length of the line sections and the line speed. The latter is the pure travel time, which gives the lowest limit a path could be run within, as it does not take into account any speed limit or acceleration/deceleration time. If the value of the line speed was lower for trains with locomotives than for ECMs, then the former, the lower value was used. The data used is publicly available on the website of the Hungarian Rail Capacity Allocation Office (Vasúti Pályakapacitás-elosztó Kft.).[25]

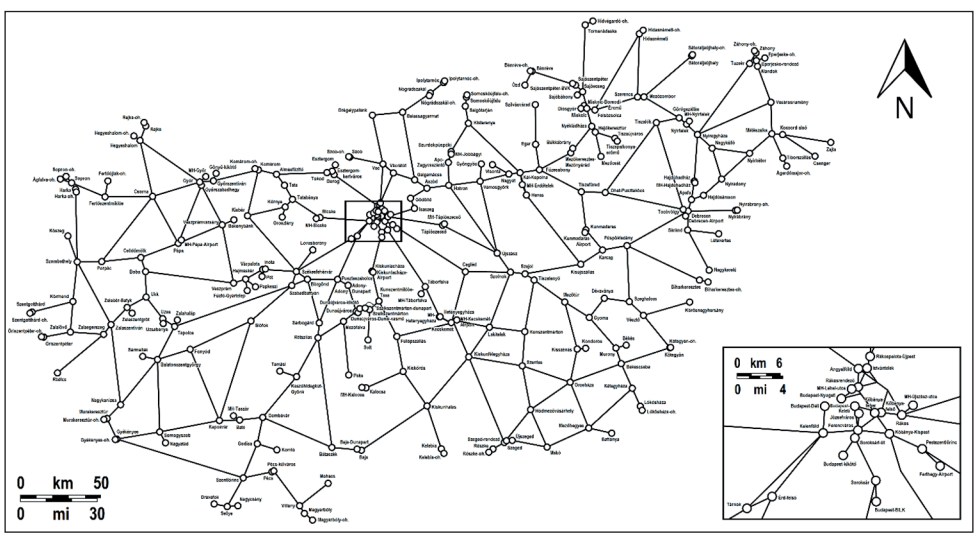


Figure 2: Diagram of the graph modelling the railway network of Hungary

Source: Compiled by the authors.

22 Tóth 2021: 567–587.

23 Government Decree 277/2014 (XI.14.) on the Amount of Fine the Railway Authority Can Issue and Detailed Rules of Its Payment, 2nd Appendix.

24 Jenelius et al. 2006: 537–560.

25 See www.vpe.hu/takt/vonal_lista.php

For locomotive reversal and direction change, 15 extra minutes were to be added. Therefore, the graph describing the network had to be expanded in order for the algorithm calculating the shortest path to add the extra time of direction changes when needed. No extra trip length or travel time was assigned to passing a station and no extra distance was assigned to reversing. The diagram of the graph is shown in Figure 2.

Methods and measures

In some cases, it is better to choose the length of the path of a train to be minimal, and in other cases the travel time to be as short as possible. The former is one of the main aspects of commercial rail transport, as both transport charges and overhead line charges are kilometre-based, and locomotives are often rented for a fixed amount per working day. However, in case of a state of emergency, time can be a quite important aspect and in many cases, the shortest route may not be the fastest.

The calculations and the visualisation of the results were performed in the R programming language and environment[26] using the *igraph* package[27] developed by Gábor Csárdi and Tamás Nepusz. The graph describing the network is encoded as a two-column matrix, a so-called edge list.[28] Each line describes a line section, the first number being the index of the origin and the second the number of the destination station of the line section. For each edge, a weight can also be assigned, using a vector with a dimension equal to the number of edges, which in our case was either the distance between the nodes representing neighbouring stations or the corresponding travel time. The shortest distance (in distance or time) between any two stations can be determined by the *distance()* function of the *igraph* package, which uses Dijkstra's algorithm[29] in graphs with positive weights (such as the one we use) by default. The function *shortest_paths()* can be used to determine which edges and nodes fall on the shortest path.

The possible locations of the new Danube bridge

In the following, from north to south in Hungary, we examine the possible locations of the new Danube bridge. For each alternative, we present the exact route, the spatial distribution of the routes passing through the bridge (i.e. which regions of the country does the bridge connect on the shortest path), the effect of the bridge on the change of the traffic of each line section in the network, and how does the traffic pass through the other bridges in light of the existence of the new one.

[26] R Core Team s. a.
[27] Csárdi–Nepusz 2006: 1–9.
[28] Tóth 2017: 52–66.
[29] Dijkstra 1959: 269–271.

Szob–Esztergom

The northernmost possible location to build the crossing is at Szob. According to our model, the track leading to the bridge branches off from Szob station and reaches the Danube with a 90-degree leftward curve. After the bridge, it immediately enters a 7 km long tunnel and at the end of it the line connects to line No. 2 (Budapest–Esztergom) at Esztergom-Kertváros (Figure 3).

Figure 3: The Szob–Esztergom bridge and planned railway line
Source: maps.google.hu

As Szob is a border station, after the Ipoly bridge, the tracks run already in Slovakia. As the left bank of the Danube is highly built-in in this region, a branching before Szob could only be solved with an even larger amount of earthworks. The issue of ownership of the northern bridgehead therefore requires an interstate solution, but several alternatives are conceivable. The most obvious solution is similar to the Losonc–Kalonda–Nagykürtös line, which is part of the Aszód–Balassagyarmat–Ipolytarnóc railway line and the Slovakian railway infrastructure manager, ŽSR, uses it as a passage line. The same model could be applied at Szob as well: the 1.5 km section to the Danube bridge after the Ipoly Bridge in Slovakia could be operated as a passage line. However, it should be emphasised that this line section would not have a connection to the Slovak railway network, although the line itself would branch off from the main line in Slovakia.

Furthermore, it is the most expensive alternative. Due to the built-in, the line should immediately enter the 7 km long tunnel at the southern bridgehead all the way to Esztergom Diósvölgy, from where it would be connected to line No. 2 at Esztergom-Kertváros.

Dunaföldvár–Solt

The 13 km long single-tracked, non-electrified Solt–Dunaföldvár railway line, which is numbered 151a, was finished in 1940. The bridge over Dunaföldvár, through which

it crossed the river, was originally designed exclusively for road traffic and the tracks were built in only during the construction of the railway line when it was converted into a common crossing. The bridge would have played a role in replacing the railway ring road outside the country borders mentioned earlier, as line No. 151a was intended to be part of an "internal railway ring". The line would have continued from Solt to Fülöpszállás (the sectioning of the line also started at Fülöpszállás station); but the latter section was never built.

We examined 6 alternatives at the Dunaföldvár bridge. Alternatives 1–3 took into account the Solt–Dunaföldvár section with the original route and only a higher line speed (120 km/h) was assumed for the existing lines. Alternatives 4–6 took into account the planned Fülöpszállás–Solt line section with the same line speed, too (Figure 4).

Alternatives 1, 2 and 3

In case of the first three alternatives, only the existence of the Dunaföldvár–Solt line section including the bridge was assumed with the same length as it was at the time of its closure (13 km). Alternative 1 takes into account line No. 151a only with 60 km/h line speed. Alternative 2 further supposes the line speed of lines No. 42 (Pusztaszabolcs–Mezőfalva–Dunaföldvár–Paks), 43 (Mezőfalva–Rétszilas) and 151 (Kunszentmiklós-Tass–Solt) to be 120 km/h. In addition to these, Alternative 3 also takes into account railway line No. 150 (Budapest–Kelebia) with a line speed of 120 km/h (Figure 4).

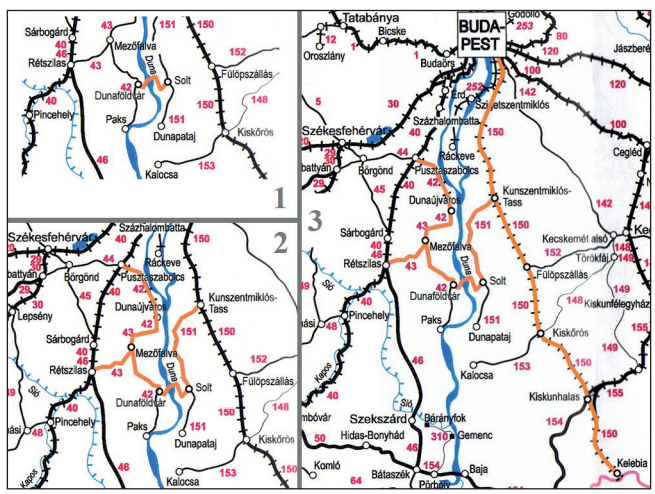


Figure 4: Alternatives 1, 2 and 3 of the Dunaföldvár–Solt bridge

Note: The railway lines to be developed are marked with orange.

Source: Compiled by the authors based on www.logsped.hu/vasutterkep.htm

Alternatives 4, 5 and 6

Alternatives 4, 5 and 6 assume that line No. 5 (Székesfehérvár–Komárom), 44 (Pusztaszabolcs–Székesfehérvár), 42, 150 and 152 (Fülöpszállás–Kecskemét) have a line speed of 120 km/h. This is considered to be sufficient to lead the traffic to the bridge that replaces the Southern railway bridge in case of its disruption. As currently lines No. 1, 80, 100 and 120, which are all radial lines connecting Budapest and the country border, are the most busy in the country, in case of the damage of the Southern bridge, which is their connection point, it is necessary to have transverse lines that lead to the bypass bridge that has about the same throughput.

The infrastructure to be built as a greenfield development is only the tracks from the southeastern end of Dunaföldvár station to line No. 150. The wyes both in the northern and the southern directions at Fülöpszállás are assumed to have the same 120 km/h line speed. The connection between lines No. 42 and 44, between Zichyújfalu and Adony over line No. 40 (Budapest–Pusztaszabolcs–Pécs) was also treated in the model with 120 km/h line speed (Figure 5).

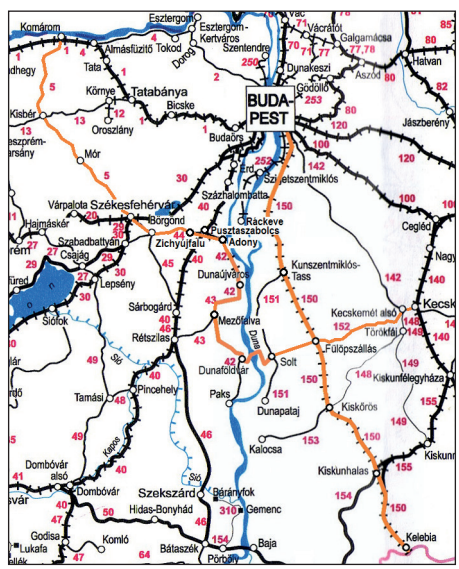


Figure 5: Alternatives 4, 5 and 6 of the Dunaföldvár–Solt bridge

Note: The railway lines to be developed are marked with orange.

Source: Compiled by authors based on www.logsped.hu/vasutterkep.htm

Alternative 4 (Figure 6) follows the original route of line No. 151a from Dunaföldvár station in the immediate vicinity of the currently existing bridge structure, then turns south and then turns back to reach Solt station from the south then it branches east from line No. 151 to approach line No. 150. Due to the narrow curves, the line speed is 80 km/h for the Dunaföldvár–Solt section.

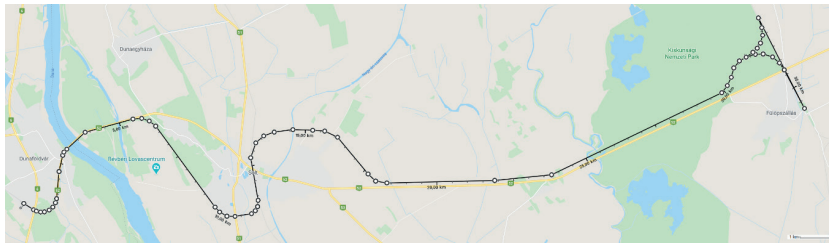


Figure 6: Alternative 4 of the Dunaföldvár–Solt bridge and planned railway line
Source: maps.google.hu

Alternative 5 (Figure 7) also crosses the Danube at the current bridge structure, but contrary to Alternative 4, it bypasses Solt from the north and then follows Road 52 on the same route as Alternative 4 until line No. 150. Due to the route, the crossing of line No. 151 can only be implemented as a separate level crossing, and Solt station can only be reached from the direction of Fülöpszállás, with a maximum speed of 80 km/h. There is a short curved section with 80 km/h line speed immediately after Dunaföldvár station, but the line speed is 120 km/h in the rest of the line.

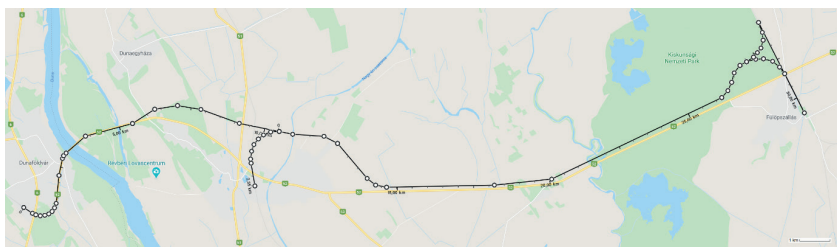


Figure 7: Alternative 5 of the Dunaföldvár–Solt bridge and planned railway line
Source: maps.google.hu

Alternative 6 (Figure 8) follows a completely different route: here, road and rail bridges would be spatially separated. As a result, the line speed may be 120 km/h along the totally new line No. 151a, as there is no need for narrow curves. The line bypasses Solt from the south and provides a connection from the direction of Fülöpszállás to the line No. 151, which curve, however, can only be built with a line speed of 60 km/h due to the built-in vicinity of the branching.

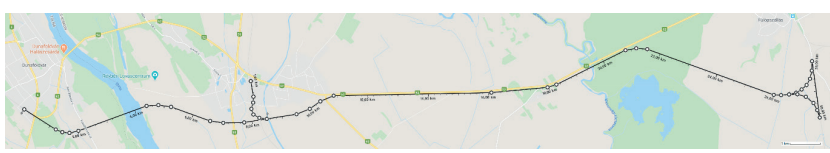


Figure 8: Alternative 6 of the Dunaföldvár–Solt bridge and planned railway line
Source: maps.google.hu

Dunaújváros–Szalkszentmárton

The Dunaújváros bridge would be built at the former crossing between the bridgeheads of the former TS floating bridge.[30] The newly built tracks branch off at Rácalmás from line No. 42 and run along the embankment to Szalki Island to the bridgehead of the TS floating bridge, with a curve of 60 km/h line speed. After the Szalkszentmárton bridgehead, it follows the existing embankment, but unlike the current line, it bypasses the village of Szalkszentmárton from the north (Figure 9).

Two alternatives were examined. In both, the new line sections and the existing lines No. 42, 44, 5 and 150 have a line speed of 120 km/h, and the separate level connection between Adony and Zichyújfalu was also taken into account. In Alternative 1, the Greater Burma line in Budapest is assumed to be rebuilt with 120 km/h line speed, and in Alternative 2, line No. 152 is assumed to be developed to 120 km/h line speed (Figure 8).

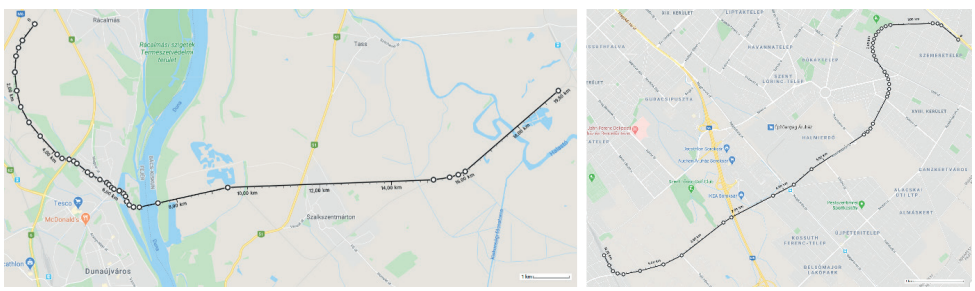


Figure 9: The Dunaföldvár–Solt bridge and planned railway line (left) and the Greater Burma railway (right)

Source: maps.google.hu

Paks–Kalocsa

The bridge between Paks and Kalocsa would be established as a completely new crossing between two railway lines on the two banks of the Danube. As the Paks Nuclear Power Plant regularly uses line No. 42, it is in relatively good condition. The route is the continuation of line No. 42 from Paks and it connects into the endpoint of line No. 153 (Kiskőrös–Kalocsa) at Kalocsa. More precisely, it runs on the path of the industrial tracks of Foktő.

The nuclear power plant should be bypassed from the west while maintaining an adequate safety distance, so the line runs along Highway No. 6. The crossing of the northern entrance of the nuclear power plant cannot be planned as a level crossing, so after the endpoint of Paks station, the lowering of the tracks must be started immediately so that the railway can be taken to a depth of 5 m during this 2–2.5 km long section, which means a 2–2.5‰ fall. Bypassing the nuclear power plant and the planned location of Paks II from the south, it crosses the Danube north of Foktő, then the line runs along the embankment

[30] Szászi 2013a: 101.

of the vegetable oil factory to Kalocsa station. This means a total of 18.9 km of new tracks (Figure 10).

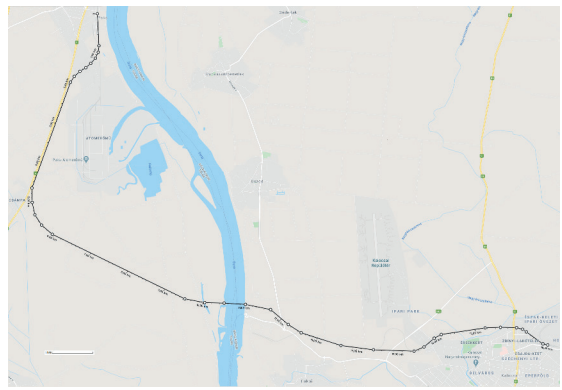


Figure 10: The Paks–Kalocsa bridge and planned railway line

Source: maps.google.hu

We examined two alternatives here, too. Both include the new track with a line speed of 120 km/h for lines No. 42, 44, 5, 150 and 153 and the Adony–Zichyújfalu connection, too.

In addition, in case of Alternative 1, the line speed of line No. 152 was assumed to be 120 km/h while in case of Alternative 2, a wye at the junction of lines No. 150 and 153 was inserted in the direction of Kiskunhalas to make line No. 155 (Kiskunahalas–Kiskunfélegyháza) accessible without a change in the direction.

Results

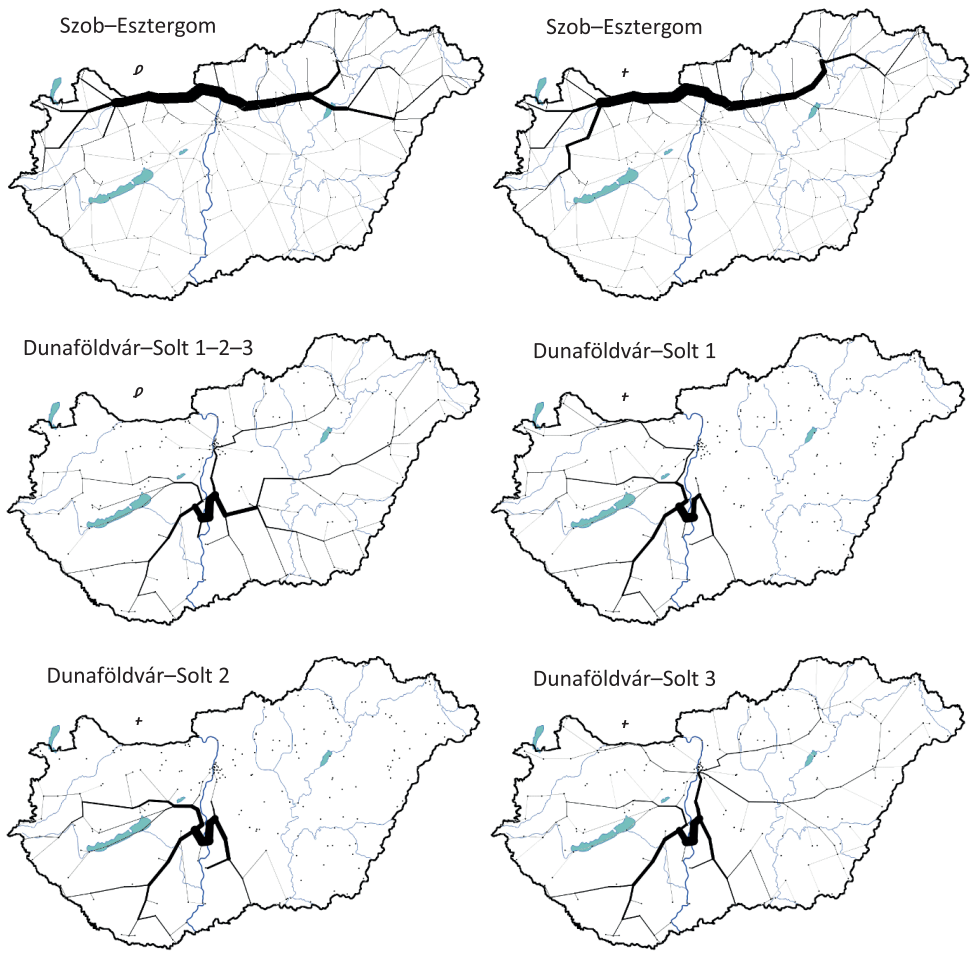
Determining the minimal distance and minimum travel time between all pairs of stations and selecting the ones that cross the new bridge we get the plot in Figure 11.

We can see that the Szob–Esztergom bridge (due to its location) only carries traffic between the northeastern and northwestern parts of the country, the paths that have their origin or destination more to the south still mostly use the Southern Railway Bridge for both minimum path length and minimal travel time.

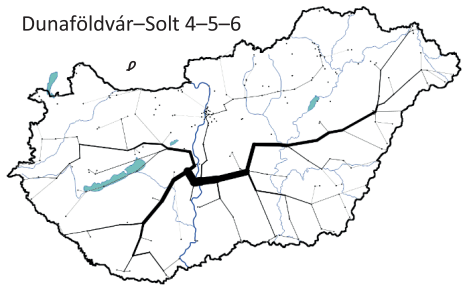
The Dunaföldvár–Solt bridge is extensively used by almost all paths that run on the main lines to cross the Danube. However, in case of Alternatives 1, 2 and 3, it appears that the traffic on line No. 150 is high in case of a minimum path length, while, in case of minimal travel times, due to the low line speed, they run on line No. 150 even when the line speed is not increased. This situation changes fundamentally for Alternatives 4, 5 and 6, as these routes become optimal even for minimal travel times. In this case, line No. 5 also connects significant directions, because then it is better to travel in this direction than through Kelenföld station where a change of direction is necessary. However, partly because of this, there are only a few routes from the northeastern part of the country as they use mostly the Southern bridge.

The Dunaújváros–Szalkszentmárton bridge is the one that essentially serves the whole country, as routes pass through it from all regions of Hungary. In case of the two alternatives, the geographical distribution of the paths are practically the same, except for the calculation taking into account the travel due to the effect of lines No. 152 and the Greater Burma line.

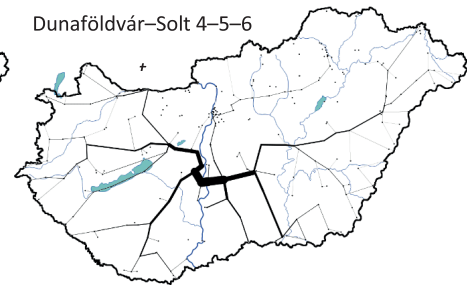
The Paks–Kalocsa bridge, being the southernmost crossing, is used by routes connecting the southern regions of the country. However, the calculations show that even some paths from Hegyeshalom and Záhony, the northwestern and northeastern "gates" of Hungary use it, which indicates that even this bridge can be a real alternative to the Southern Railway Bridge. The reason for this is the higher line speed of the connecting lines through which the new bridge can be reached quickly.



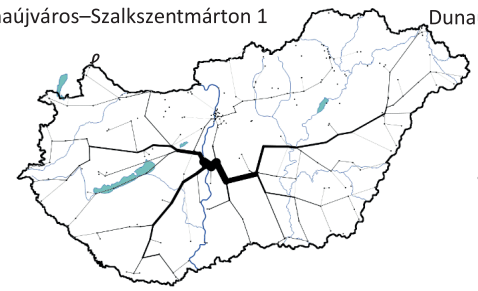
Dunaföldvár–Solt 4–5–6



Dunaföldvár–Solt 4–5–6

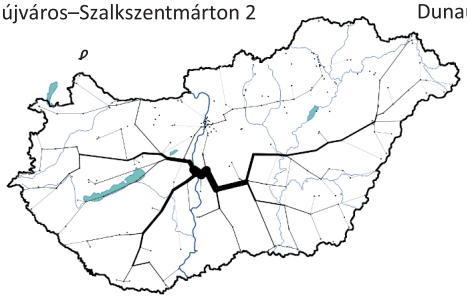


Dunaújváros–Szalkszentmárton 1

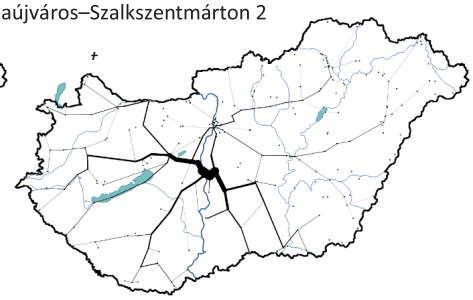


Dunaújváros–Szalkszentmárton 1

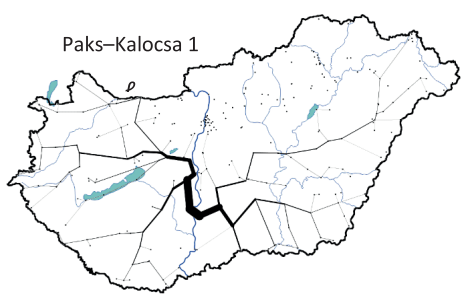
Dunaújváros–Szalkszentmárton 2



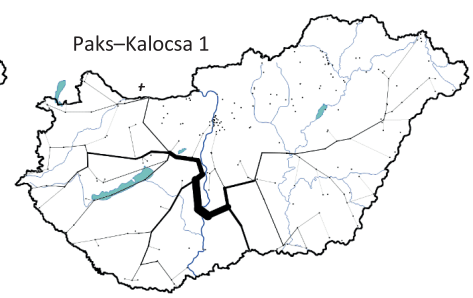
Dunaújváros–Szalkszentmárton 2



Paks–Kalocsa 1



Paks–Kalocsa 1



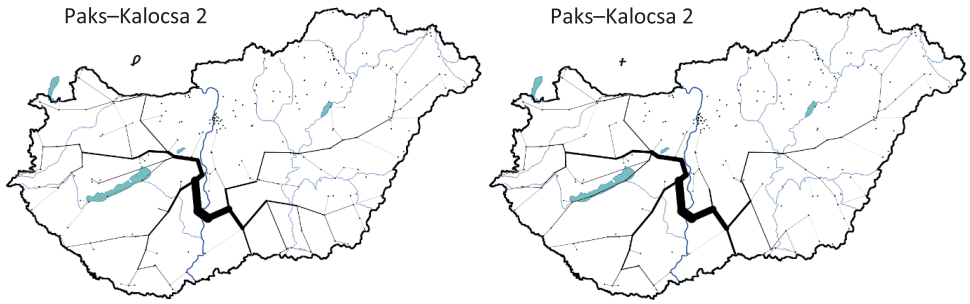


Figure 11: The geographical distribution of the paths passing through each new Danube bridge alternative for minimal path lengths (left column) and minimal travel times (right column)

Note: The thickness of the lines is proportional to the number of paths. The number of paths passing through the new bridge is taken to be 100%.

Source: Compiled by the authors.

However, examining the number of paths passing through the new bridge in each alternative the picture becomes different (Table 1): only 1.5% of all paths pass through the Paks–Kalocsa bridge in both alternatives, which is a very small ratio. It means that only those paths choose this crossing that connect the stations in the immediate vicinity of the bridge with the more remote regions of the country on the opposite bank of the Danube.

For Alternatives 4, 5 and 6 of the Dunaföldvár–Solt bridge and of the Dunaújváros–Szalkszentmárton bridge, 5.5% of all train paths pass through them in case of minimal travel times. What seems surprising at first is the case of Alternative 3 of the Dunaföldvár–Solt bridge, as its traffic is almost 8%. The reason for this is to be found in the increase in the line speeds of the connecting lines: as long as the line speed of lines No. 150, 44 and 5 are unchanged, the paths prefer to use the Dunaföldvár bridge to avoid the slow line No. 150 in approaching Budapest. But as soon as it is possible to travel faster on these lines, the Southern Railway Bridge becomes preferred again. In case of the Dunaújváros–Szalkszentmárton bridge, the connecting lines were already taken into account at a higher speed, which means that in terms of traffic, this bridge is essentially the same as the Dunaföldvár–Solt bridge, regardless of its more northern location.

At the same time, 8.5% of all paths pass through the Szob–Esztergom bridge. This means that though it provides faster and shorter connection only between the northern parts of the country, it could play a key role in rerouting the northwestern–northeastern traffic and could have the role that the Újpest railway bridge and the connecting lines lack as a northern bypass route.

The bridges of Dunaújváros–Szalkszentmárton and Dunaföldvár–Solt play a similarly significant role in rerouting the traffic of the Southern Railway Bridge. In case of Alternative 2 of the Dunaújváros–Szalkszentmárton bridge, in case of minimal travel times, the traffic of the Southern bridge at Budapest would decrease by 9% and by 19% in case of minimal path lengths. In cases of Alternatives 4–6 of the Dunaföldvár–Solt bridge, these numbers become 11 and 19%, respectively. This means that only half of the shortest

routes would be faster using this bridge than the Southern bridge in Budapest, i.e. the significant increase in the path length can only be partially compensated by the increase in the line speed.

The Szob–Esztergom bridge shows another behaviour: paths with minimal length cause a 7%, while paths with minimal travel time cause a 17% in the traffic of the Southern Railway Bridge. 60% of the paths that are faster via this bridge, are longer in kilometres, which means that the development of the connecting lines causes significant decrease in the travel times while similarly make the paths to bypass Budapest.

So far, however, the short and long, and slow and fast routes have been treated equally. But making short and slow routes faster is not as significant for the network as a whole, as it would be to achieve a reduction in travel times in all routes of a region connected only by slow paths. To measure this property, we calculate the decrease in the presence and absence of the new Danube bridge by summing the length or the travel time of all the shortest paths between all pairs of stations.

As the results show, both alternatives of the Dunaújváros–Szalkszentmárton bridge and Alternatives 4–6 of the Dunaföldvár–Solt bridge are outstanding: they cause a decrease of more than 0.8% in the total network path length and more than 0.6% decrease in the total network travel time. One of the reasons for this is the behaviour seen above: since many routes previously passing through Budapest cross these two bridges, the reduction in length and travel time caused by them is added together.

Alternative 2 of the Dunaföldvár–Solt bridge and the Szob–Esztergom bridge cause only a moderate decrease in the total network path length and the total network travel time, about 0.4%, despite the fact that the traffic of these bridges are roughly the same or even slightly higher than the previous ones. This means that the traffic-reducing effect does not necessarily lead to a significant reduction in journey times. Alternatives 1 and 3 of the Dunaföldvár–Solt bridge and both alternatives of the Paks–Kalocsa bridge result in only a minimal reduction about 0.2%, which is not surprising at all considering the traffic load of the bridges.

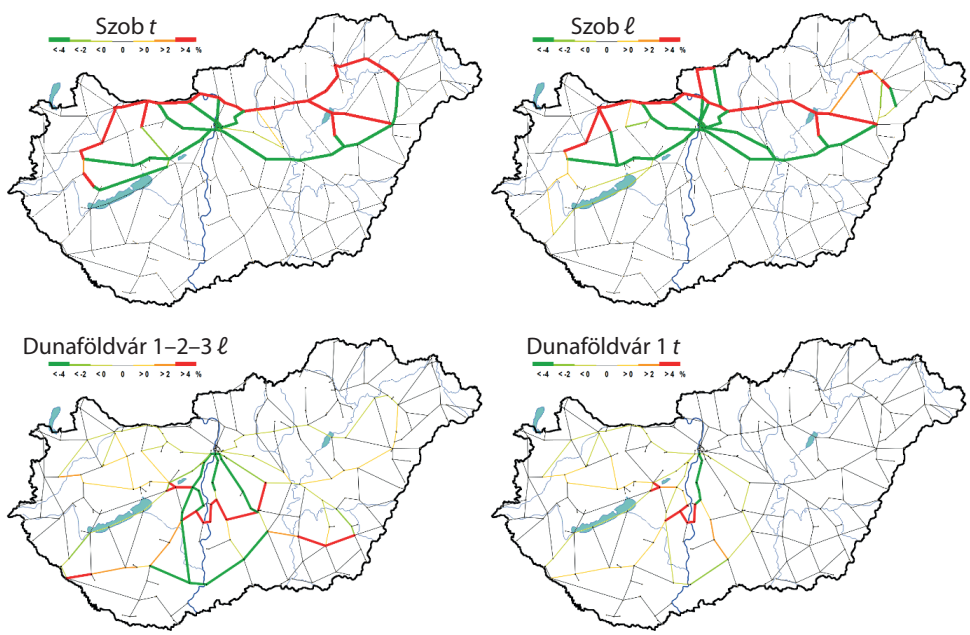
Table 1: The percentile change in the measures used to describe the alternatives

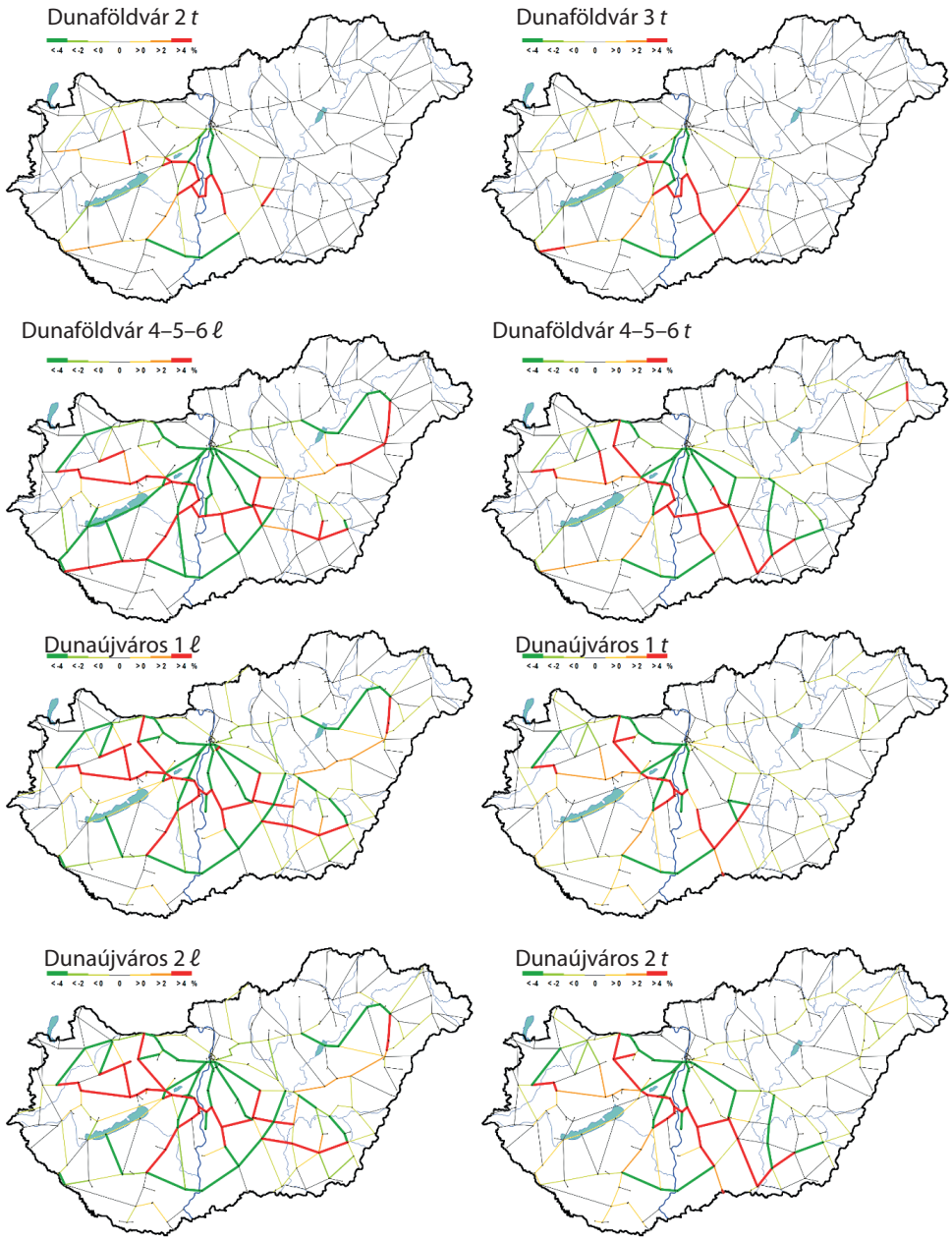
	Szob–Esztergom		Dunaföldvár–Solt									
	distance	time	distance				time					
Alternative			1–3	4	5	6	1	2	3	4	5	6
Decrease in the total network path length/travel time if the new bridge is implemented (%)	0.57	0.80	0.41	0.88	0.92	1.02	0.12	0.41	0.12	0.70	0.84	0.87
Decrease in the traffic of the most heavily loaded line section if the new bridge is implemented (%)	6.86	17.47	6.16	18.88	19.49	19.68	1.22	6.16	1.22	10.95	11.72	11.64

Alternative	Szob–Esztergom		Dunaföldvár–Solt									
	distance	time	distance				time					
			1–3	4	5	6	1	2	3	4	5	6
Ratio of paths passing through the new bridge (%)	8.52	8.47	7.92	7.80	8.02	8.75	7.46	7.92	7.46	5.19	5.53	5.52

Alternative	Dunaújváros–Szalkszentmárton				Paks–Kalocsa			
	distance		time		distance		time	
	1	2	1	2	1	2	1	2
Decrease in the total network path length/travel time if the new bridge is implemented (%)	1.01	1.01	0.65	0.73	0.28	0.28	0.29	0.31
Decrease in the traffic of the most heavily loaded line section if the new bridge is implemented (%)	19.29	19.15	6.58	9.00	3.28	3.29	3.14	3.14
Ratio of paths passing through the new bridge (%)	8.38	8.28	4.13	5.12	1.55	1.55	1.57	1.71

Source: Compiled by the authors.




Dunaföldvár 2 *t*
Dunaföldvár 3 *t*
Dunaföldvár 4–5–6 *ℓ*
Dunaföldvár 4–5–6 *t*
Dunaújváros 1 *ℓ*
Dunaújváros 1 *t*
Dunaújváros 2 *ℓ*
Dunaújváros 2 *t*

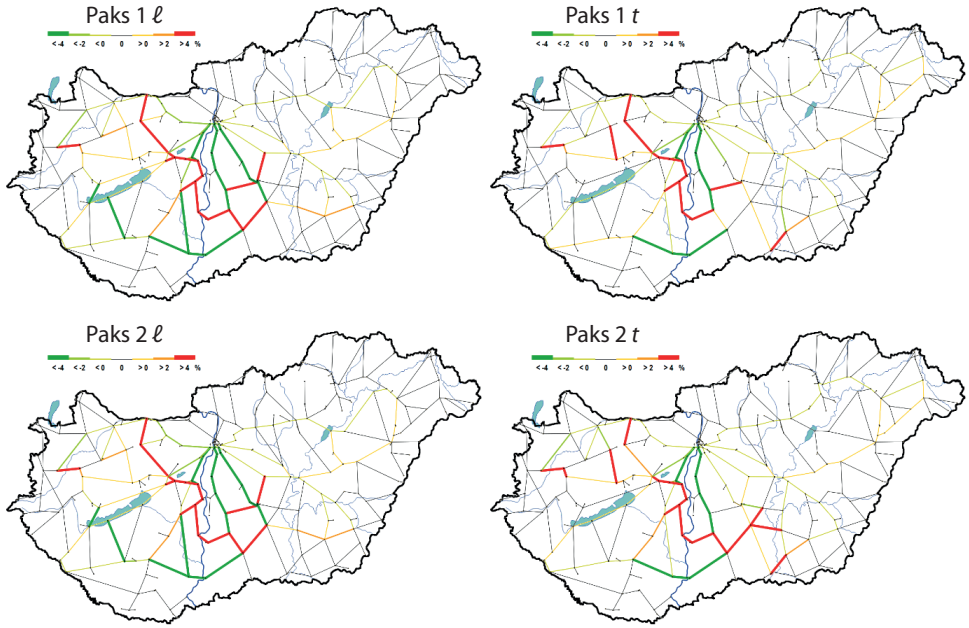


Figure 12: The change in traffic caused by each alternative of the new Danube bridge compared to the present situation

Source: Compiled by the authors.

Figure 12 illustrates the results of the study, the change in the traffic of each line section, and the rerouting effect on the traffic of each bridge. The Szob–Esztergom bridge "attracts" paths from lines No. 100 and 20 (Székesfehérvár–Szombathely) to lines No. 2, 4 and 80: it makes the paths to move north. However, while the impact of this bridge extends to remote regions, Alternatives 1–3 of the Dunaföldvár–Solt bridge make only the paths in the immediate vicinity of the bridge to reroute, the longer paths run on their current route. And this, as we have seen before, is not sufficient in any case to significantly reduce the total network travel time.

In contrast, Alternatives 4–6 of the Dunaföldvár–Solt bridge cause a significant reduction in traffic on the main lines leading to Budapest and also on the Baja bridge, mostly handling traffic between the southeastern and southwestern regions of Hungary. Thus, this bridge directs the routes to the central regions of the country: from line No. 1 to line No. 20, from line No. 80 to line No. 100.

Both alternatives of the Dunaújváros–Szalkszentmárton bridge have a similar effect, but due to the proximity to Budapest, it serves more as an alternative to northwestern–southeastern routes in bypassing the capital, and only slightly affects the traffic between the northeastern and southwestern regions of Hungary.

The two alternatives of the Paks–Kalocsa bridge only cause a local change in traffic. Due to the low traffic on the bridge, the decrease in the number of paths entering

the capital is only symbolic, its effect only noticeable up to Komárom and to line No. 140 (Cegléd–Szeged).

Summary

The heavy traffic of the railway lines running through Budapest is continuously increasing due to the large suburban passenger traffic and the east–west freight trains, which in some periods already made the network overloaded according to the standards[31] set by the UIC.[32] This is especially true for the Southern Railway Bridge, the only double-tracked and electrified bridge over the Danube in Hungary which is already operating at the limit of its capacity; therefore, it is necessary to somehow reduce its traffic.

In this paper, we examined 4 bridge locations and a total of 11 route alternatives using mathematical modelling to determine the optimal place for a bridge to be built. Basically, brownfield developments were taken into account, i.e. where there is already the railway infrastructure on both banks of the Danube. Therefore, its costs can be significantly smaller than in case of a completely new line with more than 100 km of new tracks to be built as a greenfield development. Based on the calculations, the best place for the bridge to be (re) built, but on a more favourable route is between Dunaújváros and Szalkszentmárton, the former site of the TS floating bridge. Between Dunaföldvár and Solt, where there has been a railway bridge until 2000, is also a very favourable location.

References

Berényi, János – Lévai, Zsolt (2020): CORCAP – a környezetbarát áruszállítási folyosók kialakítása útján. In Horváth, Balázs – Horváth, Gábor (eds.): *X. Nemzetközi Közlekedéstudományi Konferencia* [10th International Conference on Transport Sciences]. Győr: Széchenyi István Egyetem Közlekedési Tanszék – Közlekedéstudományi Egyesület.

Boda, József – Boldizsár, Gábor – Kovács, László – Orosz, Zoltán – Padányi, József – Resperger, István – Szenes, Zoltán (2016): A hadtudományi kutatási irányok, prioritások és témakörök. *Államtudományi Műhelytanulmányok*, 1(16), 2–23.

BRNS (2019): *Budapest Rail Node Study.* Online: http://bvs.hu/wp-content/uploads/2019/04/BRN_elsoszakcikk_v7.pdf

Csárdi, Gábor – Nepusz, Tamás (2006): The Igraph Software Package for Complex Network Research. *InterJournal, Complex Systems*, 1695(5), 1–9.

Dijkstra, Edsger W. (1959): A Note on Two Problems in Connexion with Graphs. *Numerische Mathematik*, 1(1), 269–271. Online: https://doi.org/10.1007/BF01386390

Haig, Zsolt (2016): Katonai műszaki tudományok a 21. században. *Hadtudomány*, 26(1–2), 115–116. Online: https://doi.org/10.17047/HADTUD.2016.26.1-2.115

[31] UIC Leaflet Nr. 406 Capacity. Paris, 2003.

[32] Union Internationale des Chemins de fer – International Union of Railways.

Horváth, Attila (2006): A közúti, vasúti és vízi közlekedés terrorfenyegetettségének jellemzői. In Tálas, Péter (ed.): *A politikai marketing fogságában.* Budapest: Mágustúdió. 321–336.

Jenelius, Erik – Petersen, Tom – Mattsson, Lars-Göran (2006): Importance and Exposure in Road Network Vulnerability Analysis. *Transportation Research Part A,* 40(7), 537–560. Online: https://doi.org/10.1016/j.tra.2005.11.003

Kristóf, János – Lévai, Zsolt (2002): Vágányzári forgalmi technológiák a gyakorlatban. *Forgalom,* 4(1), 3–6.

Lakatos, Péter – Szászi, Gábor – Taksás, Balázs (2016): A logisztikai infrastruktúra szerepe a regionális versenyképesség alakításában. In Csath, Magdolna (ed.): *Regionális versenyképességi tanulmányok.* Budapest: NKE. 181–288.

Lévai, Zsolt (2020): A vasúti alágazat jelenkori kapcsolódása a közlekedési támogatás rendszeréhez. *Katonai Logisztika,* 28(1–2), 198–223. Online: https://doi.org/10.30583/2020/1-2/198

R Core Team (s. a.): *R: A language and environment for statistical computing. R Foundation for Statistical Computing.* Online: www.R-project.org/

Szászi, Gábor (2007): Magyarország közlekedési infrastruktúrájának fejlesztése napjainkban: Közút vagy vasút? *Katonai Logisztika,* 15(2), 32–59.

Szászi, Gábor (2010): Katonai vasúti szállítások a Magyar Honvédség missziós feladatainak rendszerében. *Szolnoki Tudományos Közlemények,* 16, 101–118.

Szászi, Gábor (2013a): *A vasúti hálózati infrastruktúrával szemben támasztott újszerű védelmi követelmények kutatása, a továbbfejlesztés feltételrendszerének vizsgálata.* PhD thesis. Budapest: NKE. Online: https://doi.org/10.17625/NKE.2014.028

Szászi, Gábor (2013b): Long-span Railway Bridges in the Transport System of Hungary. *Hadmérnök,* 8(2), 98–107.

Szászi, Gábor (2014): Nagyfolyami vasúti hidak, mint közlekedési létfontosságú rendszerelemek. In Horváth, Attila – Bányász, Péter – Orbók, Ákos (eds.): *Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről.* Budapest: NKE. 25–48.

Tóth, Bence (2017): Állomások és állomásközök zavarának gráfelméleti alapú vizsgálata a magyarországi vasúthálózaton. *Hadmérnök,* 12(4), 52–66.

Tóth, Bence (2018): A magyarországi vasúthálózat zavarainak gráfelméleti alapú vizsgálata. In Horváth, Balázs – Horváth, Gábor – Gaál, Bertalan (eds.): *Közlekedéstudományi konferencia. Technika és technológia a fenntartható közlekedés szolgálatában.* Győr: Széchenyi István Egyetem Közlekedési Tanszék. 505–519.

Tóth, Bence (2021): The Effect of Attacks on the Railway Network of Hungary. *Central European Journal of Operations Research,* 29(2), 567–587. Online: https://doi.org/10.1007/s10100-020-00684-8

Tóth, Bence – Horváth, István (2019): How the Planned V0 Railway Line Would Increase the Resilience of the Railway Network of Hungary Against Attacks. *AARMS,* 18(3), 109–129. Online: https://doi.org/10.32565/aarms.2019.3.9

AARMS Vol. 22, No. 3 (2023) 43–62.

10.32565/aarms.2023.3.3

Quantitative Analysis of the Possible Sites of a New Danube Bridge to Bypass Budapest on Rail – Part 2[1]

Bence TÓTH,[2] Zsolt LÉVAI[3]

Since 1920, almost all the traffic on rail crossing the Danube in Hungary, crosses it in Budapest via the Southern Railway Bridge which makes it overloaded. This is a very disadvantageous situation not only for commercial shipping but also for military uses as there is certain heavy military equipment that can only be transported via rail.

In our two-part article, we examine the locations of new bridges that could be alternatives to bypass Budapest and thus to reduce the traffic load on the railway lines of the capital. In this second part, we examine the situation on the river Tisza by simulating the existence of several bridge alternatives, both newly built and developed existing ones. We also suggest a combined way of development to treat the capacity changes in the context of the whole network by building two new bridges, one on each river.

Keywords: *railway, bridge, graph theory, redundancy, military engineering*

Introduction

The railway network of Hungary has developed to be central to Budapest. The lines that currently form the core network were built at the second half of the 19th century and the function of the branch lines were to help to transport the goods to the stations at the main lines. Therefore, the main directions led from the big cities to the capital. As a result, the railway crossing over the Danube was not a priority at that time. An eclectic example: while nine railway bridges were built on the river Tisza, only five were built on the Danube.[4]

But as the need for transportation grew over the different regions of Hungary, an efficient way of transportation, which was at that times solely the trains, was missed more and

[1] This publication was prepared with the professional support of the Doctoral Student Scholarship Program of the Co-operative Doctoral Program of the Ministry of Innovation and Technology financed from the National Research, Development and Innovation Fund.

[2] Assistant Professor, University of Public Service, e-mail: toth.bence@uni-nke.hu

[3] PhD student, University of Public Service, Faculty of Military Science and Officer Training, Doctoral School of Military Engineering, e-mail: levai.zsolt@kti.hu

[4] Lévai 2020: 198–223.

more. To enable the fast transverse movement of trains without the need to enter Budapest, the then Minister for Transportation, Gábor Baross, led the construction of a railway ring through which the bigger cities could be circumnavigated. This ring line connected the cities (from northwest clockwise) Lučenec, Rožňava, Košice, Chop, Korolevo, Satu Mare, Oradea, Arad, Timişoara and Subotica. However, these cities are nowadays in Slovakia, Ukraine, Romania and Serbia due to the Treaty of Trianon of 1920 which, after losing World War I, cut these regions from the Kingdom of Hungary. Only three bridges over the Danube remained in the country, two at Budapest and one at Baja, 144 km south of the capital close to the southern border. On the river Tisza, there are seven bridges: at Tokaj-Rakamaz, Tiszafüred, Kisköre, Szolnok-Szajol, Tiszaug, Szentes-Csongrád and Algyő.

In Part 1 of our paper, we analysed where a new bridge on the Danube can be built. The main criteria for the locations were that existing branch lines or at least railway tracks be present on both banks of the Danube between which a bridge can be built, and that the bridge should not only be an effective bypass route for the Southern bridge but also an important element of the undisrupted network. The optimal solution was calculated for a bridge between Dunaújváros and Szalkszentmárton, where the former TS floating bridge has already existed.

But as traffic is expected to grow over the Danube, the capacity of the Tisza bridges have to be increased, too. We cannot ignore the traffic impact of the new Danube crossing on the railway crossing on the river Tisza, therefore, in this paper, we will discuss the possible solutions for a new Tisza bridge which would not only enable a higher traffic but could also play an important role in the defence preparations of the country.[5]

The existing bridges in the network

The increasing share of rail freight transport and the growing environmental consciousness of transport mode choice will increase the number of freight trains.[6] The Institute for Transport Sciences (KTI) has recently carried out several publications on the transformation of the rail freight market, which identify the rail sub-sector as one of the possible means of bringing Chinese goods to Europe.[7] This could have a significant impact on the already significant east–west rail traffic.

The railway infrastructure of Budapest has not changed since the 1950s, and the circular railway system established then is still in operation, with the major disadvantage that it does not offer the possibility of a round trip, so the two railway bridges over the Danube in the capital are not an alternative to each other.[8] All these reasons have led Budapest to become a bottleneck as the Southern Railway Bridge, which carries significant passenger and freight traffic, and is the only realistic alternative for east–west traffic, is operating at the limits of its capacity.[9] This bridge is double-tracked and electrified and a third track

5 Szászi 2010: 101–118.
6 Berényi–Lévai 2020.
7 Schváb–Lévai 2022: 172–183.
8 Szászi 2013b: 98–107.
9 Lévai 2020: 198–223.

is currently being built. The two other bridges, the Újpest bridge in the northern part of Budapest and the Türr István bridge at Baja have only a regional role. This is because only the Southern bridge is double-tracked and electrified. The Újpest bridge is singe-tracked, and though it is electrified, it lies on line No. 2 (Budapest–Esztergom) and it is connected to the core network via line No. 4 (Esztergom–Almásfüzitő), which is also a single-tracked line but not electrified. Therefore, the electric locomotives cannot be used to bypass Budapest through these lines.

The Baja bridge is a single-tracked road–rail bridge with no electrification. This suggests that neither the road nor the rail traffic is so heavy that a separate bridge is needed. Also, the loss of one bridge necessitates the use of a significant length of bypass.[10]

The bridge at Komárom connects the Hungarian and Slovakian railway network and has neither a domestic role nor can play a part in the defence preparations of the country.

The state of the Tisza bridges is similar. From the seven bridges, only two, the Tokaj–Rakamaz and the Szolnok–Szajol bridges are electrified and only the Szolnok–Szajol bridge is double-tracked. The Tokaj–Rakamaz bridge would make an efficient bypass route was it double-tracked[11] as it is the connection between lines No. 100 (Budapest–Cegléd–Szolnok–Debrecen–Nyíregyháza) and 80 (Budapest–Hatvan–Miskolc–Nyíregyháza).

The Szolnok–Szajol bridge is at a good location, i.e. the middle of the country and is in good condition. It was reconstructed in 2015, the common structure of the two tracks was changed for two single-tracked truss structures and the *Überleitstelle* Millér was installed to increase the capacity of the line section. However, in case of the (temporal) loss of this bridge, no real alternative is available to handle the traffic.[12] Therefore, a solution has to be found.

Building a second track for the Tokaj–Rakamaz bridge would be important. However, as three of the four Danube bridge alternatives presented in the first part of this paper is to the south of the Szolnok–Szajol bridge, both the shortest and the fastest paths would pass through the river Tisza at Szolnok.[13] This suggests that a bridge over the river Tisza should be built in the southern region of the country.

Bridge alternatives

Szeged

Until 1944, a bridge existed between Szeged and Újszeged. This was part of the Budapest–Arad–Timișoara line and was part of the line leading to Subotica. Line No. 140 approached Szeged from the north and after Szeged-Rendező station it took a leftward curve to the main station of the city. Here, the tracks were already elevated and arrived at the second floor of the station building as it was the beginning of the bridge: after the station, the

[10] Kerényi–Tóth 2020: 79–99.
[11] Tóth 2019: 74–86.
[12] Szászi 2007: 32–59.
[13] Szászi 2014: 25–48.

tracks turned right with a 90-degree curve on the bridge at the end of which was the station Újszeged.

Nowadays, both Szeged and Újszeged are head stations and handle a minimal freight traffic. Also, it is impossible to rebuild the bridge on the same route, as there are buildings in the path, only a new line in a tunnel would be possible. However, there were already plans in the 1930s to substitute the steep curve in the downtown. This meant that the line would continue straight after Szeged-Rendező station and cross the Tisza south of the city. This would have meant that the downtown station was to be used only by the passengers and the freight trains would bypass the city on the southern route and connect to the line on the other bank at Szőreg station. This plan was revived in 2006 when a plan was made by the Department of Highway and Railway Engineering of the Budapest University of Technology and Economics.[14]

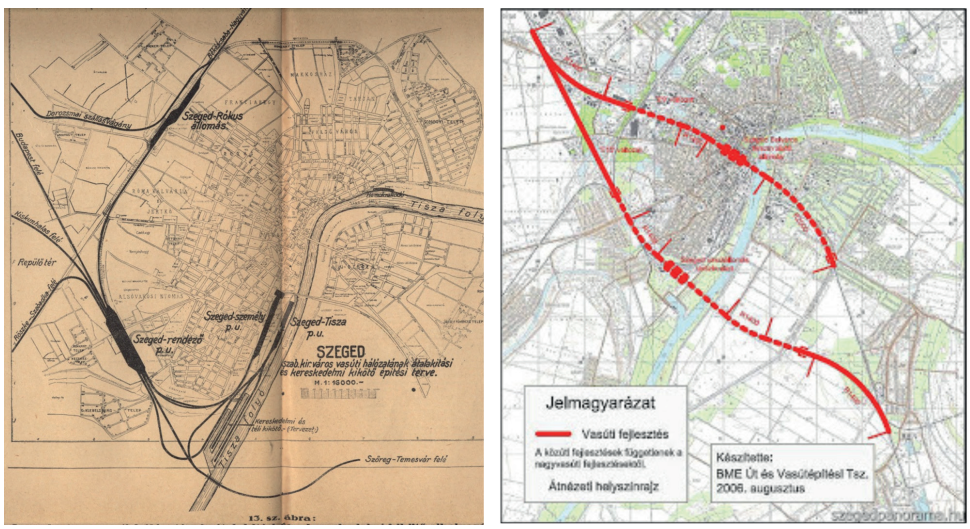


Figure 1: The southern alternative of the Szeged bridge

Source: https://szegedpanorama.blogspot.com/2013/07/a-transzbalkani-vasut-hajdanvolt.html

[14] *A Szeged–Szőreg vasútvonal fejlesztésének megvalósíthatósági tanulmányterve* 2006.

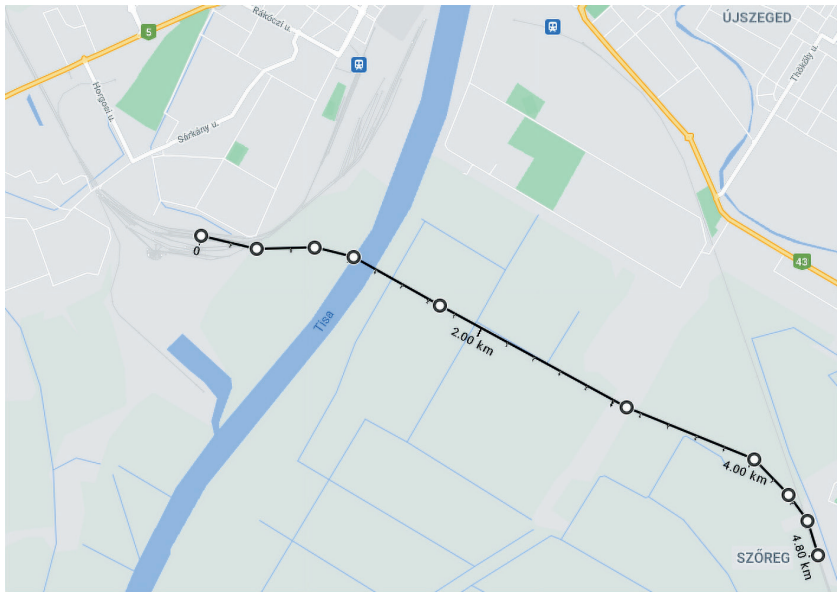


Figure 2: The Szeged-Rendező–Szőreg bridge and planned railway line

Source: maps.google.hu

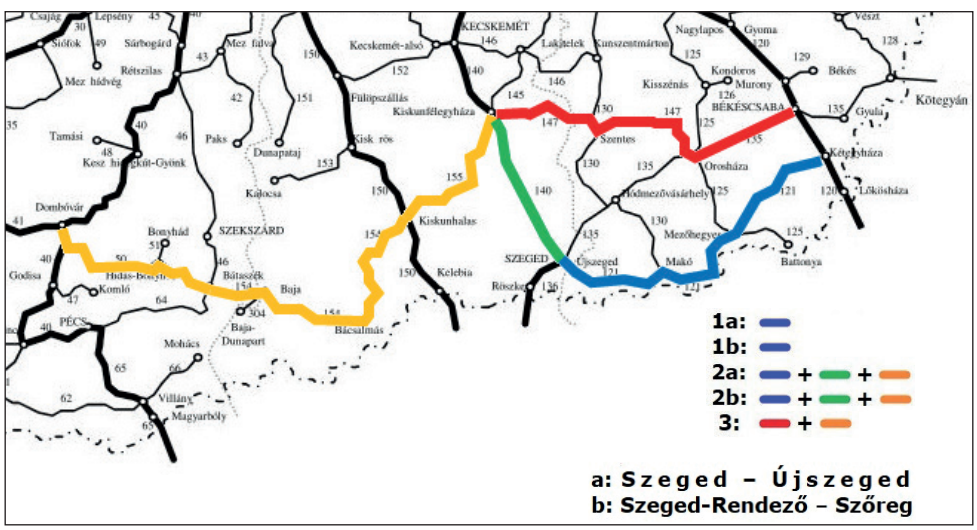


Figure 3: The five alternatives of the new Tisza bridge and the railway lines to be developed

Source: Compiled by the authors based on www.logsped.hu/vasutterkep.htm

Here, we analyse five route alternatives. In the 1a and 1b alternatives, line No. 121 (Újszeged–Makó–Kétegyháza) was assumed to have a line speed of 120 km/h, instead of the current

30 km/h. The difference between them is the location of the bridge. In Alternative 1a, the former Szeged–Újszeged bridge was assumed with 60 km/h line speed between Szeged and Újszeged stations. In Alternative 1b, the Szeged-Rendező–Szőreg bridge was assumed with 120 km/h line speed on the whole line (see Figure 3, blue line).

In Alternatives 2a and 2b, the line speed of lines No. 140 between Kiskunfélegyháza and Szeged and lines No. 50 (Dombóvár–Baja), 154 (Baja–Kiskunhalas) and 155 (Kiskunhalas–Kiskunfélegyháza) was assumed to be 120 km/h. Additionally, a wye at Kiskunfélegyháza and Kétegyháza was added in order to make the direct connection available between lines No. 155–140 and 121–120, respectively. The distinction between Alternatives a and b was the same as previously: the downtown and the southern route (see Figure 3, blue, green and orange lines).

However, Szeged is very close to the border of the country and there is a 3.5 km section of line No. 121 where it runs parallel with the Hungarian–Romanian border in only 50 m distance. This situation makes it a vulnerable line and one should look for another possible alternative that is deeper inside the country.[15]

Szentes–Csongrád

Therefore, an existing bridge was chosen to analyse the effect of its development: in Alternative 3, the Szentes–Csongrád bridge and the line it lies on, line No. 147 (Kiskunfélegyháza–Szentes–Orosháza) and the Orosháza–Békéscsaba section of line No. 135, which connects it to the core network was assumed to be developed to 120 km/h line speed. A wye at Kiskunfélegyháza and Békéscsaba was planned to make lines No. 155 and 147 and lines No. 135 and 120 accessible for each other without a need for a change in the direction (see Figure 3, red and orange lines).

The graph model of the railway network of Hungary

The graph model used for our calculations has been presented in detail in a previous paper,[16] thus we will only discuss it here briefly.

A weighted directed graph was used to model the railway network of Hungary. The nodes of the graph represented the stations where a change in the direction is possible, i.e. not the middle stations of a railway line.[17] Stops with no switches were not included in the model either. As our goal was to analyse the effect of the developments on the defence preparations of Hungary, the sidings of the Hungarian Army were also included in the model.[18]

---

15 Horváth 2006: 321–336.

16 Tóth 2021: 567–587.

17 Jenelius et al. 2006: 537–560.

18 Government Decree 277/2014 (XI.14.) on the Amount of Fine the Railway Authority Can Issue and Detailed Rules of Its Payment, 2nd Appendix.

The edges of the graph represented the line sections between these stations. Two weights could be assigned to each edge: the length of the corresponding line section or the ratio of the length of the line sections and the line speed, the so-called pure travel time, which gives the lowest limit a path could be run within, as it does not take into account any speed limit or acceleration/deceleration time. If the value of the line speed was lower for trains with locomotives than for ECMs, then the former, the lower value was used.

For locomotive reversal and direction change, 15 extra minutes were to be added. Therefore, the graph describing the network had to be expanded in order for the algorithm calculating the shortest path to add the extra time of direction changes when needed. No extra trip length or travel time was assigned to passing a station and no extra distance was assigned to reversing.[19]

The data used is publicly available on the website of the Hungarian Rail Capacity Allocation Office (Vasúti Pályakapacitás-elosztó Kft.).[20] With these data, the length and the duration of every path can be calculated and the shortest and the fastest path between any pair of station can be determined.

The calculations and the visualisation of the results were performed in the R programming language and environment[21] using the *igraph* package[22] developed by Gábor Csárdi and Tamás Nepusz. The graph describing the network is encoded as a two-column matrix, a so-called edge list.[23] Each line describes a line section, the first number being the index of the origin and the second the number of the destination station of the line section. For each edge, a weight can also be assigned, using a vector with a dimension equal to the number of edges, which in our case was either the distance between the nodes representing neighbouring stations or the corresponding travel time. The shortest distance (in distance or time) between any two stations can be determined by the *distance()* function of the *igraph* package, which uses Dijkstra's algorithm[24] in graphs with positive weights (such as the one we use) by default. The function *shortest_paths()* can be used to determine which edges and nodes fall on the shortest path.

Results

The distribution of the paths for Alternatives 1a, 1b, 2a and 2b are visually the same (see Figure 4 left). One end of the paths is distributed almost in the entire country but the other end is located in the southeastern part of Hungary. This means that these bridges serve only this small region which is otherwise not too important. Some paths even cross the Szolnok–Szajol bridge, too and thus do not make its traffic decrease but increase.

---

19 Tóth 2018: 505–519.
20 See www.vpe.hu/takt/vonal_lista.php
21 R Core Team s. a.
22 Csárdi–Nepusz 2006: 1–9.
23 Tóth 2017: 52–66.
24 Dijkstra 1959: 269–271.

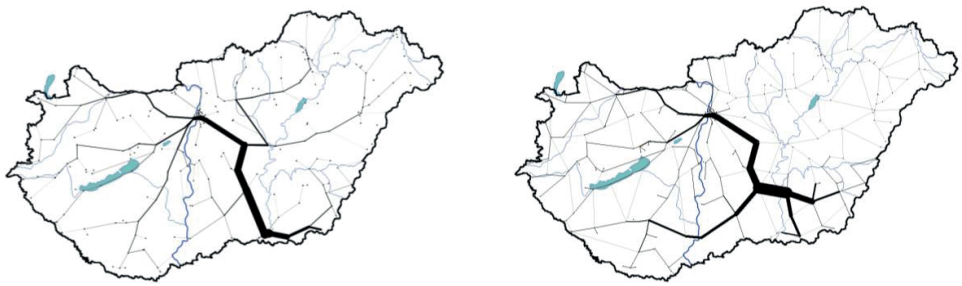


Figure 4: The geographical distribution of the paths passing through the Szeged bridge (left) and the Szentes–Csongrád bridge (right)

Note: The thickness of the lines is proportional to the number of paths. The number of paths passing through the new bridge is taken to be 100%.

Source: Compiled by the authors.

On the contrary, Alternative 3 is used by paths from smaller regions like the northwestern and the southwestern parts of the country and paths that also pass through core lines (see Figure 4 right). The other end of the paths occupy a larger portion of the southeastern region of the country and it is obvious from the figure that it could be used as an alternative for line No. 120 in approaching this region. These paths do not cross the Tisza via other bridge(s) and therefore it could be a real alternative for the Szolnok–Szajol bridge even in the undisrupted network.

Table 1: The percentile change in the measures used to describe the alternatives

	Distance					**Time**				
Alternative	**1a**	**1b**	**2a**	**2b**	**3**	**1a**	**1b**	**2a**	**2b**	**3**
Decrease in the total network path length/travel time if the new bridge is implemented (%)	0.18	0.32	0.16	0.30	0.33	0.50	0.34	1.2	1.1	0.57
Decrease in the traffic of the most heavily loaded line section if the new bridge is implemented (%)	0.70	1.3	0.59	1.2	1.5	0.59	1.2	0.48	1.0	1.4
Ratio of paths passing through the new bridge (%)	1.9	2.7	2.2	2.7	3.5	1.7	2.4	2.0	2.6	3.1

Source: Compiled by the authors.

In Table 1, the percentile values of the decrease in the total network path length/total network travel time if the new bridge is implemented, the decrease in the traffic of the most heavily loaded line section if the new bridge is implemented and the ratio of paths passing through the new bridge are shown. Overall, the values are quite disappointing. The decrease in the total network trip length and the total network travel time is very low, only in two cases higher than 1%. This means that neither of them has such a good overall effect on the total network to be worth building it.

Neither causes the new bridge a decrease in the traffic of the line section with the heaviest traffic, which is the Ferencváros–Kelenföld line section with the Southern Railway Bridge.

In the view of the traffic passing through the new bridge, Alternative 3 is the best solution. This is due to its more central location, i.e. the paths do not have to travel down to Szeged which decreases both the path length and the travel time. The alternatives with the city bridge are in every case worse than the alternatives, which include the path that bypasses Szeged to the south. In addition, the alternatives which assume the Baja bridge and its connecting lines to have a higher line speed are better than the ones that do not. However, it is obvious from these measures that neither of these alternatives causes alone a significant improvement of the network.

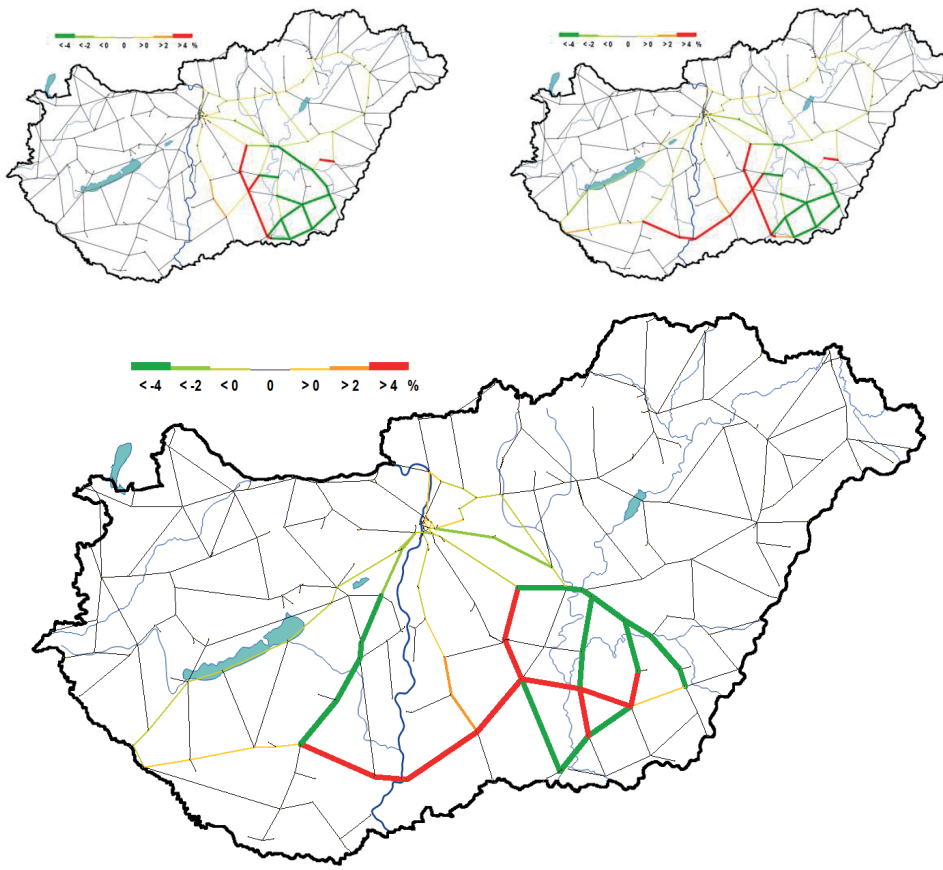


Figure 5: The change in traffic caused by each alternative of the Szeged bridge for minimal path length (top left) and for minimal travel times (top right) and for the Szentes–Csongrád bridge (bottom) compared to the present situation

Source: Compiled by the authors.

As it is seen from Figure 5 (in accordance with Figure 4) that the Alternatives 1a, 1b, 2a and 2b do not cause a decrease in the traffic of Budapest but as the traffic on lines No. 80 and No. 100 is slightly increased, so do the lines inside the capital. Thus, due to the way the paths redistribute in the country in the presence of this bridge the traffic passing through Budapest becomes higher.

The bridge according to Alternative 3, however, causes the traffic of the main lines leading to Budapest to decrease, for some even with a ratio greater than 4%. This should clearly have a positive effect on the traffic load of the capital because fewer paths have to pass through it using its railway infrastructure. As it can be seen in Figure 5, the redistribution makes the traffic on the Baja bridge increase significantly, which was the goal of its assumed reconstruction. As the traffic of core line No. 120 is decreased.

Redundancy

If a shortest path passes through line section *v* in the undisrupted network, on the disruption of line section *u* there are three scenarios, two of which are irrelevant for us. First, if the shortest path passes through line section *v* in the disrupted network, too, then the disruption has no effect on *v* as it is still useable. Second, if the disrupted line section, *v*, makes at least one pair of stations unreachable for each other, then there is no possible alternative path (see Figure 2). Therefore, these two scenarios are left out of the calculations.

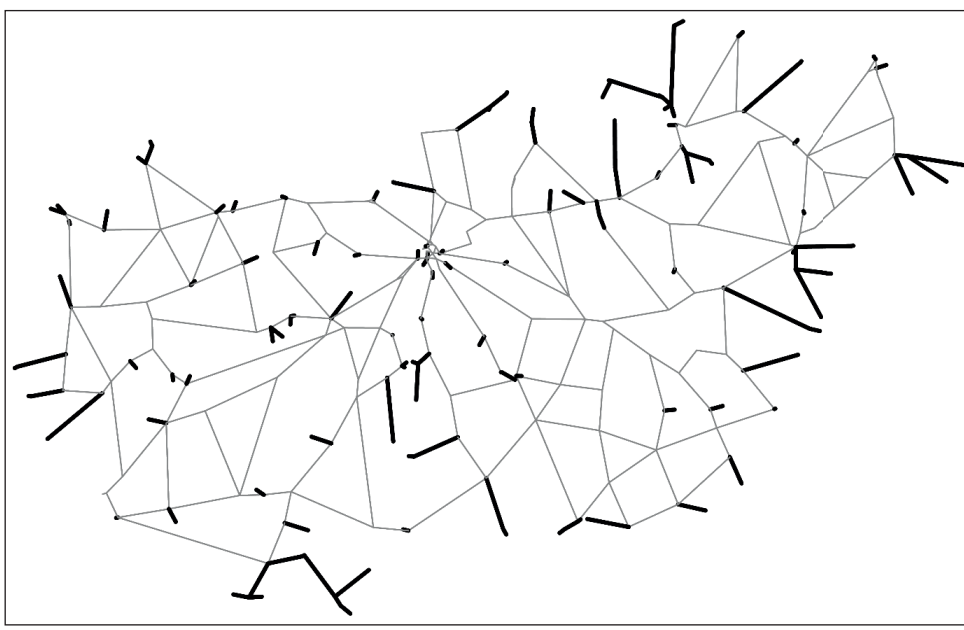


Figure 6: Line sections the disruption of which make stations unreachable for others
Source: Tóth 2020: 358–367.

The Network Robustness Index

The Network Robustness Index (NRI) was introduced by Scott et al.[25] as a global measure to quantitatively describe the overall resilience of a network against disruptions. The NRI can be calculated for all edges of the graph based on which the importance of the individual line sections can be determined.

To calculate the NRI for line section *v,* the shortest paths between all pairs of stations in the undisrupted graph have to be determined. Then, the lengths or durations of these paths have to be summed, the value of which is denoted by *c.*

Then, the edges representing line section *v* are deleted from the graph. Again, the shortest paths between all pairs of stations are determined and their lengths or durations are summed. This value is denoted by c^v. The NRI is calculated as the difference of these two values and is denoted by q^v*:*

$$q^v = c^v - c \tag{1}$$

The difference is made in this order for q^v to be non-negative since for most kinds of weights the deletion of a line section increases the sum of the weights of the shortest paths (or at least does not decreases it, but for a famous exception that occurs in flow models, the Braess paradox[26]). This can be done for all line sections or for multiple line sections. If line sections *v* and *u* are simultaneously deleted, the NRI is calculated as

$$q^{uv} = c^{uv} - c \tag{2}$$

The value of q_{ab}^v (the difference in the shortest path between stations *a* and *b* in the disrupted and in the undisrupted network) shows if the shortest path in the undisrupted network passes through line section *v.* If $q_{ab}^v = 0$, then line section *v* is not part of the shortest path between stations *a* and *b* neither in the undisrupted network nor in the network without line section *v.* If $q_{ab}^v > 0$, then by deleting line section *v,* the length or duration of the shortest path between station *a* and *b* increases compared to the shortest path in undisrupted network. This means that line section *v* was part of the shortest path in the undisrupted network but there is still a non-infinite route between stations *a* and *b* in the disrupted network.

The redundancy index

The Network Robustness Index measures the increase in the total network trip length or the total network travel time in case of the deletion of a line section. But on the disruption of line section *v,* the exact route of the shortest path between stations *a* and *b* changes compared to the shortest path in the undisrupted network.

Let us assume that the shortest path between stations *a* and *b* in the undisrupted network did not pass through line section *u* but in the network without line section *v* it does. How

[25] Scott et al. 2006: 215–227.
[26] Braess 1968: 258–268; Braess et al. 2005: 446–450.

much would be the additional increment in the shortest path if *u* would be deleted, too? This increase is the redundancy provided by line section *u* to line section *v.* Paths that pass through line section *u* neither in the undisrupted nor in network without line section *v,* or pass through it in both are not relevant, since they are not sensitive for the disruption of line section *v.*

The r^{uv} redundancy index is defined by the sum of the increase of the shortest paths in the network without line section *v* and *u* compared to the sum of the shortest paths in the network without *v:*

$$r^{uv} = q^{uv} - q^{v} = (c^{uv} - c) - (c^{v} - c) = c^{uv} - c^{v} \tag{3}$$

By calculating r^{uv} for all *u* line sections that are only in the shortest paths between stations *a* and *b* in the network without line section *v* but are not in the shortest path in the undisrupted network and summing them up one gets the total redundancy that line section *u* provides to the network:

$$r^{u} = \Sigma_{v} r^{uvv} = \Sigma_{v}(q^{uv} - q^{v}) = \Sigma_{v}(c^{uv} - c^{v}) \tag{3}$$

This definition was introduced by Erik Jenelius.[27]

Application on 1-edge-connected graphs

It can be seen from the definition, that if such line sections are deleted from the graph that make at least one station unreachable from the others, the value of both q^{v} and r^{u} becomes infinity. The railway network of Hungary has this property, which means that the graph describing it is a so-called 1-edge-connected graph.

In several cases, by deleting only one line section from the network, the graph will remain connected. However, if two line sections are deleted, the number of reasonable results will rapidly decrease. If all these line sections were excluded from the calculations, only a few would remain and if only those line sections were excluded which give infinity as a result in that particular calculation, then different line section would be taken into account for each *v* line section, which would make the obtained r^{u} values incomparable to each other.

Therefore, it is practical to use the reciprocals of the travel time and trip length values of the shortest paths. By changing the order in which the difference is calculated in the summation of Equation (2), the redundancy index remains positive since longer distances mean shorter values in the reciprocal space.

By summing the values of the redundancy indices calculated in the reciprocal space for all *v* line sections one gets the total redundancy of a line section *u:*

$$\sum_{v} r_{\ell}^{uv\prime} = \sum_{v}(c_{\ell}^{v\prime} - c_{\ell}^{uv\prime}) = \sum_{v}\left(\sum_{\langle a,b\rangle}\frac{1}{\ell_{ab}^{v}} - \sum_{\langle a,b\rangle}\frac{1}{\ell_{ab}^{uv}}\right) \tag{5}$$

[27] Jenelius 2010: 129–137.

$$\sum_v r_t^{uv\prime} = \sum_v (c_t^{v\prime} - c_t^{uv\prime}) = \sum_v \left(\sum_{\langle a,b \rangle} \frac{1}{t_{ab}^{v}} - \sum_{\langle a,b \rangle} \frac{1}{t_{ab}^{uv}} \right) \tag{6}$$

However, it is more informative to normalise these values with values of the total trip length or the total travel time of the undisrupted network (which value is denoted by c_ℓ' and c_t', respectively):

$$r_\ell^{u\prime} = \frac{\sum_v r_\ell^{uv\prime}}{c_\ell'} = \frac{\sum_v (c_\ell^{v\prime} - c_\ell^{uv\prime})}{c_\ell'} = \frac{\sum_v \left(\sum_{\langle a,b \rangle} \frac{1}{\ell_{ab}^{v}} - \sum_{\langle a,b \rangle} \frac{1}{\ell_{ab}^{uv}} \right)}{\sum_{\langle a,b \rangle} \frac{1}{\ell_{ab}^{0}}} \tag{7}$$

$$r_t^{u\prime} = \frac{\sum_v r_t^{uv\prime}}{c_t'} = \frac{\sum_v (c_t^{v\prime} - c_t^{uv\prime})}{c_t'} = \frac{\sum_v \left(\sum_{\langle a,b \rangle} \frac{1}{t_{ab}^{v}} - \sum_{\langle a,b \rangle} \frac{1}{t_{ab}^{uv}} \right)}{\sum_{\langle a,b \rangle} \frac{1}{t_{ab}^{0}}} \tag{8}$$

The $r^{u\prime}$ redundancy index is the total relative decrease in the reciprocal trip length or travel time for those shortest paths that do not pass through the line section *u* in the undisrupted network but pass through it in case of the disruption of line section *v* with line section *u* fixed for the calculation.

Results – Danube

The redundancy value of the three existing Danube bridge and the modelled fourth one was calculated for each alternative. The results can be seen in Figure 7. In general, the redundancy of the bridges become more even than it is currently. This is a good indication that a new bridge would make a good replacement of any of the others.

The highest redundancy value is the one of the Dunaújváros–Szalkszentmárton bridge, the site where the TS floating bridge has once been.[28] Thus, from these results (and also combined with the traffic values presented in Part 1 of this study) this site is the optimal one to build a new bridge on the Danube.

[28] Szászi 2013a: 101.

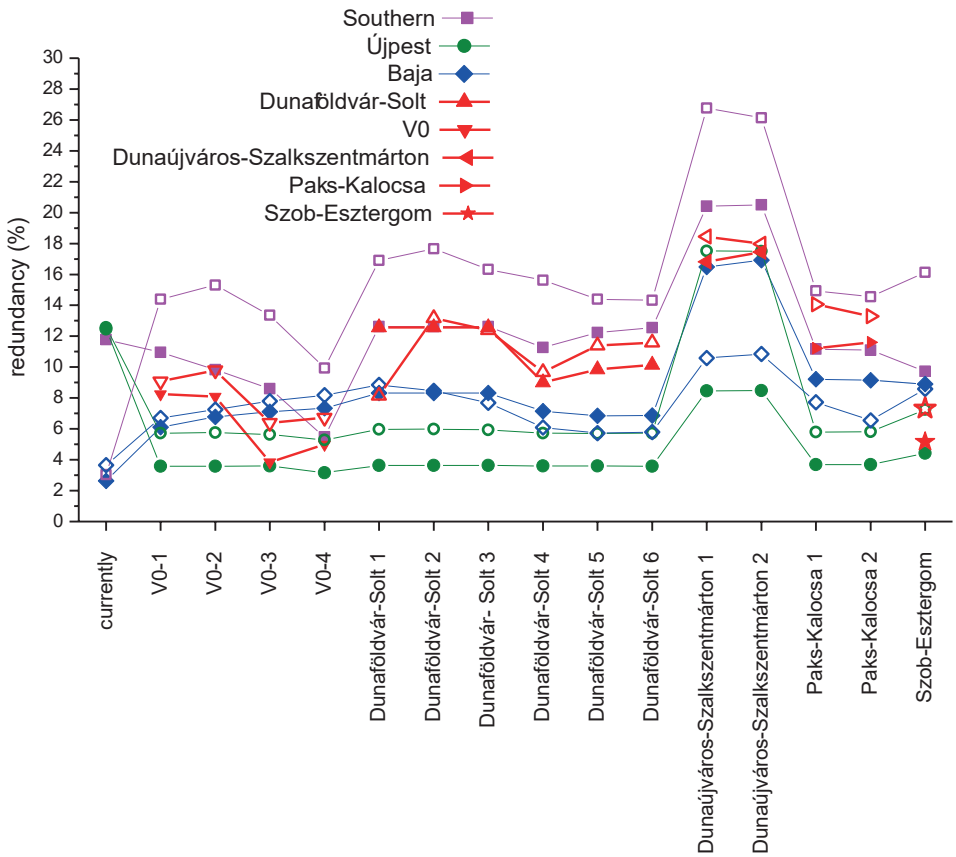


Figure 7: The redundancy values of every Danube bridge in case of each alternative for the new bridge

Source: Compiled by the authors.

Results – Tisza

The redundancy value of the existing Tisza and Danube bridges and the modelled new Tisza bridge was calculated for each of the five alternatives. The results can be seen in Figure 7 (if the bridge at Szeged is assumed, the redundancy of the Szentes–Csongrád bridge is not plotted).

The results show that no matter which alternative is chosen, the redundancy of the new Tisza bridge is the same. This means that the increase in both path length and travel time is the same if the new bridge is disrupted and its bypass route is through the Szolnok–Szajol bridge.

The redundancy values of the Danube bridges alter in the presence of a new Tisza bridge only a little, which is due to the slight redistribution of the paths to the Baja bridge

as the new Tisza bridge is in the geographical latitude range between Budapest and Baja. The values become more evenly distributed, so the new Tisza bridge is also efficient in balancing the roles of the existing Danube bridges.

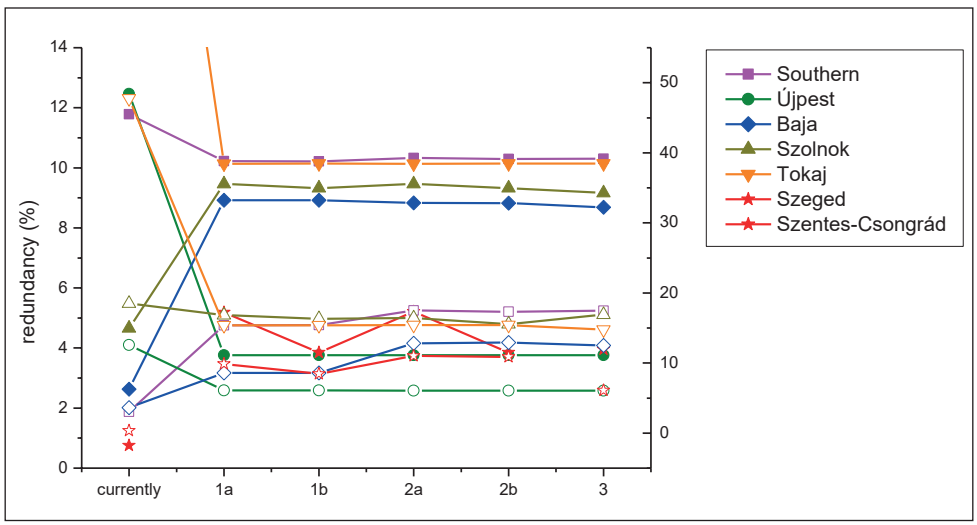


Figure 8: The redundancy values of the existing Danube bridges, the two main Tisza bridge and the new Tisza bridge in case of each alternative for the new bridge

Source: Compiled by the authors.

The redundancy values of the existing Tisza bridges change drastically (Figure 8.). As the three are distributed evenly along the river and due to its geographical position the Szolnok–Szajol bridge remains the most important one, both of them is a similar replacement for it. These results indicate that no matter which of the five modelled alternatives is built, not only the substitution of Tisza bridges become possible on more reasonable routes in case of a disruption but also the traffic on the Danube bridges becomes more evenly distributed.

One new bridge on both rivers

As we have seen here and in Part 1 of the study, the Dunaújváros–Szalkszentmárton and the Dunaföldvár–Solt bridges can be an effective new crossing over the Danube. But as we have emphasised there, without a new bridge over the Tisza, the increase in the traffic through the Danube and through the country the new bridge could handle, could not pass through the existing Tisza bridges. This problem would not have been solved by the planned V0 railway either as it would lead until Szolnok, at maximum.[29]

As it was seen, the best alternative for a new Tisza bridge is to develop the Szentes–Csongrád bridge and the lines connecting it to the core network to have a second track and

[29] Tóth–Horváth 2019: 109–129.

a line speed of 120 km/h, i.e. Alternative 3 but without a reconstructed Baja bridge. This bridge also has the advantage of being more centrally located in the country than a bridge at Szeged which is important in its military applications.

Therefore, we adjusted our graph to include Alternative 3 and either of the two Dunaújváros–Szalkszentmárton and Alternatives 4, 5 and 6 of the Dunaföldvár–Solt bridge. The first two alternatives will be referred to as Dunaújváros Szentes 1 and 2, the latter three as Dunaföldvár–Szentes 4, 5 and 6 to make comparison with previous results easier.

Note, that these scenarios only include a new bridge over the Danube and a developed one on the Tisza as the Baja bridge and its connecting lines were not assumed to be developed. This is due to its southern position in the country and that the traffic should pass through the new bridge which is not too far from Budapest, unlike the Baja bridge. A train in a northwest–northeast direction, which is the most common in the freight transport corridor of Hungary,[30] will not travel that south if there is a bridge halfway.

Results

Calculating the paths that pass through each bridge we get the plots shown in Figure 9.

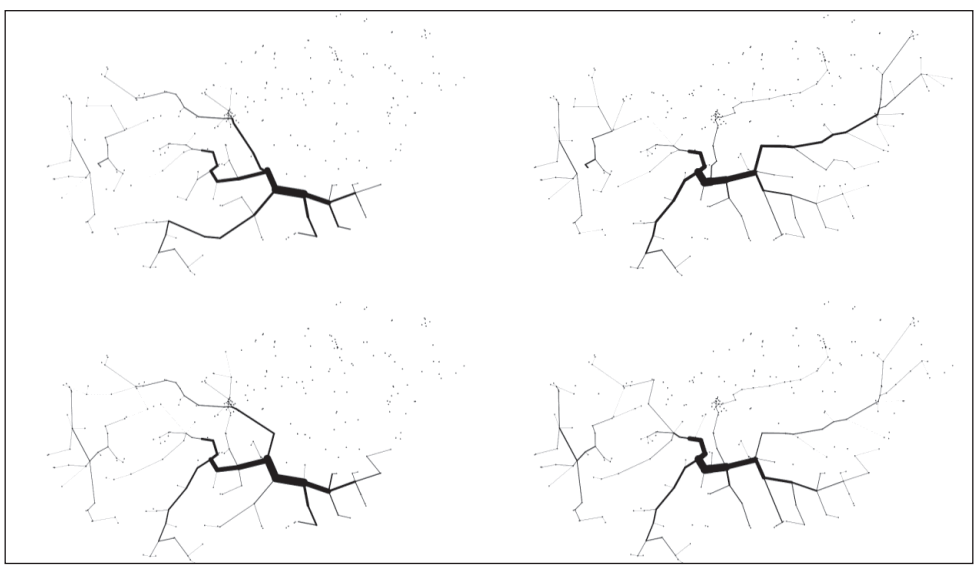


Figure 9: The geographical distribution of the paths passing through the Szentes–Csongrád bridge (left) and the Dunaföldvár–Solt bridge (right) for minimal trip lengths (top) and for minimal travel times (bottom)

Note: The thickness of the lines is proportional to the number of paths. The number of paths passing through the bridge is taken to be 100%.

[30] Lakatos et al. 2016: 181–288.

Source: Compiled by the authors.

The results for Alternatives 4, 5 and 6 are practically the same. The Danube bridge connects distant regions of the country including important international border crossings like Hegyeshalom, Rajka, Záhony, Lőkösháza, Röszke or Gyékényes via the core network. The Tisza bridge has the same role, except that the paths of the northeastern part of Hungary do not pass through it, they cross the Tisza via the Szolnok–Szajol bridge.

The numerical values of the measures describing the network as a whole can be seen in Table 2.

Table 1: The percentile change in the measures used to describe the alternatives

Dunaföldvár–Szentes	**Distance**			**Time**		
Alternative	**4**	**5**	**6**	**4**	**5**	**6**
Decrease in the total network path length/travel time if the new bridge is implemented (%)	8.6	8.6	8.8	9.4	9.6	9.6
Decrease in the traffic of the most heavily loaded line section if the new bridge is implemented (%)	11.8	12.3	12.3	14.7	15.4	15.4
Ratio of paths passing through the new bridge (%)	8.3	8.6	9.3	7.2	7.5	7.4

Source: Compiled by the authors.

It seems that the three alternatives are essentially the same, Alternative 6 being a slightly better one. The total network travel time decreases with almost 10% which is an outstanding value compared to the alternatives in the first part of the study where there was no new Tisza bridge just a new Danube bridge. The change in the traffic of the busiest line section, the one of the Southern bridge is the same to the alternatives when there were no development of Tisza bridges which means that a Danube bridge alone would make many of the paths to reroute, though there were no capacity for them to pass through the Szolnok–Szajol bridge.

The effect of the alternatives on the traffic of Budapest is plotted in Figure 10.

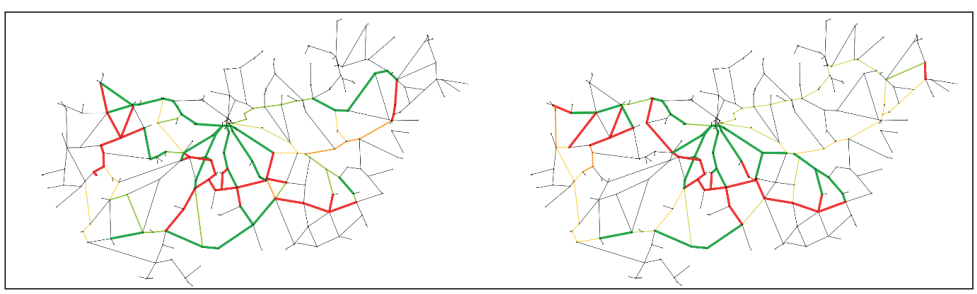


Figure 10: The change in traffic for minimal trip lengths (left) and for minimal travel times (right) compared to the present situation

Source: Compiled by the authors.

Though all three alternatives have practically the same effect on the capital, it is a very positive effect. The traffic of all radial main lines decreases with a significant amount.

This not only makes Budapest less congested but also as seen from the maps of Figure 10, makes use of both the Dunaföldvár–Solt bridge and the Szentes–Csongrád bridge.

Summary

We analysed the possible paths of a new Tisza bridge at Szeged and the possible development of the already existing Szentes–Csongrád bridge. The calculations showed that all alternatives have practically the same effect on the railway network of Hungary but these effects are not as advantageous to suggest the realisation of one of the alternatives.

Comparing with the results of the first part of this study, several locations of both a Danube and a Tisza bridge were tested and the results of this combined development plan was convincing. In summary, we can say on the basis of our model that one bridge alone is not enough as currently there are only one high capacity crossing on each river and thus one new is needed on each. If the exact location is determined in a well-established way, not only the problems of Budapest originating in the high traffic can be treated but more transportation capacity can be put in the network which can boost the economic benefits of the international trade routes passing through the country.

References

A Szeged–Szőreg vasútvonal fejlesztésének megvalósíthatósági tanulmányterve (2006). Budapest: BME Út- és Vasútépítési Tanszék.

Berényi, János – Lévai, Zsolt (2020): CORCAP – a környezetbarát áruszállítási folyosók kialakítása útján. In Horváth, Balázs – Horváth, Gábor (eds.): *X. Nemzetközi Közlekedéstudományi Konferencia* [10th International Conference on Transport Sciences]. Győr: Széchenyi István Egyetem Közlekedési Tanszék – Közlekedéstudományi Egyesület.

Braess, Dietrich (1968): Über ein Paradoxon aus der Verkehrsplanung. *Unternehmensforschung*, 12(1), 258–268. Online: https://doi.org/10.1007/BF01918335

Braess, Dietrich – Nagurney, Anna – Wakolbinger, Tina (2005): On a Paradox of Traffic Planning. *Transportation Science*, 39(4), 446–450. Online: https://doi.org/10.1287/trsc.1050.0127

Csárdi, Gábor – Nepusz, Tamás (2006): The Igraph Software Package for Complex Network Research. *InterJournal, Complex Systems*, 1695(5), 1–9.

Dijkstra, Edsger W. (1959): A Note on Two Problems in Connexion with Graphs. *Numerische Mathematik*, 1(1), 269–271. Online: https://doi.org/10.1007/BF01386390

Jenelius, Erik (2010): Redundancy Importance: Links as Rerouting Alternatives during Road Network Disruptions. *Procedia Engineering*, 3, 129–137. Online: https://doi.org/10.1016/j.proeng.2010.07.013

Jenelius, Erik – Petersen, Tom – Mattsson, Lars-Göran (2006): Importance and Exposure in Road Network Vulnerability Analysis. *Transportation Research Part A*, 40(7), 537–560. Online: https://doi.org/10.1016/j.tra.2005.11.003

Horváth, Attila (2006): A közúti, vasúti és vízi közlekedés terrorfenyegetettségének jellemzői. In Tálas, Péter (ed.): *A politikai marketing fogságában.* Budapest: Mágustúdió. 321–336.

Kerényi, Levente – Tóth, Bence (2020): Alternatív vasúti útvonalak minősítése a Magyar Honvédség szállítási feladatainak ellátásában. *Katonai Logisztika,* 28(1–2), 79–99. Online: https://doi.org/10.30583/2020/1-2/079

Lakatos, Péter – Szászi, Gábor – Taksás, Balázs (2016): A logisztikai infrastruktúra szerepe a regionális versenyképesség alakításában. In Csath, Magdolna (ed.): *Regionális versenyképességi tanulmányok.* Budapest: NKE. 181–288.

Lévai, Zsolt (2020): A vasúti alágazat jelenkori kapcsolódása a közlekedési támogatás rendszeréhez. *Katonai Logisztika,* 28(1–2), 198–223. Online: https://doi.org/10.30583/2020/1-2/198

R Core Team (s. a.): *R: A language and environment for statistical computing. R Foundation for Statistical Computing.* Online: www.R-project.org/

Schváb, Zoltán – Lévai, Zsolt (2022): A vasúti árufuvarozás versenyképességének javítása az árufuvarozási folyosók fejlesztésével. In Duleba, Szabolcs (ed.): *Logisztikai Évkönyv 2022.* Budapest: Magyar Logisztikai Egyesület. 172–183. Online: https://doi.org/10.23717/LOGEVK.2022.16

Scott, Darren M. – Novak, David C. – Aultman-Hall, Lisa – Guo, Feng (2006): Network Robustness Index: A New Method for Identifying Critical Links and Evaluating the Performance of Transportation Networks. *Journal of Transport Geography,* 14(3), 215–227. Online: https://doi.org/10.1016/j.jtrangeo.2005.10.003

Szászi, Gábor (2007): Magyarország közlekedési infrastruktúrájának fejlesztése napjainkban: Közút vagy vasút? *Katonai Logisztika,* 15(2), 32–59.

Szászi, Gábor (2010): Katonai vasúti szállítások a Magyar Honvédség missziós feladatainak rendszerében. *Szolnoki Tudományos Közlemények,* 16, 101–118.

Szászi, Gábor (2013a): *A vasúti hálózati infrastruktúrával szemben támasztott újszerű védelmi követelmények kutatása, a továbbfejlesztés feltételrendszerének vizsgálata.* PhD thesis. Budapest: NKE. Online: https://doi.org/10.17625/NKE.2014.028

Szászi, Gábor (2013b): Long-span Railway Bridges in the Transport System of Hungary. *Hadmérnök,* 8(2), 98–107.

Szászi, Gábor (2014): Nagyfolyami vasúti hidak, mint közlekedési létfontosságú rendszerelemek. In Horváth, Attila – Bányász, Péter – Orbók, Ákos (eds.): *Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről.* Budapest: NKE. 25–48.

Tóth, Bence (2017): Állomások és állomásközök zavarának gráfelméleti alapú vizsgálata a magyarországi vasúthálózaton. *Hadmérnök,* 12(4), 52–66.

Tóth, Bence (2018): A magyarországi vasúthálózat zavarainak gráfelméleti alapú vizsgálata. In Horváth, Balázs – Horváth, Gábor – Gaál, Bertalan (eds.): *Közlekedéstudományi konferencia. Technika és technológia a fenntartható közlekedés szolgálatában.* Győr: Széchenyi István Egyetem Közlekedési Tanszék. 505–519.

Tóth, Bence G. (2020): Redundancy Analysis of the Railway Network of Hungary. In Tóthné Szita, Klára – Jármai, Károly – Voith, Katalin (eds.): *Solutions for Sustainable Development.* London: CRC Press. 358–367. Online: https://doi.org/10.1201/9780367824037-42

Tóth, Bence (2021): The Effect of Attacks on the Railway Network of Hungary. *Central European Journal of Operations Research,* 29(2), 567–587. Online: https://doi.org/10.1007/s10100-020-00684-8

Tóth, Bence – Horváth, István (2019): How the Planned V0 Railway Line Would Increase the Resilience of the Railway Network of Hungary Against Attacks. *AARMS,* 18(3), 109–129. Online: https://doi.org/10.32565/aarms.2019.3.9

AARMS Vol. 22, No. 3 (2023) 63–76.

10.32565/aarms.2023.3.4

Boosting Effect of Startup Ecosystems through Next Generation Digital Technologies in Hungary[1]

Judit SZAKOS[2]

In time of crisis, developing Next Generation Digital Technologies in the innovation network, with special attention to startup companies, can be a key to economic thrive. This paper reviews the current and emerging technological trends and how they are connected to the hype surrounding startup companies and their ecosystem, with particular attention to the role of the state. The analyses use Ramstad's Expanded Triple Helix Model as a framework but with opening its workplace dimensions to subgroups.

In Hungary, digital or technology-led startups are relevant in their numerical and economic volume. Narrowing them further down to artificial intelligence-based companies, one can see that innovation-led cooperations are already state facilitated and could cover every aspect of the ecosystem model. Analysing its operation could lead to good practices for further usage in other technological fields. On the other hand, further qualitative research on their innovation partnership should be conducted to avoid any bias.

Keywords: *Next Generation Digital Technologies (NGDTs), emerging technologies, dual-use technologies, artificial intelligence, digital transformation, startup, innovation ecosystem, startup ecosystem, Expanded Triple Helix Model*

Introduction

Although – as countries face new economic and security challenges – the Covid-19 pandemic seems far behind, its impact on every aspect of our life with digital technologies remains. While lockdown-based economic challenges have become an everyday problem, the digital market has been accelerating, and its ongoing rise should be investigated further. Today, with the rise of a new crisis, ecological and wicked issues, lessons learned from the past could be favourable for policy-makers and further actors of the ecosystem, such as the

[1] This publication was prepared in the framework of Project no. TKP2021-NKTA-51, which has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NKTA funding scheme.

[2] University of Public Service, Institute for American Studies, e-mail: szakos.judit@uni-nke.hu

usage of big data for adequate problem solving or the importance of cybersecurity due to the velocity of digitalisation.

As economies have not recovered from previous and ongoing shocks, the competitiveness of a region could be boosted by fast-growing, information and communication technology (ICT) based companies. On the other hand, rising technologies can have disruptive effects, causing not just opportunity but several challenges, too. Cho et al. (2023) refer to these new and emerging complementary digital technologies as Next Generation Digital Technologies (NGDTs). Their terminology includes: internet of things (IoT), mobile devices, big data, cloud computing, artificial intelligence (AI), blockchain, virtual/augmented reality, robotics and 3D printing, separating the definition from the undefined Industry 4.0 category, as the former is not explicitly focused on manufacturing while their definition does.[3]

Further insights about technological development prediction are available. The annual 2022 Gartner Hype Cycle for Emerging Technologies explores more than 2,000 technologies with high potential. It summarises 25 of them in three categories, potentially impacting the next 2 to 10 years. The categories are the following: 1. evolving/expanding immersive experiences; 2. accelerated artificial intelligence automation; and 3. optimised technologist delivery.[4]

Similar technologies got into the focus in the defence innovation industry. The North Atlantic Treaty Organization (NATO) focuses on the following areas: 1. AI; 2. data; 3. autonomy; 4. quantum-enabled technologies; 5. biotechnology; 6. hypersonic technologies; 7. space; 8. novel materials and manufacturing; 9. energy and propulsion.[5] NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) accelerates further the investment into boosting these areas. An obvious consequence of the NATO directions is that the National Military Strategy of Hungary is in line with it, listing likewise key technologies from AI to nanotechnology.[6] Nowadays, these dual-use technologies are not just spinning from military to civilian use,[7] but market-based innovations can be found useful in the defence sector.[8] Innovation researches and cooperations are interoperable, with actors often overlapping.

Change in technology use also demands "a more inclusive approach to digital transformation",[9] as its society-shifting effects are remarkable. In parallel, social transition can be a precondition for further growth, and an interrelated connection is apparent again.

Technology innovation is also an opportunity for countries without significant natural resources. It allows for building a (continuously) learning[10] economy and learning

---

3 Cho et al. 2023: 1.
4 Perri 2022.
5 NATO 2022.
6 Government Decree 1393/2021 (VI.24.) on the National Military Strategy of Hungary.
7 For example, when the U.S. Department of Defense set out in the 1960s to create a decentralised postal service so that the traditional mail system would not collapse in the event of the centre's destruction. The research they funded led to the birth of email, an innovation that truly decentralised communication (Kornai 2010: 2).
8 Like facial biometrics, where GaussianFace facial identification algorithm – developed at the Chinese University of Hong Kong in 2014 – reached scores of 98.52% (Lu–Tang 2015: 1–13).
9 OECD 2020: 13.
10 Lundvall 2016.

society.[11] To do so, boosting the economy through supporting startup companies is a trending tool. States have space for manoeuvre, regardless of whether it has a liberal or an entrepreneurial, mission-oriented view of the responsibilities that they follow. They can – with strategies, regulation, policies, direct and indirect incentives by their choice and opportunities – orient the move of the market and every relevant actor with it.

Conceptual background

Innovation has become a selling buzzword on the market, although it has a well-defined theoretical background. Related concepts are invention as well as research and development. However, these two do not necessarily appear in the market, while one can only talk about innovation if they reach the customer. At the same time, innovation does not always necessarily root in R&D activities. According to the widely used definition of the European Commission, innovation is "the successful production, assimilation and exploitation of novelty in the economic and social spheres. It offers new solutions to problems and thus makes it possible to meet the needs of both the individual and society."[12] Technology-based innovation has social innovation as a precondition. Workplace innovations are also necessary for introducing new tools in a company, although it is a common default to avoid dealing with organisational learning and its longer timeframe.[13] Innovation varies in several forms; there are several clustering options. Based on the latest Organisation for Economic Co-operation and Development (OECD) Oslo Manual, "innovation is a new or improved product or process (or combination thereof) that differs significantly from the unit's previous products or processes and that has been made available to potential users (product) or brought into use by unit (process)".[14] To the extent of change, one can distinguish between incremental and radical innovation.

Radical economy and society revolutionising innovation have cyclicality; the most well-known approach to this is technological revolutions. Perez (2002) makes a difference between the two phases of these revolutions. The techno-economic paradigm, "which breaks the existing organizational habits in technology, the economy, management and social institutions" and a significant surge of development, "which represents the process of installation and deployment of each revolution and its paradigm in the economic and social system", aka diffusion in every sphere in the society. They together are the steps of a technological revolution, which "can be defined as a powerful and highly visible cluster of new and dynamic technologies, products and industries, capable of bringing about an upheaval in the whole fabric of the economy and of propelling a long-term upsurge

[11] On the other hand, previously the concept of the knowledge economy was connected to the Triple Helix Model in literature. Meanwhile, knowledge society and knowledge democracy came from Quadruple Helix Model, and the socio-ecological transition was linked to the theory of the Quintuple Helix Model (Carayannis et al. 2012: 1–12).

[12] European Commission 1995: 1.

[13] Makó–Illéssy 2014: 4–20.

[14] OECD 2018: 20.

of development". Techno-economic paradigms have a strong connection with technical innovations.[15]

Perez specifies five technological revolutions (Figure 1), where the latest is the age of information and telecommunication. At the time of the paradigm's rise, we do not yet know which might be the determining technologies of the next revolution, but its development might already be ongoing; therefore, one can just predict what the sixth will be. Still, long-term growth assumes the creation of future-oriented policies, which – even with uncertainty – lead to support technologies listed before.

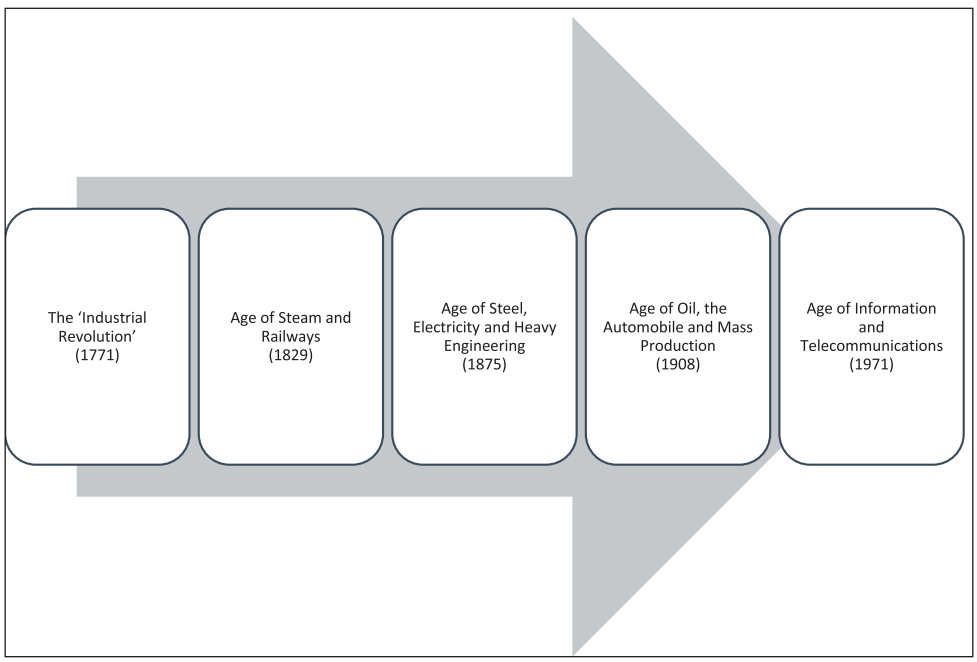


Figure 1: Technological revolutions

Source: Compiled by the author based on Perez 2002: 11.

Including future-oriented policies, the role of the state in these turbulent times appears in many aspects. The most obvious of those related to the topic – research institutions – can support technological development. Furthermore, at the time of crisis, the double role of the state appeared: it provides stability of everyday operations and agility with new challenges simultaneously. With various tools available, bureaucracies can drive innovation,[16] shape markets and define future goals.[17]

[15] Perez 2002: 7–8.
[16] Kattel et al. 2022.
[17] Mazzucato 2016: 140–156.

As one can see from its roles, the state is an inevitable actor, but its activity is interdependent with further actors' behaviour. When one looks at it from a research, development and innovation perspective, innovation models can help to draw the necessary connections.

The first innovation models analysed the path between an idea/R&D result and the market (linear models, within the factory),[18] later systemic approach was unfolded, which included non-technological innovations and every relevant actor outside of the company (organisations, institutions) to be further highlighted as a relevant factor. They could perceive how different performance appears in two companies that operate in the same way. The answer lay in their out-of-the-factory connections.[19]

One feedback-based, systemic innovation model is the Triple Helix Model, which lists states, universities and industries as part of the network. Their cooperation is capable of formulating an innovation-boosting space. Cooperation includes knowledge transfer, interactions, motivating each other for development, and even taking each other's role. This equal partnership is a delicate balance; moving away from this cooperation can lead to inefficiency.[20] Extended versions are the Quadruple Helix (adding media-based, culture-based public and civil society)[21] and the Quintuple Helix Model (adding to the latter natural environment system).[22]

Ramstad (2009) expanded the Triple Helix Model within its dimensions to reach joint knowledge creation, use and dissemination. Actors are policy-makers, workplaces and R&D units. The cooperation happens through policy-making, research, consulting, education and development. The outcome of the different actors turns out to be:

- Workplaces: "comprehensive development, better practices and routines, increased expertise on development, improvement of performance" and quality of working life (QWL)
- R&D units: "improved expertise, education and regional activities, new methods and tools, publications, scientific research"
- Policy-makers: "infrastructure improvement, improved expertise on the R&D field, new roles"
- Society: "generative knowledge and practices created, databanks, national, regional and sectoral infrastructures"[23]

Not explicitly stated in the innovation models but focusing on technology development inevitable factors, the newly formed innovative companies often appear as so-called startup companies. By definition, they are 1. younger than 10 years; 2. have (highly) innovative technologies and/or business models used; and 3. reach or strive for great employee and/or sales growth.[24] Also important that they are preparing for the international market from the start.

---

18 Marinova–Phillimore 2003: 44–53.
19 Makó et al. 2020: 96–123.
20 Etzkowitz 2008: 1–8.
21 Carayannis–Campbell 2009: 201–234.
22 Carayannis–Campbell 2010: 41–69.
23 Ramstad 2009: 186.
24 Kollmann et al. 2016.

Lányi (2017) summarises why one is formulating policies around startup companies, whereas a learning society can grow through innovation. She states that startups can introduce new competition into the existing economic system, bringing dynamism and vitality to the market, stimulate a research-based innovation system, especially in applied and high-technology research; promote proactivity as a social value alongside the values of expertise, creativity and responsibility.[25] Therefore, dedicated courtesy goes to startups when an analysis searches for a technological growth catalysator.

It leads this paper to the next concept of bringing together startups and the innovation ecosystem. The term startup ecosystem has not been as thoroughly elaborated as the innovation one. Jáki et al. (2019) state that the Hungarian startup ecosystem's most important actors are startup companies with their support organisations.[26] In this case, where a specific aspect, the technological development of the Hungarian economy is analysed, the two approaches – the startup and innovation ecosystem – are not needed to differ strictly. The reason is that normally startup companies can be formed on R&D or without, but in case of Next Generation Digital Technologies using startups, almost exclusively R&D-based ideas go to market. Based on the definition of innovation above, one can realise that the investigated market segment's framework is the innovation ecosystem, with special attention to startups in its economic dimensions.

Therefore, this paper works with the approach of Ramstad's (2009) Expanded Triple Helix Model, opening up the workplace dimension and analysing it as a multisegmented network of economic actors, putting startup companies at the centre of the research (Figure 2).

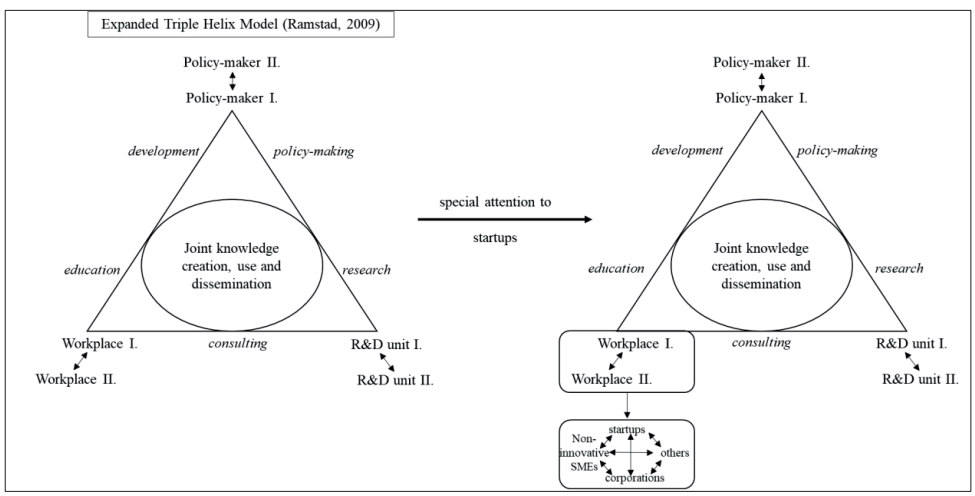


Figure 2: Expanded Triple Helix Model based on Ramstad 2009: 186 and its rethought view with special attention to startups, as one of the "problem owner" and knowledge creators

Source: Compiled by the author.

[25] Lányi 2017: 79.
[26] Jáki et al. 2019: 2–12.

Methodology

The research question of this paper: How does new technology (AI) implementation/ development appears in the Hungarian innovation (startup) ecosystem level, focusing on synergies?

To answer this question, the paper concentrates first on the broadly defined startups, followed by narrowly classified technology-based startups and their attributes available. Data comes from the Hungarian Central Statistical Office (available between 2019–2021), the Startup Hungary organisation's publications and the Dealroom.co startup database. International statistics are available in the latter, completed by a detailed collection of operating companies at the "Hungarian Ecosystem at a Glance" subpage, powered by Dealroom.co and Express Innovation Agency (Hungary). Used data is based on the latest available update (28 October 2022). A comprehensive source of knowledge about the ecosystem is the Hungarian Startup Report, which the Startup Hungary organisation releases for the previous year since 2021.

To see the whole ecosystem, further related actors are investigated. Information is available specifically to the AI boosting network; therefore, the AI ecosystem will be the deeply analysed case of the study. It will be tested whether all roles of the rethought version of the expanded Triple Helix Model are covered in the Hungarian AI network.

The Hungarian (technological) startup landscape

The number of startups in Hungary differs in each source as a direct consequence of ambiguous and unregulated business forms, causing difficulties in a thorough investigation. Additionally, idea stage startups have not even had a legal form yet. The further point is that failed startups are not necessarily motivated or dedicate time to delete themselves from databases after closure.

As an orientation, the Hungarian Startup Report for the year 2021 assumes that the number of active startups is about 1,000.[27] In contrast, the Dealroom.co database counts 1,470 and presents the lack of unicorns.[28] The numbers are presenting again that lack of proper definition and data complicates the analysis.

The Hungarian Central Statistical Office has collected data about startups since 2019. Available information is limited: founders, financial sources and net income are presented.

[27] Startup Hungary 2022: 6.

[28] Startups with a $1 billion valuation are called unicorns. 2 potential unicorns are listed in Hungary: Seon and bitrise. (Data last checked at the Dealroom.co webpage: 30 December 2022.)

Table 1: Hungarian Central Statistical Office: Distribution of startup founders and companies by their main characteristics

Name	Ratio (%)		
	2019	2020	2021
Distribution of startup founders by age group			
Younger than 25 years old	5.8	7.9	9.4
25–34 years old	29.7	30.8	31.4
35–44 years old	35.7	34.8	31.2
45–54 years old	15.8	17.2	18.1
55–64 years old	7.7	6.9	7.0
65 years old and older	5.3	2.5	2.9
Sum	100	100	100
Of which: women	26.6	24.8	23.7
Distribution of startup founders by education			
Academic degree (PhD)	4.0	6.2	6.8
University degree	57.5	61.5	63.0
High school degree	36.9	30.2	27.2
Other/no data	1.6	2.2	3.0
Sum	100	100	100
Distribution of startups by number of founders			
1 founder	42.3	41.2	37.8
2 or 3 founders	50.4	50.6	51.6
More than 3 founders	7.4	8.2	10.6
Sum	100	100	100
Of which: companies with foreign founder	8.5	9.4	7.8

Source: Hungarian Central Statistical Office 2022a.

Table 1 shows that the 25–34 age group (31.4% in 2021) and the 35–44 age group (34.8% in 2021) are the most active in startup creation. This contrasts with the stereotype that startup founders are typically university students. Two-thirds of the founders have a tertiary education: 63% had a university degree in 2021, plus 6.8% also have a science degree. The slow rise in the number of PhD holders could also herald a revival in the market roll-out of research. Furthermore, scientific knowledge can be a boost for emerging technology-based startups. Unfortunately, disciplinary distribution between degrees is not available (Table 1).

Funding sources are mostly based on the founders' own assets (in 2021: 76.8%), but every internationally recognised option is available, as Table 2 presents.

Table 2: Hungarian Central Statistical Office: Proportion of all startups by the source of funding in a given year

Funding sources	2019	2020	2021
Founders' own assets	78.9	77.2	76.8
Family, friends	12.6	12.7	12.5

Funding sources	2019	2020	2021
Support of the state	7.9	10.3	12.8
Business/angel investor	3.2	2.6	4.3
Venture capital investment	14.4	12.7	17.6
Incubator/accelerator	5.8	6.1	7.1
Bank loan	3.5	3.8	4.5
Crowdfunding	0.4	1.0	0.6
Other supports, sources	3.6	4.5	3.7

Source: Hungarian Central Statistical Office 2022b.

Regarding the net sales for 2021, available data is just a current expectation, but it shows a rise in every life cycle of the companies. The more mature the companies are, the more summarised net income they reach, as Table 3 presents.

Table 3: Hungarian Central Statistical Office: Average net sales of startups by startup life cycle stage

Startup life cycle phases	2019	2020	*2021**
Average net sales (thousands HUF)			
Idea, pre-seed	4,988	4,657	*7,367*
Early stage	22,154	19,091	*29,491*
Growth stage or later	33,325	43,574	*45,212*
All startups	20,496	20,812	*22,543*

** Expected data for 2021.*

Source: Hungarian Central Statistical Office 2022c.

Within the Dealroom.co, the "Hungarian Ecosystem at a Glance" have 493 registered startups,[29] where one can search within attributes, like which next generation digital technologies they use. As they usually use more technologies, usage numbers are higher than the summary of the relevant 165 startups. It means a third of the added startups in the database use some new technology. Deep tech (94) is the most common one, followed by mobile apps (47), big data (34) and AI (31). Startup Hungary found similar trends:[30] web/mobile application was the most common product or service. The verticals described the most companies answered the questionnaire for 2021 were: AI/machine learning, big data, fintech, hardware, education, medtech.[31]

Terminology inconsistencies appear in supporting organisations as well. There is no proper division in business incubators, which are dedicated to specific startup needs, but 21 listed accelerators in the Dealroom.co database should indicate the least amount of proper actors. European Union and government grants were available to some of them.

[29] Added startups are less than a third of their summed 1,470, but still, this is the most accurate search option.

[30] The categorisation of the Dealroom.co and Hungarian Startup Report are not identical; therefore, direct comparison is not possible, but both leads present similar trends in technology use.

[31] Startup Hungary 2022: 27, 29.

Similar tenders were available for venture capital building, next to the full state-owned capital Hiventures Ltd.; therefore, financing is not appearing to be a huge problem in the country.

From an educational perspective, the Hungarian Startup University Program is running for two years around the country as an elective course to teach students how the ecosystem works and how to set up their own businesses. Regarding the specific technological knowledge, Hungary is said to have historical roots in science, technology, engineering and mathematics (STEM) field, but that does not necessarily mean that any level of education adequately prepares students for developing in an emerging area – one has to investigate further in that topic.

Artificial Intelligence Coalition

Based on the webpage of the Hungarian AI Coalition, its goal is to "be at the forefront of artificial intelligence developments and applications in Europe and to become an important member of the international AI community". It aims to create a forum where relevant actors "jointly define the directions and frameworks for the domestic development of artificial intelligence".[32]

The mission of the AI Coalition is to:

- "propel Hungary to the European forefront in the area of AI developments
- facilitate the participation of Hungarian start-ups and SMEs in AI development activities in partnerships with large enterprises, universities or international partners
- strengthen the competitiveness of domestic enterprises through extensive dissemination and utilization AI-based use-cases
- make sure that the government, as a user of AI-powered solutions, should be actively engaged in developing the local AI ecosystem by systematically utilizing the national data asset pool"[33]

The AI Coalition together with the relevant ministry created Hungary's Artificial Intelligence Strategy (2020–2030), adopted by Government Resolution 1573/2020 (IX.9.). The AI Coalition's assignment is to review the Strategy with its milestones.

The 392 member organisations include more than 900 experts in 6 working groups. Working groups are the following:

- Technology and security
- Use cases and market development
- Data industry and data asset pool
- Education and awareness raising
- Regulation and ethical framework
- International relations

[32] Artificial Intelligence Coalition webpage.
[33] Artificial Intelligence Coalition webpage.

The board's composition is a good illustration of a mapping of the logic of innovation ecosystems. Board members represent the science community, public administration, Hungarian SMEs, mid-sized enterprises, chambers, professional organisations and startups. Both the user and the developer sides are presented. Joining the Coalition is possible for companies and organisations with a registered seat/branch in Hungary.

Next to its forum providing work, it also offers educational opportunities for all (AI Academy, AI Podcast), creates an AI Marketplace and disseminates success stories, involving a wider audience and raising social awareness.

Discussion and conclusions

Although there are many lessons to learn from the Hungarian startup scene, and actors from the ecosystem are still searching for their exact role in the system, it can be already predicted that digital startups could have the potential to thrive, and with them, economic growth of the country could be expected. Usage of Next Generation Digital Technologies around startups is common; their digitalisation is present from the ground. Detailed information about digital business connections is less available than those dealing with AI-connected technologies. Therefore, the organised form of the AI Coalition and its members are tested in the chosen innovation model.

The expanded Triple Helix Model has three main dimensions, where workplaces are further itemised to see the role of startups. R&D units incorporate universities and research institutes. In the Coalition, 18 universities took part from various fields of studies, including STEM, social sciences and art. State and privately funded research organisations are both present.

From the policymaker dimension, many ministries, agencies, and state-owned companies (both from the regulatory and user side) are involved. This model also assigns industry-related organisations, such as trade unions and chambers of commerce, to the policymaker side. Both Hungarian and international (American, French, Swiss) chambers of commerce are taking part, together with many associations and organisations bringing together representatives of a profession or a scientific field. The former Ministry of Innovation and Technology and now its successor, the Ministry of Technology and Industry, is not just taking part in the Coalition but also plays the role of a facilitator.

Companies cover the spectrum of startups, corporations, non-innovative SMEs and other businesses. Their cooperation within the Coalition or as business/research partners bring them even closer to the down model.

Next to the state, academia and market, AI cooperations also include social stakeholders.

In the Minister's Greeting of the Hungarian AI Strategy, László Palkovics states that the Strategy is a "joint, action-oriented product of the Coalition's professional community" and it "initiated exemplary bottom-up cooperation and market creation among the stakeholders, as part of which an action plan was developed as early as in the autumn

of 2019 to perform tasks not requiring government decisions. The implementation of the Strategy is also based on this cooperation".[34]

This paper can conclude that cooperation within the AI Coalition looks alike with the Extended Triple Helix Model as described and based on the documents issued. One can see that all searched "workplace" actor is present; startups have a role in the network. Its practical effect will be visible with time, but the first milestone – publishing a strategy – is already achieved. The state appears both in regulatory and facilitator roles.

Good practice of this concrete technology-driven segment can be taken to other digital ecosystems or even to further cooperations. At the same time, one has to keep in mind that many practical issues might have occurred that a research cannot see; therefore, further quantitative research is required to avoid information asymmetry-led bias.

References

Carayannis, Elias G. – Barth, Thorsten D. – Campbell, David F. J. (2012): The Quintuple Helix Innovation Model: Global Warming as a Challenge and Driver for Innovation. *Journal of Innovation and Entrepreneurship*, 1(1), 1–12. Online: https://doi.org/10.1186/2192-5372-1-2

Carayannis, Elias G. – Campbell, David F. J. (2009): "Mode 3" and "Quadruple Helix": Toward a 21st Century Fractal Innovation Ecosystem. *International Journal of Technology Management*, 46(3–4), 201–234. Online: https://doi.org/10.1504/IJTM.2009.023374

Carayannis, Elias G. – Campbell, David F. J. (2010): Triple Helix, Quadruple Helix and Quintuple Helix and How Do Knowledge, Innovation and the Environment Relate to Each Other? A Proposed Framework for a Trans-disciplinary Analysis of Sustainable Development and Social Ecology. *International Journal of Social Ecology and Sustainable Development*, 1(1), 41–69. Online: https://doi.org/10.4018/jsesd.2010010105

Etzkowitz, Henry (2008): *The Triple Helix. University–Industry–Government Innovation in Action.* New York: Routledge. Online: https://doi.org/10.4324/9780203929605

European Commission (1995): *Green Paper on Innovation.* Online: https://europa.eu/documents/comm/green_papers/pdf/com95_688_en.pdf

Government of Hungary (2020): Government Resolution 1573/2020 (IX.9.) on the Artificial Intelligence Strategy of Hungary.

Government of Hungary (2021): Government Decree 1393/2021 (VI.24.) on the National Military Strategy of Hungary.

Hungarian Central Statistical Office (2022a): *9.1.1.19. Startupalapítók, vállalkozások megoszlása főbb jellemzők szerint.* STADAT-Táblák. Online: www.ksh.hu/stadat_files/gsz/hu/gsz0065.html

Hungarian Central Statistical Office (2022b): *9.1.1.20. Startupvállalkozások aránya az adott évben igénybe vett finanszírozási források szerint az összes startupvállalkozás százalékában.* STADAT-táblák. Online: www.ksh.hu/stadat_files/gsz/hu/gsz0066.html

[34] Government of Hungary 2020: 5.

Hungarian Central Statistical Office (2022c): *9.1.1.21. Startupvállalkozások átlagos nettó árbevétele és a foglalkoztatottak átlagos létszáma a startupéletciklus fázisai szerint.* STADAT-Táblák. Online: www.ksh.hu/stadat_files/gsz/hu/gsz0067.html

Cho, Jaehan – DeStefano, Timothy – Kim, Hanhin – Kim, Inchul – Paik, Jin Hyun (2023): What's Driving the Diffusion of Next-Generation Digital Technologies? *Technovation,* 119, 1–10. Online: https://doi.org/10.1016/j.technovation.2022.102477

Jáki, Erika – Molnár, Endre Mihály – Kádár, Béla (2019): Characteristics and Challenges of the Hungarian Startup Ecosystem. *Vezetéstudomány – Budapest Management Review,* 50(5), 2–12. Online: https://doi.org/10.14267/VEZTUD.2019.05.01

Kattel, Rainer – Drechsler, Wolfgang – Karo, Erkki (2022): *How to Make an Entrepreneurial State. Why Innovation Needs Bureaucracy.* New Haven – London: Yale University Press. Online: https://doi.org/10.12987/9780300235371

Kollmann, Tobias – Stöckmann, Christoph – Hensellek, Simon – Kensbock, Julia (2016): *European Startup Monitor 2016.* German Startups Association.

Kornai, János (2010): Innováció és dinamizmus. Kölcsönhatás a rendszerek és a technikai haladás között. *Közgazdasági Szemle,* 57(1), 1–36.

Lányi, Beatrix (2017): A startup vállalkozók személyiségjellemzőinek hatása az innovatív piaci jelenlétre – Különös tekintettel az egészségügyi és orvosi biotechnológiai ágazatra. *Közép-Európai Közlemények,* 10(2), 77–90.

Perri, Lori (2022): What's New in the 2022 Gartner Hype Cycle for Emerging Technologies. *Gartner,* 10 August 2022. Online: www.gartner.com/en/articles/what-s-new-in-the-2022-gartner-hype-cycle-for-emerging-technologies

Lu, Chaochao – Tang, Xiaoou (2015): Surpassing Human-Level Face Verification Performance on LFW with GaussianFace. *Proceedings of the AAAI Conference on Artificial Intelligence,* 29(1), 1–13. Online: https://doi.org/10.1609/aaai.v29i1.9797

Lundvall, Bengt-Åke (2016): *The Learning Economy and the Economics of Hope.* London – New York: Anthem Press. DOI: https://doi.org/10.26530/OAPEN_626406

Makó, Csaba – Illéssy, Miklós (2014): A szervezeti innovációk a közszféra szervezeteiben (A jó állam létrehozásának és tartós fenntartásának elhanyagolt dimenziója). *Pro Publico Bono – Magyar Közigazgatás,* (4), 4–20.

Makó, Csaba – Illésy, Miklós – Számadó, Róza – Szakos, Judit (2020): Workplace Innovation: Concepts, Regulation and Increasing Role of Knowledge Management: Theoretical Considerations and European Experiences. *Pro Publico Bono – Magyar Közigazgatás,* 8(1), 96–123. Online: https://doi.org/10.32575/ppb.2020.1.6

Marinova, Dora – Phillimore, John (2003): Models of Innovation. In Shavinina, Larisa V. (eds.): *The International Handbook on Innovation.* Oxford: Pergamon. 44–53. Online: https://doi.org/10.1016/B978-008044198-6/50005-X

Mazzucato, Mariana (2016): From Market Fixing to Market-creating: A New Framework for Innovation Policy. *Industry and Innovation,* 23(2), 140–156. Online: https://doi.org/10.1080/13662716.2016.1146124

NATO (2022): Emerging and Disruptive Technologies. *NATO,* 08 December 2022. Online: www.nato.int/cps/en/natohq/topics_184303.htm

OECD (2018): *Oslo Manual 2018. Guidelines for Collecting, Reporting and Using Data on Innovation. The Measurement of Scientific, Technological and Innovation Activities.* Paris: OECD. Online: https://doi.org/10.1787/9789264304604-en

OECD (2020): *OECD Digital Economy Outlook 2020.* Paris: OECD. Online: https://doi.org/10.1787/bb167041-en

Perez, Carlota (2002): *Technological Revolutions and Financial Capital. The Dynamics of Bubbles and Golden Ages.* Cheltenham–Northampton: Edward Elgar Publishing. Online: https://doi.org/10.4337/9781781005323

Ramstad, Elise (2009): Developmental Evaluation Framework for Innovation and Learning Networks: Integration of the Structure, Process and Outcomes. *Journal of Workplace Learning*, 21(3), 181–197. Online: https://doi.org/10.1108/13665620910943924

Startup Hungary (2022): *Hungarian Startup Report 2021.*

AARMS Vol. 22, No. 3 (2023) 77–90.

10.32565/aarms.2023.3.5

Combustion Gas Examination of a Battery Housing in Electrically Driven Heavy Goods Vehicle

Antal APAGYI,[1] Rajmund KUTI,[2] Csenge PAPP[3]

Nowadays, electrically propelled vehicles are becoming more and more popular. Due to the propulsion system, the risks derived from the operation have changed, compared to the conventionally driven vehicles. The investigated vehicle has the same, new risk factor originating from the behaviour of rechargeable energy storage system (RESS) during combustion and there is only a minority of available literature dealing with the investigation of the battery housing. According to our assumption the housing is a fire comburent material that hinders the work of first responders. In this research we conducted the laboratory examination of a prismatic $LiFePO_4$ battery cell and battery pack cover used in electrically driven vehicles during burning. Combustion gases were collected and were evaluated with the help of gas chromatography. Our results show that plastic housing and cell covers are not recommended in automotive industrial use, because of their comburent characteristics, also the combustion gases are severely harmful. This paper includes the method of sampling, the experiment itself and the results.

Keywords: *electromobility, electric heavy goods vehicle, operational safety, battery fire, combustion gases*

Introduction

Recently, electromobility gained ground in the field of air pollution reduction. In the European Union, in 2018, for the 29% of the total economic emission of gases causing greenhouse effect, inland and international transport were responsible. Light-duty and commercial vehicles (passenger car, van) in 15%, while heavy-duty vehicles (lorry and bus) in 5% contribute to the European emission rate originated from transportation greenhouse

[1] PhD student, Széchenyi István University, Doctoral School of Multidisciplinary Engineering Sciences, e-mail: apagyi.antal@sze.hu

[2] Full Professor, Széchenyi István University, Department of Automatization and Mechatronics, e-mail: kuti.rajmund@sze.hu

[3] PhD student, University of Public Service, Doctoral School of Military Sciences, e-mail: papp.csenge@stud.uni-nke.hu

gases.[4] Mainly this causes severe air pollution in towns. Because of increasing road freight transport, harmful emission was still rising, in spite of the increasing efficiency of fuel-consumption. The EU 2019/1242[5] norm dealing with the CO_2 emission of heavy-duty vehicles was put into action on 14 August 2019, in which goals were set to decrease the average CO_2 emission of lorries by 2025 and 2030.[6] Nowadays, in this perspective, the goal of any type of vehicle manufacturer is to decrease the CO_2 emission of their product. This process determines the way of vehicle development, thus, propulsion electrification takes place worldwide. This progress in the heavy-duty vehicle sector happens in small steps, the reason behind this can be traced back to batteries, since in case of road freight transport the daily 500–1,000 km distance is not practically achievable with one charging. The size and mass of battery pack create a narrow cross-section, because if the number of batteries is increased, the effective load space and the effective transportable mass is decreased. Therefore, a compromise between the range and effective payload is made. Battery driven lorries can be used in such areas, where the distances are measurable in a few hundreds of kilometres and it is possible to charge in rounds daytime, thus 24 hours service time can be ensured. This can be for instance the transportation between warehouse and premises. During unload, battery can be charged. Currently, the electric lorry visible in Figure 1, transports goods between significant logistic stores in Győr.

Figure 1: Electrically propelled heavy goods vehicle

Source: Picture made by the authors.

It is a very favourable utilisation of electric propulsion, since inside warehouses there are closed spaces, the exhaust emissions of a traditional internal combustion engine with the lack of proper ventilation expose employees to a concentrated air pollution with health damaging effects, also acoustic load of engine noise is ceased.

4 Buysse–Miller 2021.

5 Regulation (EU) 2019/1242 of the European Parliament and of the Council of 20 June 2019 on the marketing of EU fertilising products and amending Regulations (EC) No 1069/2009 and (EC) No 1107/2009 and repealing Regulation (EC) No 2003/2003.

6 European Commission 2021.

Hazards of electric propulsion

Unfortunately, electric heavy goods vehicles are not so widespread, moreover their price is multiple of one with internal combustion engine. For a logistic company, it is a convenient solution to convert a vehicle assembled with an internal combustion engine to be electric, rather than buying a new one. Since only the electric drivetrain is changed in a traditional vehicle, the cost of the conversion is part of the purchase price. Whether it is an individually built vehicle or originally electric, this reserves new, yet unknown and not-examined risks from the point of view of operational safety. Focusing on battery fires, first any kind of accident in which collision happens, should be mentioned, because the battery itself can be damaged.

In the European Union, electric vehicles participating in public transportation that are equipped with lithium-ion battery have to withstand the criteria of the UN UNECE 100 Regulation,[7] such as vibration test or mechanical impact. Due to physical damage, the cover and housing of the battery may get some injuries, causing fire in the cells. Electrolyte leakage, shortcut and electric failures can lead to certain electrochemical reactions causing a so-called thermal runaway, thus starting a fire inside the battery.[8] Secondly, operation conditions are severe for batteries used in electric vehicles, further mentioned as EV. Frequent accelerations and deceleration in traffic again mean higher probability of thermal runaway and ignition. In addition, extreme cold and extreme hot weather can influence the power and lifespan of the battery. High temperatures can result in overheated cells and chemical reactions inside the cells. Cold temperatures lead to internal resistance increase, promoting metallic dendrites increasing the chance for battery fire.[9] Moreover, charging is another potential risk from the point of view of EV fire. In certain cases, it was concluded that the cause of the fire while charging was faulty plug for the charging socket, resulting in significant resistance to current flow. This ended in high temperatures and spontaneous combustion. Short circuits also contribute to charging fires. The negligent usage of dedicated factory charger with the higher current parameters can lead to battery fire as well. Last, improperly performed maintenance is a problem resulting in EV fire. Because these systems are equipped with real-time monitoring battery management system, frequent service, upgrades and refreshment is compulsory.[10] If the battery catches fire from an external ignition source, the first part that accelerates and builds the fire is the housing and cover. Even if the fire is caused by internal thermal runaway, the combustible materials composing the housing and cover can keep the fire alive. Furthermore, the inner electrode separators are composites that are also combustible.[11] The EV batteries are tested because their compact size and high energy density suppose fire hazards. Very strict safety instructions are required in case of battery manufacturing. These tests are designated to

---

7 Regulation No 100 of the Economic Commission for Europe of the United Nations (UNECE) – Uniform provisions concerning the approval of vehicles with regard to specific requirements for the electric power train (2015/505).

8 Larsson et al. 2014: 33–44.

9 Sun et al. 2020: 1361–1410.

10 Dorsz–Lewandowski 2022.

11 Aydemir et al. 2017: 25–28; Egelhaaf et al. 2014: 221–230.

verify the battery to manufacturing failures, leakage, heat and pressure resistance, those that may occur during operation. According to the IEC 62133[12] standard, fire resistance is also measured. In this fire resistance test, different temperature limits are determined, and the reaction of the battery is monitored. Manufacturers tend to test their products and to fulfil the requirements of different national standards, but it is not compulsory, since these standards are industry standards.

When describing an incident in connection with electric vehicle battery, it is always unpredictable what kind of impacts act on the battery – thus further investigation of a housing part and cell cover can serve with information about the consequences of battery fires. With the help of the test results and proper consequences, first responders may receive better understanding about $LiFePO_4$ battery fires.

Short description of the vehicle transformation

The vehicle represented in the figure above was converted in Hungary. As a first step, the conventional internal combustion engine, the gearbox and tank of the vehicle were dismounted. In the next step, the elements of the electric drivetrain were assembled into the chassis, electric motor, battery packs and control unit, which contains the necessary power electronics. During this type of conversion, it must be taken into account that the axle load remains almost equal to the original one. Beneath the compartment, the battery was mounted in the place of the tank. From the point of view of operational safety, batteries possess high risk. In this vehicle, the safest batteries with $LiFePO_4$ cathode material, exactly 6 packs, were placed. The battery containing module has two parts, a lower holder and an upper wrapping part, this is represented in Figure 2. Their joint sponge is used as a sealing. The box cover is secured by M8 type screws. The battery has no function as frame stiffener, as the material of the box is composite. Battery packs are provided with safety functions such as fuses and ventilation holes to ensure safe operational circumstances.

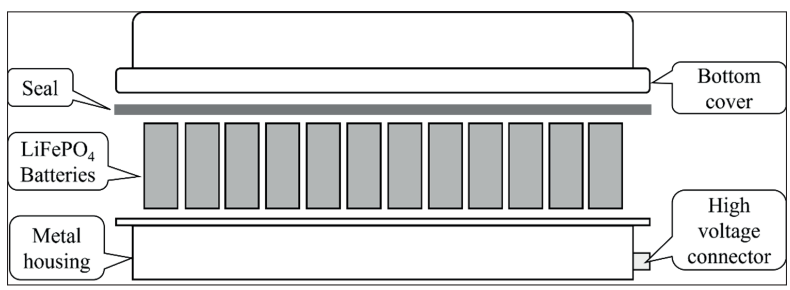


Figure 2: Exploded view of battery module

Source: Compiled by the authors.

[12] IEC 62133: Secondary cells and batteries containing alkaline or other non-acid electrolytes – Safety requirements for portable sealed secondary cells, and for batteries made from them, for use in portable applications.

EV batteries, such that were built in the described heavy goods vehicle, can have different material-made housings to ensure proper protection for the battery cells. These housings are commonly made from aluminum, steel or plastic. The chosen material depends on the environmental conditions, also on different safety level requirements and of course, weight reduction and cost are crucial aspects. Aluminum and steel-made housings have better heat ventilation, so the battery can be cooled more effectively, which contributes to longer lifespan. They are more stiff and more resistant to intrusion. Plastic housings are lighter and cheaper, but these cannot resist to external effects to the same extent (as collision or corrosion).[13]

Regarding the fire safety of batteries, choosing the right design and material plays an important role. The battery under investigation has plastic housing. The purpose of this research is to unveil harmful gases emitted from the combustion process of battery housings and cell covers and the potential risks they may cause.

Sampling

As earlier mentioned, it is becoming more and more crucial to investigate the emission gases of the batteries placed in electrically driven vehicles. Practical experiences show that the emitted gases during combustion are more severe and dangerous than fire itself.[14]

In this study we focused on the harmful gases emitted from the housing of the battery during fire. The first sample can be found in heavy goods vehicles and go-carts as well. This is a yellow-coloured cover of a battery cell represented in Figure 3; it was dismounted for the experiment and a proper-sized sample was cut from the cell cover.

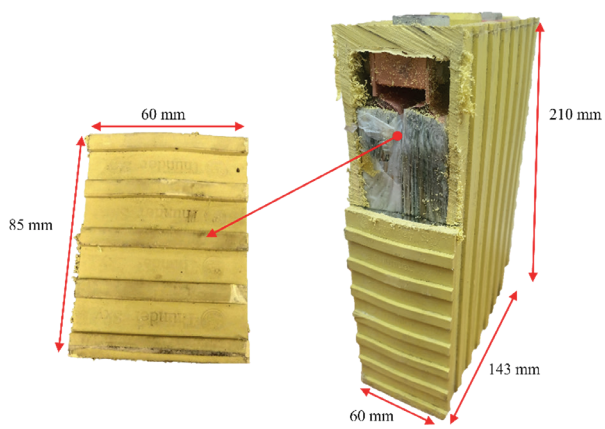


Figure 3: Dimension of Thundersky 90Ah $LiFePO_4$ battery cell

Source: Compiled by the authors.

[13] Schmerler et al. 2017: 26–31.

[14] Düser–Schramm 2019: 36–39; Larsson et al. 2017: 1–14.

The second sample is the outer part of the battery pack, which holds the housing on the chassis. This sample was cut from the housing with useful dimensions to prepare the laboratory experiment. The original sample can be observed on the next figure.

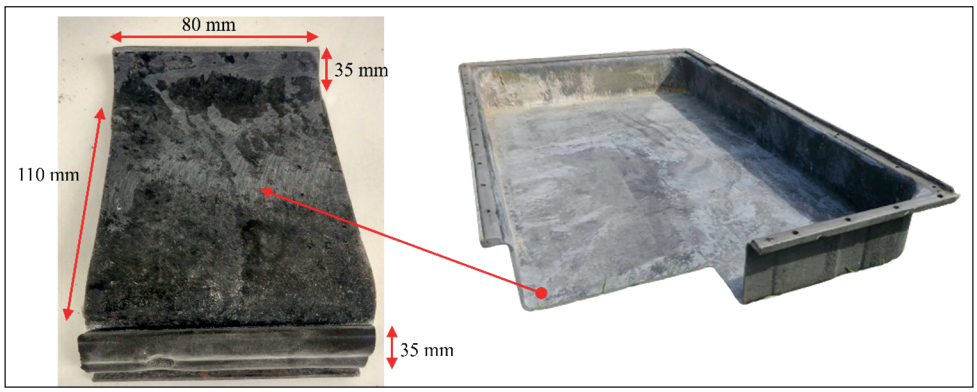


Figure 4: Sample with dimensions

Source: Compiled by the authors.

To determine the components of investigated samples, gas chromatography is used. The aim of the analytical chromatography is to detect and determine the relative ratio of the different compounds found in the gas mixture released during combustion. The burning experiment of the cell cover and the housing were conducted in the Fire Protection Laboratory of Széchenyi István University. The measurement method is represented in Figure 5, it was conducted in fume hood.

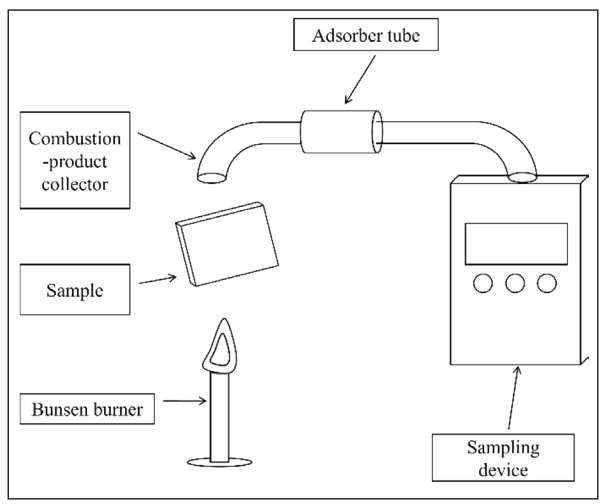


Figure 5: Measurement principle

Source: Compiled by the authors.

Before the gas chromatography examination, emission sampling must be executed on the site where the emissions of harmful compounds are released in a closed space. Since sampling is from air, atmospheric pressure, temperature and humidity must be considered in the calculations and those values are true for the day of the experiment.

Table 1: Value of influencing factors

β	1013 hPa
T_0	273 K
P	1011.38 hPa
T	292 K

Source: Compiled by the authors.

A portable gas exhauster pumps in the different gases originating from the combustion process through a short pipeline. This pipeline contains a special sample holder SKC Anasorb CSC type glass tube. The glass tube is built in the pipeline before the portable gas exhauster, thus all compounds of the smoke formed during combustion is stored. This device is transferred to a laboratory, in which, gas chromatography is conducted after preparation. Table 2 contains data about the investigated samples.

Table 2: Investigated samples

No. of sample	Name	Size	Burning time (min.)	Mass (g)
1.	$LiFePO_4$ battery housing cover	60 × 85 × 5	5:20	63.75
2.	Battery box cover	110 × 80 × 35	3:00	70.24

Source: Compiled by the authors.

Examination of battery cell cover

The mass of the battery is 2,900 g, according to its surface (1).

$$A_{cell} = 2 \times (143\ \text{mm} \times 60\ \text{mm} + 210\ \text{mm} \times 143\ \text{mm} + 210\ \text{mm} \times 60\ \text{mm}) = 102\,420\ mm^2 \quad (1)$$

The mass of the examined sample is 63.75 g, according to its area of the greatest surface (2).

$$T_{sample} = 60\ \text{mm} \times 85\ \text{mm} = 5100\ \text{mm}^2 \quad (2)$$

Ratio of the two surfaces

$$\frac{102\,420\ mm^2}{5100\ mm^2} \approx 20 \tag{3}$$

According to (1) and (2) the mass of the whole battery housing is

$$m_{housing}=20 \times 63.75\ g = 1275\ g \tag{4}$$

216 pieces of this type can be found in a heavy goods truck and their summarised mass is

$$m_{sum}= 1275\ g \times 216 = 275.4\ kg \tag{5}$$

There was no exact information about the material of the battery housing, thus it is not recorded. The cut sample was ignited with open flame ignition source (Bunsen burner). After 5 seconds, the ignition source came to a stop, the sample was capable of self-sufficient burning with great flame. Dripping was also observed, which means that liquefied plastic droplets were released during burning. After falling, they merged and continued burning. The investigated sample flowed from the sample holder, so that it was put out. Samples from flue gases were taken for 3 minutes, since after the burning process along with flame, it released gases. The burning sample and the residuals of it can be observed in the next figure.

Figure 6: Behaviour of sample during the burning process and burning residual
Source: Compiled by the authors.

Examination of battery holder cover

The mass of the battery pack cover is 7.2 kg, the 6 pieces altogether are 43.3 kg. The examination process is represented in Figure 7.

Figure 7: Investigated sample placed to ignition source

Source: Compiled by the authors.

The first part of the ignition took 5 seconds, while the sample did not catch fire. Consequently, a 15 second ignition time was required, after that it burnt with small flame, self-sufficient and soot was released. After 5 seconds, the intensity of burning increased along with grey smoke generation, without any material loss. After eliminating the heat source, before the 3 minute investigation time, burning with flames stopped; however, a glowing phenomenon and smoke generation were observed, thus 3 minutes long sampling was conducted during this experiment.

Evaluation of results

The evaluation of collected samples was conducted in Agilent Technologies 6890N Network GC system. Exploration time is 20 minutes, the solvent was carbon disulfide. The following chromatograms resulted.

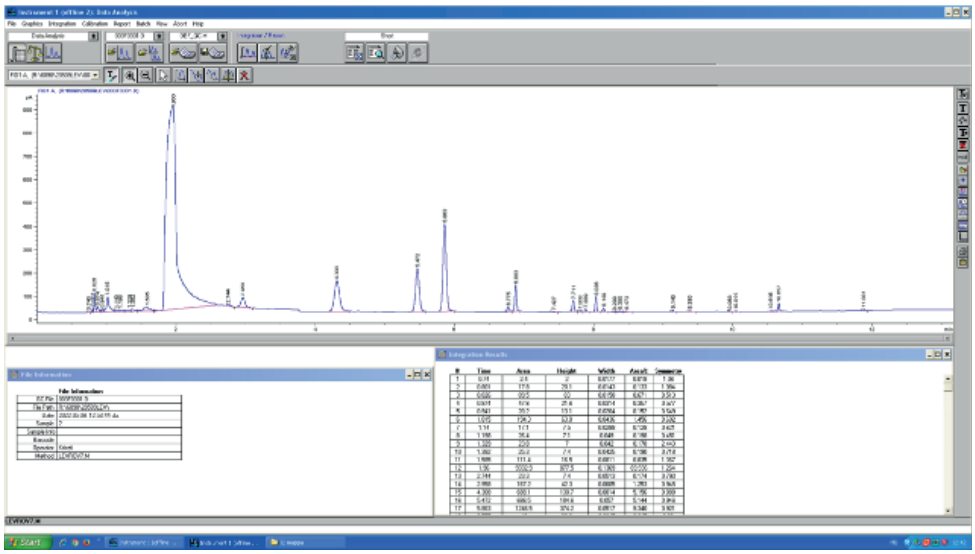


Figure 8: Chromatogram of compounds derived from the battery housing

Source: Compiled by the authors.

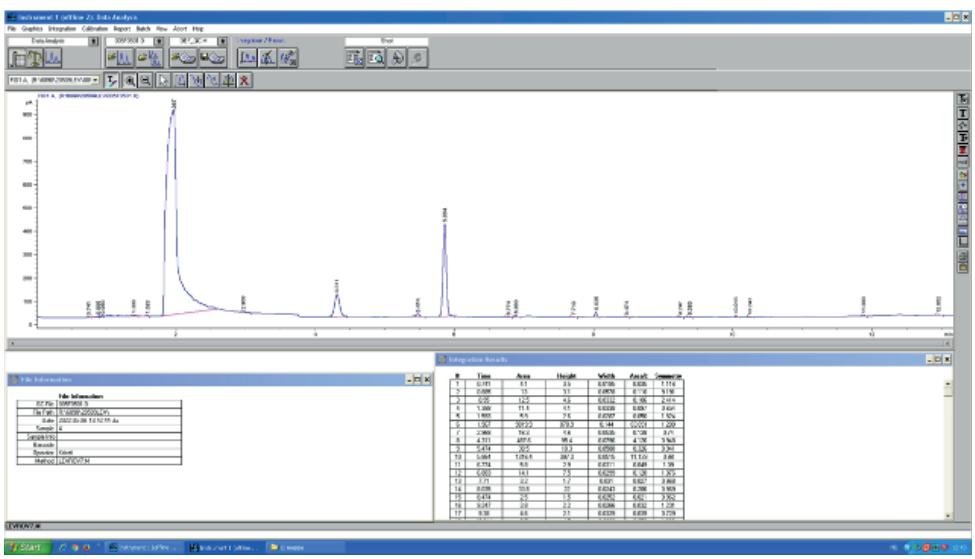


Figure 9: Chromatogram of compounds derived from the battery box cover

Source: Compiled by the authors.

To determine the different polluting compounds and their mass flow, the chromatogram of the sample is needed. Figures 8 and 9 represent the signal belonging to the searched compound, so its presence corresponding to time. This is the so-called retention time.

Concentration of compounds found in air are determined according to (6) MSZ EN 13649:2002 standard.[15]

$$c_i = \frac{m_i}{V_{cor}} \times 1000 \tag{6}$$

In the standard c_i is the concentration of the compound in gas sample (mg/m3), m_i is the mass of the compound in gas sample (mg); V_{cor} means the volume of the sample at normal state (273 K and 1013 hPa) for dry gas. To determine the concentration of normal state sample is conducted according to (7)

$$v_{cor} = V \times \frac{p_0}{p} \times \frac{T}{T_0} \tag{7}$$

in which V is the measured volume of dry gas sample, p is the pressure of sample air (hPa), p_0 = 1013 hPa, T is the real temperature of waste gas (K), T_0 = 273 K.

Table 3: Data of present compounds to determine the mass flow of housing and cover

Sample	**Cell cover**	**Housing cover**
Measured volume of dry gas sample (l)	2 l	2 l
Pressure of sample air (hPa)	1011.38	
p_0 (hPa)	1013	
T_0 (K)	273	
Real temperature of waste gas (K)	292	
$m_{benzole}$ (mg)	0.036	0.002
$m_{toluene}$ (mg)	0.042	0.003
$m_{ethylbenzene}$ (mg)	0.002	–
$m_{xylenes}$ (mg)	0.022	0.006
m_{cumene} (mg)	0.002	–
$m_{propylbenzene}$ (mg)	0.001	–
$m_{1,2,3\text{-}trimethylebenzene}$ (mg)	0.001	–
$m_{ethanol}$ (mg)	0.025	–
$m_{isopropanol}$ (mg)	0.074	–
$m_{acetone}$ (mg)	0.008	0.004
$m_{ethyl\text{-}acetate}$ (mg)	0.088	–
$m_{isobutyl\text{-}acetate}$ (mg)	0.079	–

Source: Compiled by the authors.

The volume of sample (V_{cor}) is in unit litre, at normal state p_0 = 1013 hPa and T_0 = 273 K for dry gas is according to (8) and (9)

$$V_{cor} = V \times \frac{p_0}{p} \times \frac{T}{T_0} = 5.3 \times 2 \times \frac{1013\ hPa}{1011.38\ hPa} \times \frac{292K}{273K} = 11.35\ l \tag{8}$$

[15] EN 13649:2002 Stationary source emissions – Determination of the mass concentration of individual gaseous organic compounds – Activated carbon and solvent desorption method.

$$V_{cor} = V \times \frac{p_0}{p} \times \frac{T}{T_0} = 3 \times 2 \times \frac{1013}{1011.38} \times \frac{292}{273} = 7.08\ l \quad (9)$$

Concentrations of compounds found in the air sample are represented in mg/m^3 in Table 4 and 5.

The concentration of the compounds found in the sample are calculated from the following equation with the values respected to all found compounds.

$$c_{compound} = \frac{m_i}{V_{cor}} \times 1000 \quad (10)$$

Table 4: Concentration of compounds in air sample in mg/m^3, in case of battery cell cover

Compound	**Concentration** $\left[\frac{mg}{m^3}\right]$
Benzol	3.172
Toluene	3.7
Ethylbenzene	0.176
Xylenes	1.938
Cumene	0.176
Propyl benzene	0.088
1,2,3-trimethylebenzene	0.088
Ethanol	2.202
Isopropanol	6.519
Acetone	0.704
Ethyl-acetate	7.753
Isobutyl-acetate	6.96
Isoamyl-methyl-ketone	2.555

Source: Compiled by the authors.

Table 5: Concentration of compounds in air sample in mg/m^3, in case of battery housing

Compound	**Concentration** $\left[\frac{mg}{m^3}\right]$
Benzol	0.282
Toluene	0.423
Xylenes	0.847
Acetone	0.565

Source: Compiled by the authors.

Compounds found in Table 5 were calculated with 10th equations with the unique value of the battery housing part.

It is important to remark, that in Table 4 and 5 concentrations are the values of compounds released during the combustion of samples described in Table 1. Their normal exposure limit values are determined by the World Health Organization, in the EU it is 1272/2008/EK (CLP) decree. If the whole battery system is considered, concentrations can be calculated in case the whole battery system is on fire (Table 6).

Table 6: Calculated concentration in case of 216 pcs of cells and 6 pcs of housing

Sample	1 cover	216 covers	1 housing	6 housings
Mass (kg)	1.275	275.4	7.227	43.3
Benzol	63.44	13,703	18.110	108.66
Toluene	74	15,984	27.165	162.99
Ethylbenzene	3.52	760.32	–	–
Xylenes	7.26	1,568	54.331	325.986
Cumene	3.52	760.32	–	–
Propyl benzene	1.76	380.16	–	–
1,2,3-trimethylebenzene	1.76	380.16	–	–
Ethanol	40.4	8,726.4	–	–
Isopropanol	130.38	2,8162	–	–
Acetone	14.08	3,041.28	36.220	217.32
Ethyl-acetate	155.06	33,492	–	–
Isobutyl-acetate	139.2	30,067	–	–
Isoamyl-methyl-ketone	51.1	11,037	–	–

Note: Compounds in air sample are represented in the unit of mg/m^3.

Source: Compiled by the authors.

Data represented in the table above exceed the boundary limits determined in the belonging law[16] to a great extent. All the identified gases are toxic, strongly harm human health and environment as well.

Summary

In our research work, the change of plastic cover of batteries used in an electrified heavy goods truck was investigated in laboratory burning tests. Furthermore, samples were taken from released burning gases, which were analysed, especially their compounds with gas chromatography. Sampling of the released fumes and their analysis were conducted according to MSZ standards. Sample preparation was conducted with desorption, the analysis was done with GC-FID method. During the evaluation, it was concluded that during the burning process several severe gases are released that can be harmful to the environment and to human health as well. Values presented in Table 6 exceed boundary limits determined in law. Due to the increase in electric car park, the number of accidents happening in public roads is increasing, thus the number of involved people is also increasing, as a reason of this, it is important to note that the effective and quick fire extinguishing in these cases can mean the decrease in the harmful effect of released fumes. Electrolytes of the batteries were not investigated in our examinations; these are planned to be investigated in our further research work.

[16] Government Decree 4/2011 (I.14.) on the limit values of air pollution levels and emission limit values of stationary air pollutants; EN 13649:2002 Stationary source emissions – Determination of the mass concentration of individual gaseous organic compounds – Activated carbon and solvent desorption method.

References

Aydemir, Muhammed – Glodde, Arne – Mooy, Robert – Bach, Gordon (2017): Increasing Productivity in Assembling Z-Folded Electrode-Separator-Composites for Lithium-Ion Batteries. *CIRP Annals,* 66(1), 25–28. Online: https://doi.org/10.1016/j.cirp.2017.04.096

Buysse, Claire – Miller, Josh (2021): Transport Could Burn Up the EU's Entire Carbon Budget. *The International Council on Clean Transportation,* 09 April 2021. Online: https://theicct.org/transport-could-burn-up-the-eus-entire-carbon-budget/

Dorsz, Adam – Lewandowski, Mirosław (2020): Analysis of Fire Hazards Associated with the Operation of Electric Vehicles in Enclosed Structures. *Energies,* 15(11). Online: https://doi.org/10.3390/en15010011

Düser, Dominic – Schramm, Thomas (2019): Battery Housing for Lithium-ion Batteries. *ATZheavy Duty Worldwide,* 12(3), 36–39. Online: https://doi.org/10.1007/s41321-019-0036-4

Egelhaaf, Markus – Wolpert, Dieter – Lange, Thomas (2014): Fire Fighting of Battery Electric Vehicle Fires. In Andersson, Petra –Sundström, Björn (eds.): *Proceedings from 3rd International Conference on Fires in Vehicles – FIVE 2014.* Borås: SP Technical Research Institute of Sweden. 221–230.

European Commission (2021): *Reducing CO Emissions from Heavy-duty Vehicles.* Online: https://ec.europa.eu/clima/eu-action/transport-emissions/road-transport-reducing-co2-emissions-vehicles/reducing-co2-emissions-heavy-duty-vehicles_en

Larsson, Fredrik – Andersson, Petra – Mellander, Bengt-Erik (2014): Are Electric Vehicles Safer than Combustion Engine Vehicles? In Sandén, Björn – Wallgren, Pontus (eds.): *Systems Perspectives on Electromobility.* Göteborg: Chalmers University of Technology. 33–44.

Larsson, Fredrik – Andersson, Petra – Blomqvist, Per – Mellander, Bengt-Erik (2017): Toxic Fluoride Gas Emissions from Lithium-ion Battery Fires. *Scientific Reports,* 7, 1–14. Online: https://doi.org/10.1038/s41598-017-09784-z

Schmerler, Rico – Gebken, Tobias – Kalka, Sebastian – Reincke, Tobias (2017): Multi-functional Battery Housing for Electric Vehicles. *Lightweight Design Worldwide,* 10(5), 26–31. Online: https://doi.org/10.1007/s41777-017-0043-z

Sun, Peiyi – Bisschop, Roeland – Niu, Huichang – Huang, Xinyan (2020): A Review of Battery Fires in Electric Vehicles. *Fire Technology,* 56(4), 1361–1410. Online: https://doi.org/10.1007/s10694-019-00944-3

AARMS Vol. 22, No. 3 (2023) 91–107.

10.32565/aarms.2023.3.6

Digitalisation in the Western Balkans[1]

Tibor ÖRDÖGH[2]

Digitalisation has been a top priority in the Western Balkans for the past decade. The European Union, recognising it as a driver of economic growth, is encouraging the countries of the region to invest in digital development from 2017. The necessary legislation has been adopted, the institutions responsible for this have been set up and developments have been launched to provide citizens with a wide range of services. At different times, all the countries in the region have set up their own e-public administration portals, which they are working to improve with their own resources and with the support of the European Union. A strong emphasis is being placed on developing the digital skills of the younger generation, as this kind of relationship between the state and its citizens will become the new norm for the generations to come. However, not only the citizens, but also economic operators will benefit from the transition, with reduced costs and faster turnaround times, which could also be an advantage for economic operators.

Keywords: *digitalisation, Western Balkans, e-public administration*

Introduction

The digitalisation of public administrations is a process whereby the previous paper-based, multi-step process is being replaced by online administration. Western European countries have been developing their e-public administration activities for several decades now, while the more backward countries of the Western Balkans have only recently started to introduce eGovernment. Digitalisation is transforming many areas of social and economic life, such as communication, shopping habits and education. And, not least for the topic at hand, the relationship with the state.

In the majority of the Western Balkan countries, the introduction of e-public administration has been linked to the spread of the Covid-19 pandemic, which has led to an even faster pace of development, so that at least this one positive consequence of the health emergency for the region can be mentioned. Progress has been made in a number

[1] This publication was prepared in the framework of Project no. TKP2021-NKTA-51, which has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NKTA funding scheme.

[2] Associate Professor, University of Public Service, Department of European Studies, Faculty of Public Governance and International Studies, e-mail: ordogh.tibor@uni-nke.hu

of areas in recent years, covering a wide range of areas such as the digitalisation of public administration, education and healthcare systems.

It is important to note that the Internet penetration rate in the region has been quite high in the last few years, and has continued to increase. Figure 1 shows that in 2020, Albania had the lowest internet penetration among the states of the region, with 75.2 percent of the Albanian population using some form of Internet. Perhaps surprisingly, the highest figure, 96.4 percent, was measured in Kosovo. However, some argue that this is not surprising, as in countries where the normal system is slow, citizens are more confident in using online e-public administration systems.

Table 1: Internet penetration in the Western Balkans

	Albania	**Kosovo**	**Montenegro**	**North Macedonia**	**Serbia**
2019	73.5%	93.2%	74.3%	81.8%	80.1%
2020	75.2%	96.4%	80.3%	79.9%	81.0%

Source: Jashari 2022: 13.

My hypothesis is that since the 2017 agreement, we have seen a big step forward in the development of e-public administration in the region. My study is divided into two parts. In the first half, I will present the European Union's relationship with the region in relation to digitalisation. In the other half of the paper, I will summarise the steps and achievements of the Western Balkan countries so far. Albania, North Macedonia, Kosovo, Montenegro and Serbia are the countries under study. Bosnia and Herzegovina is unfortunately excluded from the analysis due to lack of available data.

The role of the European Union – Digital Agenda

In July 2017, as the next step in the European integration of the Western Balkans and as part of the Berlin Process,[3] the EU – Western Balkans Summit[4] was held in Trieste. The aim of the summit was to establish new directions for the region in the process of catching-up as well as to identify key areas where cooperation could be enhanced. As part of the agreed multi-annual scheme,[5] the Regional Economic Area formed by the Western Balkan states foresaw cooperation in four areas, with digitalisation as one of the pillars.[6]

The Digital Agenda for the Western Balkans[7] was a joint vision of the six countries of the region and the European Commission, presented on 6 February 2018 as one of the six flagship initiatives of the commitment objectives in the Communication on a credible enlargement perspective and enhanced EU engagement with the Western Balkans. In May 2018, all six regional states pledged their support for the initiative, and in June, the EU

3 Momčilo 2020.
4 EWB 2017.
5 Shift2Rail Joint Undertaking 2020.
6 European Commission 2017.
7 Western Balkans Info Hub 2018.

formally launched its scheme at the Sofia Summit.[8] In April 2019, at the Western Balkans Digital Summit in Poznan,[9] participants committed to launching the Digital Agenda, which included a roadmap for reducing roaming charges between the EU and its Western Balkan partners.

The Digital Agenda for the Western Balkans aims to support the region's transition to a digital economy, highlighting the benefits of digital transformation, such as faster economic growth, more jobs and better services.[10] In 2018, the six Western Balkan countries – Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia – committed to the following:

1. Investment into broadband connection:
   A good digital infrastructure is essential for the roll-out of broadband in the Western Balkans. Through the Western Balkans Investment Framework (WBIF), €30 million of EU funding will be made available to build broadband infrastructure in the region to mobilise strategic investments and promote socio-economic growth. A technical assistance package has already been approved for Albania as one of the first investment packages under the WBIF.[11] To achieve this objective, two tasks have been identified: harmonisation of roaming tariffs and deployment of broadband internet.
   a) With the new agreement on regional roaming charges, at the Digital Assembly in Belgrade (4–5 April 2019), the six participating countries agreed to extend the previous agreement on the subject from four to six countries (with the accession of Albania and Kosovo) and to gradually reduce price rates until 2021. "38 telecommunication operators from the EU and the Western Balkans have agreed to make data roaming between the Western Balkans and the EU more affordable for citizens and businesses in both regions. Maximum retail price levels ('price caps') for 1 gigabyte will decrease from October 2023 to 2028 as follows: €18 from 1 October 2023, €14 from 2026, and €9 from 2028."[12]
      In case of roaming rules between the EU and the Western Balkan states, it was pointed out that there is no legal basis for expectation and implementation until their EU accession. The establishment of voluntary, commercial agreements between operators is the basis for, and the need to meet the following expectations in the economic environment for telecoms operators: equal and fair treatment; rule of law, enforcement of existing rules; harmonisation and market-based spectrum and construction license fees, etc.; rationalisation and simplification of investment and deployment procedures.
   b) In terms of broadband access, the huge digital divide between the Western Balkans and the EU are pointed out. Remote areas are not well-connected and generally have low average connection speed. Broadband is at the heart of digital transformation (e.g. eGov, eHealth, digitisation of the industry, research and innovation, small and medium enterprises and startups, education, digital

8 European Council 2018.
9 European Commission 2019.
10 Western Balkans Info Hub 2018.
11 European Commission 2018.
12 European Commission 2023.

skills). Its development is crucial for the region's economic growth. Businesses can reduce their costs by relocating to rural regions, increasing local employment opportunities, tax revenues and investment. Future developments (smart cities, autonomous vehicles, 5G deployment, etc.) will be based on broadband access.
The discussions on 5G development in the region started in October 2020, including kick starting the implementation of the Memorandum of Understanding on 5G Roadmap for Digital Transformation in the Western Balkans signed during the third WB Digital Summit held in Tirana in October 2020. In three Western Balkan economies all three 5G pioneer bands are free (Montenegro, North Macedonia and Serbia) and in two economies only 700 MHz band is not freed up (Albania and Kosovo). Three economies are preparing for 5G auction in 2022.[13]

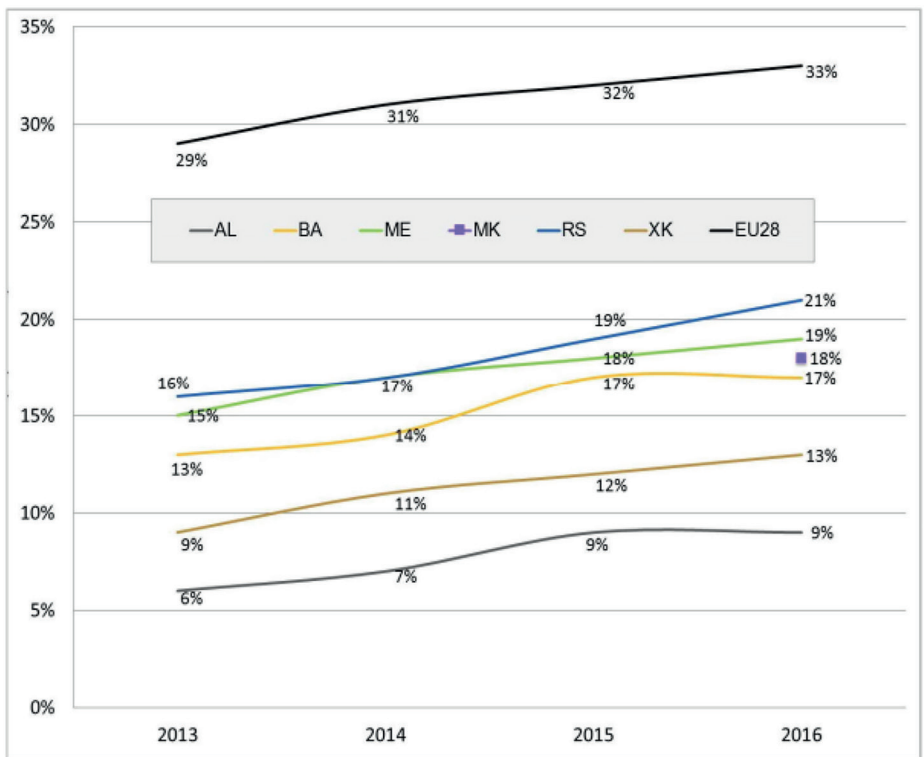


Figure 1: Broadband internet access (proportional to population)

Source: Compiled by the author.

2. Increasing cybersecurity, trust and digitisation of the industry:
The EU and the Western Balkans share a common goal of improving online security and trust. The Digital Agenda for the Western Balkans supports capacity building

[13] Regional Cooperation Council s. a.

in trust and security and the digitalisation of industry in the Western Balkans to ensure that all sectors benefit from digital innovation.[14] The cooperation aims to adopt regional cybersecurity projects to enhance cyber resilience. Digital Innovation Centers – One Stop Shops where firms (especially SMEs and startups) – can access technology testing, funding advice, market intelligence and networking opportunities.

3. Strengthening the digital economy and society:
   The Digital Agenda will support the use of e-government, e-procurement and e-health tools and help citizens to develop their digital skills. This is done by supporting the participation and representation of the Western Balkans in EU initiatives and events. This has included the 2018 Startup Europe Summit in Sofia, which enabled regional startups to network with major European hubs; opening digital internships for students and young people in the Western Balkans to gain first-hand training in digital areas; opening EU Code Week to all Western Balkan partners, bringing coding skills and digital literacy to the region.[15]
   Relevant areas of harmonisation with the EU include: eGovernment Action Plan (public administration); ISA scheme for digital public services and cross-border interoperability; eProcurement; eHealth network.
   Digital skills development is being implemented through the following projects in the region: Code Week; developing coding skills and digital literacy; Digital Opportunity Traineeships for students.
4. Promoting research and innovation:
   The Digital Agenda will facilitate the setting up of national research facilities and the development of state-of-the-art e-infrastructures in the Western Balkans as well as integrating them into an emerging digital European Research Area. This effort will provide world-class training for a new generation of researchers and engineers and foster interdisciplinary collaboration across Europe.[16]

Following a decision in 2017, the European Union also provided funding for the development of digital infrastructure through the Western Balkans Investment Framework (WBIF). In December 2019, the scope of support was extended to cover the interconnection of administrative, research and education networks, as well as high-performance computing. The new sector was developed in line with the European Commission's policies and strategies, the Digital Agenda for the Western Balkans, the Southeast Europe 2020 strategy and the infrastructure needs identified in the ONE Project. The organisation has supported 13 projects in 2022 with an investment value of up to €682,399,619.[17]

[14] European Commission 2018.
[15] European Commission 2018.
[16] European Commission 2018.
[17] WBIF s. a.

Digitalisation and the Western Balkans

Among the challenges facing the region, the most significant factor influencing economic development is the advance of digitalisation. A main question is the extent to which citizens can manage their affairs online and the interconnectivity of these e-public administration systems. Last but not least, the economic aspect should be mentioned, as in the 21st century, electronic administration allows businesses to save costs and communicate quickly. To this end, the Western Balkan countries have introduced and developed their own e-public administration portals to serve both 'types of customers'.

Table 2: e-Government portals in the Western Balkans

Country	E-gov portal
Albania	https://e-albania.al/
North Macedonia	www.uslugi.gov.mk/
Kosovo	https://ekosova.rks-gov.net/
Montenegro	www.euprava.me/en
Serbia	https://euprava.gov.rs/

Source: Compiled by the author.

Digitalisation is both an opportunity and a challenge for governments, as secure use requires the right legal framework and safeguards to protect data against cyberattacks. The countries of the region have adopted a number of standards for digitisation, which are reflected in legislation in several areas.

Table 3: Legislation concerning digitalisation in the Western Balkans

Country	Legislative background
Albania	Law on Electronic Signatures Data Protection Law Law on Electronic Communications Law on Electronic Commerce Law on Electronic Documents Law on State Database
North Macedonia	Law on e-Government and e-Services Law on Electronic Documents, Electronic Identification and Trust Services Law on the Central Population Register Law on the Protection of Personal Data Law on Free Access to Public Information
Kosovo	Law on the Protection of Personal Data Law on Access to Public Documents Law on Governmental Bodies of the Information Society Law on Electronic Communications Regulation on Electronic Databases Law on Local Self-Government Regulation on Minimum Requirements for Public Consultation Draft Law on Digital Identification and Trust Services in Electronic Transactions Draft Law on Cybersecurity

Country	Legislative background
Montenegro	Law on Electronic Administration Law on Electronic Identification and Electronic Signature Law on Information Society Law on Electronic Documents
Serbia	Law on Electronic Communications Law on Electronic Documents, Electronic Identification and Security Services Law on Electronic Commerce Law on Electronic Administration Law on Free Access to Information of Public Interest Act on the Protection of Personal Data

Source: Jashari 2022: 21.

As we reviewed the regulatory background and the portals that operate, the remainder of the paper will describe the practical operation, positive and negative experiences of each state.

Albania

In Albania, a total of 7,705,068 applications for e-services have been made through the separate platforms provided by the different institutions, and a total of 1,210,093 citizens and businesses have applied through the e-Albania portal.[18]

In its Digital Agenda Horizontal Strategy 2015–2020,[19] Albania has set the objective of increasing and promoting the use of e-services, promoting ICT in education, consolidating digital infrastructure. During this period, public attention has focused on the creation and operation of a government portal through which citizens and businesses can access public e-services. The continuation of this strategy is still to be developed for the period 2021–2026.[20]

For the practical implementation of e-public administration in Albania, the government has set up the institutions responsible for its efficiency and legality: the National Authority for Electronic Certification and Cybersecurity (NAECCS), the National Agency for Information Society (NAIS), the Ministry of Energy and Infrastructure, the Ministry of Finance and Economy, the Ministry of Education, Sports and Youth, the Public Services Information Centre and the Commissioner for the Right of Information and Personal Data Protection.[21]

e-Albania has completed 95% of the public e-services, reaching 1,217 services, of which 300 are business-related. Currently, the e-Albania portal is the only platform in the region where citizens can receive their personal public services electronically.[22]

The ease of access to services in Albania is demonstrated by the widespread use of e-Albania. In 2020, a total of 7,705,068 e-service requests were submitted by

[18] Jashari 2022: 13.
[19] Ministry of Innovation and Public Administration 2018.
[20] Jashari 2022: 16.
[21] Jashari 2022: 19.
[22] Jashari 2022: 23.

1,210,093 citizens and businesses. A total of 12,000 administrative staff have been trained to deliver digitised, electronically signed public services, as well as 2,000 employee-based customer contact staff to help citizens apply online for the services they require from the public administration. 180 public institutions have created a total of 13 million official electronic documents to assist citizens. To increase the number of portal users and facilitate the understanding of the digital procedures for accessing public services online, NAIS aims to produce 132 promotional and training videos, mainly related to e-services, 141 e-Albania infographics and instructions on how to use specific e-services, and 30 explanatory media materials by the end of 2022.[23]

According to the Law on Cybersecurity,[24] NAECCS is the authority responsible for cybersecurity in Albania, whose tasks include contributing to the development, implementation and monitoring of law enforcement in the field of cybersecurity. According to the Commissioner for Information Rights and Personal Data Protection,[25] 308 complaints from citizens have been handled this year about the misuse of their personal data for marketing purposes, including online platforms during the Covid-19 pandemic. The report also shows that there are problems with the implementation of all steps of data management by public institutions, lack of legal and technical knowledge, lack of management of legal guarantees based on contractual relationships, lack of training of staff dealing with data management, lack of a data processing strategy. As regards the reporting of cybercrime, the responsibility for mitigating cybercrime lies with the State Police in conjunction with its associated institutions, while cyber incidents are dealt with by cybersecurity institutions, in this case infrastructure operators.[26] An OECD report praised Albania for enhancing intragovernmental cooperation, emphasising the cross-cutting character of ICT in its development strategies, and allocating resources towards the implementation of its digital strategy. Despite the proliferation of such policies, however, the country is currently the 5th largest source of cybercrime in Europe, suffering at least 1.3 million cyberattacks yearly.[27]

Kosovo

Kosovo launched its national e-services portal in February 2021, with a total of 5,945 registered citizens and businesses who have used 57,414 services through the site, mainly in the areas of tax, police and healthcare.[28]

Kosovo has also demonstrated political will and strategic commitment through the adoption and implementation of legislation, such as the Open Government Partnership (OGP). A strategy has been developed in the areas of cybersecurity, public administration

[23] Jashari 2022: 29.
[24] CMS s. a.
[25] *Commissioner for the Right of Information and Personal Data Protection Report* 2020.
[26] Jashari 2022: 32.
[27] OECD 2018.
[28] Jashari 2022: 13.

reform, e-government, with the aim of promoting an interoperability system through the e-Kosovo portal.[29]

Within the Information Society Agency, the e-Government Development Department of Kosovo is responsible for the implementation of e-Government, which consists of two sectors: the policy, monitoring and analysis sector and the sector of online support and promotion of e-Government.[30]

Kosovo has seen significant developments taking place since 2020: 1. the development of the e-Kosovo national e-services portal, which is continuously being expanded with new e-services in cooperation with other institutions; 2. the creation of an interoperability platform that allows secure data exchange between several institutions, such as the Kosovo Business Registration Agency, the Civil Registry Agency, the Kosovo Tax Authority, the Customs, the Kosovo Cadastral Agency, etc.; 3. Draft Law on electronic identification and reliable services in electronic transactions. These recent developments are promising so far, though they are only the first steps towards the widespread use of e-services.[31]

In Kosovo, the Kosovo Institute of Public Administration (IPAK) within the Ministry of the Interior and Public Administration is responsible for building the capacity of civil servants and increasing the sustainability of the civil service. The IPAK trains civil servants responsible for IT management in individual institutions, but attendance at these training courses is not very high as they are not mandatory and civil servants are not encouraged to participate as, in terms of ICT training for the general public, in addition to the many projects implemented by ODK and other Kosovo NGOs, the ongoing "KODE" project,[32] implemented by the Ministry of Economy with the following main components, and aiming at addressing ICT capacity is publicly available: funding for Digital Connectivity, National Spectrum Monitoring, training for unemployed and underemployed young people through the Youth Online and Upward (YOU) scheme, and the National Research and Education Network.[33]

Kosovo launched a national e-services portal in February 2021 with a low number of services due to 1. the identification of e-services currently offered at central and local levels, which requires time and extensive research; 2. the need to inform public institutions and facilitate the migration of their e-services from their websites to e-Kosovo; and 3. the lack of legislation on digital signature/stamping, which hinders the full online availability of certain documents. As this portal is relatively new, there has not been a large-scale promotional campaign, which is also the case for other e-services offered by other public institutions.[34]

In Kosovo, the government body responsible for cybersecurity is the Agency for Information and Society within the Directorate for Operations and Security. As no legislation directly addresses cybersecurity, a Law on Cybersecurity is currently being drafted. The law foresees the creation of a State Cybersecurity Agency responsible for

[29] Jashari 2022: 16.
[30] Jashari 2022: 19.
[31] Jashari 2022: 23.
[32] Kosovo Digital Economy Project s. a.
[33] Jashari 2022: 26.
[34] Jashari 2022: 29.

overseeing, monitoring and defining cybersecurity standards, and the creation of two state teams (one for cyber emergencies and the other for cybersecurity incidents).[35]

Montenegro

In Montenegro, e-services have been available since 2017, with a total of 491 applications submitted through the e-services portal in the first half of 2020.[36]

Despite changes in the structure of government in Montenegro, the quality of eGovernment remains a priority. The adopted Montenegrin strategies supporting the Digital Agenda are the Public Administration Reform Strategy 2016–2020, the Cybersecurity Strategy 2018–2021, the Information Society Development by 2020 and the OGP National Scheme 2018–2020.[37]

In Montenegro, the Ministry of Public Administration, Digital Society and Media (MPADSM) is responsible for implementation. The Ministry also deals with digital transformation in the Montenegrin public administration system, aiming at better quality of services and provision of new digital services. The other ministries involved in the process are the Ministry of Finance and Social Welfare, the Ministry of the Interior, the Ministry of Health and the Ministry of Education, Science, Culture and Sports.[38]

Some e-services are offered through the national e-services portal and some through the websites of individual institutions. Montenegro also uses a document management system, where more than 680,000 cases and more than one million documents have been registered so far. Recently, significant progress has been made in the use of digital signatures and electronic identification. In the past, digital certificates were predominantly used by companies in their communication with the tax authorities (20,000 companies in 2018), but not so much by individuals (400 individuals in 2018). With the introduction of the new chip ID cards in 2020 and the planned amendments to the Electronic Documents Act, negotiators estimate that around 70,000 people (more than 10% of the population) have new electronic ID cards.[39]

Data on the specific forms of developing and upgrading the digital skills of civil servants or citizens has yet to be collected. The MPADSM objectives include the development of common information systems: electronic identity system, electronic payment system for administrative and other fees, electronic data exchange system, development and application of e-administration, development and application of modern e-government portal and training on the use of common information systems.[40]

In Montenegro, a positive development in promoting and improving access to e-services is the upgrade of the government website launched in mid-May 2021. The new layout for the website is mainly focused on greater citizen orientation, better presentation

35 Vllahiu 2022.
36 Jashari 2022: 13.
37 Jashari 2022: 16.
38 Jashari 2022: 19.
39 Jashari 2022: 23.
40 Jashari 2022: 26.

of services, information and news about government meetings, ministry news, etc. In addition, most e-services can be found on the e-government portal (www.euprava.me), which currently contains 596 services from 52 institutions, of which 187 can be fully completed electronically. The portal has a "Frequently Asked Questions" section, which contains only five questions, but there is customer service available via the contact person's e-mail address and a short guide on how to use the portal. Unfortunately, it is currently not possible to file a complaint via the portal. The design of the portal is outdated and not very user-friendly compared to the new government website.[41]

The Montenegrin Directorate for Information Security and Computer Identity (CIRT) is one of the key mechanisms in the field of information and cybersecurity. One of the most significant achievements in this area is the adoption of the Law on Information Security, which transposed the EU Directive on Network and Information Security. In addition, the Regulation on Information Security Measures and the Law on the Designation and Protection of Critical Infrastructures have been adopted. The strategic planning of cybersecurity in Montenegro was based on the 2018–2021 Cybersecurity Strategy, which defines the mechanisms and tools for the implementation of national security interests, and on the work of the Information Security Council, which was established in 2019. When it comes to changes in this area, the most important compared to the baseline report is that the activities of the CIRT teams have been transferred to the competence of the Qualified Directorate for Data Protection, which operates within the Ministry of Defence, according to the amendments to the Law on Data Protection adopted at the end of 2020.[42] The government has not adopted a new Cybersecurity Strategy after the last one became outdated in 2021. In July 2021, the then Minister of Public Administration, Digital Society and Media, Tamara Srzentic, said that the government would improve its administrative capacities in the cybersecurity sector, and push for international cooperation and staff education.[43]

North Macedonia

In North Macedonia, the national e-services system was launched only in December 2019. In 2020, there were 17,241 registered users on the portal, and this number had doubled by 2021 (34,834 registered users). No information on the number of cases opened was provided by the North Macedonian authorities.[44]

North Macedonia has a number of documents that provide relevant guidance, but these are considered outdated rules. New opportunities to support the Digital Agenda are provided by the scheme for 2021–2023[45] adopted by the Ministry of Finance and the

41 Jashari 2022: 29.
42 Jashari 2022: 32–33.
43 Kajosevic 2022.
44 Jashari 2022: 14.
45 *Economic Reform Program for the period 2021–2023.*

strategic plan for 2021–2023 of the Ministry of Information Society and Administration (MISA). The preparation of the National Strategy[46] on Artificial Intelligence is underway.[47]

In case of North Macedonia, MISA is the central body in charge of the coordination process, with its own completed projects, strategic plan and annual work scheme.[48] Its activities are related to the development and promotion of the information society, as well as to the integrated information and communication network, databases, interconnection and exchange of information, security aspects and infrastructure development.[49]

MISA has developed a new document management system where, according to the survey, only 9 out of 101 institutions responding to the survey noted that they had a DMS. Nevertheless, North Macedonia has a national interoperability framework covering legal, organisational, semantic and technical interoperability.[50] In addition, the Law on Electronic Management and Services and the Law on Electronic Documents, Electronic Identification and Trust Services (MISA) issued by the competent authority are at an advanced stage of implementation.[51]

Research shows that digital skills are lacking not only among the general population of North Macedonia, but also in its public administration. With this level of digital skills, the transition to fully digital operations and services will be neither quick nor easy, and the state needs to adopt a strategic approach promptly for the mitigation of the problem.[52] The latest European Commission progress report[53] on the country states that the drawing-up of a Digital Skills Development Strategy is on its way and digital literacy is a priority in the new Education Strategy, which is likely to be coordinated by the Ministry of Education and Science (although MISA may turn out to be the coordinator). In this respect, a National ICT Strategy 2021–2025 is to be adopted, but it is still yet to occur.[54]

In North Macedonia, the national e-services portal is being promoted as the main tool for citizens to access e-services with a total of 151 e-services. Accordingly, the concept of "One Stop Shop for services and e-services intermediary" is a temporary or complementary solution that would allow all citizens to access e-services quickly and easily. In line with this, the implementation of the DA is being monitored by a strong NGO sector, of which the Metamorphosis Foundation for Internet and Society and the Center for Change Management stand out as two specialised NGOs that have carried out a number of research projects. Through their research and publications, they have a significant influence on the collection of data and the publication of research results that allow the country to be measured and compared with other countries. However, the institutions have made very little effort to promote the portal and the e-services offered through it.[55]

---

46 *National Strategy for Artificial Intelligence* s. a.
47 Jashari 2022: 16–17.
48 *North Macedonia Scheme Regarding e-Governance Coordination* 2020.
49 Jashari 2022: 19.
50 *North Macedonia National Operability Framework* s. a.
51 Jashari 2022: 23.
52 ITU 2021.
53 European Commission 2020.
54 Jashari 2022: 26.
55 Jashari 2022: 30.

North Macedonia has a National Cybersecurity Strategy[56] for the Republic of Macedonia 2018–2022. The rules on the security and integrity of networks are set by the Electronic Communications Agency (AEC) with the rules to ensure the security and integrity of networks, public electronic communications networks and services and actions that operators must take in the event of a personal security breach, dated 2015 and amended in 2019. In addition, the Electronic Communications Act established the National Centre for Computer Incident Response, MKD-CIRT, as a separate entity. It is the department of the AEC that institutionalises the protection of network and information security, especially for entities with critical infrastructure.[57]

Serbia

As of April 2020, the number of registered users of the Serbian eGovernment portal has skyrocketed from 17,857 to 1,026,347, representing 15% of the country's population. However, the number of services provided has not changed compared to the previous period, with an average of 76,028 requests per month.[58]

Serbia is showing political will and strategic commitment to move forward in the field of eGovernment. Serbia has adopted the eGovernment Development Scheme and Action Plan for 2020–2022, which paves the way for further development of eGovernment.[59] The scheme is expected to deliver 300 new e-services to citizens and the economy over the next two years.[60]

In Serbia, the main body overseeing and implementing e-government is the Information Technology and e-Government Agency. The Office is responsible for the design, harmonisation, development and operation of e-public administration and information systems and infrastructure for public administrations and government services.[61] The preparation of the legislative framework is the responsibility of two ministries: the Ministry of State Administration and Local Government, which is in charge of administrative reform and e-government, and the Digital Agenda Department of the Ministry of Trade, Tourism and Telecommunications.[62]

In contrast, Serbia's eGovernment portal was launched in 2010 and now has 1,026,347 registered users. In 2020, the portal underwent a major overhaul, with a two-step authentication process to improve the security of user profiles, a new design and enhanced functionality. More importantly, the portal has linked 15 different public registers and made them accessible to users.[63]

---

56 *North Macedonia National Cybersecurity Strategy of the Republic of Macedonia 2018–2022.*
57 Jashari 2022: 33.
58 Jashari 2022: 14.
59 *eGovernment Development Scheme* 2020.
60 Jashari 2022: 17.
61 *Office for IT and Government in Serbia* s. a.
62 Jashari 2022: 19.
63 Jashari 2022: 23–24.

Serbia is the only country in the region with a strategic approach to digital literacy, i.e. The Digital Skills Strategy 2020–2024.[64] It aims to develop the digital skills of citizens with the aim of fully exploiting the potential of information and communication technologies to improve the level of standard and quality of services.

The latest information on digital literacy for 2020 shows that 51% of the population of Serbia is digitally illiterate, 15% is only partially literate, leaving the remaining 34% of the population fully literate. As for the gender gap, the female population has 4% higher digital illiteracy than the male population.[65]

In 2020, the Serbian e-government portal underwent a major overhaul, improving online security for profile users and adapting the portal to the parameters for accessing services via mobile platforms. With around 15% of the population registered as users, the number of users has increased by 2% in the last year. The portal lists services provided by 124 institutions at local and national level, with one of the most frequently used services being the registration of children in kindergarten, which was used by 47,964 parents.[66]

Meanwhile, Serbia has recently renewed the Strategy for the Development of the Information Society and Information Security[67] in the Republic of Serbia for the period 2021–2026, in line with EU directives. In addition, the Law on Information Security regulates this field. According to the Law on Information Security, the Regulatory Agency for Electronic Communications and Postal Services has become the National Center for the Prevention of Security Risks in ICT Systems of the Republic of Serbia (CERT),[68] which is supervised by the competent authority, the Ministry of Trade, Tourism and Telecommunications. The national CERT collects and exchanges all information related to information security risks, and notifies, alerts and advises ICT management teams in the Republic of Serbia, as well as the general public.[69] So far, there are 15 registered CERT members, most of which are large business companies.[70]

Summary

Digitalisation is a new area of cooperation in the Western Balkans, where the European Union foresaw developments in 2017. As can be seen, over the last decade, the states in the region have gradually established e-public administration portals where they can now manage a wide range of transactions electronically. Financial support is provided jointly by the individual states and the European Union. Cooperation is proceeding according to the roadmap set out in the agreement, which initially involved a reduction in roaming charges between the two countries. Reforms also require an appropriate legislative

64 *Strategy for the Development of Digital Skills for the period 2020–2024 in Serbia* 2020.
65 *Serbia's Statistical Yearbook* 2020.
66 Jashari 2022: 30.
67 *Strategy for the Development of Information Society and Information Security in the Republic of Serbia for 2021–2026.*
68 *National Center for the Prevention of Security Risks in ICT Systems of the Republic of Serbia* s. a.
69 *Serbia National CERT* s. a.
70 *Registered CERT Associates in Serbia* s. a.

framework, which has been adopted in all the countries concerned, albeit in a fragmented way, but with a number of laws dealing with e-government, personal data protection or cybersecurity challenges. By setting up coordinating institutions, we can be confident that digitisation will proceed at the right pace and even that good practices will be shared across the region. And the increase in the number of cases and users suggests that e-public administration has been increasingly used in recent years, with large-scale developments, especially during the Covid-19 pandemic, and citizens learning and getting used to using these platforms.

References

CMS (s. a.): *Data Protection and Cybersecurity Laws in Albania.* Online: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/albania

Commissioner for the Right of Information and Personal Data Protection Report (2020). Online: www.idp.al/wp-content/uploads/2021/03/Raporti_IDP_2020.pdf

Economic Reform Program for the period 2021–2023 (2021). Online: https://finance.gov.mk/wp-content/uploads/2021/02/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0-%D0%BD%D0%B0-%D0%B5%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D1%81%D0%BA%D0%B8-%D1%80%D0%B5-%D1%84%D0%BE%D1%80%D0%BC%D0%B8-2021-2023.pdf

eGovernment Development Scheme (2020). Online: http://mduls.gov.rs/en/announcements/e-government-development-scheme-for-the-period-2020-2022-has-been-adopted-300-new-electronic-services-provided-to-citizens-and-the-economy/?script=lat

European Commission (2017): *Western Balkans Summit 2017: Delivering for the Region.* Online: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_2007

European Commission (2018): *European Commission Launches Digital Agenda for the Western Balkans.* Online: https://ec.europa.eu/commission/presscorner/detail/es/IP_18_4242

European Commission (2019): *Western Balkans Summit in Poznań: Strengthening Links within the Region and with the EU.* Online: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_3669

European Commission (2020): *Country Report North Macedonia.* Online: https://neighbourhood-enlargement.ec.europa.eu/system/files/2020-10/north_macedonia_report_2020.pdf

European Commission (2023): *Decrease of Data Roaming Fees between the Western Balkans and the EU.* Online: https://neighbourhood-enlargement.ec.europa.eu/news/decrease-data-roaming-fees-between-western-balkans-and-eu-2023-05-03_en

European Council (2018): *EU – Western Balkans Summit in Sofia, 17 May 2018.* Online: www.consilium.europa.eu/en/meetings/international-summit/2018/05/17/

EWB (2017): Meeting of WB Foreign Ministers with Hahn, Discussing Regional Economic Area. *European Western Balkans,* 20 September 2017. Online: https://europeanwesternbalkans.com/2017/09/20/meeting-wb-foreign-ministers-han-discussing-regional-economic-area/

ITU (2021): *Digital Skills Assessment Republic of North Macedonia.* Online: https://northmacedonia.un.org/sites/default/files/2022-04/ITU_NorthMacedonia_DigitalSkillsAssessment_20211223_FINAL.pdf

Jashari, Bardhyl ed. (2022): *Digital Agenda Observatory 2021. Cumulative Report on Digital Agenda Advancement in Albania, Kosovo, Montenegro, North Macedonia and Serbia.* Skopje: Metamorphosis Foundation for Internet and Society.

Kajosevic, Samir (2022): Montenegro Still Assessing Damage From Mystery Cyber Attacks. *Balkan Insight,* 29 August 2022. Online: https://balkaninsight.com/2022/08/29/montenegro-still-assessing-damage-from-mystery-cyber-attacks/

Kosovo Digital Economy Project (s. a.). Online: https://kodeproject.org/en/home-2/

Ministry of Innovation and Public Administration (2018): *Cross-cutting Strategy on Digital Agenda 2015–2020 (CSDA).* Online: https://akshi.gov.al/wp-content/uploads/2018/03/Strategjia_e_Axhendes_Dixhitale_shqip.pdf

Momčilo, Radulović ed. (2020): *Implementation of Berlin Process in the Western Balkans Countries.* Online: https://kki.hu/wp-content/uploads/2020/12/V4-countries-in-the-process-of-EU-integration-of-the-WB6.pdf

National Center for the Prevention of Security Risks in ICT Systems of the Republic of Serbia (s. a). Online: www.cert.rs/en

National Strategy for Artificial Intelligence (s. a). Online: https://vlada.mk/node/24948

North Macedonia Scheme Regarding e-Governance Coordination (2020). Online: www.mioa.gov.mk/sites/default/files/pbl_files/documents/reports/izveshtaj_za_realizacija_na_gp_za_2020_godina.pdf

North Macedonia National Cybersecurity Strategy of the Republic of Macedonia 2018–2022 (2018). Online: www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_sajber_bezbednost_2018-2022.pdf

North Macedonia National Operability Framework (s. a.). Online: www.mioa.gov.mk/?q=mk/node/1320

OECD (2018): *Digital Society in South East Europe.* Online: https://doi.org/10.1787/9789264298576-15-en

Office for IT and Government in Serbia (s. a.). Online: www.ite.gov.rs/tekst/en/124/office-for-it-and-eGovernment.php

Regional Cooperation Council (s. a.): *Broadband and 5G.* Online: www.rcc.int/priority_areas/54/broadband-and-5g

Registered CERT Associates in Serbia (s. a.). Online: www.cert.rs/en/evidencija-certova.html?page=2

Serbia National CERT (s. a.). Online: www.ratel.rs/en/page/national-cert

Serbia's Statistical Yearbook (2020). Online: https://publikacije.stat.gov.rs/G2020/Pdf/G20202053.pdf

Shift2Rail Joint Undertaking (2020): *Multi-annual Action Plan.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2881/314331

Strategy for the Development of Digital Skills for the period 2020–2024 in Serbia (2020). Online: www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2021/Digital%20skills/4_Nevena%20Praizovic_Serbia.pdf

Strategy for the Development of Information Society and Information Security in the Republic of Serbia for 2021–2026 (2021). Online: www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2021/86/1/reg

Vllahiu, Emirjeta (2022): Kosovo to Establish Agency for Cyber Security Amid Recent Attacks. *Balkan Insight*, 14 September 2022. Online: https://balkaninsight.com/2022/09/14/kosovo-to-establish-agency-for-cyber-security-amid-recent-attacks/

WBIF (s. a.): *Digital Future.* Western Balkans Investment Framework. Online: www.wbif.eu/sectors/digital-infrastructure

Western Balkans Info Hub (2018): *Digital Agenda for the Balkans – Digitalisation.* Online: https://wbc-rti.info/theme/57#:~:text=The%20Digital%20Agenda%20for%20the,more%20jobs%2C%20and%20better%20services

AARMS Vol. 22, No. 3 (2023) 109–123.

10.32565/aarms.2023.3.7

The Role of the Indonesian National Armed Forces (TNI) in Post-Conflict Peacebuilding: A Civil–Military Cooperation (CIMIC) Perspective

Stephanus Yusuf TRI EFFENDI[1]

This paper scrutinises the assimilation of the Indonesian National Armed Forces (Tentara Nasional Indonesia – TNI) into civilian structures to shape a harmonised civil–military cooperation (CIMIC) in post-conflict peacebuilding initiatives. Acting as a crucial state apparatus, the TNI confronts a spectrum of threats, upholds national integrity, and follows Law No. 34/2004 by promoting soft power in non-combative military operations. Notwithstanding concerns raised by peace activists regarding potential human rights breaches during armed interventions, peacebuilding heavily depends on trust-building, which is a key catalyst for stakeholder cooperation. In contradiction to activists' apprehensions, 2022 surveys reveal an impressive public trust level of around 93% towards the TNI. This robust public confidence sets a promising stage for the active engagement of the TNI in peacebuilding. To ensure effective participation, the TNI must demonstrate human rights commitment and adaptability to civilian protocols and guarantee non-repressive methodologies in peace missions. Leveraging its soft power, the TNI can cultivate productive alliances with civil institutions via joint ventures under civilian supremacy within a regulated CIMIC construct. The theory of change offers a unique perspective on the intertwined dynamics of civil–military collaboration, public trust and soft military power in peacebuilding, steering state policy outcomes. These are shaped by the government's ability to reshape military duties devoid of military overreach. In conclusion, civilian control over the military materialises through shared accountability in peacebuilding endeavours, encapsulated within the CIMIC framework.

Keywords: *trust-building, soft power, peacebuilding, CIMIC, social conflict*

[1] Military officer, Indonesian Air Force Headquarters Intelligence Staff, e-mail: stephanus.effendi@gmail.com

Introduction

Indonesia is a diverse country of various cultures, ethnicities, languages and religions. As a unitary state, the primary threat it faces is the potential disintegration of the nation. Failure to address these differences adequately can lead to social conflicts, resulting in social change. Over the last two decades, Indonesia has experienced several social conflicts, including the Sampit–Madurese dispute resulting in massacres, the Lampung–Balinese conflict due to socio-economic gaps, the separatism of the Aceh independence movement, the religious conflict between Christians and Muslims in Ambon, and the independent Papua separatist organisation due to social development gaps.

Social conflicts are the term used to describe large-scale disputes that gain public attention. Conflict arises when different interests, goals, values, needs, expectations and social beliefs clash. As Berger and Luckman noted, ideological conflicts can escalate and become malicious.[2] Conflicts tend to escalate when one group perceives another as a threat to their power and sees any progress made by the other group as a loss for themselves. These intergroup disputes, particularly between groups of varying sizes and power levels, can be classified as micro or macro-level conflicts to help determine the appropriate intervention methods with lasting consequences for how these groups are treated in society. Conflicts at the micro or macro level are believed to stem from similar psychological factors. These include attitudes, behaviour and contradictions, the three fundamental components of conflicts.[3] To address these problems, the government must work together to prevent and decrease any resulting conflict.

The *Tentara Nasional Indonesia* (TNI), also known as the Indonesian National Armed Forces, has a crucial role in maintaining political stability. The TNI is empowered by Law No. 34/2004 to mediate social disputes and participate in military operations during both wartime and peacetime scenarios while adhering to strict regulations. The military upholds democracy, civil supremacy, human rights, and national and international legal frameworks to serve the country's best interests. It is vital in protecting the nation and its people from conventional and asymmetrical security threats, including social conflicts that could lead to separatist movements.

Despite this, the involvement of the TNI in peacebuilding missions has elicited a certain degree of apprehension among peace advocates. This scepticism primarily stems from concerns about potential human rights violations that could transpire in the wake of armed interventions. However, it is paramount to acknowledge that the TNI, in its endeavours, remains resolutely committed to fostering peace, adhering to the rule of law, and safeguarding the dignity and rights of all individuals it seeks to protect.

The discernible dichotomy between the robust public trust in the TNI, as corroborated by 2022 surveys, and the apprehensions raised by peace activists highlights the pressing need to address this issue, re-evaluate the role of the TNI, and investigate the prospects of Civil–Military Cooperation (CIMIC) in peacebuilding efforts. Furthermore, the TNI, in collaboration with civil authorities and other security agencies, works to confront

[2] Berger–Luckman 1966.
[3] Galtung 1997.

unconventional security challenges, an effort that promises significant benefits for conflict resolution. This article aims to delve into the potential strategies and approaches the TNI could implement in these missions, focusing on ensuring respect for human rights and fostering trust among conflicting parties.

Understanding conflict

Conflicts can have various causes, including conflicting material interests, absence of benefits, contrasting identities, ideological or spiritual differences, stereotypes, prejudices, interpersonal issues, insufficient knowledge and experience in resolving differences. Conflict is an interaction between actors (individuals, groups, organisations) where at least one actor senses incompatibilities between their thinking, imagination, perception, and/or feeling and those of the others. The factors underlying conflict are threefold: interdependence, differences in goals and differences in perceptions. According to Galtung, conflict is a dynamic process in which structure, attitudes and behaviours constantly influence one another.[4] Meanwhile, Wall argues that conflict is when two or more parties attempt to frustrate attaining the other's goals.[5]

Understanding the natural causes of conflict involves recognising the various stages of conflict: before it starts, during its occurrence and after it concludes. Glasl presents a staircase model that offers a framework for comprehending conflict dynamics, specifically focusing on how conflicts can escalate and de-escalate.[6] This model consists of several steps, beginning with a discussion of the underlying contradiction, progressing to heightened hostility, and ultimately culminating in a violent phase where the involved parties seek to eliminate each other. It can be likened to climbing a staircase, where each step necessitates effort and perseverance. According to this model, if a conflict remains unresolved, it can intensify over time. Nevertheless, reversing the escalation requires more time and energy than descending the stairs. The further one drops, the more challenging it becomes to resolve the conflict independently.

To establish enduring and secure peace in a post-conflict situation, it is essential for the involved parties to mutually agree on tackling the fundamental causes of the conflict, which can be traced back to various forms of structural violence. Galtung suggests that addressing structural violence requires adopting an approach emphasising peace through cooperation.[7] This entails replacing conditions characterised by exploitation, elitism and isolation with requirements that prioritise fairness, harmony and interdependence, which are more compassionate. In simple terms, attaining peace does not involve segregating or isolating opposing parties. Instead, it necessitates promoting effective communication and collaboration across all segments of society while encouraging interdependence and exchanging ideas and resources among organisations and individuals.[8]

4 Galtung 1997.
5 Wall 1985.
6 Glasl 1999: 84–85.
7 Galtung 1975a.
8 Galtung 1975b.

Correctly identifying and comprehending the potential reasons behind a conflict is crucial for effectively resolving it, and it is an essential component of conflict analysis. Conducting a thorough analysis of the conflict is crucial, as it enables the development of appropriate interventions. Typically, interventions are implemented during the active conflict phase rather than before or after. This is primarily due to the crisis that inevitably emerges during the conflict. Nevertheless, the intervention during the pre-and post-conflict stages can be immensely valuable in preventing violence and, consequently, mitigating the impact of the conflict phase.

CIMIC: A concise overview

CIMIC, a strategy pioneered by NATO in the late 1990s, has become essential for merging military and civilian efforts in conflict and post-conflict areas. This doctrine emphasises the importance of building strong collaborations between military organisations and civilian groups, such as international bodies, non-governmental organisations (NGOs), local governments and civilians.[9] CIMIC principles are the foundation for civil–military interactions (CMI) during operations and are essential for commanders, staff and troops to follow. By adhering to these guidelines, a well-rounded operational strategy can be developed.

CIMIC aims to achieve mission objectives by working with non-military stakeholders in operational zones and promotes positive relationships between military organisations and civilian entities through a comprehensive approach. Ideally, all parties involved should work together seamlessly. However, if this is impossible, interactions should be carefully planned to avoid negative outcomes in operations or civilian settings. This approach ensures that each stakeholder can progress without encountering obstacles and minimises unintended conflicts.

CIMIC adopts a comprehensive approach to military operations that extends beyond traditional warfare. This approach empowers military units to engage in missions that involve dispensing humanitarian aid, supervising reconstruction efforts and spearheading development initiatives. It also recognises the military's obligation to maintain security. This two-fold responsibility is designed to be cohesive rather than contradictory. By embracing this broader role, military entities can enhance the resilience and stability of societies grappling with post-conflict situations, thus improving the prospects of achieving enduring peace and sustainable progress.

Executing CIMIC principles as actionable strategies presents its own set of challenges. To effectively deploy CIMIC, it is crucial to establish seamless coordination, clearly defined roles, and equitable resource distribution amongst military and civilian factions.[10] However, achieving these prerequisites in convoluted, ever-changing and demanding scenarios is challenging. Military personnel must also be versatile and attuned to civilian traditions and requirements, which requires profound training sessions to equip them with

[9] NATO Standard AJP-3.19 2018.
[10] De Coning 2017: 145–160.

the necessary skills. Additionally, reconciling military goals with humanitarian tenets such as neutrality, impartiality and independence often poses collaboration hurdles. The effective role of CIMIC in peace initiatives requires an added layer of complexity to achieve mutual comprehension and respect for each stakeholder's principles and limitations.

The role of CIMIC in peacebuilding

In conflict or post-conflict environments, stability and development are crucial. CIMIC acknowledges that military forces alone cannot handle all the complex challenges and needs in such situations. Collaborating and engaging with civilian authorities, NGOs and local communities can help military forces leverage their unique capabilities and resources while benefiting from civilian actors' expertise, knowledge and relationships. The CIMIC activities aim to reduce the adverse effects of military operations on the civilian population and promote trust and confidence between military and civilian actors.

CIMIC has various roles in supporting peacebuilding efforts. These include effective law enforcement, assisting with the disarmament, demobilisation and reintegration of former combatants, and providing security sector reform assistance. Additionally, CIMIC facilitates the delivery of humanitarian aid and development assistance to communities affected by conflict. This support includes logistical aid, protection of aid workers and coordination with NGOs to address the population's immediate needs, such as food, water, healthcare and shelter. CIMIC also plays a crucial role in rehabilitating and developing essential infrastructure in post-conflict areas, including reconstructing roads, bridges, schools, hospitals and other critical facilities. Furthermore, CIMIC supports peacebuilding efforts by contributing to local institutions' and communities' capacity building and training. Military forces provide training and mentorship to local security forces, support establishing effective governance structures, promote human rights and the rule of law, and facilitate community reconciliation and dialogue processes. By engaging with local communities, CIMIC fosters positive civil–military relations and trust-building between military forces and the civilian population. This interaction helps overcome cultural barriers, reduce tensions and build mutual trust, which is essential for sustainable peacebuilding. Lastly, CIMIC promotes information sharing and coordination among military forces, civil authorities, NGOs and other relevant actors to ensure a comprehensive understanding of the local context, avoid duplication of efforts, and enable effective collaboration in implementing peacebuilding strategies.

Using a multidimensional and collaborative approach, CIMIC in peacebuilding acknowledges the significance of civilian expertise, local ownership and inclusive decision-making processes. It combines military capabilities, civilian resources and knowledge to contribute to sustainable peace, reconciliation and the long-term development of post-conflict societies. CIMIC is crucial in promoting effective collaboration, mutual understanding and synergy between military and civilian entities, ultimately leading to stability, peacebuilding, and the well-being of affected populations.

Trust-building: A crucial element in post-conflict peacebuilding

In situations of violent conflicts, rebuilding trust becomes a critical element in the process of peacebuilding. The pivotal role of community trust in government agents, both military and civilian, cannot be ignored when it comes to successful peacebuilding activities. Trust is the very foundation on which relationships between different agencies are built. Institutions that are trusted can establish lasting peace and earn enduring legitimacy.

Although the TNI was once viewed as oppressive, it is vital to establish trust with civil society. Recent surveys indicate that the TNI enjoys an exceptionally high level of trust among the public. According to the Indonesian Political Indicators (IPI) survey conducted on 24 June 2022, 93.2% of the respondents expressed trust in the TNI. Furthermore, on 27 September 2022, a study by the Center for Strategic and International Studies (CSIS) revealed that 93.5% of the respondents were satisfied with the performance of the TNI in upholding democracy.[11] With such remarkable trust and satisfaction, TNI has a solid foundation to enhance its professionalism continually. Despite unfavourable portrayals by the media and activists, the public's confidence in the Indonesian military remains unwavering. This trust would benefit the successful involvement plan of the TNI in peacebuilding initiatives.

In terms of a collective understanding of security, soldiers are increasingly challenged to do their job amidst civilian society. The military needs sufficient understanding, capabilities and possibilities to meet these challenges. The military must cooperate with civilians to achieve successful peacebuilding after a conflict. This collaboration helps address trust, professionalism and human rights issues. However, differing viewpoints between civilian and military leaders can harm confidence in the community. Therefore, it is vital to demonstrate to civilians that the TNI is a dependable partner in peacebuilding efforts aligned with the civilians' objectives.

There exists a diversity of viewpoints regarding the collaboration between civilians and the military in peacebuilding. While some contend that conflict resolution should be the responsibility of the military, others posit that political engagement is vital and that societal factors and contexts must be considered before deploying the military. If military intervention is deemed necessary, it should be initiated early and gradually withdrawn. Furthermore, minimal force should be prioritised during the initial stages to avoid adverse political ramifications.

Evaluating the implementation of post-conflict peacebuilding in Indonesia

To effectively apply CIMIC in Indonesia, adherence to established norms and universal rules governing the military's involvement in post-conflict peacebuilding endeavours is crucial. The conduct of the TNI is guided by Law No. 34/2004, which outlines the responsibilities and principles that the TNI must uphold. This includes operating as

[11] Antara 2022.

professional soldiers aligned with the nation's political policies, strongly emphasising democratic principles, civil supremacy, human rights, adherence to national legislation, and ratified international laws. Article 2 d. of the law explicitly outlines the commitment of the TNI to these principles. Article 6 c. also highlights the role of the TNI in restoring state security in disruptions caused by security disturbances. Furthermore, Article 7 (2) b. states that the TNI engages in military operations other than war to support peacebuilding efforts, aligning with foreign policy objectives and assisting regional government tasks. As a result, the involvement of the TNI in post-conflict peacebuilding is constitutionally grounded, and their role in peacekeeping, peacemaking, and peacebuilding emerges as both legitimate and lawful within this framework. The question remains the identification of the standard norms and universal rules the Indonesian military can adopt to guide their engagement in post-conflict peacebuilding endeavours.

There has yet to be an instance where TNI were asked to participate in post-conflict peacebuilding initiatives by a civilian entity. Human rights advocates have often pointed to TNI as instigators of human rights abuses and barriers to peacebuilding efforts. This perception is likely due to the TNI's repressive reputation and association with forceful tactics. It is crucial to note that the TNI's mandate, under the Pancasila ideology and the 1945 Constitution of the Republic of Indonesia, is to safeguard the

nation's territorial integrity, protect the people from threats, and preserve national unity through warfare and other military operations. Hence, all missions undertaken by the TNI are directed by the political choices of civilian leadership for the state's welfare. However, the involvement of the TNI in national conflicts has been limited to prevention and tactical execution, excluding any post-conflict recovery efforts.

To tackle conflicts, Indonesia has implemented several strategies. Key contributors in conflict mediation have been the Coordinating Ministry for Political, Legal and Security Affairs and international bodies. Legal avenues have also been pursued to address social tensions. In an attempt to grant more power to local communities, Indonesia has adopted a policy of decentralisation. Entities like the Ministry of Education and Culture, religious groups and NGOs have initiated programs fostering intercultural and interfaith dialogue. Peacebuilding efforts have included reconciliation measures, notably truth and reconciliation commissions. Economic programs have been launched to target poverty and inequality, recognised as the underpinning causes of conflict. In more extreme cases, deploying security forces has been necessary to maintain peace, though this has led to some claims of human rights violations.

Civil–military interaction post-conflict: Indonesia's experience

From the beginning of the 2000s, the TNI has moved towards a more cooperative stance with civilian groups, aiming to establish connections, promote shared comprehension and pursue shared peacebuilding objectives.[12] This change in military tactics is a notable

[12] Laksmana 2011: 63–83.

shift from traditional military practices, recognising the vital importance of civilian participation and collaboration in ensuring enduring peace and consistent growth.

After the Aceh conflict concluded in 2005, the role of the TNI in post-conflict peacebuilding became prominent. During this transition, the TNI extended beyond their conventional security functions to significantly aid in the disarmament process, a vital step in moving from conflict to peace. They also took on the significant challenge of helping reintegrate ex-combatants back into society. To successfully handle this task, the TNI employed a method that incorporated diplomacy, meticulous planning, patience and extensive reintegration programs.[13] Additionally, the TNI was instrumental in restoring crucial infrastructures such as roads, schools and hospitals, re-establishing critical services, rejuvenating the local economy, and bringing a semblance of normalcy to the citizens.[14] The TNI also adopted CIMIC strategies during this period, emphasising cooperative peacebuilding efforts and enhancing ties between military units and civilian entities, including global peacebuilding bodies. Research indicates that such strategies have effectively fostered partnerships between military and civilian stakeholders, addressed the complexities of post-conflict peacebuilding, and fostered a collaborative and trusting environment.[15]

The significant involvement of the TNI in peacebuilding, while crucial, has not been without its hurdles and contentious points. Detractors point out the potential for the role of the TNI in post-conflict scenarios to intensify strains, particularly in areas with strained civil–military relationships, possibly weakening the essential trust-building activities for peace processes.[16] Additionally, the historical stance of the TNI in conflict mediation, often perceived as oppressive, has shaped peace activists' views, amplifying their reservations about the military's peacebuilding role. Apprehensions about possible human rights breaches tied to the activities of the TNI in peacebuilding emphasise the imperative need for the military body to adhere to human rights, maintain legal principles and synchronise its actions with civilian guidelines.[17] This depiction, primarily propelled by peace activists, raises significant challenges for the TNI, rooted in the belief that military intervention is fundamentally at odds with peacebuilding. Yet, the situation appears to be more layered, given the public's substantial trust in the TNI. It implies that despite criticisms, the TNI has earned a reputable societal status, laying a solid foundation for its future peacebuilding endeavours.

In the complex post-conflict landscape of Indonesia, the role of the TNI in peacebuilding is undebatable. A strengthened relationship between civilians and the military, increased civilian oversight over military actions, and integration of a human rights-focused approach in peacebuilding initiatives are pivotal for sustained peace and stability.[18] For the TNI to address these matters adeptly, it is essential to manifest a genuine dedication to human rights, showcased by its adherence to civilian standards, especially during peace missions. Introducing measures to build trust – emphasising transparency, holding

---

13 Kingma 1997: 151–165.
14 Barakat–Zyck 2009: 1069–1086.
15 Caspersz–Wallis 2006: 1–26.
16 Schulze 2007.
17 Human Rights Watch 2006.
18 Tadjbakhsh–Chenoy 2007.

individuals accountable for past misdeeds and providing assurances against oppressive actions towards conflicting parties – can be highly beneficial. Concurrently, the TNI ought to utilise its soft power effectively by deepening ties with civilian entities in collaborative projects, emphasising civilian leadership. Such tactics can help nurture an environment favourable to civil–military relations, mitigating existing negative views and redefining the place of the TNI in the overarching peacebuilding framework. Indeed, the interplay of human rights, building trust within the community, and fostering robust civil–military collaborations are vital for the positive impact of the TNI on Indonesia's peacebuilding initiatives. Grasping these intricacies is central to this study, offering a perspective to assess and steer the forthcoming peacebuilding actions of the TNI.

Civilian concerns about the involvement of the TNI in peacebuilding missions

The history and dynamics of the relationship between the TNI and civilians have evolved over the years, yet a shadow of mistrust continues to linger among a segment of the civilian population. This mistrust primarily stems from historical episodes and perceptions regarding the involvement of the TNI in human rights violations. There are several reasons why civilians may harbour doubts or prejudices towards the TNI, especially when considering their involvement in peacebuilding missions:

- Historical involvement in governance. Under the "*Dwifungsi*" policy of the Suharto era, the military had defensive and governance roles. During this period, military personnel were involved in both security and civil bureaucracy, leading to potential conflicts of interest and unchecked power.[19] Such dominance in political and civil spheres contributed to an environment where abuses could occur without adequate checks and balances.
- Allegations in conflict zones. Regions like Aceh, Papua, and West Papua have been flashpoints for tensions between separatist groups and the Indonesian state. There have been persistent allegations of human rights abuses by security forces in these areas.[20] Whether substantiated or not, such accusations contribute significantly to the public's perception of the TNI.
- Past lack of accountability. In the past, there were limited mechanisms in place to hold military personnel accountable for alleged misconduct or human rights abuses. This perceived impunity could exacerbate civilian concerns about the actions of the TNI, especially in regions with ethnic, religious or political tensions.
- Transitioning roles and modernisation. As the TNI has been retracting its role from politics and undergoing modernisation, there has been a push toward external defence. However, given the historical context, some civilians may still associate the TNI with its previous internal security roles, leading to concerns about potential overreach in peacebuilding missions.

[19] Mietzner 2006.
[20] Hernawan–Indarti 2008.

Involving the TNI in peacebuilding missions brings both challenges and opportunities. While the military's expertise can be invaluable in maintaining stability and rebuilding conflict zones, it is crucial to address the legacy of mistrust to ensure that such missions are both effective and perceived positively by civilians. Efforts toward transparency, accountability, and community engagement can go a long way in building trust and collaboration.

Examining the involvement of the TNI in post-conflict peacebuilding through the lens of the theory of change

According to the "theory of change", action X will lead to outcome Y, and as such it provides a structured framework to assess and understand the potential integration of the TNI into peacebuilding efforts. It facilitates an in-depth exploration of the relationships between CIMIC, public trust, the application of non-aggressive military power, and their potential influences on state policies. This theory presents a testable hypothesis for the anticipated process of change. It comprises two components: the "if" and the "then", suggesting a pathway for the military to align with civilian-led post-conflict peacebuilding initiatives through non-violent interventions. This method is an analytical tool to trace the evolution of the roles and functions of the TNI as they incorporate civilian methodologies. Intervention efforts should focus on the root problem or contradiction that instigates and exacerbates the conflict.

Galtung views conflict as a dynamic process where structure, attitudes and behaviours constantly change in relation to each other.[21] Accordingly, he posits that resolving conflict requires transforming relationships between the parties involved, much like the principles of civil–military cooperation. Consequently, it becomes plausible to consider the involvement of the TNI in post-conflict peacebuilding missions through cooperation with civilian institutions. This prospect remains unexplored in Indonesia. This approach gains relevance in a military context that is increasingly adopting cooperation with non-military personnel and organisations.

Civil–military relations are conceptualised as the interaction between political and military leadership, with the key question being civilian supremacy over the military.[22] Thus, TNI is portrayed as a "political army" – a term used for military institutions that see their involvement in – or control over – domestic politics and government affairs as an essential aspect of their legitimate duties.[23] This characterisation suggests the enduring presence of the TNI as a political force in Indonesia. As a "political army", the TNI has a significant tie with the nation's destiny, places a priority on order, and incorporates these elements into a comprehensive military doctrine.[24]

---

21 Galtung 1997.
22 Rukavishnikov–Pugh 2003: 131; Feaver 1999: 211; Burk 2002: 7.
23 Koonings–Kruijt 2002.
24 Koonings–Kruijt 2002.

Bland's theory of shared responsibility proposes that civilian control of the military is established and maintained through the shared responsibilities of civilian leaders and military officers, influenced by a set of principles that have evolved nationally.[25] Concurrently, Schiff's concordance theory asserts that civilian control is achieved when the military, political elites and the general populace have a cooperative relationship and agree on four key factors: the social composition of the officer corps, the political decision-making process, recruitment methods and military style.[26]

Huntington maintains a distinct separation between civilian and military groups, where civilians act as political masters, and the military's primary role is to safeguard society from external threats.[27] From a sociological standpoint, the principle of civilian supremacy and the level of political culture relate to the military's predisposition, motivation and opportunity to intervene, among other potential factors.[28] The primary focus of military organisations is internal and external control. However, these arguments predominantly explore how the military integrates with civilian structures, often leading to a merging of the two.

A more comprehensive dialogue is needed to understand how norms and practices shape the relationship between military leaders and civilian authorities in the context of peacebuilding missions. This discourse can yield academically robust insights and be easily understood by a wider audience.

Strategies for enhancing the involvement of the TNI in post-conflict peacebuilding

TNI faces a fundamental challenge: a narrative promulgated by peace activists that perceive military power as inherently incompatible with peacebuilding efforts. In contrast, the significant public trust in the TNI suggests an established societal credibility that could underpin their potential role in peacebuilding. To ameliorate these issues, the TNI should display an unwavering commitment to human rights and an ability to operate under civilian guidelines during peacebuilding missions. Possible confidence-building measures encompass initiatives promoting transparency, holding individuals accountable for any past misconduct, and providing assurances to parties involved in conflicts against the institution of repressive practices.

The synergy between military and civilian entities can culminate in holistic and enduring solutions for areas plagued by discord, setting the foundation for socio-political tranquillity and economic growth. CIMIC acts as a linchpin, addressing the cultural, procedural and resource-driven disparities that might hinder a cohesive peacebuilding strategy. In essence, the pivotal role of CIMIC is highlighted by its capability to balance the immediate security priorities of military units with the enduring development

[25] Bland 1999: 7–25.
[26] Schiff 1995: 7–24.
[27] Huntington 1985.
[28] Janowitz 1964; Finer 2002.

aspirations of civilian stakeholders. This collaborative endeavour facilitates swift conflict resolution and fosters prolonged restoration, rebuilding and advancement in areas affected by war. This emphasises the practical and strategic relevance of CIMIC in the aftermath of conflicts.[29]

Merging military assets with civilian know-how within the framework of CIMIC presents avenues for enhanced cultural comprehension. These disparate groups' inherent exchanges and discussions can deepen mutual appreciation, dismantling existing cultural and communicative divides.[30] This appreciation transcends simple collaboration, affecting societal dynamics. Significantly, the augmentation and adept execution of CIMIC approaches can play a key role in restoring public confidence, especially in areas with a history of fractious civil–military relations. By rigorously upholding human rights, cultivating a collaborative ethos with civilian bodies, and positively impacting community well-being, military units can pave the way for societal healing.[31] Such a potential shift in public sentiment and confidence illuminates the immense value of intensifying the role of CIMIC in peacebuilding initiatives.

While CIMIC presents inherent challenges, its potential for growth is vast. This potential primarily rests in the continuous learning, adapting and refining cycle, drawing from past experiences and acquired lessons. Incorporating these learnings into military doctrine and training evolution is pivotal. At the same time, civilian organisations can significantly benefit from a deeper insight into military outfits' operational nuances and limitations. This reciprocal process of education and comprehension strengthens the bond between these two vital peacebuilding cornerstones. Simultaneously, the TNI could augment its soft power by partnering with civilian institutions under the aegis of civilian supremacy; thus, the TNI could counter the prevailing narrative and underscore its potential value in these crucial endeavours by effectively demonstrating its capacity in conflict resolution and peacebuilding missions.

Conclusions

The Indonesian military is undergoing a significant transformation in response to non-traditional security challenges, specifically social conflicts. Concerning the role of the armed forces in these challenges, it is vital to ensure adherence to the rule of law during the execution of their duties. An overzealous role of the armed forces could compromise and infringe upon universally respected norms, including human rights and the responsibility to protect civilians from mass atrocities and crimes against humanity. Concrete decisions from political authorities should be explicitly provided regarding the armed forces' tasks, particularly in peacebuilding to deter illegitimate role allocation. Such decisions should be balanced with the roles of civil institutions in managing peacebuilding missions

[29] Pugh et al. 2004.
[30] Bryden–Hänggi 2005.
[31] Tadjbakhsh–Chenoy 2007.

and highlight the critical role of the TNI in post-conflict peacebuilding in Indonesia, emphasising the importance of CIMIC in fostering sustainable peace and stability.

The nature of the mission and the blend of civil–military organisational components necessitate careful consideration in the planning and execution of command-and-control arrangements in peacebuilding forces. The TNI must adapt its culture and integrate mechanisms that evolve duties based on values and heritage to engage civilian leaders and communities, showcasing the inherent military identity, skill and capabilities within the armed forces. Additionally, trust, a pivotal element in relationships affecting individuals and organisations, should form the cornerstone of successful civil–military cooperation, mandating prioritisation of trust-building efforts preceding mission execution. Civil–military activities necessitate an interdisciplinary approach, and the collaboration between military and civilian institutions in post-conflict peacebuilding efforts should commence with political policy outcomes drawn from the government's capacity to modify the military's responsibilities, missions, organisation, and the application of force, all independent of military interference or domination.

In summary, while there are worries about human rights violations, the involvement of the TNI in peacebuilding after conflicts is showing potential. The public has faith in the ability of the TNI to use peaceful methods to achieve stability. However, for the TNI to continue gaining public support and make progress in Indonesia's peacebuilding efforts, they must prioritise human rights and follow civilian guidelines. To ensure the successful integration of the TNI into these missions, it is imperative that civilian leaders and military officers work together within the CIMIC framework.

References

Antara (2022): TNI Must Maintain Professionalism, Public Trust. *Antara News*, 06 October 2022. Online: https://en.antaranews.com/news/253589/tni-must-maintain-professionalism-public-trust

Barakat, Sultan – Zyck, Steven A. (2009): The Evolution of Post-Conflict Recovery. *Third World Quarterly*, 30(6), 1069–1086. Online: https://doi.org/10.1080/01436590903037333

Berger, Peter L. – Luckmann, Thomas (1966): *The Social Construction of Reality. A Treatise in the Sociology of Knowledge*. New York: Doubleday & Company.

Bland, Douglas L. (1999): A Unified Theory of Civil–Military Relations. *Armed Forces and Society*, 26(1), 7–25. Online: https://doi.org/10.1177/0095327X9902600102

Bryden, Alan – Hänggi, Heiner eds. (2005): *Security Governance in Post-Conflict Peacebuilding*. Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Burk, James (2002): Theories of Democratic Civil–Military Relations. *Armed Forces and Society*, 29(1), 7–29. Online: https://doi.org/10.1177/0095327X0202900102

Caspersz, D. – Wallis, J. (2006): The Role of the Military in Post-Conflict Peacebuilding: What Does the 'New Agenda' Mean for Inter-Agency Cooperation. *Journal of Peace, Conflict, and Development*, 8, 1–26.

De Coning, Cedric (2017): Peace Enforcement in Africa: Doctrinal Distinctions between the African Union and United Nations. *Contemporary Security Policy,* 38(1), 145–160. Online: https://doi.org/10.1080/13523260.2017.1283108

De Groot, Tom – Regilme, Salvatore S. F. (2022): Private Military and Security Companies and the Militarization of Humanitarianism. *Journal of Developing Societies,* 38(1), 50–80. Online: https://doi.org/10.1177/0169796X211066874

Feaver, Peter D. (1999): Civil–Military Relations. *Annual Review of Political Science,* 2(1), 211–241. Online: https://doi.org/10.1146/annurev.polisci.2.1.211

Finer, Samuel E. (2002): *The Man on Horseback. The Role of the Military in Politics.* New Brunswick: Transaction Publishers.

Franke, Volker (2006): The Peacebuilding Dilemma: Civil–Military Cooperation in Stability Operations. *International Journal of Peace Studies,* 11(2), 5–25.

Galtung, Johan (1975a): *Essays in Peace Research. Volume 1. Peace: Research – Education – Action.* Copenhagen: Ejlers.

Galtung, Johan (1975b): Three Approaches to Peace: Peacekeeping, Peacemaking, and Peacebuilding. In *Essays in Peace Research. Volume II. Peace, War and Defense.* Copenhagen: Ejlers. 282–304.

Galtung, Johan (1997): *Peace by Peaceful Means. Peace and Conflict, Development and Civilization.* Oslo: International Peace Research Institute. Online: https://doi.org/10.4135/9781446221631

Glasl, Friedrich (1999): *Confronting Conflict. A First-Aid Kit for Handling Conflict.* Stroud: Hawthorn Press.

Haspeslagh, Sophie – Yousuf, Zahbia eds. (2015): *Local Engagement with Armed Groups. In the Midst of Violence.* Online: https://rc-services-assets.s3.eu-west-1.amazonaws.com/s3fs-public/Local_engagement_with_armed_groups_in_the_midst_of_violence_Accord_Insight_2.pdf

Hernawan, Budi J. – Indarti, Poengky (2008): *The Practice of Torture in Aceh and Papua, 1998–2007: With an Annex on the Situation of Human Rights in Timor Leste. Report.* Jakarta: SKP Jayapura.

Human Rights Watch (2006): *Too High a Price: The Human Rights Cost of the Indonesian Military's Economic Activities.* New York: Human Rights Watch.

Huntington, Samuel P. (1985): *The Soldier and the State. The Theory and Practice of Civil–Military Relations.* Cambridge, Mass.: Belknap Press of Harvard University Press.

Janowitz, Morris (1964): *The Military in the Political Development of New Nations.* Chicago: Chicago University Press.

Kingma, Kees (1997): Demobilization of Combatants after Civil Wars in Africa and Their Reintegration into Civilian Life. *Policy Sciences,* 30(3), 151–165. Online: https://doi.org/10.1023/A:1004215705156

Koonings, Kees – Kruijt, Dirk eds. (2002): *Political Armies. The Military and Nation Building in the Age of Democracy.* London: Zed Books.

Laksmana, Evan (2011): Indonesian Military Reform, 1998–2011: A Retrospective. *Security Challenges,* 7(2), 63–83.

Major, David M. (1999): *From Peacekeeping to Peacebuilding: Theory, Cases, Experiments and Solutions.* Online: www.researchgate.net/publication/262423503_

From_Peacekeeping_to_Peacebuilding_Theory_Cases_Experiments_and_Solutions/link/00b7d537b5a60edc2c000000/download

Mietzner, Marcus (2006): *The Politics of Military Reform in Post-Suharto Indonesia: Elite Conflict, Nationalism, and Institutional Resistance.* Washington, D.C.: East–West Center.

NATO Standard AJP-3.19 (2018): *Allied Joint Doctrine for Civil–Military Cooperation*. Brussels: NATO Standardization Office (NSO).

Pugh, Michael – Cooper, Neil – Goodhand, Jonathan (2004): *War Economies in a Regional Context. Overcoming the Economic and Social Legacies of Conflict.* Boulder: Lynne Rienner Publishers.

Rigby, Andrew (2006): *Is There a Role for the Military in Peacebuilding?* Online: www.c-r.org/downloads/review32.pdf

Rukavishnikov, Vladimir O. – Pugh, Michael (2003): Civil–Military Relations. In Caforio, Giuseppe (ed.): *Handbook of the Sociology of the Military.* New York: Kluwer Academic. 131–150. Online: https://doi.org/10.1007/0-387-34576-0_8

Schiff, Rebecca L. (1995): Civil–Military Relations Reconsidered: A Theory of Concordance. *Armed Forces and Society,* 22(1), 7–24. Online: https://doi.org/10.1177/0095327X9502200101

Schulze, Kirsten E. (2007): *Mission Not So Impossible. The Aceh Monitoring Mission and Lessons Learned for the EU.* Stockholm: International Policy Analysis.

Tadjbakhsh, Shahrbanou – Chenoy, Anuradha M. (2007): *Human Security. Concepts and Implications.* London – New York: Routledge. Online: https://doi.org/10.4324/9780203965955

Wall, James A. (1985): *Negotiation: Theory and Practice.* Glenview, IL: Pearson Scott Foresman.

AARMS Vol. 22, No. 3 (2023) 125–135.

10.32565/aarms.2023.3.8

The Prevalence of External States' Covert Interests over Overtly Emphasised International Conflict Resolution Agendas Throughout a Decade of Libyan Uncertainty

Bálint KÁSA[1]

This study offers a comparative perspective on four external states' behavioural tendencies in contrast to their officially upheld ambitions witnessed throughout the past ten years in Libya. Sound promises on conflict resolution, mitigation and alleged alignment with R2P principles is of course nothing new in the international arena, nor is the fact that the parallel existence of selfish agendas constitute an "innovation". Nevertheless, the case of failed reconciliation and stabilisation process of Libya despite seemingly massive international support offers a recent sphere for investigating the whole spectrum of underlying opposition among the external parties. What started out as a domestically rooted conflict, soon developed into an increasingly international one. After several attempts at the establishment of a truly unified government, interests have never got sufficiently close to each other. What this article sets out to expand on is a fundamentally balance of threats motivated geostrategic opposition, which was only seemingly centred around local key figures like Haftar, Sarraj or even influential tribal leaders. Numerous foreign stakeholders were acting against the very declarations and statements they themselves called their fellows to comply with via means of proxy actions and in hopes of capitalising on the advantages stemming from the status quo. This work discusses the means these states acted counter-productively against the Libyan conflict resolution.

Keywords: *Libya, proxy war, balance of threat, Russia, Turkey, France, Italy*

Introduction

The initially widely celebrated movements of the Arab Spring in the MENA region were fuelled with optimism in relation to a promise of democratisation waves. In most cases though, these promises were never fulfilled and a regional instability as well as uncertainty spread out. Reigns of regional leaders were challenged and, in some cases, defeated as

[1] Corvinus University of Budapest, e-mail: balint.kasa@outlook.com

part of the unfolding events. In Libya, these have resulted in the fall of the country's notorious dictator and in evolving subsequent civil wars that saw the state falling apart. Many researchers argued it to be a failed state[2] in the absence of capable governing forces and fundamental characteristics of statehood itself.

The Middle East has often been an area accommodating conflicts due to the lack of economic development, presence of significant ethnic and religious diversities and above all because of the operating types of regimes.[3] Additionally, it has always been a region penetrated by foreign powers with significant influence over matters of security, trade and politics. Recently, there has been an increased instability following the Arab Spring movements, greater influx of arms,[4] an arisen power vacuum rooted in the disengagement of the U.S. that is sought to be filled by regional and other international actors and finally the lack of coherent regional dispute resolution mechanisms as well as insufficient norms of internationally mediated conflict resolution.[5] Not surprisingly, competing international actors disadvantageously effect prospects on peacebuilding.[6] Notably, these factors directly impact the endurance of conflicts besides their more frequent occurrences. It seems there is a vicious circle that involuntarily the whole region became a part of, and Libya is not different.

As it is going to be elaborated on, official conflict resolution agendas and deniable proxies can coexist, and they provide a comparatively advantageous way of intervention for actors seeking to avoid overt involvement. Most importantly, they carry the potential to enhance the enforcement of one's will while holding the umbrella against full-scale international condemnation and marginalisation. Unfortunately, from the perspective of war-torn countries, the coexistence of these two support the prolongation and further escalation of conflicts themselves that by definition also means the failure of conflict resolution programs.

Given states' perceivably selfish preference of goals, this work somewhat pessimistically reasons those efforts on the true resolution of conflict will be ineffective as long as terms are not acceptable for stakeholders across the national border. It does not argue for the total ineffectiveness of non-state actors to swiftly resolve a conflict and maintain a high importance of humanitarian needs, but it states that unity is key in achieving those goals.

Accordingly, the following pages will argue that *conflict resolution strategies in Libya proved to be insufficient because of persisting incoherence among states, oftentimes allies.*

Official standpoints

In accordance with the standard and rightfully expected norms, states of the international arena have all expressed their desire of seeing swift conflict resolution in Libya. In fact, this occurred on numerous instances over the years via statements, joint declarations,

2 Harkai 2017: 123–137.
3 Sørli et al. 2005: 141–165.
4 Wezeman et al. 2018.
5 Cammack–Dunne 2018.
6 Lu–Thies 2013: 239–253.

enhanced mediatory roles, various contributions to physical security, etc. Some of these states have also taken on prominent roles in the related processes within the UN, NATO, the EU and other alliances they were members of. These altogether constitute the official set of goals of these actors that were not met for more than a decade now, which legitimises the quest of exploring the perceived, or even said real foreign policy ambitions they have pursued during the same period. For obvious risks and reasons of accountability though, those could not have equalled the officially articulated goals.

Real motives under the surface

Throughout the past few years, a complex struggle has developed among an increasingly wide range of international actors attempting to carve bigger shares of influence on the Libyan stage.

The following pages are going to discuss four of them that perceivably were among the most influential ones. Precisely, Russia, Turkey, France and Italy have all contributed to a meaningful extent via either military, financial or political means. Importantly, they have carried different stakes and interest for which they were willing to take a certain level of risk. Libya's location, its abundance of easily and cheaply extractable hydrocarbon resources, exposure to extremists and insurgents over the past decade as well as strategic advantages in the international migration routes flowing through its territory qualify the country strategically important sphere of interest for many. The below pages will elaborate on these four states' oftentimes competing actions.

The Russian Federation

Russia did not veto the UNSC resolution 1973, but it abstained during the vote on the no-fly zone over Libya. Its official standpoint was the support of the GNA but its support towards General Haftar – which have manifested on multiple occasions via frequent high-level meetings, not to mention the supply of weapons, trainings that have fundamentally contributed to the further escalation of the conflict[7] – was hard to misinterpret. The General's three years long siege of Benghazi, takeover of essential oilfields providing the financial means for subsequent operations could hardly have been successful lacking such foreign contributions. Importantly, these events have aided him to greater popularity in Cyrenaica as he capitalised on local tribes' decades-old sense of oppression.[8] Most certainly, a list of norms and embargoes are in place to prevent arms' supply into a civil war-torn area, but attainments of proxy warfare secure non-overt means to contribute. In this specific case, weapons may have reached their destination to fight proponents of the GNA via indirect routes while President Putin may have officially called for ceasefire

[7] Pusztai 2017.
[8] Lefèvre 2014: 268–273.

in alignment with the requirements of the international public opinion.[9] Additionally, Moscow was suspected of having printed Libyan dinars to resolve the LNA's liquidity problem – which also indirectly further destabilised the country's economy – probably in exchange for a beneficial share from the oil reserves in abundance on the territory controlled by the General's forces.[10] Finally, Moscow's smooth diplomatic operation conducted simultaneously with later deployment of air force to halt the LNA's pushback[11] and enhanced level of supply of modern weaponry was a further example of tactical manoeuvring.

Notwithstanding, it seems that the Russian strategy was not based on Haftar's identity, rather on what he represented: the potentially greatest challenger of the GNA supported by many groups within society opposing the Tripoli establishment, who – should things develop in the desired way – would have been able to grant the Kremlin a beneficial position. Consequently, his support was conditional, and it may have lasted only as long as it was in alignment with the demands of Moscow. Naturally, the issue of morality is relevant in this context, even though the Kremlin provably did not break any regulations. The past ten years' valuable experience (Crimea, Syria and of course Libya) that has enrichened Russian strategies is part of this story. This is how Russian mercenaries called the Wagner group[12] are fighting and providing intelligence to local militias[13] in Tripoli allegedly without the President's awareness or endorsement – similarly to the little green men in the Ukrainian crisis[14] – ensuring neutrality in advance, would these soldiers get involved in atrocities with Turkish, etc. troops.

The central motive of the Putin-led Russia's Libya strategy was to hinder any Western-friendly government's consolidation of power, for that would definitively have revoked any prior successes and would have pulled Russia into an unfavourable negotiating position in relation to any trade or commercial agreement, not to mention the harm it would have caused to the ambitions in the Mediterranean. An aspect of this strategy was to step up as a mediator – that has aided Russia to remain a prominent shareholder in Libya – coordinating with foreign and domestic actors. These efforts have particularly intensified after the offensive against Tripoli – which has commenced in April 2019 – when Russia did not sign the common UN declaration, rather published its own statement. All in all, the Russian involvement cannot be described as constructive. It rather carried the characteristics of a strategy seeking to shape classic geopolitical influence in a beneficial manner. It also carried characteristics of impropriating long-term economic gains. A soon

9 Saleh et al. 2020.
10 Ramani 2020.
11 Dixon 2020.
12 Approximately 2,000 soldiers were fighting in Libya. They have reached their destination indirectly, through Syria, Egypt and Jordan to Benghazi. President Putin has on multiple occasions claimed that the group is a strictly private entrepreneurship with no ties to the Russian Government. Furthermore, he stated that even though Russian citizens might be among the members, they are not acting upon the Kremlin's orders.
13 Turak 2020.
14 Shevchenko 2014.

de-escalation of the conflict under certain conditions could be in its interest, but Moscow became very cautious over the course of past years.[15]

The Turkish stance

A recent study conducted on tendencies of Turkish conflict resolution efforts has revealed that Ankara tends to regionally rely on tools of hard, rather than soft power and it often acts as an insider peace enforcer, even if a sufficiently coherent strategy based on the cases where it was an active stakeholder cannot be concluded.[16] Furthermore, it applies a dual approach within its conflict resolution strategy with the combination of bilateral and multilateral elements, which entails diplomatic and military tools on the one hand and an engagement with other external actors on the other. However, the former clearly outweighs the latter.[17]

Turkey's role is special in the sense that both its applied rhetoric and exercised behaviour endowed diplomacy a secondary role behind military force in pursuing its foreign policy goals. President Erdoğan did participate in multiple conferences on the requirements of peace, but ensuing events suggest that he valued palpable military intervention to be more expedient. Throughout the year of 2020, Turkish military presence in Tripoli got considerably strengthened: the few hundred military instructors and advisors, drones were accompanied by warships carrying modern weaponry, vehicles and supply, Turkish soldiers and Syrian mercenaries.[18] This was a clear and impossible to misread declaration that Ankara supports the internationally acknowledged GNA against Haftar. This cooperation was also strengthened when President Erdoğan signed an agreement on security cooperation and a shared maritime border with Prime Minister al-Sarraj and proceeded with providing vital intelligence to allied militias.[19] It is important to add that Ankara had already sent weapons and military supply to back up GNA militias even before it had its own boots on ground;[20] however, it must have realised the level of danger the dragging assault on Tripoli and the simultaneously increased military and financial capabilities of the LNA represented.

Scrutinising further motives behind the intervention of this magnitude, it can be ascertained that the decision-making process was not dominated by ideological interests, even if one cannot neglect to interpret it within the context of Sunni world and what a Muslim Brotherhood[21]-supporting government of Libya would mean[22] apart from the realist framework. Moreover, even though the President's domestic rhetoric occasionally

---

15 Moscow perceived to have been outplayed by Western states in Libya as their contribution to the UNSC resolution was followed by a NATO intervention.

16 Dal 2018a: 2291–2314.

17 Dal 2018b: 2207–2221.

18 Magdy 2020.

19 Naar 2020.

20 Gall 2020.

21 Initially arrived at the country from neighbouring Egypt in 1949 and established the Libyan branch in 1968, the group consisted of a few thousand individuals in 2011 aiming for legitimacy and acceptance.

22 Ahmed 2020.

included a reminiscence on the Ottoman era with a sense of nostalgia, both timing and the scale of tackled risk refuted the possibility of increased participation stemming from a contingent, historic bond-fed cultivation of relationship between Turkey and Libya. A far more likely scenario would be President Erdoğan's accurate interpretation of the status quo – similarly to the one he capitalised on in Northern Syria – and a recognition of a potent strategy through which Ankara would be able to place itself into a more advantageous position in yet another dispute. Namely, the signed maritime agreement would enable an enhanced military presence and influence in the Mediterranean that can provide the higher ground in the quarrel with Cyprus and Greece. It should also not be neglected that the area that Turkey can now consider to be legally part of its own Exclusive Economic Zone (EEZ) has rich sources of natural gas and crude oil that Ankara wanted to exploit,[23] while it is also ready to take part in post-conflict infrastructure reconstruction programs.[24]

It is indisputable that Turkey took the advantages of the possibilities stemming from the divided Libya and Tripoli's hard situation to facilitate the come about of such a beneficial agreement. Firstly, the GNA's room for movement at the time was significantly narrower by this putting Turkey into a more advantageous negotiating position when it came to post-conflict commercial and trade agreements. Turkey's economy – that suffered greatly over the past decade[25] – could profit a lot from the materialisation of such agreements especially considering the outstandingly high rates of unemployment. Also, it had the benefit of aligning with the international community's official agenda, which would ensure no punitive actions and wide-scale condemnations would follow its overt involvement. The only exception in this perspective was the maritime agreement that did not only create new turbulent waves among regional powers[26] but also escalated the whole Libyan civil war into a complex case of international law as Egypt and Greece have signed their own agreement responding to their perceived threat.

Thirdly, many regional rivals already supported the LNA, so the potential gains of siding with the opposite party were immensely higher. Indeed, Turkey proved to be a more reliable ally of Tripoli than Italy, and without its help the al-Sarraj Government would likely have been defeated. Furthermore, Turkey's support provided the sufficient aid to break Haftar's siege of Tripoli and to start pushing the LNA back.[27] Notwithstanding, this scale of commitment unavoidably triggered greater risks that was well perceived in Ankara. In light of all these, the primary Turkish goal was that the Tripoli Government would not fail, since that would have meant Ankara's simultaneous loss of a main ally and an outpost of its power projection, as well as prestige. Thus, the mission of Turkish troops in Libya was to strengthen and defend the GNA while pushing back and weakening LNA forces and its allies.

---

23 Pitel–Sheppard 2020.
24 Coskun–Gumrukcu 2020.
25 Goodman 2019.
26 Butler–Gumrukcu 2019.
27 As part of Operation Peace Storm.

European allies' conflict of interests

Examining the EU's approach towards Libya is an exceedingly difficult task predominantly due to Member States' immensely different views on the appropriate strategy for handling mass migration, which oftentimes hindered arising drafts of resolution with promising practical relevance like a 'bureaucratic anchor'. Statements and reactions by representatives of various member states suggest that conflict resolution is a surpassingly important matter for Southern member states – that is understandable given the more direct and greater challenges these countries face –, while for others this equation appears to be more complex. One should not neglect the danger of the already discussed dominant members of regime when it comes to alliance politics, including techniques of securitisation that is a truly influential tool.[28] Numerous indicators highlight that unofficial and selfish foreign policy goals played their part in the background, too. Within the Libya analogy, a French–Italian opposition has been evolving over the course of the years that did not only create a political dispute – to which member states may have joined alongside moral, political or economic interests – but it indirectly contributed to the weakening of the EU's relative power. One clear manifestation of this was the fact that Turkey could obtain control over some parts of the flow of migration from North Africa that was certainly a scenario to be avoided for Europe. The significance of the EU's internal opposition overwrote the factors of geographic realities and commercial potential that would predestine the EU to be the most influential stakeholder in the region. Precisely, the above-described incoherence has undermined this position and aided others to greater influence. There are no other two countries better exemplifying the intra-organisational lack of cohesion within recent context of common foreign and security policy than Italy and France.

Prime Minister Silvio Berlusconi's friendly relationship with Gaddafi proved to be insufficient in the prevention of the NATO intervention. Later, a prominent role was taken on that manifested in the *Skhirat Agreement* establishing the GNA, which involved significant backing from Italy that decreased substantially once the attack on Tripoli unfolded and Haftar was recognised as a legitimate actor.[29] In the subsequent maze, Rome experienced the negative effects of the above articulated lack of synergies in Europe and has implemented a new and reasonably potent strategy: instead of conducting negotiations with GNA politicians immensely dependent on the backing of the UN, it has directly reached out to leaders of major tribes[30] and decided to finance and train the Libyan coastguard in order to attempt decreasing the pressure stemming for migration over the course of past years.[31] This was a vital turning point suggesting that Italy comprehended

---

28 McDonald 2008: 563–587.

29 The intention was to step up as a mediator facilitating unity between opposing parties, but it proved to be a false strategy inasmuch as Haftar felt he had the higher ground and was not willing to settle for anything less than total victory that ultimately made Rome look as a weak and untrustworthy ally of the GNA. The incurred loss of credibility overwrote Italy's perceived capability of regional influence – and essentially marginalised it on the benefit of other actors – and it haunted later efforts seeking settlement as well.

30 Reynolds 2018.

31 Dominioni 2020.

the workings and mechanisms running the Libyan society which – although has developed since the colonial times – did not change fundamentally.

In the aftermath of GNA militias' military success significantly aided by Turkish troops, Rome wanted to re-establish trust with Tripoli that might have been beneficial for both parties. Specifically, securing the production of crude oil and natural gas in Libya is in the fundamental interest of *Eni*, Italy's greatest energy corporation, which is one of the most important partners of Libya's NOC but suffered significant losses this decade.[32] On the other hand, decreasing the international marginalisation and furthering the number of tangible allies was in the interest of the al-Sarraj Government as it would be important to the new government, too. Nevertheless, a military involvement was unlikely because of the already persisting domestic tension circulating around the financial aid Italy was providing to Tripoli, as well as the until then experienced tendencies.

The first and foremost important contribution of France was of course through bombing which it evaluated as a great success amid of strong division among allies.[33] What followed was a behaviour with a blurry set of ambitions since multiple Presidents of France got involved in scandals suggesting a variation between articulated and real goals. More and more tangible pieces of information indicated that Paris supported Haftar despite of UN and EU directives.[34] Instances backing this allegation included the arrest of French diplomats at the Tunisia border transporting weapons, questionable intelligence operations[35] and the bombing of Chadian troops[36] – potentially marching to fight Haftar – by the French Air Force, etc. Presumably, geopolitical reasoning was behind this tactic inasmuch as France attempted to enhance its regional influence in order to gain access to natural resources, including to uranium in the South,[37] as well as crude oil in the East.[38] Arguably, had Gaddafi not spoken out about the funds he donated to the campaigns of Sarkozy,[39] the French contribution to *Operation Unified Protector* would not have been so outstanding. Nevertheless, President Macron's role as pragmatic mediator did not represent a fundamental alteration from the Hollande Government's Libya strategy. The French behaviour suggested for a long time that it recognised Haftar to be the reality on the ground, while later it seemed to have reached a stalemate due to developments, and so it took on a more distant, neutral position measuring its options. Obviously, France could not have raised its objection to Turkey's enhanced involvement, but it did not fail to miss the chance to openly criticise Ankara in relation to the breach on international law triggered by the Ankara–Tripoli pact,[40] and allegedly it did so in order to stand with its

32 Sertin 2020.
33 Grand 2015: 183–204.
34 Taylor 2019.
35 Chassany–Saleh 2016.
36 Amiel 2019.
37 El-Gamaty 2018.
38 El Wardany 2019.
39 Jarry 2018.
40 Momtaz 2020.

European partners Greece and Cyprus. Paris even attacked the behaviour of Ankara as a NATO ally[41] that played its part in a fragmentation amongst alliance members.[42]

Conclusion

These competing set of actions have resulted in a universal inability to consolidate power by either domestic party in Libya. In the abundance of this magnitude of foreign support, domestic actors appeared to be less open to negotiate or compromise that resulted in the persistence of domestic actors without sufficient nation-wide recognition or acceptance, whose sphere of authority lied on sub-regions. Whereas in some cases local proxies were exceedingly dependent on certain external actor's support, proxy-initiated exploitation of masters also occurred multiple times throughout the years. The various examples have clearly proven that official conflict resolution agendas and deniable proxy relationships can and do coexist, and in Libya they have provided a comparative advantage for those actors that aimed to intervene but wanted to avoid overt means.

References

Ahmed, Omar (2020): Turkey May Have Reclaimed the Leadership of Sunni Islam from Saudi Arabia. *Middle East Monitor,* 30 July 2020. Online: www.middleeastmonitor.com/20200730-turkey-may-have-reclaimed-the-leadership-of-sunni-islam-from-saudi-arabia/

Amiel, Sandrine (2019): French Fighter Jets Bomb Chadian Rebels in Support of Deby's Regime. *Euronews,* 07 February 2019. Online: www.euronews.com/2019/02/07/french-fighter-jets-bomb-chadian-rebels-in-support-of-deby-s-regime

Butler, Daren – Gumrukcu, Tuvan (2019): Turkey Signs Maritime Boundaries Deal with Libya Amid Exploration Row. *Reuters,* 28 November 2019. Online: www.reuters.com/article/us-turkey-libya/turkey-signs-maritime-boundaries-deal-with-libya-amid-exploration-row-idUSKBN1Y213I

Cammack, Perry – Dunne, Michele: Fueling Middle East Conflicts – or Dousing the Flames. *Carnegie Endowment for International Peace,* 23 October 2018. Online: https://carnegieendowment.org/2018/10/23/fueling-middle-east-conflicts-or-dousing-flames-pub-77548

Chassany, Anne-Sylvaine – Saleh, Heba (2016): Three French Soldiers Killed in Helicopter Crash in Libya. *Financial Times,* 20 July 2016. Online: www.ft.com/content/eb86e8d8-4e6d-11e6-88c5-db83e98a590a

Coskun, Orhan – Gumrukcu, Tuvan (2020): Turkey Ready for Fast Reconstruction in Conflict-torn Libya, Official Says. *Reuters,* 19 June 2020. Online: www.reuters.com/article/turkey-libya-security-idUSL8N2DW37O

[41] Irish–Emmott 2020.
[42] Peel et al. 2020.

Dal, Emel Parlar (2018a): Assessing Turkey's Changing Conflict Management Role after the Cold War: Actorness, Approaches and Tools. *Third World Quarterly*, 39(12), 2291–2314. Online: https://doi.org/10.1080/01436597.2018.1522956

Dal, Emel Parlar (2018b): Rising Powers in International Conflict Management: An Introduction. *Third World Quarterly*, 39(12), 2207–2221. Online: https://doi.org/10.1080/01436597.2018.1503048

Dixon, Robyn (2020): Russia's Ally in Libya Is Battered by Defeats. But Moscow Has Wider Goals to Expand Its Influence. *The Washington Post*, 06 June 2020. Online: www.washingtonpost.com/world/europe/russia-libya-war-putin/2020/06/05/c3956bf4-a109-11ea-be06-af5514ee0385_story.html

Dominioni, Irene (2020): Italy Refinances Immigration Agreement with Libya Amid Protests. *Forbes*, 18 July 2020. Online: www.forbes.com/sites/irenedominioni/2020/07/18/italy-refinances-immigration-agreement-with-libya-amid-protests/#88ab1a53c49a

El-Gamaty, Guma (2018): Libya Conflict: Is France an Honest Broker? *Middle East Eye*, 29 May 2018. Online: www.middleeasteye.net/opinion/libya-conflict-france-honest-broker

El Wardany, Salma (2019): Total Gets Libya's Approval to Acquire Marathon Oil's Assets. *World Oil*, 11 December 2019. Online: www.worldoil.com/news/2019/12/11/total-gets-libya-s-approval-to-acquire-marathon-oil-s-assets

Gall, Carlotta (2020): Turkey, Flexing Its Muscles, Will Send Troops to Libya. *The New York Times*, 02 January 2020. Online: www.nytimes.com/2020/01/02/world/europe/erdogan-turkey-libya.html

Goodman, Peter S. (2019): Turkey's Long, Painful Economic Crisis Grinds On. *The New York Times*, 08 July 2019. Online: www.nytimes.com/2019/07/08/business/turkey-economy-crisis.html

Grand, Camille (2015): The French Experience: Sarkozy's War? In Mueller, Karl P. (ed.): *Precision and Purpose. Airpower in the Libyan Civil War.* Santa Monica: RAND Corporation. 183–204.

Harkai, István (2017): Líbia – a beavatkozás dilemmái egy bukott államban [Libya – The Dilemmas of Intervention in a Failed State]. In Marsai, Viktor – Vogel, Dávid (eds.): *Közel Afrikához* [Close to Africa]. Budapest: Dialóg Campus. 123–137.

Irish, John – Emmott, Robin (2020): France–Turkey Tensions Mount after NATO Naval Incident. *Reuters*, 07 July 2020. Online: www.reuters.com/article/us-nato-france-turkey-analysis-idUSKBN2481K5

Jarry, Emmanuel (2018): France's Sarkozy Told He Suspected of Taking Gaddafi Election Money. *Reuters*, 21 March 2018. Online: www.reuters.com/article/us-france-sarkozy-libyaidUSKBN1GX0LR

Lefèvre, Raphaël (2014): Commentary on Current Events. *The Journal of North African Studies*, 19(2), 268–273. Online: https://doi.org/10.1080/13629387.2014.898377

Lu, Lingyu – Thies, Cameron G. (2013): War, Rivalry, and State Building in the Middle East. *Political Research Quarterly*, 66(2), 239–253. Online: https://doi.org/10.1177/1065912912448538; DOI: https://doi.org/10.1177/1065912912448538

McDonald, Matt (2008): Securitization and the Construction of Security. *European Journal of International Relations*, 14(4), 563–587. Online: https://doi.org/10.1177/1354066108097553

Magdy, Samy (2020): US: Turkey-sent Syrian Fighters Generate Backlash in Libya. *The Washington Post*, 02 September 2020. Online: www.washingtonpost.com/world/middle_east/us-turkey-sent-syrian-fighters-generate-backlash-in-libya/2020/09/02/db9a148e-ed58-11ea-bd08-1b10132b458f_story.html

Momtaz, Rym (2020): Macron Criticizes Turkey but Raises Prospect of Dialogue. *Politico*, 10 September 2020. Online: www.politico.eu/article/emmanuel-macron-calls-out-turkey-while-extending-dialogue-branch/

Naar, Ismaeel (2020): Turkish Intelligence Agents, Foreign Fighters Arrive in Libya: Sources. *Al Arabiya*, 06 January 2020. Online: https://english.alarabiya.net/News/north-africa/2020/01/06/Turkish-intelligence-agents-foreign-fighters-arrive-in-Libya-Sources

Peel, Michael – England, Andrew – Mallet, Victor – Pitel, Laura (2020): French Spat with Turkey over Libya Lays Bare European Divisions. *Financial Times*, 05 July 2020. Online: www.ft.com/content/3b85dd0e-1f2e-40b0-b44b-947b7f75a03e

Pitel, Laura – Sheppard, David (2020): Turkey Fuels Regional Power Game over Mediterranean Gas Reserves. *Financial Times*, 18 July 2020. Online: www.ft.com/content/69a222d4-b37c-4e7e-86dc-4f96b226416d

Pusztai, Wolfgang (2017): The Haftar–Russia Link and the Military Plan of the LNA. *ISPI*, 02 February 2017. Online: www.ispionline.it/it/pubblicazione/haftar-russia-link-and-military-plan-lna-16289

Ramani, Samuel (2020): Russia's strategy in Libya. *Royal United Services Institute (RUSI)*, 07 April 2020. Online: https://rusi.org/explore-our-research/publications/commentary/russias-strategy-libya

Reynolds, James (2018): Marco Minniti: The Man Who Cut the Migrant Flow to Italy. *BBC*, 20 September 2018. Online: www.bbc.co.uk/news/world-europe-45575763

Saleh, Heba – Pitel, Laura – Foy, Henry (2020): Putin and Erdogan Call for Ceasefire in War-ravaged Libya. *Financial Times*, 08 January 2020. Online: www.ft.com/content/823220de-3238-11ea-a329-0bcf87a328f2

Sertin, Carla (2020): ENI and Libya NOC's Joint Venture Is Losing $9.4 mn Per Day. *Oil and Gas Middle East*, 02 February 2020. Online: www.oilandgasmiddleeast.com/drilling-production/35946-eni-and-libya-nocs-joint-venture-is-losing-94mn-per-day

Shevchenko, Vitaly (2014): Little Green Men or Russian Invaders? *BBC*, 11 March 2014. Online: www.bbc.com/news/world-europe-26532154

Sørli, E. Mirjam – Gleditsch, Nils P. – Strand, Håvard (2005): Why Is There so Much Conflict in the Middle East? *The Journal of Conflict Resolution*, 49(1), 141–165. Online: https://doi.org/10.1177/0022002704270824

Taylor, Paul (2019): France's Double Game in Libya. *Politico*, 17 April 2019. Online: www.politico.eu/article/frances-double-game-in-libya-nato-un-khalifa-haftar/

Turak, Natasha (2020): Russian Mercenaries, a CIA-linked General and Lots of Oil: Explaining Libya's War. *CNBC*, 29 January 2020. Online: www.cnbc.com/2020/01/29/libyas-war-explained-khalifa-haftar-oil-cuts-uae-airstrikes-and-russian-mercenaries.html

Wezeman, Pieter D. – Fleurant, Aude – Kuimova, Alexandra – Tian, Nan – Wezeman, Siemon T. (2018): Trends in International Arms Transfers. *SIPRI Fact Sheet*, March 2018. Online: https://doi.org/10.55163/KFLQ6518

Contents