HADMÉRNÖK

Kiemelt közlemények

18. évf. (2023)
4. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

Hadmérnök
Katonai műszaki tudományok online folyóirata
ISSN 1788-1919 (elektronikus)

Nemzeti Közszolgálati Egyetem
1101 Budapest, Hungária krt. 9–11.
Postacím: 1581 Budapest, Pf. 15.
„A" épület 9. emelet, 901. iroda
Telefon: +36-1-432-9000/29-289/ Fax: +36-1-432-9025
E-mail: hadmernok@uni-nke.hu
Web: https://folyoirat.ludovika.hu/index.php/hadmernok

Kiadó
Nemzeti Közszolgálati Egyetem, Ludovika Egyetemi Kiadó
Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
A kiadásért felel: Deli Gergely rektor
Olvasószerkesztők: Bujdosó Hajnalka, György László, Resofszki Ágnes

Tartalom

Fórum

HADMÉRNÖK
HADITECHNIKA

18. évfolyam (2023) 4. szám 5–17.
DOI: 10.32567/hm.2023.4.1

Gajdács László[1]

„Látni és láthatóvá válni" megoldások drónokhoz

„See and be Seen" Solutions for Drones

Absztrakt

A légi közlekedés közvetlen és közvetett résztvevőire napjainkban egyre nagyobb feladat hárul. Egyrészt évről évre növekvő tendenciát mutat a kereskedelmi és teherszállító légi járművek járatainak száma, másrészt pedig egyre gyakoribb a pilóta nélküli légi járművek jelenléte, amely komoly kihívást jelent a légi forgalmi irányítás és a légijármű-vezetők számára egyaránt. Ahhoz, hogy ez a kétféle módon „vezethető" légi jármű biztonságosan közlekedhessen egy adott légtér szegmensében, tudnunk kell egyrészt, ki és mivel repül, továbbá, hogy mi a haladási iránya, magassága stb. Ehhez nyújtanak segítséget az olyan rendszerek, mint például: FLARM[2]; ADS-B[3]; OGN[4]; Remote ID.[5] Az említett technológiai alkalmazások legfőbb célja, hogy az érintett légi jármű láthatóvá váljon a légi közlekedésben a többi résztvevő számára, beleértve a légi forgalmi irányító szolgálatokat és a hatóságokat is.

Kulcsszavak: FLARM; ADS-B; OGN; Remote ID

Abstract

The direct and indirect participants in air transport are today facing an increasing challenge. On the one hand, the number of commercial and cargo aircraft flights is increasing year on year and, on the other hand, the presence of unmanned aircraft is on the rise, posing

[1] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Repülő Intézet Fedélzeti Rendszerek Tanszék, e-mail: gajdacs.laszlo@uni-nke.hu
[2] Flight Alarm – ütközések elkerülését támogató rendszer.
[3] Automatic Dependent Surveillance-Broadcast – ütközések elkerülését támogató rendszer.
[4] Open Glider Network – drónok és más légi járművek egységes nyomkövetési platformja.
[5] A drónok távoli azonosítására kifejlesztett műszaki megoldás.

a major challenge to air traffic control and to aircraft operators. In order to be able to fly safely in a given airspace segment, these aircraft, which can be ‚piloted' in two ways, need to know who is flying and what they are flying, their heading, altitude, etc. This is helped by systems such as FLARM; ADS-B; OGN; Remote ID. The main purpose of using these systems is to make the aircraft concerned visible to other air traffic participants, including air traffic control services and the authorities.

Keywords: FLARM; ADS-B; OGN; Remote ID

Bevezetés

A repülésben a „látni és láthatóvá válni" elv megvalósítása minden légi jármű esetében nélkülözhetetlen a biztonságos légi közlekedéshez.[6] A pilóta nélküli légi járművek érzékelésére számos technológia nyújthat segítséget, azonban a különböző műszaki, technológiai megoldások között különbség van hatékonyságukat illetően. A repülésben már használt SAA[7]- vagy DAA[8]-rendszerek olyan technológiai megoldások, amelyek használatával biztonságosabban közlekedhetnek a légi járművek. Azonban szükség van ilyen és hasonló rendszerek átalakítására, illetve a drónok fedélzetére történő implementálására annak érdekében, hogy azok minél biztonságosabban integrálhatók legyenek a légi közlekedésbe. Ezáltal elkerülhetők lennének a veszélyes megközelítések és az esetleges összeütközések a pilótával vezetett és a pilóta nélküli légi járművek között. Továbbá ezen műszaki rendszerek használatával különféle drónműveletekre is engedélyt kaphatunk az illetékes hatóságtól, például látóhatáron kívüli repülés esetén (BVLOS[9]).[10]

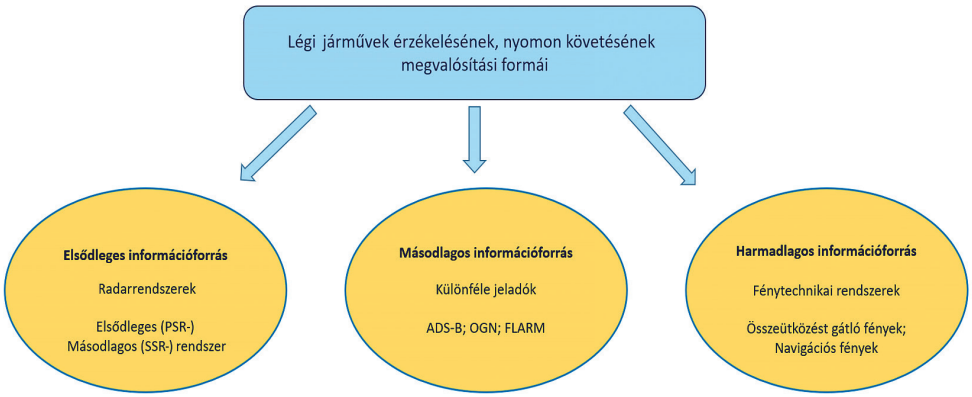
A fent említett technológiáktól függetlenül a közös cél az, hogy a drónok valamilyen műszaki megoldás használatával láthatóvá váljanak a repülésük folyamán.

Légi járművek érzékelése különböző módon történhet.

Másképpen fogalmazva: különböző csatornákból kaphatunk és adhatunk információt magunkról és mások jelenlétéről. Attól függően, hogy milyen méretű légi járműről van szó, illetve milyen hatótávolságon belül szeretne információt adni magáról, illetve kapni másoktól, annak megfelelően vagyunk képesek alkalmazni különböző típusú műszaki rendszereket (1. ábra).

A drónok biztonságos integrálása a hagyományos légi közlekedésbe napjainkban kiemelt feladatnak számít.

[6] Gajdács 2022.
[7] Sense and Avoid – érzékelés és elkerülés.
[8] Detect and Avoid – felismerés és elkerülés.
[9] Beyond Visual Line of Sight – látóhatáron kívüli repülés.
[10] *Tecnology Editor, Sense and Avoid Technology* é. n.



1. ábra: Légi járművek érzékelésének lehetséges információforrásai
Forrás: a szerző szerkesztése

Szerencsére számos módja létezik már annak, hogy a kereskedelmi forgalomban kapható, alapvetően kisméretű drónokat megjelenítsük az égbolton műveletük folyamán.

Légi járművek érzékelését és összeütközésük elkerülését támogató rendszerek:

- FLARM
- ADS-B
- OGN
- Remote ID

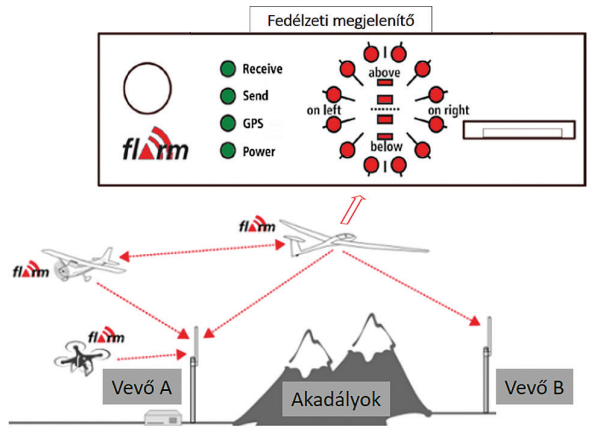
A FLARM alaprendszer bemutatása, képességei

A FLARM- (a *Flight* és az *Alarm* szavakból) rendszer egy légiforgalom-figyelő és egyben az ütközés elkerülését támogató technológiai vívmány. Eredetileg a vitorlázó repülésben részt vevőknek fejlesztették ki azért, hogy minél kevesebb legyen az ütközés a levegőben. Manapság több mint 50 000 hagyományos repülőgép használja nap mint nap, és egyre több pilóta nélküli légi jármű is. Alapvetően az FL100[11] alatti légtérben hivatott funkcióját megvalósítani.

Működése a rádiókommunikációin belül megvalósuló digitálisadat-cserén alapszik, hasonlóképpen, mint az ADS-B rendszer. A fedélzeten elhelyezett FLARM-adó kisugározza a légi jármű helyzetkoordinátáit és irányadatait, amit a „közelben tartózkodó" másik légi jármű a saját FLARM-rendszerével képes venni és feldolgozni. A fedélzeti FLARM-modul egy 16 csatornás GPS-vevőtől kapja az aktuális pozíciókoordinátákat, s az egyedi azonosítót és a tervezett repülési útvonal meghatározásához szükséges adatokat kisugározza a környezetébe. Az adatok kisugárzása másodpercenként 1-2 üzenetcsomagot jelent, amely Európában 868,2 MHz és 868,4 MHz frekvencián valósul meg. Amennyiben a vételi távolságon belül közlekedik egy másik FLARM-mal

[11] Flight Level 100 – 10 000 feet, ami 3048 méter magasságnak felel meg.

felszerelt légi jármű, akkor a beérkezett adatok feldolgozását követően meghatározza a rendszer, hogy veszélyt jelenthet-e a másik jármű repülési iránya és útvonala, vagy nem. Amennyiben fennáll az összeütközés veszélye, akkor a rendszer jelzést ad a pilóta számára. A FLARM-rendszer által biztosított további szolgáltatás, hogy a légi járművek környezetében megtalálható természetes akadályokról (oszlopok, különféle drótakadályok, magasfeszültségű távvezetékek és oszlopai) is információkat ad (2. ábra).[12]



2. ábra: A FLARM-rendszer felépítése, fedélzeti megjelenítője
Forrás: Operating Manual FLARM Collision Avoidance System 2016; Wang–Tresoldi é. n.

A rendszernek alapvetően két üzemmódja van: a „Nearest" és a „Collision". A „Nearest" üzemmódban csak jelzi a rendszer a közelben lévő légi járművet, ebben az esetben nem jelent veszélyt az idegen jármű jelenléte. Ha azonban az bekerül az úgynevezett ütközési veszélyzónába, akkor a rendszer átvált „Collision" üzemmódba, ilyenkor ugyanis fennáll az ütközés lehetősége. A rendszer hatótávolsága egy 3 km sugarú kör vízszintesen, függőlegesen pedig 500 m.

Atom-modul

A FLARM-rendszernek létezik egy kifejezetten a pilóta nélküli légi járműveknek szánt megoldása, nevezetesen az Atom UAV, egy átfogó, teljes funkcionalitású FLARM-rendszer (lásd 3. ábra). Ez az alaprendszer megoldást kíván nyújtani a pilóta nélküli légi járművek láthatóságára és nyomonkövethetőségére. Az Atom tartalmaz egy FLARM rádió adó-vevőt, egy ADS-B vevőt és egy wifiadót, amely támogatja többek között a távoli azonosítást is a megfelelő szabványoknak megfelelően, így alkalmazható Európában és az Egyesült Államokban is. A forgalmi adatok wifin vagy soros porton keresztül valósulnak meg.[13]

[12] *Operating Manual FLARM Collision Avoidance System* 2016.
[13] *Atom UAV Manual* 2021; *ATOM UAV. The Detect & Avoid Solution for Drones* é. n.

3. ábra: FLARM Atom modul kifejezetten a pilóta nélküli légi járművek számára
Forrás: ATOM UAV – Flarm for Drones é. n.

A modult kétféle kivitelben is gyártják, tokozva és tokozás nélkül. A rendszer képes használni a GPS-, Galileo-, EGNOS- és WAAS-rendszerek műholdjait. Tömegét (< 50 g) és méretét tekintve már kisméretű drónok fedélzetére is hatékonyan integrálható.

Aurora modul

Az Aurora szintén drónoknak szánt kisméretű modulegység. Gyakorlatilag a gyártó által kínált legkisebb, miniatürizált FLARM és Remote ID jeladót tartalmazó egység (lásd 4. ábra).

4. ábra: FLARM Aurora modul
Forrás: FLARM module Aurora é. n.

A rendszer egyik fő előnye, hogy használatával más FLARM-mal felszerelt légi járművek is képesek látni a környezetükben repülő pilóta nélküli légi járműveket. Így az a drón, amelyiknek a fedélzetén integrálva van a modul, alkalmas Európában és az Egyesült Államokban is drónműveletek végrehajtására, mivel megfelel a távoli azonosítási követelményeknek. Műszaki paramétereit tekintve

- modul tápenergia igénye 5 V (USB-C),
- frekvenciatartomány 868 Mhz (adás),
- a távoli azonosítást integrált wifimodul (2,4 GHz) biztosítja stb.

A modul kompatibilis számos gyártó, többek között a DJI termékekhez, mint például Matrice, Mavic, továbbá az Autel EVO 2 típushoz.

Open Glider Network – OGN

A légi forgalomban a „látni és elkerülni" elv betartása nélkülözhetetlen a biztonságos közlekedés érdekében. Légi járművek detektálására és nyomon követésére hatékony megoldás a hagyományos radarrendszerek alkalmazása. Azonban radarlefedettség hiányában lehetőség van más forrásból megszerezni adatokat, úgynevezett másodlagos információt szolgáltató rendszerek alkalmazásával. Ezen rendszerek egyik közös eleme a GNSS-alapú rendszerek által nyújtott helyzeti információkat tartalmazó adatok. Ezen adatok rendelkezésre bocsájtása a légtérben közlekedők számára, továbbá eljuttatása a földi irányítás számára, nagymértékben elősegítheti a biztonságos légi közlekedést.[14]

Egy másik megoldás is segítséget jelenthet a repülő társadalomnak, nevezetesen az „Open Glider Network", vagy ismertebb, rövidített nevén OGN-rendszer. Mivel bárki csatlakozhat a rendszerhez, így nemcsak egyre nagyobb felhasználói réteg alakul, hanem egyre több információnk lehet légi járművek, illetve drónok repülési helyzeti adatairól. A drónok fedélzetén nincs olyan jeladó, amely sugározza hollétüket, így csak nehézkesen lehet őket észrevenni és nyomon követni. Ennek egyik megoldása lehet egy jeladó regisztrálása az OGN-hálózatba, majd használata repülése folyamán. Így azokon a területeken, ahol van OGN-hálózati lefedettség, azonnal láthatóvá válik a környezetében közlekedő egyéb légi közlekedő számára, amennyiben a fedélzetén felhelyezésre került egy OGN-jeladó (tracker).

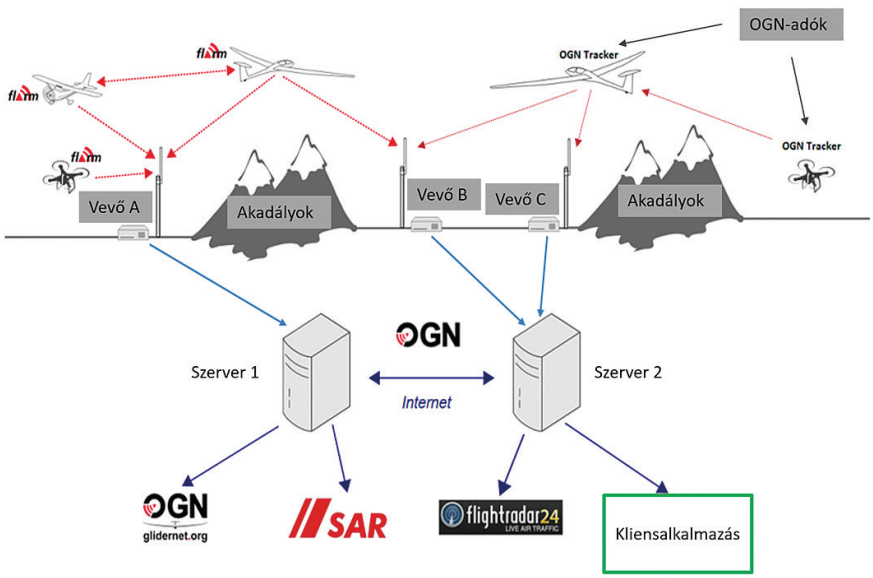
A rendszer nyújtotta előnyök közé tartozik továbbá, hogy hatékonyan alkalmazható speciális mentési műveletekben is (például SAR[15]). Egy ilyen mentési feladatban a legfontosabb az információk gyors és minél pontosabb megszerzése, annak érdekében, hogy a mentés mihamarabb megkezdődhessen.

Az OGN-rendszer alapjait a FLARM (Flight Alarm) adta, ami a továbbiakban is fontos szerepet játszhat légi járművek biztonságos közlekedésének támogatásában. Azonban az OGN-rendszer adóit (tracker) más funkciókkal is lehet bővíteni, mint például telemetriás vagy éppen meteorológiai adatok vételére és azok továbbítására.

[14] Makkay 2019.
[15] SAR, Search and Rescue – kutatás-mentés.

Az OGN-rendszert eredetileg a vitorlázórepülők biztonságosabb közlekedése érdekében hozták létre. A kezdeti fejlesztések a 2010-es évekig nyúlnak vissza. A rendszer folyamatos fejlesztésének, fejlődésének köszönhetően manapság közel 2000 OGN-vevőállomás létezik, 20 000 regisztrált felhasználóval, s eredményesen használható gyakorlatilag minden pilótával vagy anélkül vezetett repülőeszköz, légi jármű számára is, mint például drónok, kisrepülőgépek illetve siklóernyők (5. ábra).

Mi sem mutatja jobban a rendszerben rejlő potenciált, minthogy a 2019-ben megrendezett AERO 2019 kiállításon az EASA[16] első díjjal jutalmazta a rendszer egyik fejlesztőjét, Sebastian Chaumont-et.[17]



5. ábra: Az OGN-rendszer felépítése
Forrás: Open Glider Network é. n.

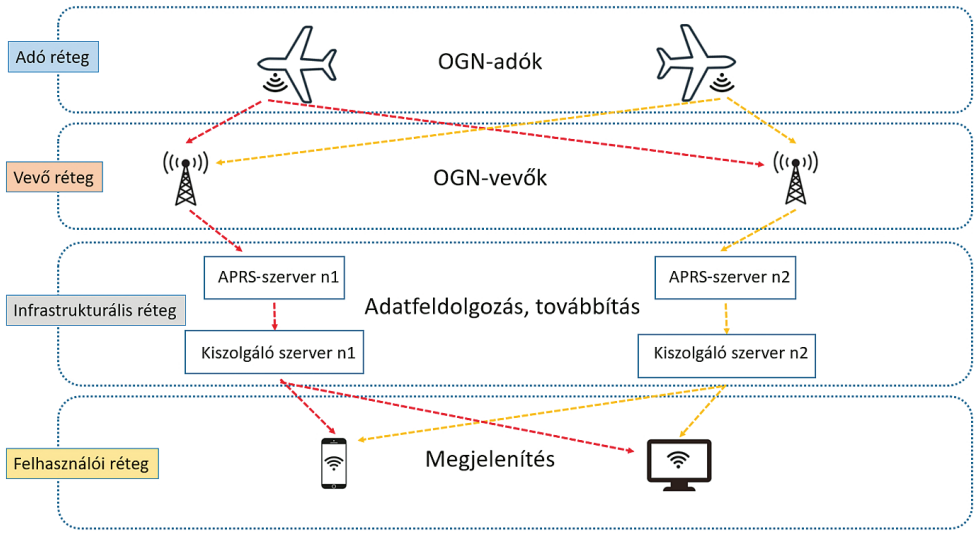
Maga a rendszer nyílt forráskódú adatátviteli protokollal működik. Ingyenes, bárki számára hozzáférhető és használható, amennyiben rendelkezik a felhasználó a minimális infrastrukturális feltételekkel.

A rendszer az alábbi összetevőkből épül fel:

- földi telepítésű OGN-vevőállomások;
- a légi járműveken elhelyezett OGN-adók (tracker);
- APRS (Automatic Packet Reporting System) Linux-alapú szerverek, amelyek fogadják és továbbítják a szükséges adatokat;
- adatokat feldolgozni és/vagy megjeleníteni képes webhelyek és alkalmazások;
- a humán szegmensből, akik használják a rendszert és a fejlesztők.

[16] EASA, European Union Aviation Safety Agency – Európai Repülésbiztonsági Ügynökség.
[17] *EASA Announces Winners of First GA Safety Award* 2020.

Az OGN-hálózat strukturális felépítése négy fő részre osztható: adó, vevő, infrastrukturális, felhasználói réteg (6. ábra).

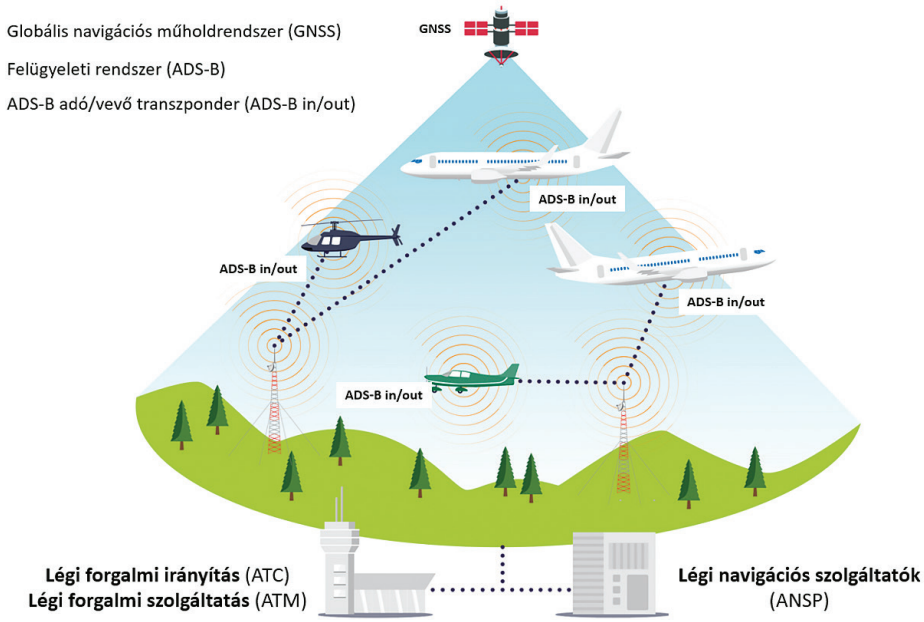


6. ábra: Az OGN-hálózat strukturális felépítése
Forrás: About OGN é. n.

Alapvetően három fő rétegre, szintre osztható a rendszer. Vevő, infrastrukturális és a felhasználói réteg. A vevő réteghez kapcsolódnak közvetlenül az OGN tracker adók. Ezek az adók szolgáltatják a légi jármű alaphelyzeti adatait további feldolgozásra. A vevőállomások között nem történik közvetlen kommunikáció. Azonban a vevők közötti információcsere az OGN infrastrukturális szinten valósul meg. Az APRS-szerverekhez kapcsolódnak a kliensszerverek, amelyeken keresztül az adatok nyilvánosan elérhetők a különböző webes felületeken (Gliderradar, Live Glidernet, Live Safesky stb.).

ADS-B rendszer

Az „Automatic Dependent Surveillance-Broadcast" (ADS-B) egy olyan komplex adó-vevő rendszer, amelynek célja, hogy beazonosíthatók és maghatározhatók legyenek a légi járművek repülésük alatt, mind a légtérben közlekedők számára, mind pedig a földi irányító szervezeteknek egyaránt (7. ábra).



7. ábra: ADS-B rendszer felépítése
Forrás: Introduction to ADS-B é. n.a

Az adó-vevők által kisugárzott adatok tartalmazzák a légi jármű helyzeti koordinátáit, azonosítóját és a magasság- és sebességadatokat. Az információcsomagokat rádiófrekvencián (978 MHz és/vagy 1090 MHz) sugározzák ki és veszik, így más repülőgépek és irányítóközpontok is képesek fogadni és továbbítani az információkat, valós időben. Mindez pontosabb és megbízhatóbb adatokat szolgáltat, mint a hagyományos radaralapú rendszerek.[18]

Az ADS-B adó-vevőknek alapvetően három változata létezik:

- ADS-B Out: adatok kisugárzására képes a forgalomirányítás és repülőgépek számára;
- ADS-B In: más repülőgépek pozícióadatainak fogadására képes;
- ADS-B In&Out: saját adatok küldésére és fogadására is képes.[19]

Az ADS-B Out-tal felszerelt repülőgépek adatokat sugároznak ki. Ezeket az adatokat egyrészt az ADS-B vevőállomások tudják fogadni, másrészt képesek fogadni más repülőgépek is, amennyiben fel vannak szerelve ADS-B In vevővel, illetve amennyiben vételi távolságon belül repülnek.[20]

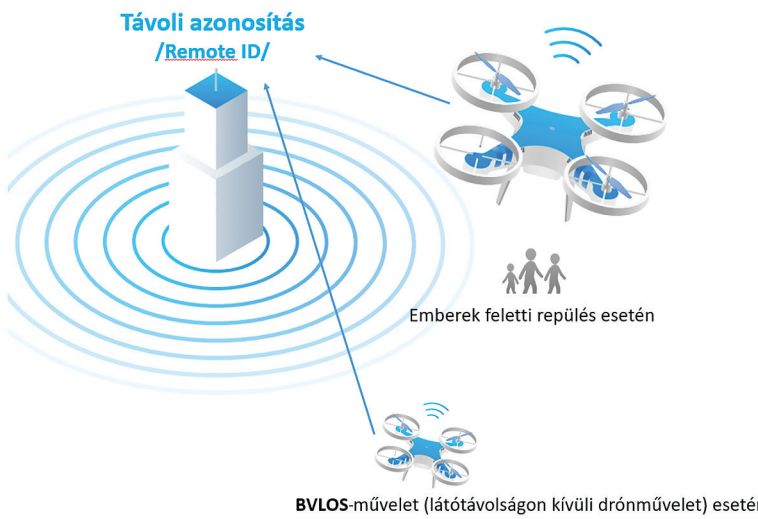
[18] *An Introduction into ADS-B* é. n.
[19] *What is an ADS-B System?* 2022.
[20] *Introduction to ADS-B* é. n.b

Remote ID

A Remote ID-t drónok azonosítása céljából fejlesztik napjainkban is. Gyakorlatilag nem más, mint a drónok „digitális rendszáma". A drón a saját azonosítószámát, illetve helyzeti adatokat sugároz ki egy hálózatba, amelyhez az illetékes hatóságok hozzáférnek. Az FAA távoli azonosítására vonatkozó irányelveket 2023. szeptember 16-ig tervezte bevezetni a drónpilóták közösségén belül. Azonban ezt az időpontot meghosszabbították 2024. március 16-ig. A bevezetendő intézkedések esetében alapvetően három opció jöhet számításba a jövőben drónok azonosítását illetően:

- Standard Remote ID modul – gyártók által beépített modul;
- Remote ID broadcast modul – a már meglévő és használatban lévő drónok fedélzetére utólagosan beépíthető modul;
- Remote ID-vel nem rendelkező drónok, amelyek csak meghatározott helyen repülhetnek e képesség hiányában (FRIAs[21]).[22]

A szabványosított, egységes rendszer bevezetésének a célja, hogy minden, 250 grammnál nagyobb tömegű drón fedélzetén legyen a Remote ID azonosító modul, amelyet vagy a gyártó már integrált a drónok fedélzetére, vagy pedig az üzemeltető utólagosan maga helyezi fel. Alapvető cél az, hogy minden olyan drónnak a fedélzetén legyen ilyen modul, illetve azonosító rendszer, amelyeket BVLOS-műveletben vagy emberek feletti területen szeretnének üzemeltetni (8. ábra).



8. ábra: Remote ID alkalmazásának vázlata
Forrás: Compliance with FAA Remote ID Regulations 2022.

[21] FAA-Recognized Identification Areas – FAA által minősített, Remote ID képesség nélkül is repülhető területek.
[22] *Remote Identification of Drones* é. n.

Most nézzük meg, hogy mi a jelenlegi helyzet Európában a távoli azonosítórendszer bevezetését illetően.

A távoli azonosító platform megvalósítását, azaz a Remote ID bevezetését, illetve az EASA-szabályoknak történő megfeleltetését 2024. január 1-jére halasztották. Az irányelvek szerint minden drónt fel kell szerelni Direct Remote ID képességgel, kivéve Class 0 osztályú drónok esetén, amikor is az MTOM[23] kevesebb mint 250 g, illetve Class 3-4 osztályú drónok esetén, amikor is az MTOM kevesebb mint 25 kg.

Az Európai Unióban a távoli azonosítás követelményrendszere szerint – alapul véve és javarészt alkalmazva az FAA irányelveit – az alábbiakat kell sugározniuk:

- drón egyedi sorozatszáma;
- drón regisztrációs száma;
- a drón földrajzi helyzetét és magasságát az adott helyhez vagy a felszállási ponthoz viszonyítva;
- a drón útvonalának irányát, sebességét;
- az üzemeltető vagy felszállási pont földrajzi helyzetét stb.[24]

A Remote ID modul felszerelésére számos gyártó kíván megoldást nyújtani (9. ábra).

9. ábra: Remote ID univerzális modulok
Forrás: Remote ID é. n.

A 9. ábrán illusztrált modulok mindegyike kompatibilis az ArduPilottal[25] így a már meglévő vagy egyedi fejlesztésű drónok fedélzetére is biztonságosan integrálhatók.

[23] Maximal Takeoff Mass – maximális felszálló tömeg.
[24] Gross 2023.
[25] Az ArduPilot egy nyílt forráskódú szoftver.

A drónygyártóknak meg kell felelni az FAA és EASA által előírt távoli azonosításra vonatkozó követelményrendszernek, amennyiben szeretnék a jövőben értékesíteni termékeiket. Ennek értelmében már számos gyártó integrálta a Remote ID képességet drónjai fedélzetére, például a DJI Mini 3, a Mavic 3 vagy az Autel Robotics Dragonfish stb.[26]

Összegzés

A pilóta nélküli légi járművek légi közlekedésbe való integrálásának folyamata napjainkban is zajlik, és kiemelt feladatnak számít szerte a világon. A hagyományos légi járművek azonosítását és adatainak a sugárzását és vételét szolgáló rendszerek mellett megjelennek olyan műszaki megoldások, amelyek képesek a drónok észlelhetőségét, nyomon követését, illetve azonosítását megvalósítani. Ezen rendszerek minél szélesebb körű használata kulcsfontosságú a légi közlekedésben részt vevők számára.

Irodalomjegyzék

About OGN [é. n.]. Online: http://wiki.glidernet.org/about#system-arch-current
An Introduction into ADS-B [é. n.]. Online: www.flightradar24.com/blog/ads-b/
Atom UAV Manual (2021). 2021. szeptember 30. Online: https://fcc.report/FCC-ID/2AXJM-FLATMUAVW/5495644.pdf
ATOM UAV – Flarm for Drones [é. n.]. Online: https://droniq.de/en/produkte/atom-uav-flarm-fuer-drohnen/
ATOM UAV. The Detect & Avoid Solution for Drones [é. n.]. Online: www.flarm.com/products/uav/atom-uav-flarm-for-drones/
Compliance with FAA Remote ID Regulations (2022). Online: https://lp.elsight.com/compliance-with-faa-remote-id-regulations
EASA Announces Winners of First GA Safety Award (2020). Online: www.easa.europa.eu/en/newsroom-and-events/news/easa-announces-winners-first-ga-safety-award
FLARM module Aurora [é. n.]. Online: www.airclip.de/FLARM-module-Aurora
Gajdács László (2022): Pilóta nélküli légijármű érzékelésének lehetséges megoldásai, *Hadmérnök,* 17(4), 17–28. Online: https://doi.org/10.32567/hm.2022.4.2
Gross, Ben (2023): *EASA Remote ID Requirements: Compliance for Drone Operators.* Online: www.elsight.com/blog/primer-on-easa-remote-id-regulations/
Introduction to ADS-B [é. n.a]. Online: https://ads-b.aviation.govt.nz/introduction/#-how-does-ads-b-work
Introduction to ADS-B [é. n.b]. Online: www.trig-avionics.com/knowledge-bank/ads-b/introduction-to-ads-b/
Makkay Imre (2019): Másodlagos információforrások a légtérben. *Repüléstudományi Közlemények,* 31(1). Online: https://doi.org/10.32560/rk.2019.1.9
Open Glider Network [é. n.]. Online: http://wiki.glidernet.org/

[26] *What is Remote ID* é. n.

Operating Manual FLARM Collision Avoidance System (2016). Version 242. 2016. december 8.
Remote Identification of Drones [é. n.]. Online: www.faa.gov/uas/getting_started/remote_id
Remote ID [é. n.]. Online: https://ardupilot.org/copter/docs/common-remoteid.html
Tecnology Editor, Sense and Avoid Technology [é. n.]. Online: www.unmannedsystemstechnology.com/expo/sense-avoid-systems/
Wang, Boya – Tresoldi, Giorgio [é. n.]: *On the Security of the FLARM Collision Warning System.* Online: https://wangboya.org/assets/pdf/Flarm_ASIACCS_camera_ready.pdf
What is an ADS-B System? (2022). Online: www.embention.com/news/what-is-an-ads-b-system/
What is Remote ID [é. n.]. Online: https://drone-remote-id.com/

HADMÉRNÖK
KATONAI MŰSZAKI INFRASTRUKTÚRA

18. évfolyam (2023) 4. szám 19–29.
DOI: 10.32567/hm.2023.4.2

Ember István[1]

Alacsony sűrűségű idomtöltetek tesztrobbantása[2]

Test Blasting of Low-Density Shaped Charges

Absztrakt

A 3D nyomtatás alkalmazása a robbantástechnikában is jelentős előnyöket hordozhat. Mivel széles körben elterjedt technológia, ezért a bevezetése nem jelenthet kihívást. A lehetséges alkalmazási terület pedig a különleges formájú idomtöltetek lehetnek. Vizsgálatomban olyan töltetek robbantási hatékonyságát mutatom be, amelyek nem tartalmaznak fémet, kizárólag alacsony sűrűségű anyagból készültek. A hatékonyságot tesztrobbantással vizsgáltam, amely során a kétféle eltérő béléstest-hajlásszöggel készült verzió megfelelt az elvárásoknak. A kevesebb befektetett energiát igénylő változat teljesítménye jobb volt, meggyőző képet mutatott.

Kulcsszavak: alacsony sűrűség, 3D nyomtatás, vágótöltet, robbantás, additív

Abstract

The use of 3D printing in blasting technology can also bring significant benefits. As a widespread technology, its introduction should not be a challenge. A potential application could be in the field of special shaped charges. In my study, I will demonstrate the explosive performance of such charges, which do not contain any metal and are made exclusively of low-density materials. The effectiveness was tested by blasting, where two versions

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Műveleti Támogató Tanszék, egyetemi tanársegéd; Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Hadtudományi Doktori Iskola, doktorandusz, e-mail: Ember.Istvan@uni-nke.hu

[2] A cikk a Kulturális és Innovációs Minisztérium ÚNKP-22-3-II-NKE-27 kódszámú Új Nemzeti Kiválóság Programjának a nemzeti kutatási, fejlesztési és innovációs alapból finanszírozott szakmai támogatásával készült.

with different liner body bending angles met the expectations. The version requiring less energy input performed better and presented a convincing picture.

Keywords: low-density, 3D printing, cutting charge, blasting, additive

Bevezetés

Az olcsó és gyors additív gyártás[3] terjedése megállíthatatlannak látszik világunkban. A manapság 3D nyomtatásnak nevezett eljárásnak több változata is lehetséges, az alacsony sűrűségű alapanyagok, polimerek esetében ez akár a háztartások számára is elérhető.

Érdemes tehát abból a szempontból is vizsgálni a technológiát, hogy miként lehet kiaknázni a benne rejlő katonai lehetőségeket. Az mindenesetre kijelenthető, hogy egy ilyen technológia robbantástechnikai implementációja illeszkedik a hadtudomány legfontosabb vizsgálandó kérdéseibe.[4]

Az általam készített és az általánosságban használt kumulatív töltetek valamilyen brizáns[5] és/vagy bináris[6] robbanóanyaggal készülnek, és a robbanás energiáját sugárba rendezve képesek értékes munkát végezni.[7] A helyszínen tölthető változatok plasztikus vagy folyékony robbanóanyaggal szerelhetők készre.

A bemutatott teszt során kizárólag alacsony sűrűségű anyagokat használtam fel a töltetek gyártásához. Ez minden alkatrészükre igaz, a béléstestre és a töltetházra egyaránt. A fémek alkalmazása kumulatív töltetekben különböző célokkal már nagy kutatási és felhasználási múltra tekint vissza, azok legtöbb paraméterét, körülményét[8] már ismerjük. Az alacsony sűrűségű anyagok alkalmazása kevésbé vizsgált, mert az ilyen béléstestek jelentősen kisebb lyukasztási és vágási képességgel rendelkeznek. Természetesen a hátrányaik mellett előnyös tulajdonságaik is vannak egyes esetekben. Vannak azonban viszonylag friss eredmények a polimerek esetében, amelyek kínai kutatók munkásságához kötődnek, ahol ezeknek az anyagoknak a megnyúlását vizsgálták a jet formálódása közben.[9] Egy másik előremutató vizsgálatot pedig szimulációs környezetben végeztek el a szakemberek.[10]

Az általam bemutatott vizsgálatok során kizárólag additív megoldással készült tölteteket robbantottam fel, két változatban, eltérő hajlásszögű béléstesttel. A feltételezésem szerint az idomtöltetek hatékonyak lesznek mindkét verzióban. Esetleges probléma a céltárgyak sarkainál jelentkezhet, ahol az acél vastagsága mérhetően nagyobb lesz a belső lekerekítés miatt. Ezeken a részeken előfordulhat, hogy részlegesen megmarad az anyagfolytonosság, de a tartószerkezeti funkció teljes megszűnését várom minden esetben.

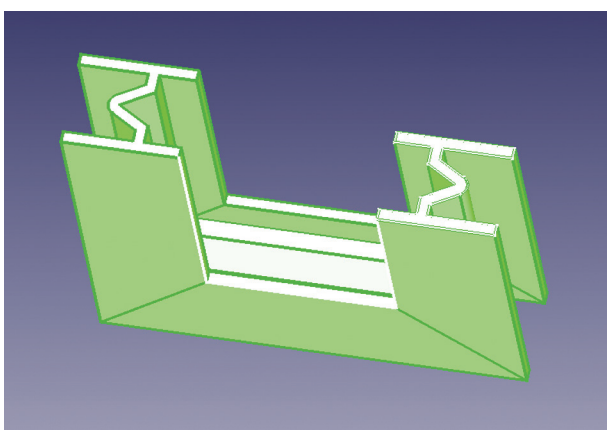
[3] Gál–Németh 2019: 233.
[4] Boda et al. 2016: 1–23.
[5] Lukács 2017: 26.
[6] Kugyela 2020: 58–75.
[7] Lukács 2010: 175–185.
[8] Doig 1998: 1–3.
[9] Yi et al. 2019: 744.
[10] Chang et al. 2019: 426–437.

A vizsgált töltetek

Minden egyes töltettípust egyedileg terveztem meg, figyelembe véve a céltárgy paramétereit. A falvastagságuk mindenhol 3 mm, amely adatot a korábbi kutatási adataimra alapozva határoztam meg.[11] Érdemes lehet vizsgálatra ennél vékonyabb vágóél is, mert a lent hivatkozott disszertációban ennél vékonyabb kumulatív béléstest is ért el viszonylag nagy átütést.[12] Véleményem szerint ez nem lehetetlen, de az eddigi tapasztalataim nem támasztják alá az állítást.

A politejsav (PLA[13]) megfelelő alapanyagnak tűnt, mert bőséges és elérhető tapasztalat áll rendelkezésre felhasználásáról. További előnye, hogy viszonylag olcsó és könnyen beszerezhető, s már személyes tapasztalataim is vannak az anyaggal,[14] ami jó alapnak tekinthető a töltetek készítésekor.

A vágótöltetek esetében olyan számvetéssel kell a méretet meghatározni, hogy a gyutacs végétől hozzávetőleg 10 mm-re éri el a detonációs sebesség a robbanóanyagra jellemző értéket. Ez persze csak egy becsült, tapasztalatokon nyugvó adat az általam alkalmazott plasztikus robbanóanyag esetében. A gyutacsoknál szintén 10 mm-t tekintek a legkisebb behelyezési mélységnek, bár ez is típusfüggő adat. Éppen ezért az idomtöltet indított oldalát 30 mm-rel hosszabbra terveztem, hogy biztosan eredményesen induljon meg a vágás a céltárgyon. A kilépő oldalon 10 mm ráhagyást hagytam annak érdekében, hogy biztosan eredményesen vágjon a céltárgy legvégén is a töltet.



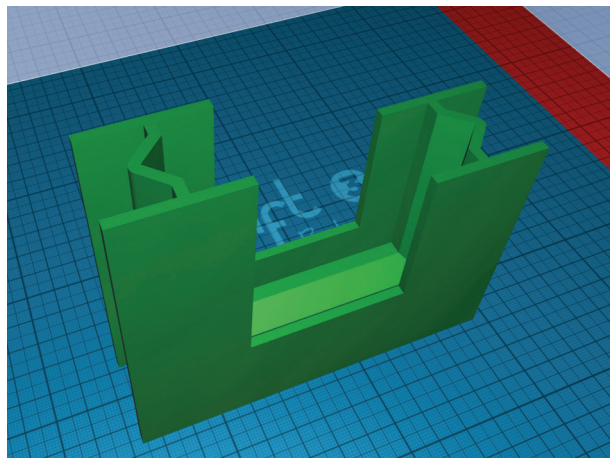
1. ábra: Egy 60°-os kumulatív idomtöltet képe a tervezőszoftverben
Forrás: a szerző szerkesztése

A béléstest a töltetházzal egy testet képez, amelyet főleg gyártástechnológiai okból alakítottam ki ebben a formában. Két hajlásszögben készültek el az idomtöltetek, a 60°

[11] Ember 2022a: 13–23; Ember 2022b: 15–20; Ember 2022c: 63–73.
[12] Agu 2019.
[13] Angolul: poly lactic acid.
[14] Ádám–Ember 2022a: 101–111; Ádám–Ember 2022b: 35–44.

és 90° teljesítménye akár jelentősen is eltérhet, a további optimalizáláshoz fontos adatokat szolgáltathatnak majd az eltérő robbantási minták. A vágóélek 15 mm-es nyílással készültek el.

Az 1. ábrán egy 60°-os változatot mutatok be a tervező szoftver felületén, amelyet 50 mm-es „U" szelvényből készült céltárgyhoz méreteztem.



2. ábra: Egy 90°-os kumulatív idomtöltetmodell a g-code előállításakor
Forrás: a szerző szerkesztése

A 3D modelleket számítógéppel támogatott tervezéssel (CAD[15]), modellezéssel készítettem el. Mivel egyedi kialakítású töltetekről van szó, ez nélkülözhetetlen feladat volt. A modelleket FreeCAD 0.19 szoftverrel készítettem. A nyomtatást minden esetben „duál extruderes"[16] CraftBot 3 nyomtatóval végeztem. A fúvóka 0,8 mm-es volt, amely lehetővé tette, hogy viszonylag gyorsan elkészíthessem a tárgyakat. A gyártáshoz ugyanazon gyártó eltérő színű, de egyező minőségű filamentjeit[17] használtam fel.

Mivel szálhúzásos vagy szálolvasztásos (FDM[18]) rendszerű gyártást alkalmaztam, ezért ennek előnyeit, hátrányait és nyomtatóképességeit már a tervezés során figyelembe kellett vennem. Az eljárás sajátossága, hogy a tárgyasztalra merőleges és egy meghatározott hajlásszög felett álló felületeket csak alátámasztással képes elkészíteni. A tervezés már e támaszok optimális kialakítása mellett zajlott, mert ezek anyagfelhasználás és a végleges felület minősége szempontjaiból nagy hatással lehetnek. A támaszok kialakíthatók vízben oldható anyagból (PVA[19]) is, amely nagyban növeli a termék felületének minőségét, és eltávolítása ugyan egyszerű, de jelentős költséggel jár, ezért alkalmazását elvetettem.

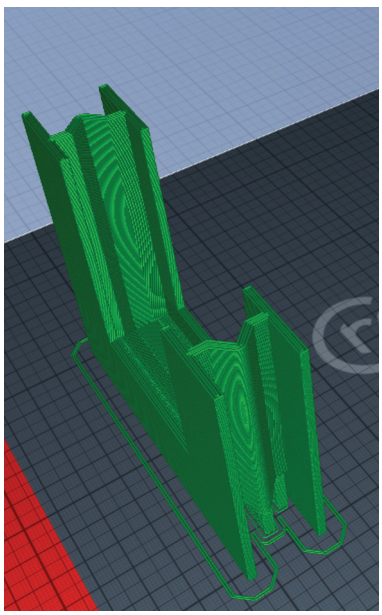
15 Angolul: computer-aided design.
16 Két nyomtatófej egyidejű vagy váltott alkalmazására képes.
17 Tekercselt alapanyagszál, amelyet a nyomtató megolvaszt.
18 Angolul: fused deposition modelling.
19 Polivinil-alkohol.

1. táblázat: A nyomtatások idő- és anyagszükségletei

Fsz.	Típus	Filament hossz (m)	Nyomtatási idő (min)
1.	15–60–U50	46,7	314
2.	15–90–U50	38,9	258

Forrás: a szerző szerkesztése

A gyártás időszükséglete az 1. táblázatban látható, amely a valóságban kismértékben nagyobbnak bizonyult. A felhasznált filament becsült hosszát a CraftWare szoftver számította ki, amellyel a g-code[20] előállítását végeztem.



3. ábra: Egy 60°-os kumulatív idomtöltet a g-code előállításakor
Forrás: a szerző szerkesztése

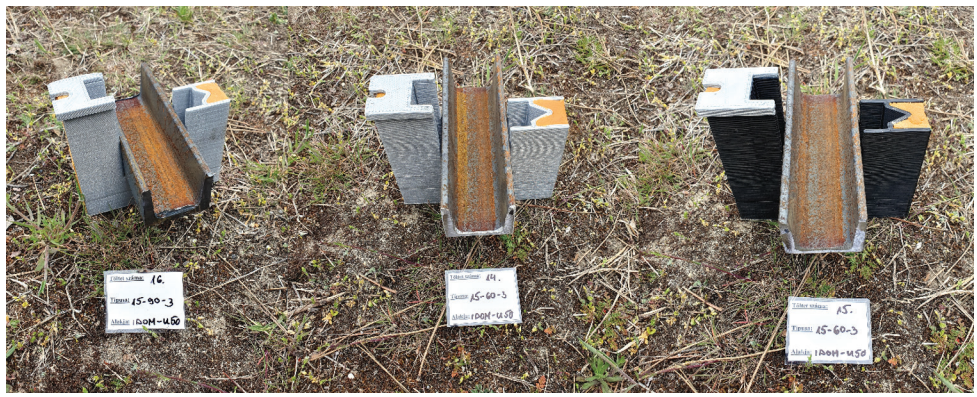
A vizsgálat körülményei

A gyakorlati vizsgálatokat a Magyar Honvédség (MH) robbantási területén, Táborfalván végeztem el, amelyhez az MH 1. Tűzszerész és Folyamőr Ezred (MH 1. TFE) minden feltételt biztosított.

A robbantási feladat során villamos gyújtóhálózatot alkalmaztam, soros kapcsolásba rendezett villamos gyutacsokkal. Mivel a Semtex-H tulajdonságai kiválóan

[20] A nyomtató által feldolgozható adatokat tartalmazó fájltípus, amely a nyomtatás paramétereit hordozza.

alkalmasak a legyártott töltetek helyszíni feltöltéséhez és a kumulatív hatás hatékony kialakításához,[21] ezért erre a robbanóanyagra esett a választásom. Minden idomtöltetet egy fedlappal egészítettem ki, hogy a gyutacs központi elhelyezése, ezzel a detonáció optimális elindítása biztosítva legyen. A fedlap által vezetett helyzetben a gyutacsokat pontosan 10 mm-re helyeztem be a robbanóanyagba.



4. ábra: A 60°-os kumulatív idomtöltetek 50 mm-es „U" szelvény céltárgyakkal
Forrás: a szerző felvétele

A robbantás során egy 150 cm mély árok aljában kialakított 30 x 30 x 30 cm-es ágyakban helyeztem el a céltárgyakat a rájuk rögzített töltetekkel. Ebben a formában a detonációk nem lehettek hatással egymásra. A biztonság – mint legfontosabb tényező a robbantási feladatoknál[22] – nem sérült. Repeszkiszóródást nem lehetett azonosítani a gyújtóhelyről és a helyszíni nyomokból sem.

5. ábra: A 90°-os kumulatív idomtöltetek 50 mm-es „U" szelvény céltárgyakkal
Forrás: a szerző felvétele

[21] Daruka 2016: 39; Daruka–Csurgó 2017: 44–55.
[22] Padányi 1994: 63.

A töltetek tömegét, feltöltöttségét külön-külön méréssel ellenőriztem, amely adatok a 2. táblázatban láthatók. A táblázat alapján azonosítható, hogy hajlásszögenként 3–3 db nyomtatott idomtöltet készült. Mivel egy típusú céltárgy volt a vizsgálat tárgya, amely melegen hengerelt, szabványos, 50 mm-es „U" szelvény volt (150 mm hosszúra darabolva), ezért a fenti adatokkal kombinálva összesen 6 db felrobbantandó töltetre volt szükségem. Mindegyikük (4. és 5. ábra) rövidítésekből álló elnevezést kapott, amely a vágóél belső szélességéből mm-ben (15 mm), a vágóél hajlási szögéből (60° vagy 90°) és a céltárgy típusából épült fel.

2. táblázat: A felrobbantott töltetek paraméterei

Fsz.	Típus	Töltetház tömege (g)	Robbanóanyag tömege (g)	Szerelt tömege (g)
1.	15–60–U50	121	179	300
2.	15–60–U50	121	179	300
3.	15–60–U50	120	178	298
4.	15–90–U50	99	141	240
5.	15–90–U50	100	143	243
6.	15–90–U50	100	142	242

Forrás: a szerző szerkesztése

A töltetházak tömegadatai szinte tökéletesen egyező képet adnak a feltöltés és a gyártás sikerességéről. Mindkét esetben egyaránt csupán 1–2 g-os eltérés jelentkezett. A robbanóanyagnál a tömeg akár a hatékonyságra is hatással lehet, de ez a szinte jelentéktelen eltérés nem befolyásolhatta számottevő módon az eredményeket.

A robbantás előkészítésének folyamata az alábbi lépésekből állt:

- a gyutacs illesztésére szolgáló fedlapok rögzítése;
- a töltetházak tömegének ellenőrzése üres állapotban;
- a töltetek feltöltése plasztikus robbanóanyaggal;
- a töltetek tömegének ellenőrzése digitális mérleggel;
- a töltetek rögzítése a céltárgyakhoz ragasztószalaggal;
- a céltárgyak és töltetek behelyezése a robbantásra kialakított gödrökbe;
- a villamos gyutacsok behelyezése a töltetekbe.

A vizsgálati eredmények

Az 1. töltettípus 15 mm-re nyitott vágóéllel rendelkezett és 60°-os hajlásszöggel készült. A céltárgyat 50 mm-es szabvány „U" szelvényből daraboltam. A robbantás eredményei a 6. ábrán láthatók.

Az első töltet teljes vágást eredményezett, a vágott felületen jelentős mértékben szakadásos képlet látható. A robbantott keresztmetszet torzult, összenyomódott. A céltárgy egyik fele nem került elő, mert a kialakított védmű beomló fala maga alá temette, de ez az eredményt nem kérdőjelezi meg.

A második töltet esetében is fellépett anyagtorzulás a robbantott keresztmetszetben. Az indított oldalon határozott vágás látható, a hosszú oldalon 24 x 13 mm-es lyuk alakult ki, és 6 mm-en valamelyest megmaradt az anyagfolytonosság, bár repedezett a felület. A hátsó oldalon szintén azonosítható a vágás, azonban 10 mm-en egyben maradt a céltárgy.

A harmadik céltárgy a másodikkal egyező módon torzult. Az indított fele teljesen elvált, a hosszú oldalon 22 x 10 mm-es lyukasztás tapasztalható, és 15 mm-en nem történt csak részleges vágás. A hátulsó oldal esetében egy 15 mm-es szakaszon anyagfolytonosság látható.

6. ábra: Az 1. töltettípus vágási eredményei
Forrás: a szerző felvétele

A 2. töltettípus 15 mm-re nyitott vágóéllel és 90°-os hajlásszöggel készült. A céltárgyat itt is 50 mm-es szabvány „U" szelvényből daraboltam. A robbantás eredményei a 7. ábrán láthatók.

Az első és a második töltet képes volt a teljes vágásra, a vágott felületen meghatározó mértékben szakadásos képlet látható. A robbantott keresztmetszet súlyosan összenyomódott.

A harmadik céltárgy a robbantott keresztmetszetben összenyomódott. Az indított fele teljesen és szabályosan elvált. A hosszú oldalon 23 x 12 mm-es lyukasztás tapasztalható, elenyésző 3 mm-en részlegesen egyben maradt a két oldal. A hátulsó oldalon szintén nem vált szét egy 7 mm-es szakasz.

7. ábra: A 2. töltettípus vágási eredményei
Forrás: a szerző felvétele

Összegzés

Elsősorban a tervezés és paramétermeghatározás során kalkulált adatokat szeretném összegezni. A 3 mm-es anyagvastagság megfelelőnek és hatékonynak bizonyult. A test kibírta a töltés erőhatásait, a béléstest pedig képes volt eredményes és hatékony vágást produkálni. A 30 mm-es bemeneti és a 10 mm-es kimeneti oldali túlnyúlás is teljesítette az elvártakat, a detonáció rendezetten ki tudott alakulni, ezzel megteremtve a vágás feltételeit a töltetben.

A 60°-os változat eredményesen szerepelt. Egy esetben teljesen elérte a célját, de a másik két céltárgy esetében is olyan jelentős volt a roncsolás, hogy azok alapfunkcióját egy tartószerkezetben minden kétséget kizáróan megszüntette volna a robbanás.

A 90°-os típus szerepelt hatékonyabban a teszteken, annak ellenére, hogy gyártási ideje (–18%), a felhasznált alapanyag (–17%) és robbanóanyag mennyisége (–21%) is kevesebb volt ezeknél a tölteteknél. Két céltárgyat teljesen elvágtak ezek a változatok, és a harmadik esetében is csak szinte jelentéktelen mennyiségben maradt meg az anyagkapcsolat.

Az kijelenthető, hogy ezek a 90°-os vágóéllel készült idomtöltetek alkalmasabbak lehetnek tartószerkezetek elemeinek rombolására, mint a 60°-os változatok. Ennek minden kétséget kizáró eredményéhez és a késztermék optimalizációjához azonban még szükségesek lehetnek további vizsgálatok, robbantások. A bemutatott változat azonban ebben a formájában is alkalmas a céltárgy profiljából készült tartók megsemmisítésére.

További érdekes kutatási irány lehetne a nagyobb átmérőjű, hengeres alakú katonai eredetű robbanótestek[23] vagy akár improvizált robbanótestek[24] készítésekor felhasznált hadi alapanyagok esetében is megvizsgálni az alkalmazhatóságát az ilyen idomtölteteknek.

Érdekes és elgondolkodtató lenne mesterséges intelligencia (MI) és a 3D nyomtatás kombinált felhasználásának elemzése. Minkettő esetében folynak kutatások, amelyek a katonai alkalmazás lehetőségeit vizsgálják. A MI katonai alkalmazásának előnyeihez nem igazán férhet kétség,[25] de a 3D nyomtatás hozadéka a katonák[26] vagy akár a katonai felsőoktatás számára[27] egyaránt jelentős lehet a jövőben. A két terület fúziójának kutatását kifejezetten fontos vizsgálati iránynak tartom.

Irodalomjegyzék

ÁDÁM Balázs – EMBER István (2022a): Béléstestek készítésének technikai lehetőségei alacsony sűrűségű anyagból. *Műszaki Katonai Közlöny,* 32(4), 101–111. Online: https://doi.org/10.32562/mkk.2022.3.6

[23] DARUKA 2014: 70–78.
[24] KOVÁCS 2012a: 37–52; KOVÁCS 2012b: 35–44; DARUKA–KOVÁCS 2013: 384–389.
[25] NÉMETH–VIRÁGH 2022: 21; FAZEKAS 2022: 51–52; TÓTH–VÉG 2022: 114.
[26] VÉGVÁRI–HEGEDŰS–ZENTAY 2022: 58–62.
[27] GYARMATI–HEGEDŰS–GÁVAY 2022: 125–126.

Ádám Balázs – Ember István (2022b): Kumulatív töltetházak 3D nyomtatása. *Hadmérnök,* 17(3), 35–44. Online: https://doi.org/10.32567/hm.2022.3.2

Agu, Henry Obediah (2019): *The Effect of 3D Printed Material Properties on Shaped Charge Liner Performance.* PhD-disszertáció. Cranfeld University. Online: https://dspace.lib.cranfield.ac.uk/handle/1826/15285

Boda József et al. (2016): A hadtudományi kutatási irányok, prioritások és témakörök. *Államtudományi Műhelytanulmányok,* (16), 1–23. Online: www.med.u-szeged.hu/download.php?docID=90702

Chang et al. (2015): Numerical Simulation of Modified Low-Density Jet Penetrating Shell Charge. *International Journal of Simulation Modelling,* 14(3), 426–437. Online: https://doi.org/10.2507/IJSIMM14(3)5.295

Daruka Norbert (2014): Robbanótestek I. – Amit a bombákról tudni érdemes. *Műszaki Katonai Közlöny,* 24(4), 68–82. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/2298/1565

Daruka Norbert (2016): Robbanóanyag-ipari alapanyagok és termékek osztályozásának lehetőségei. *Műszaki Katonai Közlöny,* 26(1), 26–44. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/2187/1456

Daruka, Norbert – Kovács, Zoltán (2013): IEDD: Improvised Explosive Device Disposal. In Krivanek, Vaclav – Stefek, Aleksandr (szerk.): *International Conference on Military Technologies: ICMT 2013.* Brno: University of Defence, 383–390.

Daruka, Norbert – Csurgó, Attila (2017): Military Explosive Ordnance – The Bomb. In Beňovský, M. (szerk.): *Trhacia technika 2017: Zborník prednášok.* Banská Bystrica: Slovenská spoločnosť pre trhacie a vŕtacie práce, 44–55.

Doig, Alistair (1998): Some Metallurgical Aspects of Shaped Charge Liners. *Journal of Battlefield Technology,* 1(1), 1–3.

Ember István (2022a): Hatásvizsgálati robbantás kumulatív töltetekkel. *Műszaki Katonai Közlöny,* 32(4), 13–23. Online: https://doi.org/10.32562/mkk.2022.3.2

Ember István (2022b): Modern kumulatív töltetek hatékonyságának vizsgálata. *Haditechnika,* 56(6), 15–20. Online: https://doi.org/10.23713/HT.56.6.03 ; DOI: https://doi.org/10.23713/HT.56.6.03

Ember István (2022c): 3D nyomtatott lyukasztó töltetek hatásvizsgálata. *Hadmérnök,* 17(4), 63–73. Online: https://doi.org/10.32567/hm.2022.4.5

Fazekas, Ferenc (2022): Application of Artificial Intelligence in Military Operations Planning. *AARMS,* 21(2), 41–54. Online: https://doi.org/10.32565/aarms.2022.2.3

Gál Bence – Németh András (2019): Additív gyártástechnológiák katonai alkalmazásának vizsgálata, különös tekintettel a katonai elektronika területére. *Hadmérnök,* 14(1), 231–249. Online: https://doi.org/10.32567/hm.2019.1.19

Gyarmati József – Hegedűs Ernő – Gávay György (2022): Automata sebességváltóban alkalmazott kapcsolt bolygóművek – Wilson-váltó: Harckocsi-sebességváltó modell kialakítása 3D nyomtatással oktatási célból. *Műszaki Katonai Közlöny,* 32(3), 113–126. Online: https://doi.org/10.32562/mkk.2022.3.7

Kovács Zoltán (2012a): Az improvizált robbanóeszközök főbb típusai. *Műszaki Katonai Közlöny,* 22(2), 37–52. Online: https://mkk.uni-nke.hu/document/mkk-uni-nke-hu/2012_2_03 IED-k f%C5%91bb t%C3%ADpusai–Kov%C3%A1cs Z.pdf

Kovács Zoltán (2012b): Fontos létesítmények IED elleni védelme. *Műszaki Katonai Közlöny,* 22(ksz), 35–44. Online: https://mkk.uni-nke.hu/document/mkk-uni-nke-hu/2012_k_05 IED elleni v%C3%A9delem–Kov%C3%A1cs_Z.pdf

Kugyela Lóránd (2020): A többkomponensű robbanóanyagok múltja, jelene és jövője. *Katonai Logisztika,* 28(4), 58–75. Online: https://doi.org/10.30583/2020.4.058

Lukács László (2010): A kumulatív töltetek és gyakorlati alkalmazásuk. *Műszaki Katonai Közlöny,* 20(1–4), 175–185. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/2866/2122

Lukács László (2017): *Szemelvények a magyar robbantástechnika fejlődéstörténetéből, Különös tekintettel a továbbfejlesztés várható irányaira és a kor új kihívásaira*. Budapest: Dialóg Campus.

Németh András – Virágh Krisztián (2022): Mesterséges intelligencia és haderő – A mesterséges intelligencia fejlődéstörténete I. rész. *Hadmérnök,* 56(1), 17–22. Online: https://doi.org/10.23713/HT.56.1.03

Padányi József (1994): *A Magyar Honvédség műszaki csapatainak lehetőségei és feladatai békeidőben a természeti- és civilizációs katasztrófák megelőzésében és a következmények felszámolásában*. Kandidátusi értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem.

Tóth József Lukács – Vég Róbert (2022): Autonóm terepjáró eszközök. *Műszaki Katonai Közlöny,* 32(2), 107–116. Online: https://doi.org/10.32562/mkk.2022.2.8

Végvári Zsolt – Hegedűs Ernő – Zentay Péter (2022): A 3D nyomtatás és katonai alkalmazásának lehetőségei I. rész. *Haditechnika,* 56(6), 58–62. Online: https://doi.org/10.23713/HT.56.6.09

Yi, Jianya et al. (2019): Simulation Study on Expansive Jet Formation Characteristics of Polymer Liner. *Materials,* 12(5), 744. Online: https://doi.org/10.3390/ma12050744

HADMÉRNÖK
KIKÉPZÉS ÉS FELKÉSZÍTÉS

18. évfolyam (2023) 4. szám 31–51.
DOI: 10.32567/hm.2023.4.3

Kovács Gergely[1]

A védelmi szférában alkalmazható VR-alapú képzés/felkészítés lehetséges negatív fizikai és pszichológiai hatásai II.

Possible Negative Physical and Psychological Effects of VR-Based Training/Preparation in the Defence Sector II.

Absztrakt

Az elmúlt évtized digitális területen történt paradigmaváltásai a legimmerzívebb technológiák alkalmazását is magukkal hozták, mint például a VR, amely az oktatásban és képzésben is megjelent. E technológia rendszeresítése és tömeges alkalmazása előtt nagyon időszerűek a VR-alapú képzéssel, oktatással és annak fizikai, valamint pszichológiai hatásaival kapcsolatos vizsgálatok. A szerző cikksorozatban mutatja be ez irányú kutatásait, amelynek első részében elemezte a virtuális valóság (VR) védelmi területen való alkalmazásának lehetőségeit. Jelen cikkben empirikus kutatásban vizsgálja, hogy mi befolyásolja a VR-alapú oktatás és képzés hatékonyságát, elemzi a felhasználót érintő lehetséges negatív hatásokat. Vizsgálja a VR-használati hajlandóság néhány kérdését annak érdekében, hogy javaslatot tegyen a VR-alapú képzés hatékonyságának növelésére és az eszközhasználat lehetséges negatív hatásainak kiküszöbölésére.

Kulcsszavak: katonai felkészítés, virtuális valóság, fizikai és pszichológiai érzet, kiberbetegség, tanulási hatékonyság

[1] XR-kutató, Védelmi Innovációs Kutatóintézet, e-mail: Kovacs.Gergely@uni-nke.hu

Abstract

The paradigm shifts in the digital field over the last decade have brought with them the use of the most immersive technologies, such as VR, which has also been introduced in education and training. Studies on VR-based training and education and its physical and psychological effects are very timely before the systematic and mass adoption of this technology. The author presents his research in this area in a series of articles, the first part of which analyses the potential of virtual reality (VR) in the field of defence. In the present article, she uses empirical research to investigate the impact of VR-based education and training on its effectiveness, analysing the potential negative effects on the user. It examines some issues of VR user willingness in order to propose ways to increase the effectiveness of VR-based training and to eliminate possible negative effects of VR use.

Keywords: military training, virtual reality, physical and psychological sensation, cybersickness, learning effectiveness

Bevezetés

A jelenlegi geopolitikai viszonyok és egyéb sajnálatos tényezők számos területen fokozzák a globális feszültségeket.[2] A nagyhatalmak rivalizálása, a regionális konfliktusok,[3] a hagyományos és az aszimmetrikus hadviselés, a terrorizmus[4] és a kiberhadviselés[5] stb. mind olyan hatások, amelyek a védelmi szférában növelik az igényt az oktatás/képzés hatékonyságának növelésére.[6] Ebben a komplex kihívásokkal terhelt és kiszámíthatatlan biztonsági környezetben a hatékony oktatás, képzés, kiképzés, felkészítés és továbbképzés[7] nagyon fontos elemei az ütőképes erő kialakításának. Ez a védelmi szféra bármely területére érvényes, de kiemelten fontos a katonai erő vonatkozásában, hiszen ahogy az információs technológia és a modern fegyverek fejlődnek, a hadviselési stratégiák és taktikák is gyorsan változnak. A felkészülésük során folyamatosan alkalmazkodniuk kell az új típusú fenyegetésekhez, mert ezek a tényezők még komplexebbé és kiszámíthatatlanabbá teszik a feladataikat. A katonáknak és más védelmi terület szakembereinek fizikailag és szellemileg felkészültnek kell lenniük, de digitális képességekkel, megfelelő digitális kompetenciával is rendelkezniük kell. A védelmi szakembereket képző rendszereknek nemcsak a hagyományos, hanem az új típusú kihívásokra választ adó oktatásra is fel kell készülniük. A jelenleg is zajló digitális forradalom, a digitális fejlesztések előrehaladása elérte az oktatást, új utak jelentek meg. Mára már egyre elterjedtebb a VR-AR-technológián alapuló képzési forma. A fejlődés az eszközök és eljárások egyszerűsödését is hozta. Az LCNC- „Low

[2] Resperger–Kiss 2014: 25; Resperger 2005: 23; Hornyacsek 2020: 81.
[3] Szuhai–Tálas 2017: 10.
[4] Horváth–Lévai 2021: 131.
[5] Kovács 2023: 7.
[6] Benkő 2019: 154.
[7] A fogalmak más-más oktatási formát takarnak, de ebben a tanulmányban egymás szinonimájaként használom ezeket, és összefoglaló fogalommal többnyire képzésnek nevezem.

Code No Code"[8] eljárások megjelenése például forradalmasítja a védelmi szektor szoftverfejlesztési módszereit, de egyben a képzési módszereket is.

Új utak: az LCNC- („Low Code No Code") és SST- („Simple Smart Tech") platformok

Az újfajta digitális megközelítések, mint a „Low Code No Code" platformok és a „Simple Smart Tech" forradalmasítják a katonai képzést és oktatást, kiemelten a V-learning,[9] azaz a virtuális tanulás irányába.

Az LCNC szoftverfejlesztési platformok lehetővé teszik különböző alkalmazások gyors és egyszerű létrehozását minimális programozási tudással, egy vizuális interfész segítségével, ahol a felhasználók komponenseket helyeznek el és kötnek össze. Ez radikálisan lerövidítheti a fejlesztési ciklusokat és demokratizálja a szoftverfejlesztést, lehetővé teszi a „nem technikai hátterű" felhasználók számára is, hogy részt vegyenek az alkalmazások kialakításában. A „low code no code" megközelítések a jövőben biztosíthatják a védelmi szakemberek számára, hogy gyorsan és rugalmasan hozzanak létre testreszabott digitális megoldásokat, mint például virtuális drónirányító rendszereket vagy VR-alapú oktató platformokat.

Az SST, vagyis a Simple Smart Tech (Technology) olyan megfizethető, mégis hatékony digitális eszközöket és megoldásokat jelent, amelyek széles körben elérhetők a kereskedelmi forgalomban és különösen előnyösnek bizonyulnak a védelmi szektorban. Ezek az eszközök az egyszerű kezelhetőségüket és a gyors integrálhatóságukat ötvözik a fejlett technológiák bizonyos aspektusaival. Így az egyszerű okostechnológiai megoldások jelentős hatékonyságnövelést képesek biztosítani különböző védelmi feladatok során, például a felderítésben, a döntéstámogatásban, kommunikációban vagy az erőforrás-kezelésben. Az SST-eszközök kulcsfontosságú szerepet játszanak abban, hogy a védelmi szektor költséghatékonyan és gyorsan alkalmazkodjon a modern kihívásokhoz. A könnyen elérhető kereskedelmi drónok vagy az oktatásban a VR-szemüvegek további előnyt kínálnak az egyre elterjedtebb V-learning számára, hiszen azonnali és költséghatékony megoldást nyújtanak az oktatási kihívásokra (motiváció, eredményesség, tartós tudás stb.). A védelmi szektorban dolgozók a V-learning platformokon keresztül gyakorolhatják a kritikus helyzetek kezelését, ami elősegíti a tudás mélyebb elsajátítását vagy akár a katonák pszichológiai terhelhetőségének növelését, de nem utolsósorban a környezetterhelés csökkentését is. Kutatások igazolták, hogy VR-technológia az immerzív oktatás egyik legerőteljesebb eszköze.[10] Ennek során a résztvevők teljes mértékben elmerülhetnek

[8] Az LCNC azaz a „low-code" és „no-code" szoftverfejlesztési platformok lehetővé teszik alkalmazások gyors és egyszerű létrehozását minimális programozási tudás igénybevételével, vizuális interfész segítségével, ahol a felhasználók komponenseket helyeznek el és kötnek össze, mint egy digitális építőkocka-játékban. Ez a megközelítés radikálisan lerövidítheti a fejlesztési ciklusokat, lehetővé teszi a „nem technikai hátterű" felhasználók számára is, hogy részt vegyenek az alkalmazások kialakításában.

[9] A V-learning: vagyis a virtuális valóság (VR-) alapú oktatási rendszerek olyan innovatív oktatási megoldást képviselnek, amely a digitális technológia legújabb fejlesztéseit használja fel a tanulási környezet és a pedagógiai interakciók bővítésére. Ezek a rendszerek immerzív, háromdimenziós virtuális térben helyezik el a felhasználókat, lehetővé téve számukra, hogy valósághű környezetben sajátítsanak el új ismereteket és készségeket.

[10] Mantovani–Fabrizia–Gianluca 2003: 173; Marlok 2021: 170.

a tanulási környezetben, ami növeli a motivációt és a megértést, ezzel javítja az oktatás hatékonyságát is. A tanulók valósághű,[11] interaktív szerepben vehetnek részt a képzésben, ami lehetővé teszi számukra, hogy gyakorlati tapasztalatokat szerezzenek anélkül, hogy valódi kockázatnak tennék ki magukat. Mindez jelentős előrelépést jelent a védelmi szektorban alkalmazott V-learning oktatásban, mert e technológiák integrálása nemcsak a katonai képzések hatékonyságát növelheti, hanem hozzájárul az állomány gyorsabb, rugalmasabb és tudatosabb döntéshozatalához is. Természetesen az SST-eszközök nem helyettesítik a high tech komplexebb megoldásokat, mint például a GTS-szimulátor,[12] így főként a skilltréningekhez és az egyszerű vagy egyedi folyamatok oktatására adhatnak hatékony választ.

A korszerű digitális technológiák tehát várhatóan nélkülözhetetlen eszközei lesznek a modern katonai képzésnek és kiképzésnek,[13] ugyanakkor még nem teljeskörűen ismertek a hibás alkalmazásból adódó konkrét hátrányaik. Felmerül az a kérdés is, hogy melyek lehetnek ezek, és mi befolyásolhatja előnyösen vagy hátrányosan a VR-ra alapuló oktatás hatékonyságát. Van-e összefüggés az alkalmazó digitáliskompetencia-szintje, a tanulási módszere és a tanulási hatékonyság (tudás) között? Vajon a hibás alkalmazási módnak milyen kihatása lehet az alkalmazók fizikai, pszichikai jólétére?

A V-learning oktatás és képzés lehetséges területei a védelmi szférában

A védelmi szféra területén felmerülő feladatok komplexek, ezért a végrehajtásukhoz is többrétű szakértelemre és összetett készségekre van szükség, hiszen nemcsak szaktudást igényelnek, hanem többnyire az emberi élet és az anyagi javak mentésére irányuló készségeket is. A katonák felkészítése a feladataik végrehajtására széles skálán mozog. Az alapkiképzés az újoncokat alapvető katonai készségekhez juttatja, mint a fegyverkezelés, fizikai felkészülés stb. A harc megvívására és a harctámogatásra is fel kell készülniük, ezért szakkiképzések is folynak. A kommunikációs és információs rendszerek működtetése terén is szükség van speciális készségekre az adat- és információkezelés, valamint a kommunikációs eszközök hatékony használatához. A katonaorvosok és egészségügyi személyzet felkészítése is sajátos képzési igényeket támaszt, kezdve az elsősegélynyújtástól egészen a katonaorvosi sebészeti stb. eljárásokig. A digitális eszközök és módszerek integrálása az oktatási folyamatokba elengedhetetlen minden területen. Ezek nem csupán lehetővé teszik a képzési anyagok személyre szabását, de veszélyes vagy költséges manőverek esetében a kockázatmentes gyakorlást, a környezetkárosítás csökkentését is biztosítják. A képzési rendszernek tehát fel kell készülnie a VR bevonására az oktatásba, annak minden előnyével és hátrányával. A VR-alapú felkészítés hibalehetőségei, az egészségügyi kockázatok, valamint a hatékonyság és pedagógiai integráció kérdései ugyanis kihívások elé állítják a képzésért felelősöket és folytatókat. Ebből adódóan

[11] Kovács 2020: 63; Hornyacsek–Kovács 2020: 154.
[12] Lásd: https://www.infinitsimulation.com/
[13] Németh–Virágh 2021: 5–6; Woodberry 2017.

a technológiai fejlődés átgondolt és tudományosan alátámasztott integrációja lehet csak a járható út. Az új digitális oktatási platformok, mint például a virtuális valóság, a V-learning és a mobilalkalmazások rövid és hosszú távú egészségügyi hatásainak kiküszöbölését célzó használati módok azonban még nincsenek kidolgozva. A tanulás hatékonysága és a VR-alapú oktatás módszere összefüggésének vizsgálata is időszerű, és nem kerülhető el a kérdés, hogy ezen megoldások rendszeresítése a pozitív előnyök mellett milyen negatív hatásokkal jár. Az alábbiakban bemutatom a témában folytatott empirikus kutatásomat.

A VR-szemüveg használata során felmerült érzetek című kutatás alapvetései és bemutatása

Az már igazolt tény, hogy a digitális transzformáció és az újfajta technológiai megközelítések, mint az előbb említett LCNC-platformok és a Simple Smart Tech alkalmazása, jelentős előnyöket nyújtanak a civil szektorban. Az ilyen eljárások alkalmazása jó példával szolgálhat a védelmi terület felé is, és a vizsgálatuk betekintést nyújthat abba, hogyan adaptálják a felhasználók ezeket az eszközöket a képzésbe. A civil felhasználók tapasztalatainak elemzésére alapulóan következtetések fogalmazhatók meg arról is, hogyan alkalmazhatók az immerzív technológiák a katonai kiképzésben anélkül, hogy negatív fizikai és pszichés hatást fejtenének ki, valamint, hogy milyen hatással vannak a katonák tanulási és műveleti képességeire.

Jelen kutatás fő célja, hogy meghatározza azokat a problémákat, amelyek a virtuális valóság és a kapcsolódó technológiák védelmi szférában történő alkalmazásának integrálását akadályozhatják, és megoldási javaslatokat adjon a használattal összefüggésben felmerülő problémákra. A cél elérése érdekében kísérletet folytattam, hogy feltárjam a tényezőket, amelyek befolyásolják a használatot és azonosítsam azokat a negatív hatásokat, amelyek kihatnak a tanulási és az alkalmazási hatékonyságra. Egy előző kutatásban a VR alkalmazásának szűk értelemben vett fizikai és pszichológiai hatásait vizsgáltam. Láthatóvá vált, hogy a fizikai és pszichológiai kihívások negatívan befolyásolják az eszközök használatának hatékonyságát. Ezek közé tartozik például a szimulátorbetegség, amely olyan tüneteket okozhat, mint hányinger, fejfájás vagy szédülés.[14] Jelen kutatásban (a lefolytatott kísérlet eredményeire alapulóan) arra is kitérek, hogyan lehet ezeket a technológiákat hatékonyan alkalmazni a védelmi szervezetekben a képzésben. Célom a VR-alapú eszközök felhasználása pozitív és negatív hatásainak feltárása mellett a tanulási hatékonyság, az életkor és a digitális kompetenciák összefüggéseinek vizsgálata.

[14] Kovács 2022: 85–106.

A tudományos probléma

A digitális eszközök és eljárások megjelenése jelentős befolyással van a védelmi szektor munkájára és az ott folyó oktatási-képzési folyamatokra. Gyakran azonban sem a tanulók, sem az oktatók nincsenek felkészülve ezen újítások integrálására a tanulás-tanítás folyamatába, ami a tanulási és az alkalmazási hatékonyság csökkenését eredményezheti.

A VR-alapú eszközök használatának potenciális negatív fizikai és pszichológiai hatásai, mint például a szimulációs betegség vagy a tanulás hatékonyságát befolyásoló fizikai tényezők, valamint az ezek kialakulását okozó használati tényezők alulkutatottnak számítanak, nincsenek beazonosítva, így a mitigációs és válaszstratégiák sem állnak rendelkezésre. Nincs tudományosan megalapozott, a negatív hatások kialakulását figyelembe vevő felhasználói módszertani útmutató a védelmi szférában folyó VR-alapú képzéshez.

A probléma súlyosbodik azzal, hogy az oktatási rendszer és a lakosság digitális-kompetenciaszintje alacsony,[15] és ennek az alkalmazási hatékonysággal és a várható negatív hatásokkal való összefüggéseit nem ismerjük. Emellett a felhasználói tudás és a használati készségek is hiányoznak az érintettek körében.[16] Ezen túlmenően, az új digitális eszközök, beleértve az XR-technológiákat is, gyakran azonnali megoldást ígérnek a képzésben felmerülő problémákra. Ugyanakkor a fenti vizsgálatok hiányában elterjedhetnek anélkül, hogy megfelelően integrálták volna őket a már jól ismert pedagógiai alapelvekbe, kutatási eredményekbe és a gyakorlati oktatásba.

Hipotézisek, célkitűzések

A kutatás hipotéziseit és célkitűzéseit négy téma köré csoportosítva fogalmaztam meg. Ezek az alábbiak:

1. Digitális transzformáció az oktatásban és digitális kompetenciák[17]

Hipotézis 1.: Feltételezem, hogy a lakosság digitáliskompetencia-szintje alacsony a VR vonatkozásában, és ez a tanulási hatékonyságra negatív hatással van. Célkitűzés 1.: Elemzem a megkérdezettek digitáliseszköz-használatát, digitális kompetenciájának jellemzőit. Azonosítom a digitális eszközök használati trendjét, felkészületlenség okait és lehetséges megoldásait *annak érdekében,* hogy javaslatot tegyek a digitális kompetencia növelésének módjaira.

[15] A digitális kompetenciák olyan készségeket jelentenek, amelyek szükségesek ahhoz, hogy az egyének és a szervezetek hatékonyan használhassák ezeket az eszközöket és technológiákat. Idetartozik az információkezelés, a kommunikáció, a tartalom-létrehozás, a biztonság és a problémamegoldás digitális eszközök segítségével.

[16] Kovácsné 2009.

[17] Digitális transzformáció az a folyamat, amely során a szervezetek átalakítják tevékenységeiket és folyamataikat a digitális technológia által biztosított előnyök kihasználása érdekében. Célja az, hogy növelje a hatékonyságot és az innovációs képességet azáltal, hogy kihasználják a digitális eszközök, például az adatfeldolgozás, az analitika és az internetes kapcsolatok nyújtotta lehetőségeket.

2. A tanulási hatékonyság, az eszközhasználati módszer és az életkor összefüggései

Hipotézis 2.: Feltételezem, hogy a VR-alapú oktatás-képzés hatékonysága összefügg az alkalmazott módszerrel és a feladat-végrehajtás egymásra épülésének mikéntjével, valamint az életkorral. Célkitűzés 2.: Vizsgálom, hogy a VR-alapú eszközökkel végzett tanulási sorrend két esete (az egyszerűtől a bonyolult felé haladás vagy a bonyolulttól az egyszerű felé haladás) és az életkor hatással lesz-e tanulásra. Mindezt *annak érdekében,* hogy javaslatot tegyek a tanulási hatékonyság növelésére.

3. Lehetséges negatív egészségügyi hatások

Hipotézis 3.: Feltételezem, hogy a VR használata során negatív fizikai és pszichikai jelenségek fordulhatnak elő. Célkitűzés 3.: Mivel a korábbi kutatások igazolták, hogy a VR-platformok oktatási alkalmazásának negatív hatásai[18] közé tartozik a cyber sickness, amely szédülést, hányingert és egyensúlyvesztést okozhat, valamint a felhasználók digitáliskompetencia-szintjének variabilitása,[19] ezért jelen kísérletben célom volt vizsgálni az eszközök használatának potenciális negatív egészségügyi hatásait *annak érdekében,* az eredmények alapján javaslatokat tegyek az egészségügyi kockázatok csökkentésének lehetséges módjaira a helyes alkalmazási módszerekre.

4. VR-használati hajlandóság

Hipotézis 4.: Feltételezem, hogy a VR-technológiák használatától sokan idegenkednek, de megfelelő felkészítéssel szívesen vállalkoznának rá, elsősorban munkahelyi környezetben.

Célkitűzés 4.: Vizsgálom, hogy az új digitális eszközök használati hajlandósága milyen, *annak érdekében,* hogy javaslatot tegyek arra, hogy lehetne motiváltabbá tenni a védelmi szakembereket a használatukra.

A kutatás módszere

A célkitűzések eléréséhez több módszer együttes alkalmazásával jutottam el. Ez magában foglalta az irodalmak és a kapcsolódó dokumentumok feldolgozását, vagyis a szekunder adatokból következtetések levonását.[20] VR-hoz kapcsolódó korábbi tanulmányokat vizsgáltam,[21] amelyek rámutattak a technológia fizikai és pszichológiai hatásaira. Emellett empirikus kutatást is végeztem kísérlet és az azt követő kérdezés (kérdőíves) formájában, hogy megerősítsem vagy cáfoljam a szekunder adatokból származó eredményeket, valamint igazoljam vagy elvessem a felállított hipotéziseket. A VR-technológia oktatásban és kiképzésben történő alkalmazásának vizsgálatát az alábbi 6 lépésben vizsgáltam:

[18] Mccauley–Sharkey 1992: 314.
[19] Golding 2016: 371–390.
[20] Kállai 2016: 26; Marlok 2022: 325.
[21] Nalivaiko at al. 2015: 586; Marlok 2021: 163; Gavgani et al. 2017: 45.

1. táblázat: A kutatás dizájnja

1. lépés	**2. lépés**	**3. lépés**
A függő változók meghatározása és a hozzájuk kapcsolódó kérdések összeállítása.	A független változók kiválasztása és a kérdőív megbízhatóságát és érvényességét befolyásoló tényezők elemzése. A kísérleti beállítás és a mérőeszköz összeállítása.	A helyszín meghatározása és a kutatási körülmények kialakítása. A vizsgálati csoport kiválasztása. Próbák lefolytatása, korrekciók.
4. lépés	**5. lépés**	**6. lépés**
A kísérlet végrehajtása. A résztvevők által végzett tevékenységek megfigyelése és rögzítése.	A kérdőív kitöltetése a résztvevőkkel, valamint szükség esetén kérdezés interjú formájában.	Az adatok értékelése a statisztikai elemzések végzése, grafikonos ábrázolás. A következtetések kialakítása.

Forrás: a szerző szerkesztése

Azonosítottam a képzés hatékonyságára ható tényezőket. Az így megszerzett információk alapján azonosítottam a függő és független változókat. A függő változók között szerepeltek a VR-technológia fizikai és pszichológiai hatásai, míg a független változók között a válaszolók demográfiai adatai, mint életkor, munkahely, lakhely, végzettség és digitáliskompetencia-szint. Ezután terveztem meg a kísérlet lefolytatásának alkalmazott módszerét, protokollját (lásd később). Ennél figyelembe vettem a hazai és nemzetközi kutatások vonatkozó eredményeit és eljárásrendeket,[22] emellett a gyártók által javasolt megoldásokat is. A kutatás egy kísérlettel indult: egy Oculus Quest[23] VR-szemüveggel feladatot kellett végezniük a résztvevőknek. A vizsgálati csoport kiválasztása random módon történt az *Egy a Természettel Világkiállítás* önként vállalkozó látogatói közül. A feladat-végrehajtást követően kérdőívet töltöttek ki a résztvevők.

A kérdőív rétegző kérdésekből és 21 szakterületi kérdésből állt, amely három kérdéscsoportra osztható. *Az első kérdéscsoport* a személyes információkra és az általános digitáliseszköz-használatra kérdezett rá. *A második kérdéscsoport* az Oculus Quest VR-szemüveg használata közben felmerülő érzeteket vizsgálta, a fizikai hatásokat, annak érdekében, hogy meghatározhatók legyenek a potenciális negatív mellékhatások vagy érzetek, különös tekintettel a szimulátorbetegségre, amelynek tüneteit és okait több korábbi kutatásban[24] is vizsgáltuk. *A harmadik kérdéscsoport* a jövőbeni használati hajlandóságot mérte.

A kérdések – az utolsó kivételével – feleletválasztó típusúak voltak, amelyek értékeléséhez Microsoft Excelt használtam. A kérdéssort a kísérlet után személyesen kellett kitölteni. A szakmai rész számos paramétert vett figyelembe, kezdve a felhasználó mozgásbiztonságától, egészen a feladat-végrehajtás és verbális megnyilvánulások minőségéig. A mozgások és az irányváltások biztonsága, valamint a mozdulatok határozottsága is kiemelt figyelmet kapott. A kérdőív emellett extra feladatokkal is

[22] Stanney et al. 2020: 1788.
[23] Az Oculus Quest II műszaki paraméterei: 1832×1920 pixel felbontású LCD-kijelző, 72Hz/90Hz frissítési ráta, Qualcomm Snapdragon XR2 chip, háromfokozatú IPD-beállítás (58 mm/63 mm/68 mm), súly: 503 gramm.
[24] Kovács 2020: 63; Hornyacsek–Kovács 2020: 154.

bővült: a résztvevőknek rangsorolniuk kellett, hogy melyik tevékenység okozta számukra a legnagyobb problémát (például féllábon állás, orr megfogása, járás, guggolás, fejbillentés, -mozgatás vagy az egyensúlyozás).

A kísérleti minta tagjaiból egy 25 fős fókuszcsoportos extra vizsgálatot is végeztünk, amely során a felhasználás közbeni viselkedést és teljesítményt elemeztem, de ezeket egy következő tanulmányban mutatom be.

Kísérletihelyszín-beállítás és feladatok

A kísérletet egy 10 x 10 méteres, zárt és külön erre a célra kialakított területen végeztük el, ahol a résztvevők fizikai mozgást is végezhettek, egy virtuális erdei környezetben. A kísérlet előtt mindenki egységes tájékoztatást kapott a célról és a kutatásnál alkalmazott Oculus Quest II VR-szemüveg használatáról. Három különböző, egyre nehezedő és összetettebb feladatot hajtottak végre, s a végrehajtás időtartamát is mértük, azaz a tanulási folyamat idejét teszteltük. A VR-környezetben egy íj üzembe helyezése és célzott lövés leadása (I. feladat), egy golyós fegyver „lőkészállapotba" hozása és célzott lövés leadása (II. feladat), valamint egy elöltöltős fegyver üzembe helyezése és lövés leadása (III. feladat) volt a feladat. A kutatásban a felhasználókat kettő csoportra osztottuk. Az egyik csoport a feladatokat fokozatosan nehezedve hajtotta végre, azaz A-B-C sorrendben. A felhasználók másik fele a feladatokat C-A-B sorrendben, azaz a legnehezebb feladattal kezdve vegyesen hajtotta végre. A fegyverösszeállítás idejét, helyességét és a lövés pontosságát mértük.

A kísérlet során és után korábbi kutatásokban kialakított és standardizált, validált úgynevezett VRSQ[25]-kérdőívből átemelt kérdéseket tettünk fel és ezek alapján értékeltük a fizikai és pszichológiai reakciókat. A szimulátorbetegséget úgynevezett SSQ-kérdések alapján mértük, amely a betegség tüneteit több klaszterre osztja, ilyen a hányinger (SSQ-H), dezorientáció (SSQ-D) és szemmozgás (SSQ-O).[26] A kísérlet során a résztvevők szóbeli visszajelzéseit is rögzítettük, amelyek olyan érzetekre terjedtek ki, amelyeket korábbi kutatások még nem vizsgáltak (csont- és izomrendszer), mint például fáradt kéz, nyakfájás, remegő láb, fájó derék, fáradt csukló vagy fejfájás.

A minta alakulása

Összesen 326 felnőtt férfi és nő vett részt a kutatásban, köztük 154 nő (47%) és 172 férfi (53%) volt,[27] akik öt korosztályba tartoztak. A mintát további demográfiai jellemzők alapján is rétegeztem, mint lakhely, foglalkozás és jövedelem. Felmértük a résztvevők

[25] Kim et al. 2018: 70.

[26] SSQ-kategóriák: 1 – Hányinger, 2 – Általános rossz közérzet, 3 – Gyomorforgás, 4 – Izzadás, 5 – Fokozott nyálelválasztás, 6 – Szédülés, 7 – Fülzúgás, 8 – Koncentrációs nehézség, 9 – Fókuszálási nehézség, 10 – Szemfáradtság, 11 – Fáradtság, 12 – Fejfájás, 13 – Homályos látás, 14 – Szédülés (csukott szemmel), 15 – Teltségérzet.

[27] A kísérlet megkezdése előtt írásbeli beleegyezést kértünk. A minta nagyságát hasonló kísérleti eljárások alapján az analógia módszerével becsültük. A neurológiai, pszichiátriai, vestibuláris vagy hallási rendellenességben szenvedők részvételét nem javasoltuk.

digitális kompetenciáját, és azt, hogy szemüveget vagy kontaktlencsét használnak-e, valamint a VR-ral és a digitális okoseszközökkel kapcsolatos tapasztalatukat.

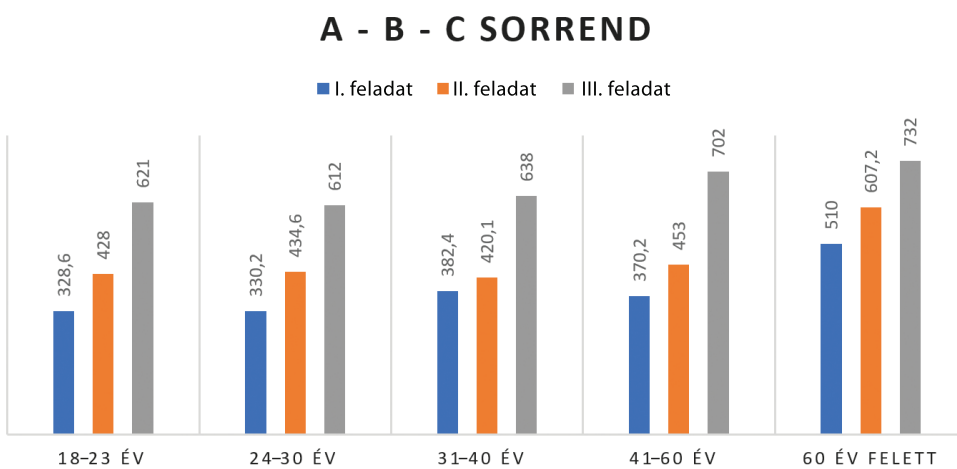
Az életkor szerinti megoszlás azt mutatja, hogy a legnagyobb csoportot a 31–40 éves korosztály alkotta (92 fő, 28%), 18–23 éves 65 fő (20%), 24–30 éves 82 fő (25%), 41–60 éves 63 fő (19%) míg a legkevesebben a 60 év felettiek voltak (24 fő, 7%). A résztvevők több mint fele városi vagy fővárosi lakos (143 fő, 44% és 114 fő, 35%), míg 21%-a falvakból vagy kistelepülésekről (69 fő) származik. A foglalkoztatás terén a megkérdezettek többsége, 152 fő (47%) alkalmazottként dolgozik, míg a tanulók aránya is jelentős: 126 fő (39%). Vezető 21 fő (6%), nyugdíjas 27 fő (8%). A jövedelem tekintetében a résztvevők többsége 231 fő (71%) a magasabb 251 000 forint feletti jövedelem kategóriába esik, a 250 000 forint alatti jövedelemmel rendelkezők 95 főt (29%) tesznek ki.

A kísérlet eredményei

Az eredmények a két fő összefüggést tekintve (sorrendiség és a tanulási [feladat-végrehajtási] hatékonyság, valamint az életkor és hatékonyság) az alábbi módon alakultak ki.

A sorrendiség és a tanulási/feladat-végrehajtási hatékonyság összefüggései

A feladatokat A-B-C sorrendben, azaz az egyszerűbbtől a bonyolultabb felé haladva, a 326 résztvevőből 152 végezte el. Az I. feladatot a leggyorsabban a 24–30 éves korosztály oldotta meg 330,2 másodperc alatt, míg a leglassabban a 60 év feletti korcsoport teljesített, 510 másodperces átlaggal (1. ábra). A II. feladat esetében a leggyorsabb csoport a 31–40 évesek voltak 420,1 másodperccel, és hasonlóan az I. feladathoz, itt is a 60 év felettiek végeztek a leglassabban, átlagosan 607,2 másodperces idővel.

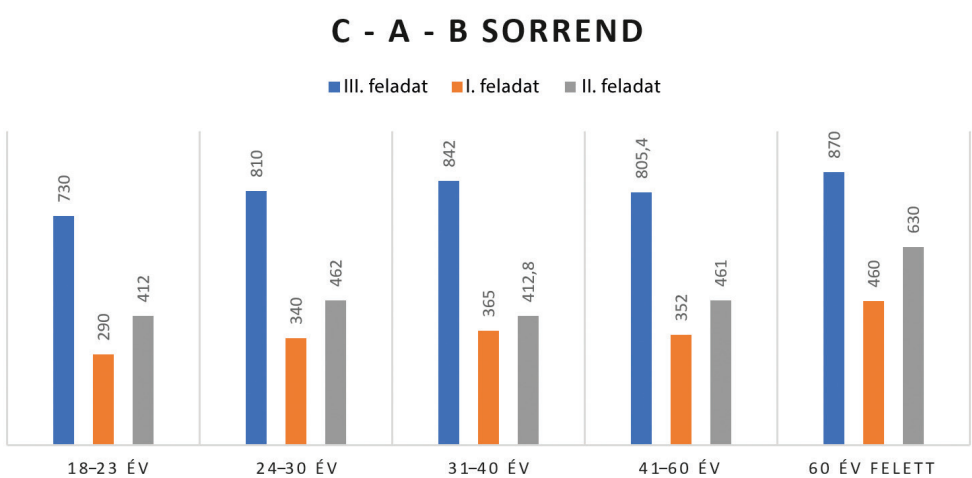


1. ábra: A-B-C sorrendben végrehajtott, I. feladat, II. feladat, III. feladat ideje másodpercben, korosztályonként
Forrás: a szerző szerkesztése

A III. feladat átlagos teljesítési ideje minden korcsoportban magasabb volt. Itt is a 60 év feletti csoport teljesített a leglassabban, 732 másodperces átlaggal, míg a leggyorsabb csoport a 24–30 évesek voltak, 612 másodperces idővel. A 18–23 és a 24–30 évesek hasonló időeredményeket értek el az I. és III. feladatban, míg a 31–40 éveseknél jelentős javulást láthatunk a II. feladatban. A középkorúak tehát jobban alkalmazkodtak a közepes nehézségű feladatokhoz, mint a fiatalabbak és az idősebbek. A 41–60 éves korcsoport átlagos teljesítési ideje viszonylag kiegyensúlyozott a három feladatban, ám a teljesítési idejük a III. feladatnál romlott a többi korcsoport átlagos növekedéséhez képest, ami arra utalhat, hogy a korosztály nehezebben alkalmazkodik a bonyolultabb feladatokhoz. Összességében a fiatalabb korcsoportok gyorsabban és hatékonyabban oldották meg a feladatokat mindkét sorrendnél, míg az idősebbeknél jelentősen hosszabb időre volt szükség, különösen a legnehezebbnek ítélt III. feladat esetében, ugyanakkor az idősebbek kevesebb, de pontosabb lövést adtak le.

A feladatokat C-A-B sorrendben a 326 résztvevőből 174 végezte el. Az I. feladatot leggyorsabban a 18–23 éves korosztály, átlagosan 290 másodperc alatt oldotta meg, míg a leglassabban a 60 év feletti csoport teljesített, 460 másodperces átlaggal (2. ábra). A II. feladatban a leggyorsabb átlagos teljesítési időt a 18–23 évesek produkálták, 412 másodperccel, azonban a 60 év felettiek itt is a legtöbb időt vették igénybe, 630 másodperccel. A III. feladatban minden korcsoport teljesítési ideje jelentősen megnőtt, ami a feladat magasabb nehézségi fokára utalhat.

A leggyorsabbak ismét a 18–23 évesek voltak 730 másodperccel, míg a 60 év felettiek ebben a kategóriában is a leglassabban végeztek, 870 másodperccel. A 31–40 éves korosztály különösen lassúnak bizonyult a III. feladatban, 842 másodperces átlagidővel, ami meglepő, tekintve, hogy az I. és II. feladatban jobban teljesítettek.



2. ábra: C-A-B sorrendben a III. feladat, I. feladat, II. feladat végrehajtási ideje másodpercben, korosztályonként

Forrás: a szerző szerkesztése

Összességében a fiatalabb korosztályok általában gyorsabban teljesítették a feladatokat, míg az idősebbeknél minden feladattípusnál hosszabb időre volt szükség. A 41–60 évesek teljesítési ideje viszonylag kiegyensúlyozott volt a különböző feladatok között, de a III. feladatban észrevehetően több időt igényelt a megoldásuk.

Elmondható, hogy az adatok alapján az A-B-C sorrendben végzett feladatoknál átlagosan jobb teljesítményt figyelhetünk meg, mint a C-A-B sorrendben. Az egymásra épülő nehézségi sorrend előnye különösen jól megmutatkozik a 60 év feletti korosztály esetében, ahol az A-B-C sorrendű III. feladatot átlagosan 732 másodperc, míg a C-A-B sorrendű I. feladatot ennél lassabban, 870 másodperc alatt oldották meg. Ez a trend a többi korosztálynál is megfigyelhető. A fiatalabb korosztály minden sorrendben jobban teljesít az idősebbeknél, de abban az esetben, ha egymásra épülő sorrendben rutint szerzett idősebb alkalmazóval hasonlítjuk össze, akkor az idősebbek jobb teljesítményt mutatnak. A feladatok nehézségének fokozatos növelése, a cselekvés automatikussá tétele segítheti tehát a koncentrációt és a teljesítőképességet, különösen az idősebb korosztálynál. Az előkészítés és a fokozatosság lehetővé teszi a résztvevők számára, hogy jobban alkalmazkodjanak és gyorsabban teljesítsenek, még a fiatalabbaknál is. Ez az összehasonlítás rávilágít arra az eredményre, hogy az idősebb korosztály képes lehet jobban teljesíteni, ha a feladatokat egymásra építve, fokozatosan nehezedő sorrendben kell végrehajtaniuk.

A VR-szemüveg használatának egészségügyi hatásai

Az 1. szempont az SSQ szerinti érzetek elemzése, a 2. szempont a csont- és izomrendszerben jelentkező érzetek vizsgálata volt.

Az SSQ tünetegyüttesekből 326 felhasználóból csupán 41 fő jelentett valamilyen negatív tünetet a teszt során. A tüneteket tapasztalók körében nem volt 18–23 éves. A 24–30 évesek esetében 13 fő (16%), a 31–40 éveseknél 12 fő (13%), míg a 41–60 éves korosztályban 11 fő (17%), 60 feletti 5 fő (21%) számolt be a virtuális valóság használata során jelentkező fizikai tünetekről. Az eredményekből kitűnik, hogy az idősebb korosztályban alacsonyabb a tünetek jelentkezése, mint amit több eddigi kutatás mutatott.[28] A tünetet jelzőknél az SSQ (lásd előző fejezet) szerinti jelenségek mindegyike előfordult. A szédülést nyitott és csukott szem esetén is vizsgáltuk, amely nem mutatott szignifikáns különbséget. Az érzetek az 1–5-ös skálán korosztályonként az alábbiak szerint alakultak (3. ábra).

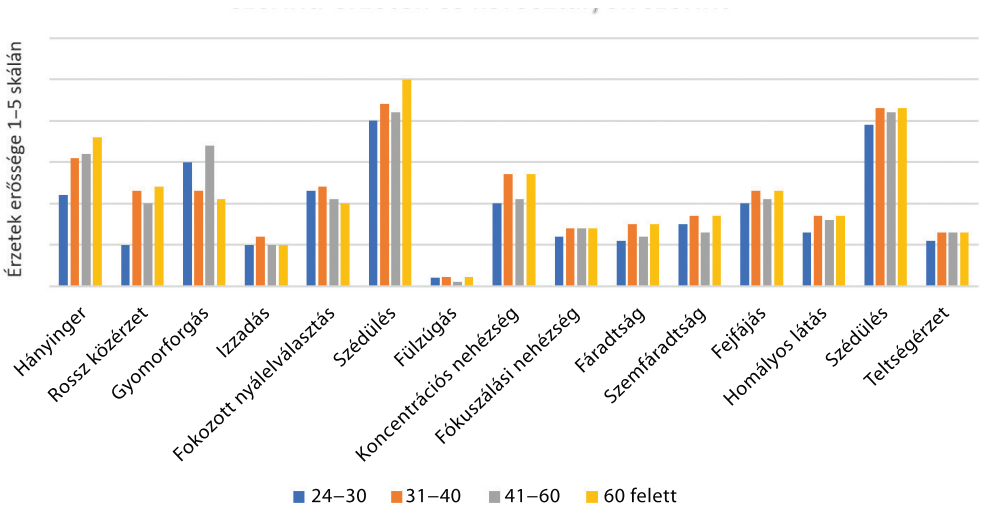
A 24–30 éves korosztály a hányinger tünetet 2,2-es átlaggal, míg a rossz közérzetet 1-es átlaggal értékelte. A gyomorforgás jelenségét viszonylag magasabban, 3-as átlaggal élték meg, ami azt mutatja, hogy ebben a korosztályban ez volt az egyik leggyakoribb panasz. A fülzúgás viszont alacsonyabb, csak 0,2-es átlagot kapott. Az izzadás és a fokozott nyálelválasztás 1, illetve 2,3-as átlaggal jelentkezett, míg a szédülés a legmagasabb átlagot érte el 4-gyel.

[28] Treleaven et al. 2015: 271; Jacqueline–Mohan–Bas 2021: 8.

A 31–40 éves korcsoportban a hányinger 3,1-es átlagot kapott, míg a rossz közérzetet valamivel magasabban, 2,3-as átlaggal értékelték. A gyomorforgás itt is jelentős kellemetlenséget okozott 2,3-as átlaggal. Az izzadás enyhébbnek tűnt 1,2-es értékkel, viszont a szédülés és a fokozott nyálelválasztás 4,4, illetve 2,4-es átlaggal magasabb kellemetlenséget jelez. A fülzúgás viszonylag alacsony 0,22-es átlagot kapott. A koncentrációs és fókuszálási nehézségek, valamint a szemfáradtság és fejfájás esetén is magasabb átlagértékek jelentek meg, illetve a szédülés és teltségérzet szintén jelentős kellemetlenséget okozott ebben a korosztályban.

A 41–60 éves korcsoportban hasonló mintát figyelhetünk meg, itt a hányinger átlaga 3,2, ami magasabb, mint a fiatalabb korosztálynál. A gyomorforgás és az izzadás átlaga 3,4 és 1, míg a fokozott nyálelválasztás és a szédülés 2,1, illetve 4,2 átlagot értek el. A fülzúgás itt is alacsony, 0,1-es átlaggal.

A 60 év felettiek főként a szédülést és a hányingert tartották erős érzetnek. A 60 év feletti korcsoportban a VR-szemüveg használata során a következő tünetek jelentkeztek: hányinger 3,6; rossz közérzet 2,4; gyomorforgás 2,1; az izzadás 1; fokozott nyálelválasztás 2; szédülés 4,9; a fülzúgás a többi korcsoporthoz hasonlóan alacsony, 0,22 értéket mutatott; a koncentrációs nehézség 2,7; a fókuszálási nehézség 1,4; a fáradtság 1,5; a szemfáradtság 1,7; a fejfájás 2,3; a homályos látás 1,7; a szédülés 4,3 és a teltségérzet 1,3 értéket mutattak.

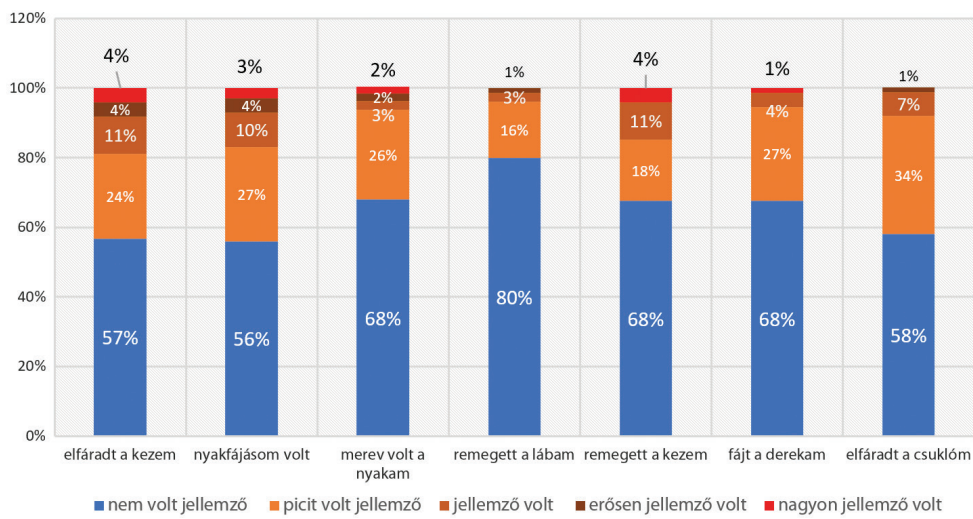


3. ábra: VR-szemüveg használatának egészségügyi hatásai – SSQ szerinti érzetek és korosztályok
Forrás: a szerző szerkesztése

Összességében elmondható, hogy a jelzett negatív érzetek széles skáláját tapasztalták a felhasználók, de a jelentős panaszt érzők száma alacsony volt, mert csak 41 fő számolt be ilyen érzetekről a 326 résztvevőből, azaz 12,5%. A vizsgálat szerint elsősorban a szédülésre, hányingerre, gyomorforgásra és koncentrációs nehézségre lehet számítani. Az elemzés rávilágít arra, hogy a virtuális valóság okozta kellemetlen tüneteknél

vannak korcsoport-specifikus különbségek. A panaszt jelzők százalékos aránya a 60 év felettieknél a legmagasabb (25%). Érdekesség, hogy a 31–40 éves korosztály a negatív érzeteket magasabb pontokkal értékelte, mint a többiek. Az interjúkban elhangzott, hogy ezen korosztály tagjai erősen törekedtek a leggyorsabb feladatvégzésre.

A csont- és izomrendszerben jelentkező érzetek alakulása: a 326 főből 322 fő válaszolta meg ezt a kérdést. Az „Elfáradt a kezem" esetében 57%, 183 fő nem érzékelt változást, 24% 77 fő érzett enyhe, 11%, 35 fő erősebb fáradtságot. 4%, 13 fő erősen érezte, 4%, 13 fő nagyon jellemzőnek találta ezt az érzést (4. ábra). A „Nyakfájásom volt" kategóriában 56%, 180 fő jelentette, hogy nem tapasztalt semmit, 27%, 87 fő némi fájdalmat érzett, 10%, 32 fő jellemzőnek ítélte a tünetet. 4%, 13 fő erősen érzékelte, és 3%, 10 fő nagyon jellemzőnek találta. A „Merev volt a nyakam" tünetnél a válaszadók 68%-a, 219 fő nem érzett semmit, 26%, 84 fő kicsit jellemzőnek érezte, 3%, 10 fő jellemzőnek találta, 2% 6 fő erősen tapasztalta és 2%, 6 fő nagyon jellemzőnek értékelte. A „Remegett a lábam" tünetet 80%, 258 fő nem érzékelte, 16%, 52 fő enyhe remegést tapasztalt, 3%, 10 fő jellemzőnek találta, és 1%, 3 fő erősen érzékelte a remegést. Jelentős remegésről senki sem számolt be. A „Remegett a kezem" esetében 68%, 219 fő nem érezte ezt a hatást, 18%, 58 fő enyhe remegést tapasztalt, 11%, 35 fő jellemzően érzékelte, míg erősen és nagyon jellemzően érzékelte 4%, 13 fő és 4%, 13 fő válaszadó. A „Fájt a derekam" szituációban 68%, 219 fő nem jelentett panaszt, 27%, 87 fő érzékelt enyhe fájdalmat, 4%, 13 fő jellemzőnek ítélte, és 1%, 3 fő erősen tapasztalta. Az „Elfáradt a csuklóm" kategóriában 58%, 187 fő nem tapasztalt változást, 34%, 109 fő érzett némi fáradtságot, 7%, 23 fő jellemzően érezte ezt az érzést, 1%, 3 fő erősen tapasztalta, nagyon jellemzőnek senki sem ítélte meg.



4. ábra: A csont- és izomrendszerben jelentkező érzetek alakulása
Forrás: a szerző szerkesztése

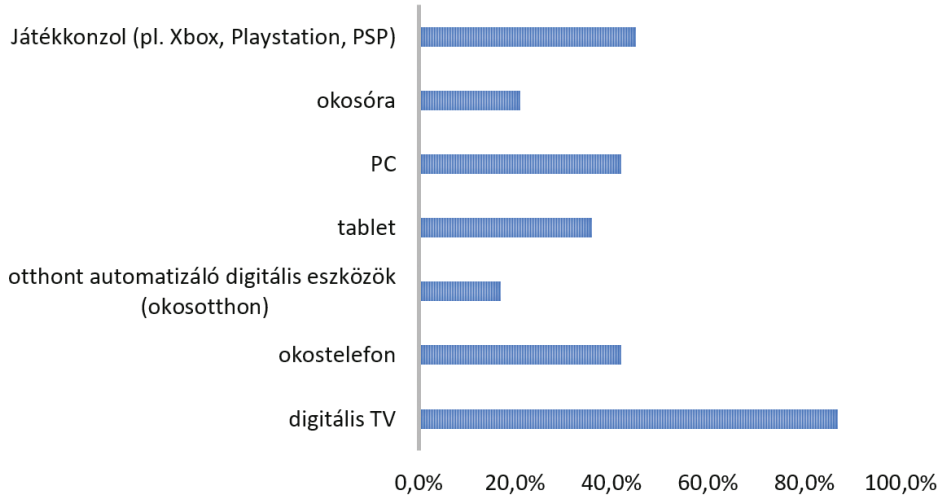
A csont- és izomrendszer igénybevételével kapcsolatos érzetek azt mutatják, hogy leginkább kéz és a nyak fárad el használat közben. A kar és a nyak fokozott igénybevétele miatt a felsőtest is terhelődik, ebből adódhat, hogy többen derékfájást is jeleztek.

A hajlandóságra vonatkozó adatok

A kérdőívben az eszközhasználati hajlandóságot is mértem (5. ábra). Arra a kérdésre, hogy használna-e VR-szemüveget a jövőben, 321 fő válaszolt. 298 fő, 93% igennel, 23 fő, 7% nemmel. Arra a kérdésre, hogy hol használná ilyen eszközt, meglepő módon az életnek nem csak egy területét jelölték meg. A válaszok alapján otthon, játékra-kikapcsolódásra a 321 főből a válaszadók 41%-a, munkahelyi feladatokban a 60%-a, és iskolában is használná 24%-a. Arra a kérdésre, hogy milyen feltételekkel használná, a legtöbben, 68% azt válaszolta, hogy ha lenne hozzá útmutató és felkészítő oktatás. Az eszköz motivációs hatását is elemeztem (6. ábra). 317 fő válaszolt. Ennek alapján a megkérdezettek 58%-a, 182 fő fantasztikusnak, 41%, 131 fő más digitális eszközhöz hasonló jónak tartotta, és csak 4 főt, 1%-ot nem érdekelte az eszköz.

5. ábra: A „Milyennek találja az eszközt?" kérdésre adott válaszok eloszlása
Forrás: a szerző szerkesztése

A válaszadók által leggyakrabban használt digitális eszközök között a digitális televízió 79%-nál, a PC 53%-nál, az okostelefonok 49%-nál és a játékkonzolok 31%-nál szerepeltek. Figyelemre méltó, hogy azok a válaszadók, akik már rendelkeznek tapasztalattal VR-eszközök használatában, nem igényeltek betanítást, és nem tapasztalták a cybersickness tüneteit. Ez a csoport átlagosan 17%-kal jobb eredményt ért el, mint azok, akik nem használtak korábban hasonló eszközöket. A digitális eszközök gyakori használata növelheti a digitális kompetenciát, az otthoni használata pedig hozzájárulhat a sikeresebb alkalmazáshoz a munkahelyen.



6. ábra: A „Ha használ digitális eszközöket, melyek azok, amelyeket a leggyakrabban használja?" kérdésre adott válaszok eloszlása
Forrás: a szerző szerkesztése

A felmérés eredményei alapján tehát összefüggés van a felhasználók digitáliskompetencia-szintje és a VR-eszközök jövőbeni alkalmazási hajlandósága között. A válaszadók 93%-a szívesen használná a jövőben.

Összegzett következtetések, javaslatok

A VR-technológia alkalmazása nemcsak a civil szférában, de a katonai szakterületen is teret hódít. A VR-alapú eszközök forradalmasítják az oktatást a védelmi szférában, mert jelentősen hozzájárulnak a környezetterhelés csökkentéséhez és meggyorsítják a tanulási folyamatot. Számtalan előnyük mellett a kutatások arra is figyelmeztetnek, hogy helytelen használat esetén negatív fizikai és pszichológiai hatása lehet. Jelen kutatás vizsgálta, hogy a VR-szemüvegben végzett feladat-végrehajtást milyen tényezők befolyásolják, vannak-e a használatból adódó negatív érzetek, és hogyan lehetne növelni a motivációt a használatra. Megállapítható, hogy a digitális kompetencia szintje, az életkor és a feladat-végrehajtás módja hatással van a VR-szemüveggel való tanulás hatékonyságára. Az életkor döntő tényező, ugyanakkor a tanulási mód jobban befolyásolja. A fiatalabb generáció feladat-végrehajtása gyorsabb, ugyanakkor az idősebb korosztály – feltéve, ha sikerül automatikussá tenni az eszközhasználatot – pontosabb a végrehajtásban. Az eredményekből látjuk, hogy a tanulás hatékonysága akkor ideális, ha a felhasználó egyre nehezedő egymásra épülő feladatokat kap, illetve a felkészítés és a tanulási folyamat megtervezése figyelembe veszi a felhasználó digitális kompetenciáját, digitális felkészültségét. A kutatás és az eredmények alapján

az első hipotézis, miszerint feltételeztem, hogy a lakosság digitáliskompetencia-szintje alacsony a VR vonatkozásában, és ez a tanulási hatékonyságra negatív hatással van, igaznak bizonyult, mert azon felhasználók, akik kevésbé voltak jártasak a digitáliseszköz-használatban vagy nem próbáltak még VR-eszközt, rosszabb eredményeket értek el. A második hipotézis, amelyben feltételeztem, hogy a VR-alapú oktatás-képzés hatékonysága összefügg az alkalmazott módszerrel és a feladat-végrehajtás egymásra épülésének miként jével és az életkorral, részben igaz, mert bár a fiatalabb korosztály jobban teljesített, mint az idősebb felhasználók, de abban az esetben, ha a feladatok nehézségi szintje egymásra épült, már az idősebb korosztály jobban teljesített, mint azok a fiatalok, akik nem fokozatosan egymásra épülő nehézségű feladatokat kaptak. A kutatásból az is kiderült, hogy a feladatok könnyű megértése kritikus tényező a felhasználói élmény és a tanulási hatékonyság szempontjából. A virtuális környezet komplexitása jelentős hatást gyakorolhat a felhasználók teljesítményére. A harmadik hipotézis, miszerint a VR használata során negatív fizikai és pszichikai jelenségek fordulhatnak elő, igaznak bizonyult, a felhasználók 12,5 % jelezett valami negatív jelenséget. A kutatásban szereplő negyedik hipotézis, miszerint a felhasználók a VR-technológiáktól idegenkednek, de megfelelő felkészítéssel szívesen használnák elsősorban munkahelyi környezetben, részben igaznak bizonyult, mert a válaszadók többsége azt jelezte, hogy szívesen használna ilyen eszközt akár otthon, tanulásra és játékra, azaz nem idegenkedik tőle, de a munkahelyi felhasználásnál már elvárt a felhasználók részéről az előzetes oktatás.

Javaslat: A virtuális tanulási platformok hatékony integrálásához elengedhetetlen a felhasználók alapos felkészítése, amely magában foglalja az alkalmazkodási időszak tudatos, egyénre szabott kialakítását és a célirányos felkészítést. Ajánlott, hogy a felhasználók számára elegendő időt biztosítsunk a feladatok elvégzése előtt az „átálláshoz", amely hozzásegíti őket a virtuális térhez való hozzászokáshoz. A feladattér optimalizálása során a VR-környezeteknek és -szimulációknak a felhasználók kognitív képességeihez és várható reakcióihoz kell igazodniuk. A feladatok jelentsenek kihívást, ugyanakkor megoldhatónak és érthetőnek kell lenniük.

A használat közben nem számottevő százalékban, de jelentkeznek a szimulátorbetegség tünetei. Akiknél jelentkezett, ott nem az életkor a döntő a kialakulás gyakorisága szempontjából, hanem a felkészítés és a jól kidolgozott oktatási módszertan hiánya okozhat több negatív érzetet. A tünetek egy része korosztályonként különbözőséget mutat. Általában hányingerre, szédülésre, gyomorforgásra és koncentrációs nehézségre lehet számítani, az idősebb korosztálynál főként a szédülés a zavaró. A középkorúak a tüneteket a skálán erősebbnek érzékelik, mint a fiatalok vagy az idősek. Az SQR-kérdőívből ismert érzetek – hányinger, fejfájás stb. – mellett a csont- és izomrendszerre gyakorolt hatást vizsgálva megállapítható, hogy a kéz és a nyak fájdalma mellett a kompenzálás miatt a derék is érintett lehet.

Javaslat: Az émelygés elkerülésére a virtuális térben távoli pontokra való koncentrálás, a szellős környezet és a stabil testtartás megtartása javasolt. Az előzetes részletes tájékoztatás szintén hozzájárul a felhasználók jobb felkészüléséhez és a tünetek csökkentéséhez. Ezenkívül a negatív hatás a képfrissítési frekvencia növelésével és a virtuális mozgások valós mozgásokkal való összehangolásával csökkenthető. Emellett a virtuális mozgásoknak valós időben kell történniük a felhasználók mozgásával, hogy

minimalizálják az agy és a vestibuláris rendszer közötti eltéréseket. A VR oktatási alkalmazások tervezésének és fejlesztésének előrehaladtával fontos lesz olyan szoftveres és hardveres megoldásokat integrálni, amelyek proaktívan kezelik a szimulátorbetegség kockázatát, valamint használati útmutatót kell adni a felkészüléshez.

A VR-alapú eszközök használatára való hajlandóság magas, a megkérdezettek főként munkahelyi környezetben alkalmaznák szívesen, és akkor, ha megfelelő felkészítést és használati útmutatót kapnak hozzá. A képzési rendszert az új típusú eszközök kihívás elé állítják, de a hátrányok kiküszöbölése esetén paradigmaváltást hozhat mind a gyakorlati munkában, mind az arra való felkészülés, az oktatás területén.

A feladatok könnyű megértése kritikus tényező a felhasználói élmény és a tanulási hatékonyság szempontjából. A virtuális környezet komplexitása jelentős hatást gyakorolhat a felhasználók teljesítményére. A feladattér optimalizálása során a VR-környezeteknek és -szimulációknak a felhasználók kognitív képességeihez és várható reakcióihoz kell igazodniuk. A feladatok jelentsenek kihívást, ugyanakkor megoldhatónak és érthetőnek kell lenniük. A tervezési folyamatnak multidiszciplináris megközelítést kell alkalmaznia, amely magában foglalja a kognitív tudomány, az ergonómia és a felhasználói élmény területeit. Cél a felhasználói interakciók természetességének növelése, a tanulási környezet hatékonyságának javítása és a VR-technológia teljes potenciáljának kiaknázása. Kezdetben egyszerű, nem szakspecifikus feladatok gyakorlásával kell kezdeni, ami segíthet a felhasználónak megszokni a virtuális tér érzetét, mielőtt bonyolultabb, szakmai feladatokra térnénk át.

A VR-szemüveg viselése: VR-szemüveg hosszabb ideig történő viselése kellemetlen érzeteket vagy fáradtságot okoz. Felhelyezésekor ügyeljünk arra, hogy a szemüveg szorosan, de kényelmesen illeszkedjen a fejhez. Kezdjünk rövidebb, 5-10 perces szoktatási időszakokkal, majd az oktatás alatt fokozatosan növeljük a folyamatos használat időtartamát, de ne haladjuk meg a 30-45 perces aktív használatot egyhuzamban. Minden használati időszak után tartsunk legalább 15-20 perces szünetet.

Fizikai terhelés, viselés közben: Amikor egy, a kísérletben is szereplő 0,5 kilogrammos Oculus Quest 2 szemüveget viselünk és a fejünket lefelé döntjük, több tényező is befolyásolja a nyaki csigolyákra gyakorolt terhelést. Ez megnövekedett nyomást jelenthet a nyaki csigolyákra és izmokra, ami hosszú távon fájdalmat vagy extra terhelést okozhat. Az ideális az lenne, ha a VR-munkaterületet és a kezelőgombokat úgy helyeznénk el a virtuális térben, hogy a felhasználónak minél kevésbé kelljen előrehajolnia vagy fejét lefelé döntenie, így csökkentve a nyaki csigolyákra gyakorolt terhelést.

A kutatás további kérdéseinek bemutatása meghaladja e tanulmány kereteit, erre a cikksorozat következő részében kerül sor.

A VR a jövő útja, amely már itt van a védelmi szervezetek mindennapjaiban. Alkalmazása azonban akkor lesz igazán hatékony, ha a használatánál a pedagógia, ergonómia, fizika, biológia, anatómia/élettan vonatkozó eredményeit figyelembe vesszük.

Irodalomjegyzék

Beams, Ryan – Kim, Andrea S. – Badano, Aldo (2019): Transverse Chromatic Aberration in Virtual Reality Head-Mounted Displays. *Optics Express,* 27(18), 877–884. Online: https://doi.org/10.1364/OE.27.024877

Benkő Tibor (2019): A Magyar Honvédség jelene és jövője. *Hadtudomány,* 29(1–2), 149–155. Online: https://doi.org/10.17047/hadtud.2019.29.1-2.149

Bodoróczki János (2020): A modern hadviselés logisztikája – a katonai logisztika jövője. *Hadtudomány,* 30(2), 98–108. Online: https://doi.org/10.17047/HADTUD.2020.30.2.98

Caserman, Polona et al. (2021): Cybersickness in Current-Generation Virtual Reality Head-Mounted Displays: Systematic Review and Outlook. *Virtual Reality,* 25, 1153–1170. Online: https://doi.org/10.1007/s10055-021-00513-6

Cho, Won Seok et al. (2020): Airgap-Embedded Robust Hazy Films to Reduce the Screen-Door Effect in Virtual Reality Displays. *Nanoscale,* 16, 8750–8757. Online: https://doi.org/10.1039/C9NR10615D

Gavgani, Alireza M. et al. (2017): Profiling Subjective Symptoms and Autonomic Changes Associated with Cybersickness. *Autonomic Neuroscience,* 203, 41–50. Online: https://doi.org/10.1016/j.autneu.2016.12.004

Golding, John F. (2006): Predicting Individual Differences in Motion Sickness Susceptibility by Questionnaire. *Personality and Individual Differences,* 41(2), 237–248. Online: https://doi.org/10.1016/j.paid.2006.01.012

Golding, J. F. (2016): Motion Sickness. *Handbook of Clinical Neurology,* 137, 371–390. Online: https://doi.org/10.1016/B978-0-444-63437-5.00027-3

Golding, John F. – Gresty, Michael A. (2015): Pathophysiology and Treatment of Motion Sickness. *Current Opinion in Neurology,* 28(1), 83–88. Online: https://doi.org/10.1097/WCO.0000000000000163

Grassini, Simone – Laumann, Karin (2020): Are Modern Head-Mounted Displays Sexist? *Front Psychologie,* 11, 1–15. Online: https://doi.org/10.3389/fpsyg.2020.01604

Hicks, Paula (2016): *The Pros And Cons Of Using Virtual Reality In The Classroom*. Online: https://elearningindustry.com/pros-cons-using-virtual-reality-in-the-classroom

Hornyacsek Júlia (2020): A klímaváltozással összefüggő katasztrófák lehetséges hatásai a lakosságra és az ezzel szembeni védettségük növelésének lehetőségei. In Földi László – Hegedűs Hajnalka (szerk.) *Éghajlatváltozás okozta kihívások és lehetséges válaszok.* Budapest: Ludovika, 75–89.

Hornyacsek Júlia – Kovács Gergely (2021): A kiterjesztett valóság alapú szemüveg alkalmazásának kihívásai a védelmi szférában a műszaki szakfeladatok ellátása során. In Földi László (szerk.): *Szemelvények a katonai műszaki tudományok eredményeiből I.* Budapest: Ludovika, 147–166.

Horváth Attila – Lévai Zsolt (2021): A magyarországi vasúthálózat létfontosságú elemeinek azonosítása. In Földi László (szerk.): *Szemelvények a katonai műszaki tudományok eredményeiből I.* Budapest: Ludovika, 131–146.

Howard, M. C. – Van Zandt, E. C. (2021): A Meta-Analysis of the Virtual Reality Problem: Unequal Effects of Virtual Reality Sickness Across Individual Differences.

Virtual Reality, 25, 1221–1246. Online: https://doi.org/10.1007/s10055-021-00524-3

Jacqueline, M. Fulvio – Mohan, Ji – Bas, Rokers (2021): Variability in Sensory Sensitivity Predicts Motion Sickness in Virtual Reality. *Entertainment Computing,* 38(5), 1–11. Online: https://doi.org/10.1016/j.entcom.2021.100423

Kállai Attila (2016): Felkészítés és kiképzés virtuális környezetben. In *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése.* Budapest: Nemzeti Közszolgálati Egyetem, 4–56.

Kennedy, Robert S. – Fowlkes, Jennifer E. (1992): Simulator Sickness Is Polygenic and polysymptomatic: Implications for Research. *The International Journal of Aviation Psychology,* 2(1), 23–38. Online: https://doi.org/10.1207/s15327108ijap0201_2

Kim, Hyun et al. (2018): Virtual Reality Sickness Questionnaire (VRSQ): Motion Sickness Measurement Indexin a Virtual Reality Environment. *Applied Ergonomics,* 69, 66–73. Online: https://doi.org/10.1016/j.apergo.2017.12.016

Kovács Gergely (2020): A kiterjesztett valóságalapú technológia alkalmazásának lehetőségei és korlátai a védelem és a polgári logisztika területein. *Katonai Logisztika,* 28(1–2), 54–78. Online: https://doi.org/10.30583/2020/1-2/054

Kovács Gergely (2022): A védelmi szférában alkalmazható VR-alapú kiképzés/felkészítés során felmerülő negatív fizikai és pszichológiai jelenségek. *Katonai Logisztika,* (30)3–4, 85–106. Online: https://doi.org/doi.org/10.30583/2022-3-4-085

Kovács Gergely – Hornyacsek Júlia (2019): Korszerű oktatási eszközök és módszerek alkalmazása a polgári védelmi felkészítésben. *Műszaki Katonai Közlöny,* 29(2), 117–132. Online: https://doi.org/10.32562/mkk.2019.2.10

Kovácsné Koreny Ágnes (2009): Digitális műveltség Európában. *Tudományos és Műszaki Tájékoztatás,* 56(6). Online: https://epa.oszk.hu/03000/03071/00022/pdf/EPA03071_tmt_2009_06_295-304.pdf

Lampton, Donald L. et al. (1994): Side Effects and Aftereffects of Immersion in Virtual Environments. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* 38(18), 1154–1157. Online: https://doi.org/10.1177/154193129403801802

Lee, J. Y. et al. (2017): *Estimating the Simulator Sickness in Immersive Virtual Reality with Optical Flow Analysis.* New York: Siggraph Asia, Association for Computing Machinery. Online: https://doi.org/10.1145/3145690.3145697

Mantovani, Fabrizia – Castelnuovo, Gianluca (2003): Sense of Presence in Virtual Training: Enhancing Skills Acquisition and Transfer of Knowledge through Learning Experience in Virtual Environments. In Riva, Giuseppe – Davide, Fabrizio – Ijsselsteijn, Wijnand A. (szerk.): *Being There: Concepts, Effects and Measurement of User Presence in Synthetic Environments.* Amsterdam: Ios Press, 164–181. Online: https://doi.org/10.1089/109493103322725487

Marlok Tamás (2021): Virtuálisvalóság-alapú taktikai szimulációs kiképző eszközök hazai fejlesztési lehetőségei. 2. rész: A technológia lehetőségei a kiképzés szemszögéből. *Hadmérnök,* 16(1), 161– 176. Online: https://doi.org/10.32567/hm.2021.1.10

Marlok Tamás (2022): A VR-eszközök alkalmazhatósága a taktikai kiképzésben. In Földi, László (szerk.): *Szemelvények a katonai műszaki tudományok eredményeiből III.* Budapest: Ludovika, 323–337.

Martirosov, Sergo – Bureš, Marek – Zítka, Tomáš (2022): Cyber sickness in Low-Immersive, Semi-Immersive, and Fully Immersive Virtual Reality. *Virtual Reality,* 26, 15–32. Online: https://doi.org/10.1007/s10055-021-00507-4

Nalivaiko, Eugene et al. (2015): Cybersickness Provoked by Head-Mounted Display Affects Cutaneous Vascular Tone, Heart Rate and Reaction Time. *Physiology & Behavior,* 151, 583–590. Online: https://doi.org/10.1016/j.physbeh.2015.08.043

Németh András – Virágh Krisztián (2021): Virtuális valóság és haderő – katonai alkalmazási lehetőségek IV. rész. *Haditechnika,* 55(5), 2–7. Online: https://doi.org/10.23713/HT.55.5.01

Nesbitt, Keith et al. (2017): Correlating Reaction Time and Nausea Measures with Traditional Measures of Cybersickness. *Displays,* 48, 1–8. Online: https://doi.org/10.1016/j.displa.2017.01.002

Oishi, Erika et al. (2016): Enhancement of Motion Sensation by Pulling Clothes. In Proceedings of the 2016 Symposium on Spatial User Interaction. New York: Association for Computing Machinery, 47–50. Online: https://doi.org/10.1145/2983310.2985749

Resperger István (2005): A nemzetközi terrorizmus ellenes küzdelem tapasztalatai és lehetséges stratégiái. In *New Challenges in the Field of Military Sciences 2005: 3rd International Scientific Conference.* Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 1–25.

Resperger István – Kiss Álmos Péter – Somkuti Bálint (2014): *Aszimmetrikus hadviselés. Kis háborúk nagy hatással.* Budapest: Zrínyi.

Stanney, Kan et al. (2020): Identifying Causes of and Solutions for Cybersickness in Immersive Technology. *International Journal of Human–Computer Interaction,* 36(19), 1783–1803. Online: https://doi.org/10.1080/10447318.2020.1828535

Stott, J. R. R. (1986): Mechanisms and Treatment of Motion Illness. In Davis, Christopher J. et al. (szerk.): *Nausea and Vomiting: Mechanisms and Treatment.* Berlin: Springer, 110–129. Online: https://doi.org/10.1007/978-3-642-70479-6_9

Szuhai Ilona – Tálas Péter (2017): A 2015-ös európai migrációs és menekültválság okairól és hátteréről. In Tálas Péter (szerk.): *Magyarország és a 2015-ös európai migrációs válság.* Budapest: Dialóg Campus, 9–34.

Treleaven, Julia et al. (2015): Simulator Sickness Incidence and Susceptibility During Neck Motion-Controlled Virtual Reality Tasks. *Virtual Reality,* 19(3–4), 267–275. Online: https://doi.org/10.1007/s10055-015-0266-4

Weech, Séamas – Kenny, Sophie – Barnett-Cowan, Michael (2019): Presence and Cybersickness in Virtual Reality Are Negatively Related: *A Review,* 10(158), 1–19. Online: https://doi.org/10.3389/fpsyg.2019.00158

Woodberry, Andrew (2017): *Government Divisions to Use VR for Training.* Online: https://readwrite.com/2017/10/26/government-vr-uses/

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
18. évfolyam (2023) 4. szám 53–62.
DOI: 10.32567/hm.2023.4.4

László Manga,[1] Lajos Kátai-Urbán,[2] József Solymosi[3]

Research and Development of Environmental Radiation Situation Assessment Procedures and Methods Following Serious Nuclear Accidents

Abstract

The environmental effects of severe nuclear accidents pose a great threat to the environment and to living organisms. Unfortunately, there have been several examples of this over time. In our work, we present development solutions and opportunities which a nuclear power plant or other nuclear facility can implement nuclear environmental monitoring even under extreme conditions. We will discuss systems and tools that can be used to increase the efficiency of the radiation situation assessment, helping decision-makers to make quick and optimal decisions, thus helping to minimise the environmental impact.

Keywords: severe nuclear accident, nuclear environmental monitoring system, radiation situation assessment, radiation detection

Introduction

The scientific achievement that defined the history of mankind was the discovery of radioactivity and its industrial technological application. Nuclear power plants receive enormous emphasis, but not only their usefulness, but also their dangers, which can even lead to a disaster.[4] Unfortunately, there have been examples of such situations in recent decades. That's why we are in parallel with the spread of nuclear power plants, the safety regulations are constantly evolving, so that energy extraction can be realised with the greatest possible nuclear safety and with the least environmental damage. In the following, in light of this, we will describe our research topic, which

[1] Emergency Preparadness and Response, Paks Nuclear Power Plant, e-mail: mangal@npp.hu
[2] Ludovika University of Public Service, Doctoral School of Military Engineering, email: katai.lajos@uni-nke.hu
[3] Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: solymosi.jozsef@uni-nke.hu
[4] Manga–Kátai-Urbán 2016: 120.

includes development proposals and tool systems created in the spirit of environmental control. Our goal is to minimise the burden on the environment in the event of a possible serious nuclear accident and thus protect people's lives and health.

The long-term strategic energy policy was affected by Hungary, but many other countries are also following the extension of the operating time of the current nuclear power plants and the establishment of new nuclear power plants.

Monitoring system developed in the environment of nuclear facilities

First, we will present the Operational Environmental Radiation Protection Control System using the example of the Paks nuclear power plant. To illustrate this, we chose Figure 1 below, as the diversity and complexity of the systems can be seen in the context of this figure.

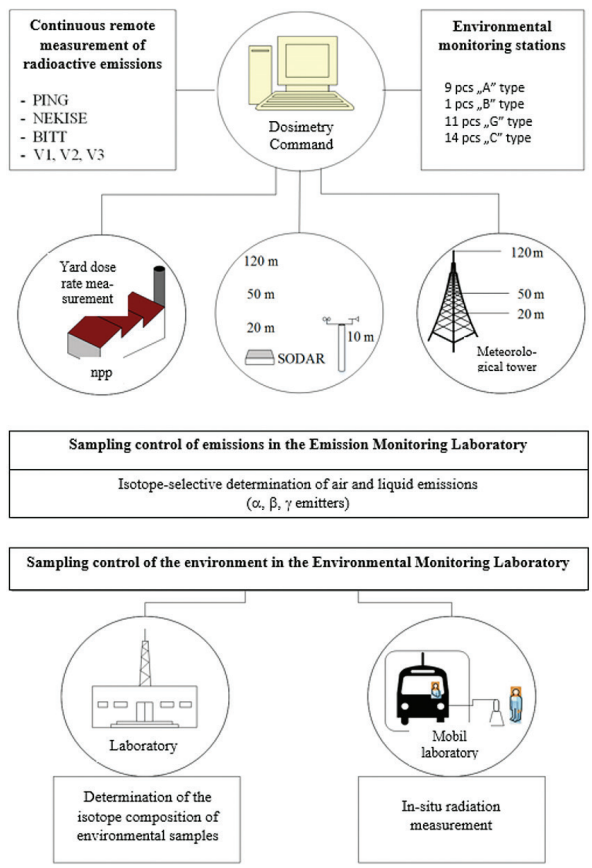


Figure 1: Operational scheme of the Operational Environmental Radiation Protection Control System of the Paks nuclear power plant

Source: MVM Paks Nuclear Power Plant 2022a: 12.6-3

The upper left side of the Figure 1 shows the transmitter systems for emission control, which include activities, activity concentrations, and dose rates based on gaseous and liquid emissions. On the right side above, you can see the telemetry systems for sampling and measuring gaseous media that have already been emitted from the power plant, which also monitor the aforementioned parameters. For both emission control and environmental control, this is supplemented by sampling-based measurements. The measurements take place in laboratory conditions after sample processing. These precision determinations with a small detection limit also allow us to infer the physicochemical characteristics of the emitted radioactive material, which, where appropriate, helps to delineate abnormal technology. In the event of a serious nuclear accident, however, we can primarily rely on rapid monitoring transmitter systems. From this point of view, the dosimetry controller – at the top of the figure, in the middle – has an important role, where the signals of the transmitter systems run. Here, permanent shift personnel monitor the incoming signals and if an anomaly is experienced or a warning and/or emergency level is generated, the "credibility test" of the measuring channel is carried out, i.e. – among other things – the radiation protection parameter of each technological system is compared, the radiation protection of the emission and environmental control with these measurements. In terms of the load on the environment, courtyard detectors play an important role, and they provide great help in identifying whether we are dealing with chimney or building emissions during a possible accident. In terms of escape routes, they also play an important role in the same way as systems providing meteorological parameters. Moving further down in the diagram, you can see a reference to the Environmental Monitoring Laboratory, which was located in the interior of Paks. In addition, the Emission Monitoring Laboratory performs measurements based on sampling, which is located in the controlled zone. The Environmental Monitoring Laboratory operates another Radiation Protection Measuring Vehicle, which in its current state is prepared for normal operating conditions and can be used for in-situ measurements and sampling.

Development of transmitter systems for nuclear environmental monitoring in the light of serious nuclear accidents

In the following, we will present our study and development proposals in the field of nuclear environmental control, which also takes into account the results of the so-called "stress test" after the severe nuclear accident in Fukushima, which all power plants in the world were required to do. Within this framework, the nuclear power plant of Paks prepared the Targeted Safety Review, which in terms of radiation protection covered the operational safety of radiation protection data provision under extreme conditions (earthquake and total power failure) and within this framework, the system elements that provide vital data in the event of a serious nuclear accident were reviewed. Most of our proposals in the field of nuclear environmental control have already been implemented, which we will describe below.

In connection with emission control, we examined the particle, iodine and noble gas (hereinafter PING) monitoring systems related to airborne emissions, as well as the isotope selective measurements of noble gases (hereinafter NEKISE). BITT probe measuring the dose rate of the air coming out of the twin chimney. Water stations that monitor the incoming and outgoing cooling water (V1, V2) and the so-called "above-balance" and treated wastewater (V3) emitted from the power plant. In connection with the environmental monitoring, the stations that monitor gaseous emissions from the power plant (A1-9, B, G1-11, C1-14). Meteorological systems that play an important role in determining the spread (SODAR, tower). Yard detectors that measure dose rate, measurements related to sampling in connection with emission and environmental control, and the available measuring vehicle.

In light of the above, we came to the conclusion that improvements can be made to the PING and NEKISE systems that measure airborne emissions, primarily by extending their upper measurement limit or in connection with changing the iodine monitor sample, however, taking into account the simplicity and economic aspects, the reinforcement of the BITT probe seemed most reasonable. Building this redundancy is advisable because it has a wide measurement range and has been providing reliable measurements for a long time. Its earthquake resistance and 72-hour protection against total voltage failure can be solved relatively easily. Even activity concentrations can be estimated from the dose rate data provided by the BITT probe. However, it is definitely advisable to supplement this measurement with another high-reliability probe that measures air circulation, from the point of view of determining the source of the emission.[5]

Earthquake resistance and protection against total loss of voltage with a bridging time of at least 72 hours is also necessary for water stations. The latter can be achieved in the case of the V1 and V2 stations by installing an additional pump with a smaller output than the operational one, which can provide even longer water samples that are continuously updated using batteries. As a result, the residence time of the sample in the sample container is longer, but it is still sufficient to maintain representativeness. In the case of the V3 station, the concept is slightly different, since there is no continuous emission here. Here, it is advisable to transform the current measurement technique in such a way that we can measure the emission line itself with a highly sensitive shield detector, which measures the activity of the medium flowing through the pipeline at the time of emission. The container can still be maintained for sampling, but it must be done in coordination with the flow conditions in the pipeline. In the interest of redundancy and diversity, our further development proposal was the establishment of a wireless data connection to the central data collector, the transition to PLC control and instead of many data concentrators and industrial computers, as well as the air conditioning of the container, which further strengthened the availability.[5]

Taking into account the efforts to extend the operating time and the possibility of integration into the future Paks 2 environmental monitoring system, the replacement of the station's power cables and signal cables should also be considered in an earthquake-resistant manner. Another option is to supply the stations with

[5] MTA EK – Kék – ScadaNet Ltd. 2016: 6–86.

aggregators, which requires the purchase of additional aggregators. In connection with A1-9- operational and B- reference station type stations, the protection against earthquakes and the protection of vital measurements against total voltage failure are also generally applicable. Furthermore, in the spirit of greater availability, the data collectors were equipped with air conditioning equipment and PLC control. The battery cells keep the so-called small-volume sampling unit, which is important in the event of an accident, in operation, which performs continuous monitoring of aerosols, elemental and organic iodine, and supplies the BITT probe with a high measurement limit outside the container with voltage with a 72-hour bridging time.

From a measurement technical point of view, replacing the NaI(Tl) heat-stabilised scintillation detector measuring organic iodine with a heat-compensated type has become expedient due to greater availability. Also from a measuring technique point of view, the "gating" of the spectrum of the four iodine isotopes based on previously difficult-to-verify mathematical efficiency calibration has been simplified to refer to the most typical isotope I-131.[5] The A1-9 and B-type stations also contain equipment important for sampling, such as a tritium and radiocarbon sampling unit, a large-volume sampling system, and vessels for dry and wet fallout sampling, but their development is not necessary from the point of view of a serious nuclear accident. Stations C1-14 do not play a role in distance measurement so we will not go into detail about them.

In the case of stations of the G1-11 type, there is no need to expand the solar cells providing autonomous power supply, which ensures the power supply of the dose rate meter with a large measurement limit. From the point of view of earthquake resistance, the support structure is qualified, the inspection of the fixing of the solar panels from the point of view of earthquakes is unnecessary, since the capacity of the batteries has been expanded as part of the development, which far surpasses the 72-hour bridging even in the event of the loss of the solar panel. Another tool under development is the replacement of radios, which was also a basic criterion for more stable communication at all other stations establishing wireless connections.[5] In connection with the 18 courtyard detectors, we also used several development opportunities. Before the development, the detectors only had a wired connection (signal cable, power cable), at our suggestion, they now also have a wireless connection and are capable of autonomous operation with a 72-hour bypass with the help of the local battery. In the framework of preparing for the danger of an earthquake, 5 courtyard detectors were moved outside the ruins, where the earthquake resistance of the surrounding object could not be verified, and a steel scaffolding with the appropriate foundations was provided, which meets the required earthquake resistance requirements.

Meteorological systems play an important role in connection with a possible serious nuclear accident, since the spreading characteristics can be determined with the help of these data. Current systems satisfy the concept of redundancy and diversity. As an advantage of the SODAR system, we would describe its simple structure without moving parts, which means that it can determine the wind profile from the reflection of the ultrasound emitted from the Earth's surface. At the time of its installation, this system already met the earthquake protection criterion system, however, we formulated development proposals regarding the battery capacity, so that it would also be able to provide the required 72-hour bridging, and we proposed the purchase of an additional

aggregator to exploit the possibility of aggregator power supply. Regarding its installation location, we also have such insights that the turbulent effect of the buildings around it may gender-distort the values typical of the power plant's environment. From this point of view, the 120 m meteorological tower is in the right place, however, unlike the SODAR system, it has not been tested against an F2 tornado, and the devices placed on it also require more maintenance. All in all, the two systems complement each other well, where prioritised data is provided by SODAR.

In connection with sampling, we have already mentioned that in the case of a serious nuclear accident there is no time or opportunity to determine the data extracted from it, however, there are cases and types of accidents where laboratory processing and the data that can be extracted from them are crucial. Therefore, with Decree 15/2001 (VI. 6.) in accordance with the Emissions and Environmental Control Regulations approved by the authority, we would add sampling and procedures in operating conditions TA2-4 – for expected operational events and planning malfunctions – and TAK1-2 – for complex and serious accidents.[6]

Study of radiation situation assessment tool systems for nuclear accident prevention in the light of serious nuclear accidents

In the following, we will also present the nuclear accident prevention system through the example of the Paks nuclear power plant, and within it, we will review the tasks related to radiation protection, as well as define the areas where we see development opportunities. In accordance with the national provisions, the Paks nuclear power plant operates an Accident Prevention Organisation, the task of which is to manage the contents of the Comprehensive Emergency Response Plan (hereinafter referred to as ÁVIT).

ÁVIT includes, among other things, the Nuclear Accident Prevention Action Plan radiation protection-related tasks are carried out by the Radiation Protection Organisation with slightly more than 50 people. Instead of the Radiation Situation Assessment Section, Radiation Protection Equipment Insurance Section, the Radio-, Biological-, Chemical (hereinafter RBV) Group and the Exemption Group are included within the organisational unit. The Radiation Pollution Measurement Department and the Radiation Detection Department with the three Radiation Detection Squadrons are located within the RBV Group. Taking into account the possible occurrence of a serious nuclear accident, we now mainly examined the means of radiation situation assessment and radiation detection. We are doing all this because, in our opinion, the decision-makers in such a situation, in addition to the technological conditions, should consider this in the first instance in order to protect the environment and people.[7] One of the key tools for beam position assessment is propagation calculation software. In the case of the power plant, this includes two pieces of software. One is the so-called Dose on Lite (simplified online dose rate calculator) software

[6] MVM Paks Nuclear Power Plant 2019b: 5–34; MVM Paks Nuclear Power Plant 2022b: 4–30.
[7] MVM Paks Nuclear Power Plant 2019a: II. 17–19.

running within the framework of the Radiation Protection Control System, which determines the dose rate values up to a distance of 30 kilometres from the power plant by extrapolation based on the equivalent environmental dose rate of gamma radiation of environmental stations.[8] The other is the so-called TREX (Transport Exchange) program, which, knowing the source member, can calculate the spatial distribution of the emitted radioactive material using a Lagrangian approach, which takes into account propagation, decay and sedimentation.[9]

The calculations are performed for a 30 km area based on predicted AROME (Application of Research to Operations at Mesoscale) data provided by the super computer of the National Meteorological Service[10] or based on the site's meteorological parameters. Our development proposal regarding the software is to feed a complex software with the already available extended radiation protection parameters. In this way, the propagation calculation (with additions of the appropriate models) can be extended not only to the 30 km area of the power plant, but the radiation conditions prevailing inside and in the immediate surroundings of the buildings could be predicted with a real source term, which, updated with further real measurements, would give the most accurate forecasts possible for decision makers.

We mentioned earlier that the power plant has a radiation protection measuring car. This car can be equipped with hand-held sampling devices and hand-held instruments, however, in the event of a major nuclear accident, it is advisable to equip it with greater capabilities. Therefore, our development proposal is that the radiation-shielded – armoured – troop transport car, which can also be found in the power plant and serves as part of accident prevention, equipped with off-road capabilities and external and internal dose performance meters, should be further developed and/or a new acquisition realised by increasing additional capabilities. The capabilities must extend to other radiation measuring devices integrated in the car, covering various radiations – α, β, γ – and measuring ranges, dose meters, route monitoring systems, surface contamination meters, gamma spectrometers, sampling devices, air, liquid, environmental samples. For the placement of marking devices suitable for marking contaminated areas, for the supply of filtered air for collective protection, for the creation of mild compression. The additional task of radiation detectors are chemical and biological detection, so it is advisable to prepare the vehicle for these tasks as well with the appropriate instrumentation, spectrometers, gas meters, pollution meters. In terms of RBV capabilities, the unit that measures meteorological parameters is also an important part of the vehicle. In addition to these, of course, communication and data transfer play a very important role, the construction of which is advisable to be installed in a redundant and diverse manner.

In the following, we will discuss the applicability of a system of tools that has not yet spread in the environment of nuclear facilities, thus an epoch-making initiative in relation to the Paks nuclear power plant. These are none other than drones. During our studies, it became clear from the beginning that aerial radiation detection can

[8] MVM Paks Nuclear Power Plant 2019c: 3–62.
[9] Transport Exchange Model Simulator (TREX) 2021: 1–76.
[10] See: www.met.hu/idojaras/elorejelzes/modellek/

be used very effectively to identify either extensive radioactive pollution or local hot spots and radiation sources. Many articles have been published under the auspices of the Doctoral School of Military Engineering in connection with helicopter or fixed-wing drone beam reconnaissance methods, which testify to the fact that they have an accuracy comparable to that of pedestrian reconnaissance, all of which can be carried out quickly and with the mapping of large areas. Taking into account the properties of drones that they are relatively cheap, can be deployed quickly, can even be used in formations, the equipment systems that can be installed (detectors, sampling and monitoring devices) are very diverse, their operation and storage are relatively cheap and simple and, last but not least, manpower can be dispensed with, thus in accordance with the ALARA principle, which is essential for the radiation protection of people. Operating on a certain, special principle – e.g. wing flapping principle – with the help of drones, although other beam detection purposes can also be achieved, e.g. inside the building. Through the appropriate communication channels, they can provide additional measurements to radiation situation assessors, which can be crucial in connection with a serious nuclear accident. Of course, in addition to those listed earlier, there are also possibilities for radio detection of large areas, taking into account the efficiency of measurement technology and communication.[11]

Conceptual development and application of complex decision support software

In the case of a nuclear facility, the biggest challenge is the occurrence of a possible serious nuclear accident and its control in such a way that the environment is burdened as little as possible. Decision-makers are in an extremely difficult situation at this time, as they have to take into account and consider a lot of data, factors and other information. That is why we think that a complex decision support software can greatly facilitate this work, because the data of the already available transmitters – supplemented by the data provided by mobile devices – and other databases, modelling and forecasting systems could be available in one place. After that, filters and algorithms can be applied, which would allow only the relevant data to remain, thus making the work of decision makers easier. The primary purpose of the decision support software is to monitor the status of technological systems as well as their radiation parameters. This is the only way to be aware of the extent of the radioactive release and the location(s) of the release. If this information is available, it is easier to make decisions taking into account the minimisation of damage to the environment. The software can also be expanded with other functions. We are thinking here of other emergency management, for example, we could mention the avoidance of dangerous substances or the activities related to fire, which entail the involvement of new specialist areas.[12] The related databases and measurement results are also available. As an additional possibility, we would like to mention that in such situations,

[11] Petrányi et al. 2023. 915–921.
[12] Cimer et al. 2021: 2–16; Érces–Vass 2018: 2–22.

the flow of data and information to the competent national bodies and authorities could be facilitated by setting the appropriate authorisations and permissions with the appropriate links – which are already largely available. In addition to the above, other non-emergency applications are possible, which can be very widely used.[13]

Summary

The spread of the use of nuclear energy is so revolutionary that it is hard to imagine life without it. The specific energy extraction of the heating elements used by nuclear power plants cannot be compared with anything at the moment, and all of this is done in an environmentally friendly way during normal operation. However, some unfortunate events of the past decades have also highlighted the fact that we also have to reckon with the occurrence of a serious nuclear accident. In such situations, reducing the load on the environment is essential. In our article, we make suggestions with this in mind. In light of this, we developed development proposals in the field of nuclear environmental control, most of which have already been implemented. These developments were generally related to protection against earthquakes and total loss of voltage, and the vital measurements were delimited, the reinforcement or replacement of which was necessary in the event of a serious nuclear accident. From the point of view of nuclear accident prevention, we focused primarily on tasks related to radiation protection, including radiation situation assessment and radiation detection tools and methods. As a development direction for the propagation calculation software, which plays an important role in the radiation situation assessment, we have given the integration of the current software and its expansion with other models, which can enable the propagation calculation based on the real source element.

Another advantage is that they can provide forecasts not only for a 30 km area, but also for the buildings and their immediate surroundings, both in the short and long term. In connection with radiation detection, we propose the development of a radiation protection measuring car and a new tool system for the applicability of drones. In connection with the radiation protection measuring car, we have listed the aspects that must be met in connection with a possible serious nuclear accident. Drones are well suited for radiation protection and economy. Both fixed-wing and rotary-wing models can be proven to have a right to exist, and they are even suitable for performing more complex tasks in combination or by using several types together. By developing a complex decision support system, the work of decision makers can be made easier, so that they can make the most optimal decision as quickly as possible. With the help of the software, you can track the technology status as well as its radiation parameters and their emission routes. By applying the appropriate algorithm and supplementing the appropriate forecasting models, the data could be filtered so that only the relevant data are available. The software can provide additional opportunities for communication and data provision to the national bodies involved in accident prevention and the authorities. Taking everything into account, thanks to our development and

[13] Csurgai et al. 2018: 171–183; Solymosi et al. 2023: 843–848.

innovation proposals, the radiation conditions can be continuously monitored and modeled, allowing decisions to be made that protect the safety of our environment, minimize its burden and protect people's lives and health.

References

Cimer, Zsolt et al. (2021): Application of Chemical Monitoring and Public Alarm Systems to Reduce Public Vulnerability to Major Accidents Involving Dangerous Substances. *Symmetry,* 13(8), 1528. Online: https://doi.org/10.3390/sym13081528

Csurgai, József et al. (2018): Dividing of Controlled Area in Nuclear Power Plants. *Hadmérnök,* 13(4), 171–183.

Érces, Gergő – Vass, Gyula (2018): Veszélyes ipari üzemek tűzvédelme ipari üzemek fenntartható tűzbiztonságának fejlesztési lehetőségei a komplex tűzvédelem tekintetében. *Műszaki Katonai Közlöny,* 28(4), 2–22.

Manga, László – Kátai-Urbán, Lajos (2016): Nukleáris balesetkből levonható tanulságok – a tudomány állása I. rész. *Bolyai Szemle,* 4(E-szám), 120–136. Online: www.uni-nke.hu/document/uni-nke-hu/bolyai-szemle-2016-04.original.pdf

MVM Paks Nuclear Power Plant (2019a): *Átfogó Veszélyhelyzet-kezelési és Intézkedési Terv* I-V m. Paks: MVM PA Zrt.

MVM Paks Nuclear Power Plant (2019b): *Kibocsátás Ellenőrzési Szabályzat V04*. Paks: MVM PA Zrt.

MVM Paks Nuclear Power Plant (2019c): *SER KK rendszer, Terjedésszámítás a Dose on Lite program algoritmusa.* Paks: MVM PA Zrt.

MVM Paks Nuclear Power Plant (2022a): *1–4. blokk Végleges Biztonsági Jelentés.* Paks: MVM PA Zrt.

MVM Paks Nuclear Power Plant (2022b): *Környezetellenőrzési Szabályzat V4*. Paks: MVM PA Zrt.

MTA EK – Kék – ScadaNet Ltd. (2016): *A sugárvédelmi ellenőrző rendszer kibocsátás- és környezetellenőrzésének felújítása, műszaki leírás V.1.2*. Budapest: EK.

Petrányi, János et al. (2023): Assessing the Radiation Contamination of Large Areas Using Advanced Technologies. *Radiation Protection Dosimetry,* 199(8–9), 915–921. Online: https://doi.org/10.1093/rpd/ncad092

Solymosi, Máté et al. (2023): Monitoring System of the Fuel-Casette-Free STATE of the Control Rod Sleeves on the PAKS NPP. *Radiation Protection Dosimetry,* 199(8–9), 843–848. Online: https://doi.org/10.1093/rpd/ncad116

TREX – Terjedési-Ülepedési Modell Szimulátor (2021). Veszprém: Radioökológiai Tisztaságért Társadalmi Szervezet.

Legal sources

15/2001 (6.VI.) KöM Decree on radioactive discharges into air and water from the use of nuclear energy and their control

Act CXXVIII of 2011 on disaster management and amending certain related acts

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

18. évfolyam (2023) 4. szám 63–78.
DOI: 10.32567/hm.2023.4.5

Gábor Deli,[1] Flóra Kulin,[2] Ágnes Angyalné Pataki[3]

Effect of Low Dose Ionising Radiation on the Amount of Mitochondrial Common Deletion and D-Loop Tandem Duplication in Human Peripheral Whole Blood

Abstract

The Hungarian Defence Forces assume a significant role in disaster prevention, including nuclear accident prevention tasks, so both the command and executive staff can stay in the higher-than-natural dose area. The current "gold standard" microscopic method aimed at determining the radiation dose suffered is the dicentric chromosome assay (DIC), although sensitive and accurate, it is very time-consuming. Monitoring changes in the amount of common deletion (CD) of mitochondrial DNA (mtDNA) and in the D-loop a tandem duplication (TD) of mtDNA may be a reliable marker of exposure to ionising radiation. This work used the PCR method to investigate how CD and TD change in human blood samples after X-ray irradiation. The CD appears to be a particularly useful marker, as its maximum is below the threshold for clinical symptoms. This work is the first to show the relationship between radiation and tandem duplication. The TD we investigated occurred more frequently in irradiated human blood samples than native ones. During the future development of the diagnostic tool, both CD and TD are informative and would be used together in a PCR system to detect acute and cumulative irradiation. In recent years, more and more health institutions are dealing with molecular biological diagnostic work. In a disaster situation, if the laboratory capacity of the Hungarian Defence Forces would not

[1] Molecular Biological Diagnostician, University of Debrecen Clinical Centre Institute of Forensic Medicine, e-mail: deligabor08@gmail.com
[2] Senior Research Fellow, Hungarian Defence Forces Health Centre, Epidemiological Scientific Research Institute, e-mail: kulin.flora@gmail.com
[3] Head of Laboratory, Hungarian Defence Forces Health Centre, Epidemiological Scientific Research Institute, e-mail: a.p.agnes@freemail.hu

be sufficient for this, more external laboratories can be involved for PCR measurements than for traditional microscopic work.

Keywords: biodosimetry, radiation detection, mitochondrion, DNA, deletion

Introduction

Due to its function, the Hungarian Defence Forces must be prepared to carry out the tasks performed in the CBRN (chemical, biological, radiological, and nuclear) operational environment, or even for disaster prevention activities for example in the event of a nuclear emergency in the domestic environment.

One of the important tasks of disaster prevention is radiation protection. However, in the event of a disaster or an unexpected situation, the pre-planned protection cannot always be implemented, or it is only partially implemented, and since the Hungarian Forces assume a significant role in the tasks of disaster prevention, including nuclear accident prevention, both the command staff and the executive staff work in an environment with higher exposure rate than normal. This, of course, comes with the risk of suffering significant radiation dose.

Radiation exposure can also occur in connection with a known radiation event, but even in this case, we do not know exactly how much radiation dose each person received based on the field conditions and the time spent. In addition, for example, radiation sensitivity may differ from person to person.

In a disaster situation, such as a nuclear or workplace accident, or during a terrorist attack, those present may be exposed to radiation, and, in the event of a large-scale industrial accident, the radiation may reach human bodies for thousands of kilometres, i.e. beyond the borders of the affected country (for example, Chernobyl or Fukushima).

The visible symptoms of radiation exposure – skin reaction, vomiting, headache, diarrhoea – only appear with a delay of several hours, depending on the situation, in the case of a larger absorbed dose of more than 1 Gray. These are nonspecific and can easily be confused with symptoms of other diseases, so patients may not receive appropriate treatment if the doctor does not suspect radiation exposure (for example, in the case of Alexander Litvinenko).[4]

During an event that affects the masses, there will be many people among a large number of injured who may not even show clinical symptoms, but in their case, the risk of various cancers will increase significantly later on, and that must be taken into account that there will be those who develop symptoms, but they did not develop in connection with radiation exposure (stress, chemicals, trauma).

In the event of a mass casualty, the responsible commander must set up an emergency sequence among those involved, this process is called triage. For persons not wearing a physical dosimeter, the level of radiation exposure can only be estimated afterwards, with the help of various biodosimetry procedures.

[4] Harrison et al. 2017: 266–278.

Biological dosimetry is a procedure for assessing the radiation dose that affected the body based on the damage caused,[5] more precisely, based on the errors accumulated during the enzymatic repair of the damage in the affected but surviving cells. DNA repair mechanisms are immediately activated and take place in both the nucleus and mitochondria. Traces of repair persist throughout the cell's lifetime, such as deletions, duplications, and translocations. If the cell is capable to divide, the new cells get and give their successors changed DNA.

Biodosimetry provides an answer to whether radiation exposure has occurred, how much radiation those present suffered, and the resulting cell damage through laboratory examination of those involved. In this way, the injured person can receive appropriate medical care and legal remedies.

These methods can be used to determine the radiation sensitivity[6] of soldiers tasked with damage rescue, and by checking people returning home with complaints or with higher radiation exposure, appropriate therapy[7] can be selected in the case of knowledge of specific radiation injuries.

For a long time, dicentric chromosome analysis using lymphocytes was the only biological dosimetry method, and it is still the most widespread, so-called gold standard technique.[8]

There are many other biological endpoints, such as micronuclei, translocations, and aberrations in early condensed chromosomes.[9] In addition to military reasons, reliable biodosimetry is also needed in occupational radiation protection to confirm or exclude suspected low-dose radiation exposure. For this, more and more laboratories are looking for new targets for example mRNA and protein expression studies,[10] mitochondrial deletion[11] to detect the radiation dose suffered, and this is made possible by rapidly developing molecular biological methods.

Our goal is to find PCR-based biodosimetry methods with higher throughput than microscopic methods, with good specificity, which we could use as a pre-screening test of the DIC method in a mass accident situation. Our current research focuses on radiation-induced mitochondrial deletions and duplications.

Human mitochondrial DNA (mtDNA) is present in several copies in individual mitochondria, on average 2-10 copies may occur. Human mtDNA is a 16.6 kb circular double-stranded DNA molecule that encodes 13 essential polypeptides for the respiratory chain and a set of RNAs (2 rRNAs and 22 tRNAs) for intramitochondrial translation.[12]

Among these tightly packed genes there is a 1.1 kb non-coding DNA region, called displacement loop (D-loop), which contains sequences important for the initiation of mitochondrial replication and transcription.[13] The location of the D-loop is at site

[5] International Atomic Energy Agency 2011.
[6] Kiss et al. 2013: 104–112.
[7] Dainiak et al. 2003: 473–496.
[8] Voisin 2015: 115–122.
[9] Deli 2018: 179–192.
[10] Schüle et al. 2022.
[11] Schilling-Tóth et al. 2011: 33–39.
[12] Anderson et al. 1981: 457–465.
[13] Clayton 1991: 453–478.

16024-576 bp according to the Cambridge reference sequence.[14] The structure consists of one double and one single DNA strand. The reason for this is that the complementary heavy strand starts to synthesise on the light chain, the process separates the original heavy chain forming a loop, hence the name of the region. Synthesis stops at the end of the D-loop, and the mtDNA becomes quiescent, and stabilising proteins bind to the single-stranded DNA stretch.[15] The duplications described in the literature develop in this area.[16]

Many mtDNA deletions are readily detected in non-dividing tissues such as the brain and muscle but are rarely detected in relatively rapidly dividing cells (such as white blood cells). The most commonly reported deletion is a 4977 bp deletion or "common deletion" (CD), originally observed in patients with mitochondrial myopathy.[17]

Materials and methods

Blood samples were collected with a venous puncture in a blood collection vacuum tube with sodium citrate. The samples were aliquoted into 1.5 ml microcentrifuge tubes according to the doses to be irradiated, during which 1.4 ml of blood was added to the tubes under atmospheric oxygen. Contact of blood with oxygen was avoided as much as possible to preserve its venous character since the free radical formation of mitochondria can be influenced by the amount of oxygen.[18] The colour of blood is the indicator of blood oxygenation. The samples were stored at room temperature until the irradiation.

Irradiation took place 2 hours after blood collection, samples were irradiated at room temperature using a Precision X-Rad 225 XLi X-ray system. The dose rates, distances and filters are indicated in Table 1. The doses were checked with a dosimeter. Irradiation was carried out at room temperature. After irradiation, the blood samples were incubated for 3, 24, or 48 hours at room temperature, protected from light.

Table 1: The dose rates, distances, and filters used

Dose	Copper filter (mm)	Distance (cm)	Time	Dose rate
0.05	6	125	3 min 18 sec	0.015 Gy/min
0.1	1	125	1 min 4 sec	0.094 Gy/min
0.5	1	60	1 min 14 sec	0.41 Gy/min
1	1	60	2 min 27 sec	0.41 Gy/min
2	1	35	1 min 38 sec	1.23 Gy/min

Source: compiled by the authors

[14] Clayton 1991: 453–478.
[15] Jiang et al. 2021.
[16] Damas 2014: 1261–1268.
[17] Wallace 1992: 628–632.
[18] Pesznyák–Sáfrány 2016: 108–110.

DNA isolation

Nucleic acid isolation was performed 3, 24, and 48 hours after irradiation using the QIAamp DNA Blood Mini Kit (Qiagen), according to the manufacturer's recommendation. The total DNA extract, containing both nuclear and mtDNA was used for polymerase chain reaction (PCR) analysis without further purification.

Primers used in this study

"CD": To detect the mitochondrial common deletion, the primer pair was designed for the two ends of the 4977 bp long deletion. Due to the short cycle time, this section cannot multiply in the wild type,[19] but it can after the formation of the deletion, so we were able to measure the amount of deleted DNA. Sequence of CD Forward primer: CCCACTGTAAAGCTAACTTAGCATTAACC,[20] sequence of CD Reverse primer: AGGTTGACCTGTTAGGGTGAGA.[21]

"TD": A back-to-back primer pair was designed for the detection of tandem duplication in the D loop of mitochondrial DNA, with 9 bases between the 5' ends of the primer pair. On the non-duplicated sequence, DNA synthesis would be initialised in the opposite direction, however, only if the duplication is present and the number of primary binding sites is also duplicated, product formation is experienced during the PCR reaction. Sequence of TD Forward primer: TTTTTGGCGGTATGCACTTTTAAC, sequence of TD Reverse primer: GAAATCTGGTTAGGCTGGTG. We designed this primer pair in such a way that they recognise and give products in case of several known duplications.

"mtDNA": replicates a section of the "minor arc" of the mitochondrial genome, which is present in both normal and deleted DNA (deletions rarely occur in this section).[22] This allows us to check the amount of all mitochondrial DNA. Sequence of mtDNA Forward primer: CTAAATAGCCCACACGTTCCC, sequence of mtDNA Reverse primer: AGAGCTCCCGTGAGTGGTTA.[23]

"GAPDH": refers to the amount of DNA (nuclear or nDNA) in the nucleus, which is proportional to the number of cells. Sequence of GAPDH Forward primer: CGACCACTTTGTCAAGCTCA, sequence of GAPDH Reverse primer: AGGGGTCTACATGGCAACTG.[24]

[19] Rogounovitch et al. 2002: 7031–7041.
[20] Rogounovitch et al. 2002: 7031–7041.
[21] Schilling-Tóth 2015: 52.
[22] Phillips 2014.
[23] Phillips 2014.
[24] Schilling-Tóth et al. 2011: 33–39.

PCR

During the PCR reaction, we used Quantinova master mix (Qiagen, Germany) containing SYBR Green intercalating dye, the measurements were performed on a BioRad CFX96 Real-Time PCR (BioRad, USA) device. With the primers described above, the relative amount of GAPDH, Minor and CD sequences were determined. After denaturation at 95 °C for 2 min, the reaction mixture was cycled 50 times at 95 °C for 30 s, 60 °C for 30 s and 72 °C for 60 s, finally extended at 72 °C for 10 min. Melting curves were detected as the first qualitative check.

Gel electrophoresis

The PCR products were checked by 1% agarose gel electrophoresis. The gels were then evaluated using an Alpha Innotech Fluorchem 5500 Gel Imaging System and were detected fluorographically under UV light transillumination after staining with ethidium bromide. During the evaluation of CD, only those samples were considered/included, where the expected 374 bp product appeared during gel electrophoresis. The samples with inappropriate products were excluded from the data analysis. Since the used primer pair may amplify many other types of deletions, we also exclude samples where other products appear alongside the expected product, and the unexpected product is more pronounced.

In the case of tandem duplication, the back-to-back primers are located in opposite directions. The primers can bind even in the absence of duplication, but no double-stranded product is formed. Samples with no specific product show a smeared line in the gel. If the duplication is present, each primer can bind to 2 places on the mtDNA molecule. That is, in the case of tandem duplication, one more binding site is formed for both primers, so the reverse and forward pairs will be opposite each other, so in such a case, the duplicated section is multiplied exponentially. When checked by gel electrophoresis in the case of the simultaneous presence of duplication (and even triplication), one (or two in the case of triplication) band is formed.

Statistical analysis

Analysis of CD: The experimental data were collected with the program of the BioRad CFX 96 instrument. Data were then arranged with MS Excel.

The number ratio of the nuclei, mitochondria, and deletion mitochondria per unit volume was calculated from the measured Ct values of GAPDH (nucleus), mtDNA (minor arc), and CD (deletion marker) samples using the formula 1/(2Ct).[25] The experimental data processed during the statistical analysis are presented in mean ± SD format per dose. Two parallel measurements were made from the

[25] Livak–Schmittgen 2001: 402–408.

samples of the 7 donors for each dose. Measurement points were excluded due to the formation of an inappropriate product (according to gel electrophoresis) resulting in a different number of measurement results being associated with each point. At the points with several measurement results, the average of the points was assigned to the given donor. An exception to this is the normality test performed during the statistical control, where the points were considered separately. The deletion rate of the 4977 bp mtDNA was investigated by one-way analysis of variance. All statistical analyses were performed using ratio-paired t-tests with GraphPad Prism6 statistical software. $P < 0.05$ was considered to indicate a statistically significant difference.

Analysis of TD: The real-time PCR curve and the melting curve are difficult to interpret due to the non-specific "smear" products produced by the unusually oriented primers.

With the PCR device, all duplications are amplified and detected, which includes the region 376-427 (almost all known duplications). We did not make any distinctions in this series of measurements. All definite bands were counted in the gels run from the PCR samples made with the intercalating dye. This amount is plotted as a function of the applied doses.

Results

Changes in the number of common deletions 3 hours after X-ray irradiation of blood samples

For the timing of the examination of the CD marker, 3 hours from the irradiation seemed promising, when the potential synthesis of genomic and mitochondrial DNA should be considered less. We observed that at this short time, there were no significant changes in Ct values for GAPDH (nuclear marker), and mtDNA (mitochondrial marker).

The amount of deleted mitochondrial DNA changes sensitively as a result of irradiation, we can observe that it reacts more sensitively to radiation exposure than the mtDNA marker. In our tests, we took into account the CD/mtDNA ratio.

Regarding to the CD marker, after the increase at low doses, a very steep drop is visible, which can be observed at about 1 Gy, see Figure 1.

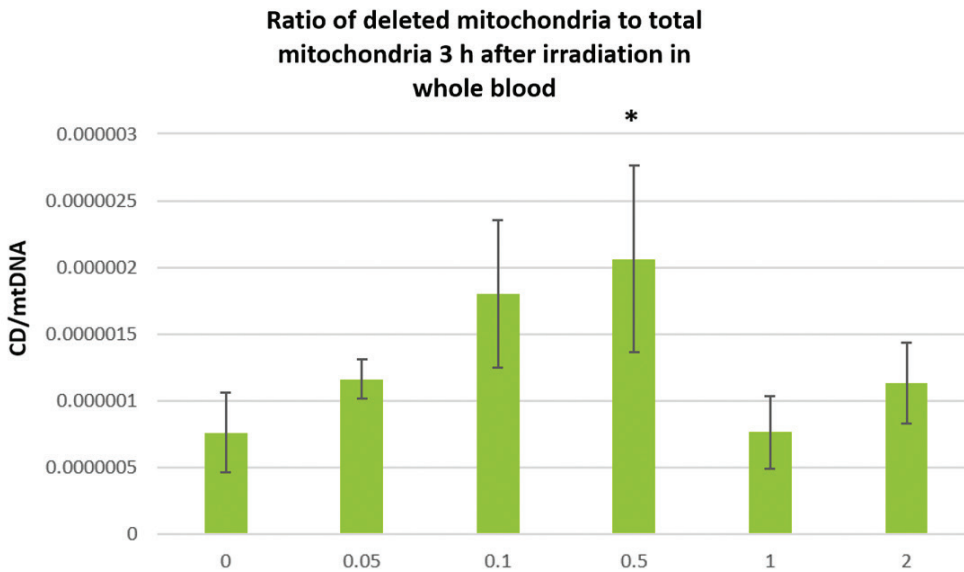


Figure 1: Quantitative change in the proportion of deleted and healthy mtDNA as a function of the irradiated dose after 3 hours (7 donors, mean, S.E.M.)

Note: An increase is observed between 0-0.5 Gy, which drops back to the baseline level at 1 Gy. (, P < 0.05, Ratio paired t-test)*

Source: compiled by Gábor Deli

We also performed the 12- and 24-hour incubations as mentioned in the methodology section, the course of the curves resembled the one presented above (see Figure 1), but the standard deviation was larger, and we did not obtain significant results.

Tandem duplication

Because of our previous experience with CD, the presence of D-loop tandem duplication was investigated 3 hours after X-ray irradiation, at 0-2 Gy dose. In the dose and time range used, the relative cell count remained unchanged, as we expected.

We counted the distinct bands in the gels run from the PCR samples made with the intercalating dye. The tendency can be observed that duplications are more likely to occur as a function of increasing irradiation dose, see Figure 2. The primer pair designed by us can theoretically amplify several known duplications.[26] Knowing the base sequence of the duplications, the method still needs to be refined by designing additional primer pairs and fluorescent probes.

[26] Damas 2014: 1261–1268.

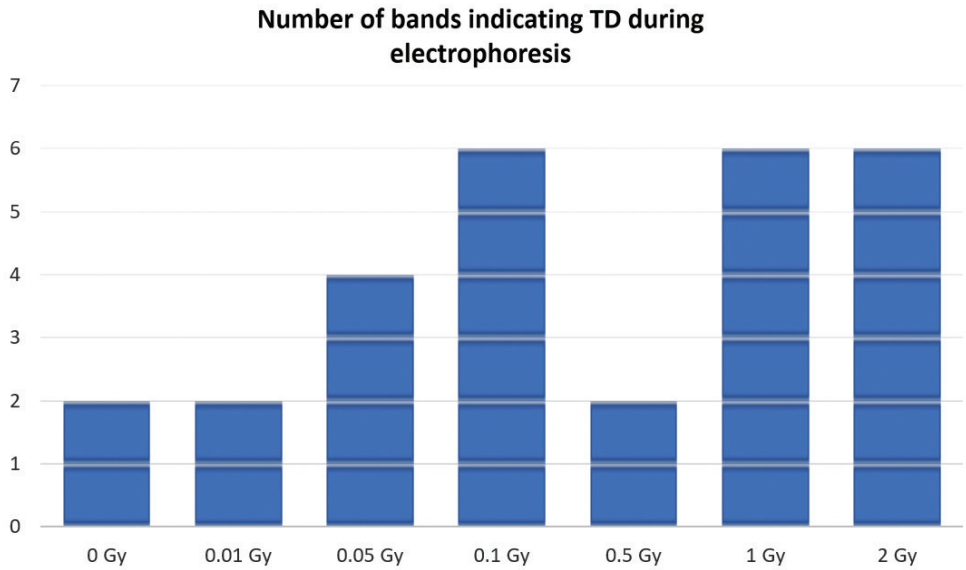


Figure 2: Duplication is rarer than CD. During the gel electrophoresis, the appearance of the bands was detected, and their sum was plotted (n = 7)

Source: compiled by Gábor Deli

Discussion

Radiation not only damages nuclear DNA but also mtDNA. After this, repair takes place in the mitochondrion, and the mtDNA resumes its circular form to avoid degradation.[27] Pieces can be lost during ring formation, less often they can be integrated, and deletions or insertions can occur.

One of these is the common deletion (CD) of mitochondrial DNA, a deletion of 4977 bp. The CD is formed in response to radiation and disappears rapidly in in vitro culture,[28] but Borghini et al. showed that the mtDNA 4977 deletion is significantly high in doctors who regularly catheterise, indicating that lifelong accumulation occurs in vivo at low doses.[29]

There are 2 identical 13 bp sequences in the mitochondrion beginning at sites 8471 and 13448 of mtDNA.[30] These two sequences are complementary, and if a double-strand break occurs anywhere in the section between them, a common deletion can occur first by pairing and then by DNA degradation. This is called the "slippage-replication" mechanism[31] and explains why random DNA damage anywhere

[27] Liao et al. 2022.
[28] Wanga et al. 2007: 433–442.
[29] Borghini et al. 2019: 976–984.
[30] Schon et al. 1989: 346–349; Yen 1991.
[31] Fontana–Gahlon 2020: 11244–11258; Shoffner et al. 1989: 7952–7956.

between the two stretches can cause such a specific deletion. The origin of synthesis of the heavy (57-441) and light chain (5721-5798) and promoter regions are not lost by the resulting degradation. Due to its unique formation mechanism, the "common deletion" is easily identified and is a very sensitive marker of mtDNA damage.

Since all genes in mtDNA are essential for the biogenesis and bioenergetic functioning of mitochondria, any mutations that lead to altered expression of these genes are expected to cause disturbances in energy metabolism and increased production of ROS released as intermediates during oxidative phosphorylation.[32] In addition to mitochondrial degenerative diseases, lifelong accumulation of mtDNA mutations and deletions is also believed to contribute to the aging process.[33] This is supported by the age-related decrease in oxidative phosphorylation and the accumulation of mtDNA mutations and deletions. As a marker of these processes, both aging and mitochondrial degenerative diseases show the accumulation of mtDNA common deletions.[34]

Studies have shown that this deletion can be used as a marker of oxidative damage to mtDNA even after very low doses of damage, as the lesion is amplified during mtDNA replication.[35]

There have been several reports that the CD form is not detectable to the same extent in whole blood.[36] Most authors use cell lines or primary tissue preparations to detect CD form after ionising radiation,[37] blood is rarely used for this purpose.[38]

Despite this, we chose whole blood, as blood is one of the most easily accessible tissues, and traditional biodosimetry tests also use blood. We also have to be very careful when taking samples, because the oxygen in the atmosphere and the oxygen bound in haemoglobin can change the tendency of DNA to break. Cell division could interfere with the effect of radiation, so we tried to minimise the time.

It was found that 3 hours after X-ray treatment, the CD increase varies according to a bell curve depending on the irradiation intensity, with the maximum observed around 0.5 Gy. The course of the curve showing the maximum of the CD/Min results is reminiscent of the course of the curve obtained by Schilling et al.[39] (on cell culture, but with a similar experimental set-up), which indicates that we are probably faced with a general phenomenon. The probable explanation for this phenomenon can be at a low dose interval that the higher the dose that hits the cell, the more breaks occur, and thus more deletions can form during the repair. However, by increasing the dose, the chance of mtDNA breaking both at the deletion site and outside of it increases, the mtDNA splits into two parts, and even during the formation of two smaller rings, no CD form is created.

[32] Kim et al. 2006: 10377–10383; Leach et al. 2001: 3894–3901.
[33] Wallace 1992: 628–632, Yen 1991; Jessie et al. 2001: 169–174.
[34] Cortopassi–Arnheim 1990: 6927–6933; Cortopassi et al. 1992: 7370–7374; Corral-Debrinski 1992: 169–180; Kaneko et al. 2012: 26–30; Lee et al. 2001: 67–74; Gerhard et al. 2002: 155–166.
[35] Ames 1989: 41–46; Fraga et al. 1990: 4533–4537.
[36] Lee et al. 1994a: 37–43; Ahmadi 2019: 250–254; Wang et al. 2013: 990–993.
[37] Schilling-Tóth et al. 2011: 33–39; Rogounovitch et al. 2002: 7031–7041.
[38] Borghini et al. 2019: 976–984.
[39] Schilling-Tóth et al. 2011: 33–39.

We observed that at this relatively short, 3 hours' time both the GAPDH and the mtDNA marker showed uniform, unchanged profiles, with a smaller standard deviation than after 24 hours.

We assumed, and our experiments seem to support, that because of radiation, not only deletion but also duplication can occur in mtDNA. The relationship between the occurrence of mitochondrial tandem duplications and ionising radiation has not yet been investigated. The D-loop is a partially duplicated section of mtDNA. If the two helices are broken at the same time because of radiation, the strands can be exchanged during the repair, and this can result in tandem duplication.

DIC is the gold standard method for biodosimetry.[40] It can be assumed that mitochondrial tandem duplicates are also radiation-specific aberrations, as are dicentric chromosomes since their formations show similar characteristics. According to the way of formation, it is understandable why and how specific the DIC formula is for ionising radiation.[41]

As a result of radiation, fractures do not occur randomly, but strictly along a straight line. In contrast, treatment with radiomimetic compounds (nitrogen mustard, 5-fluorouracil, methotrexate) usually results in random fractures.[42] Admittedly, bleomycin is an exception because one molecule can induce multiple breaks.[43] The condition for the creation of DIC is the simultaneous interruption of two DNA double helixes (four sugar-phosphate strands) that are at an adjacent location. Ionising radiation travels through tissue in no time, producing short-lived reactive radicals in its path that create side-by-side DNA double-strand breaks, and leaving other areas intact, keeping the cell alive in most cases. The formation of DIC during enzymatic repair is an exchange between the pieces of two broken double helixes, in such a way that the chromosome fragments containing the two centromeres are united. A cell containing a DIC is usually no longer capable of further division.

Translocations are radiation specific as well, they are formed in the same way as DIC, but the centromeric part is not transferred from one chromosome to another. They can be detected by fluorescent in situ hybridisation (FISH). As the further division of the cell is not hindered, so translocations persist for a long time, and the baseline is showing a significant increase with age.[44]

The tandem duplication in the D loop may therefore be promising for biodosimetry purposes if it becomes detectable in a PCR test system similar to that used for "CD". Since no genetic information is lost, we assume that loop D duplications can be detected longer than CD.

Lee et al. already observed in the early 1990s two tandem duplications (one 260 and one 200 bp) in the mitochondria of the muscles of elderly people.[45] The 200 bp repeat was found to be age dependent. Others have also observed that it

[40] International Atomic Energy Agency 2011.
[41] Hoffmann–Schmitz-Feuerhake 1999: 113–133.
[42] Deli 2022: 101–115.
[43] Deli 2023: 57–72.
[44] Whitehouse et al. 2005: 139–145; Sigurdson et al. 2008: 112–121.
[45] Lee et al. 1994b: 79–83.

often occurs in conjunction with common deletion.[46] We assume that it is difficult to separate the effects of cumulative doses of radiation and age since radiation affects our bodies throughout our lives. The 44 duplications described so far are at least partly in the area of the D-loop.[47]

This work of ours is a pioneering attempt to explore the relationship between radiation and TD. During our measurements, in the dose range, we used (0-2 Gy), the probability of the appearance of duplications also increased with the increase of the applied radiation dose. Regarding TD, PCR results are visible only after gel electrophoresis, although the use of fluorescent probes can increase the specificity of the method.

A product with a length of approximately 190 bp most often appeared in the gel as a result of X-ray radiation. This may correspond to the second most frequent duplication in the 200 bp long list compiled by Krishnan et al.,[48] and since there are 9 bases between our two designed primers, therefore the product will be shorter by that much.

The primer pair we designed can theoretically amplify 43 of 44 known duplications,[49] for the sake of clarification, we plan to check later by sequencing which one is the most frequent to collect information for the design of radiation-specific primers and probes.

The duplicated mtDNA can divide regularly and is not degraded, so there is a possibility of accumulation during life. Therefore, it is not surprising that the duplication can also appear in unirradiated samples.

After appropriate refinement of the method in the future – with NGS sequencing to a PCR probe system – we can distinguish the duplication variants, and by applying the TD together with the CD test, an informative PCR test can be produced that can also be used in radiation biology.

If both CD and TD will be detected simultaneously, the acute and cumulative effects of radiation could be detected.

Using this PCR test on the radiation effect as a pre-screening on-site examination reduces the number of people to be examined with microscopic methods, so it can help with triage and deciding on the appropriate treatment in disaster situations affecting many people.

In light of all this, measuring mitochondrial deletion and duplication can be very important from a disaster situation handling point of view.

The necessary infrastructure and the operating molecular biologists are present in several institutions of the country, in a disaster situation it is easier to involve external laboratories and find help for PCR measurements than in the case of difficult microscopic work.

[46] Krishnan–Birch-Machin 2006: 408–415.
[47] Damas 2014: 1261–1268.
[48] Krishnan–Birch-Machin 2006: 408–415.
[49] Damas 2014: 1261–1268.

References

Ahmadi, Mahboube et al. (2019): Mitochondrial Common Deletion Level in Blood: New Insight into the Effects of Age and Body Mass Index. *Current Aging Science,* 11(4), 250–254. Online: https://doi.org/10.2174/1874609812666190201163421

Ames, Bruve N. (1989): Endogenous DNA Damage as Related to Cancer and Aging. *Mutation Research,* 214(1), 41–46. Online: https://doi.org/10.1016/0027-5107(89)90196-6

Anderson, S. et al. (1981): Sequence and Organization of the Human Mitochondrial Genome. *Nature,* 290(5806), 457–465. Online: https://doi.org/10.1038/290457a0

Borghini, Andrea et al. (2019): Increased Mitochondrial DNA4977-bp Deletion in Catheterization Laboratory Workers with Long-Term Low-Dose Exposure to Ionizing Radiation. *European Journal of Preventive Cardiology,* 26(9), 976–984. Online: https://doi.org/10.1177/2047487319831495

Clayton, Davod A. (1991): Replication and Transcription of Vertebrate Mitochondrial DNA. *Annual Review of Cell Biology,* 1991(7), 453–478. Online: https://doi.org/10.1146/annurev.cb.07.110191.002321

Corral-Debrinski, M. et al. (1992): Association of Mitochondrial DNA Damage with Aging and Coronary Atherosclerotic Heart Disease. *Mutation Research,* 275(3–6), 169–180. Online: https://doi.org/10.1016/0921-8734(92)90021-G

Cortopassi, Gino A. – Arnheim, Norman (1990): Detection of a Specific Mitochondrial DNA Deletion in Tissues of Older Humans. *Nucleic Acids Research,* 18(23), 6927–6933. Online: https://doi.org/10.1093/nar/18.23.6927

Cortopassi, Gino A. et al. (1992): A Pattern of Accumulation of a Somatic Deletion of Mitochondrial DNA in Aging Human Tissues. *Proceedings of the National Academy of Sciences of United States of America,* 89(16), 7370–7374. Online: https://doi.org/10.1073/pnas.89.16.7370

Dainiak, Nicholas et al. (2003): The Hematologist and Radiation Casualties. *Hematology. American Society of Hematology. Education Program,* 2003(1), 473–496. Online: https://doi.org/10.1182/asheducation-2003.1.473

Damas, Joana et al. (2014): MitoBreak: The Mitochondrial DNA Breakpoints Database. *Nucleic Acids Research,* 42(D1), 1261–1268. Online: https://doi.org/10.1093/nar/gkt982

Deli, Gábor (2018): Cytogenetic Detection Tools for Effects of Ionizing Radiation on Human. *Hadmérnök,* 13(3), 179–192.

Deli, Gábor (2022): Mechanism of Action and Use of Radiomimetic Compounds. *Hadmérnök,* 17(1), 101–115. Online: https://doi.org/10.32567/hm.2022.1.7

Deli, Gábor (2023): Mechanism of Action and Use of Radiomimetic Compounds – Part 2. *Hadmérnök,* 18(2), 57–72. Online: https://doi.org/10.32567/hm.2023.2.3

Fontana, Gabriele A. – Gahlon, Hailey L. (2020): Mechanisms of Replication and Repair in Mitochondrial DNA Deletion Formation. *Nucleic Acids Research,* 48(20), 11244–11258. Online: https://doi.org/10.1093/nar/gkaa804

Fraga, C. G. et al. (1990): Oxidative Damage to DNA During Aging: 8-Hydroxy-2'-Deoxyguanosine in Rat Organ DNA and Urine. *Proceedings of the National Academy of Sciences of United States of America,* 87(12), 4533–4537. Online: https://doi.org/10.1073/pnas.87.12.4533

Gerhard, Glenn S. et al. (2002): Mitochondrial DNA Mutation Analysis in Human Skin Fibroblasts from Fetal, Young, and Old Donors. *Mechanisms of Ageing and Development,* 123(2–3), 155–166. Online: https://doi.org/10.1016/S0047-6374(01)00328-1

Harrison, John et al. (2017): The Polonium-210 Poisoning of Mr Alexander Litvinenko. *Journal of Radiological Protection,* 37(1), 266–278. Online: https://doi.org/10.1088/1361-6498/aa58a7

Hoffmann, Wolfgang – Schmitz-Feuerhake, Inge (1999): How Radiation-Specific is the Dicentric Assay? *Journal of Exposure Science & Environmental Epidemiology,* 9(2), 113–133. Online: https://doi.org/10.1038/sj.jea.7500008

International Atomic Energy Agency (2011): *Cytogenetic Dosimetry: Applications in Preparedness for and Response to Radiation Emergencies, Emergency Preparedness and Response.* Vienna: IAEA.

Jessie, B. C. et al. (2001): Accumulation of Mitochondrial DNA Deletions in the Malignant Prostate of Patients of Different Ages. *Experimental Gerontology,* 37(1), 169–174. Online: https://doi.org/10.1016/S0531-5565(01)00153-X

Jiang, Min et al. (2021): The Mitochondrial Single-Stranded DNA Binding Protein is Essential for Initiation of mtDNA Replication. *Science Advances,* 7(27), eabf8631. Online: https://doi.org/10.1126/sciadv.abf8631

Kaneko, Natsumi et al. (2012): Mitochondrial Common Deletion Mutation and Extrinsic Skin Ageing in German and Japanese Women. *Experimental Dermatology,* 21(Suppl 1), 26–30. Online: https://doi.org/10.1111/j.1600-0625.2012.01499.x

Kim, Grace J. et al. (2006): A Role for Mitochondrial Dysfunction in Perpetuating Radiation-Induced Genomic Instability. *Cancer Research,* 66(21), 10377–10383. Online: https://doi.org/10.1158/0008-5472.CAN-05-3036

Kiss Enikő et al. (2013): A sugárérzékenység vizsgálatának katasztrófavédelmi jelentősége. *Hadmérnök,* 8(4), 104–112.

Krishnan, Kim J. – Birch-Machin, Mark A. (2006): The Incidence of Both Tandem Duplications and the Common Deletion in mtDNA from Three Distinct Categories of Sun-Exposed Human Skin and in Prolonged Culture of Fibroblasts. *Journal of Investigative Dermatology,* 126(2), 408–415. Online: https://doi.org/10.1038/sj.jid.5700099

Liao, Siyang et al. (2022): The Fate of Damaged Mitochondrial DNA in the Cell. *Biochimica et Biophysica Acta (BBA) – Molecular Cell Research,* 1869(5), 119233. Online: https://doi.org/10.1016/j.bbamcr.2022.119233

Livak, Kenneth J. – Schmittgen, Thomas D. (2001): Analysis of Relative Gene Expression Data Using Real-Time Quantitative PCR and the 2(-Delta Delta C(T)) Method. *Methods,* 25(4), 402–408. Online: https://doi.org/10.1006/meth.2001.1262

Leach, J. K. et al. (2001): Ionizing Radiation-Induced, Mitochondria-Dependent Generation of Reactive Oxygen/Nitrogen. *Cancer Research,* 61(10), 3894–3901.

Lee, Hsin-Chen et al. (1994a): Differential Accumulations of 4,977 bp Deletion in Mitochondrial DNA of Various Tissues in Human Ageing. *Biochimica et Biophysica Acta,* 1226(1), 37–43. Online: https://doi.org/10.1016/0925-4439(94)90056-6

Lee, Hsin-Chen et al. (1994b): Ageing-Associated Tandem Duplications in the D-Loop of Mitochondrial DNA of Human Muscle. *FEBS Letters,* 354(1), 79–83. Online: https://doi.org/10.1016/0014-5793(94)01063-3

Lee, Hsin-Chen et al. (2001): Accumulation of Mitochondrial DNA Deletions in Human Oral Tissues — Effects of Betel Quid Chewing and Oral Cancer. *Mutation Research,* 493(1–2), 67–74. Online: https://doi.org/10.1016/S1383-5718(01)00160-7

Pesznyák, Csilla – Sáfrány, Géza (2016): *Sugárbiológia* [Radiation Biology]. Budapest: Typotex.

Phillips, Nicole R. et al. (2014): Simultaneous Quantification of Mitochondrial DNA Copy Number and Deletion Ratio: A Multiplex Real-Time PCR Assay. *Scientific Reports,* (4), 3887. Online: https://doi.org/10.1038/srep03887

Rogounovitch, Tatiana I. et al. (2002): Large Deletions in Mitochondrial DNA in Radiation-Associated Human Thyroid Tumors. *Cancer Research,* 62(23), 7031–7041.

Schilling-Tóth, Boglárka et al. (2011): Analysis of the Common Deletions in the Mitochondrial DNA is a Sensitive Biomarker Detecting Direct and Non-Targeted Cellular Effects of Low Dose Ionizing Radiation. *Mutation Research,* 716(1–2), 33–39. Online: https://doi.org/10.1016/j.mrfmmm.2011.07.018

Schilling-Tóth, Boglárka (2015): Investigation of Molecular Changes Induced by Ionizing Radiation in Normal Fibroblasts and Tumor Cells. Doctoral Thesis, Semmelweis University Doctoral School of Pathological Medicine.

Schon, Eric A. et al. (1989): A Direct Repeat is a Hotspot for Large-Scale Deletion of Human Mitochondrial DNA. *Science,* 244(4902), 346–349. Online: https://doi.org/10.1126/science.2711184

Schüle, Simone et al. (2022): Identifying Radiation Responsive Exon-Regions of Genes Often Used for Biodosimetry and Acute Radiation Syndrome Prediction. *Scientific Reports,* 12(1), 9545. Online: https://doi.org/10.1038/s41598-022-13577-4

Shoffner, J. M. et al. (1989): Spontaneous Kearns-Sayre/Chronic External Ophthalmoplegia Plus Syndrome Associated with a Mitochondrial DNA Deletion: A Slip-Replication Model and Metabolic Therapy. *Proceedings of the National Academy of Sciences of United States of America,* 86(20), 7952–7956. Online: https://doi.org/10.1073/pnas.86.20.7952

Sigurdson, Alice J. et al. (2008): International Study of Factors Affecting Human Chromosome Translocations. *Mutation Research,* 652(2), 112–121. Online: https://doi.org/10.1016/j.mrgentox.2008.01.005

Voisin, Philippe (2015): Standards in Biological Dosimetry: A Requirement to Perform an Appropriate Dose Assessment. *Mutation Research,* 793, 115–122. Online: https://doi.org/10.1016/j.mrgentox.2015.06.012

Wallace, Douglas C. (1992): Mitochondrial Genetics: A Paradigm for Aging and Degenerative Diseases? *Science,* 256(5057), 628–632. Online: https://doi.org/10.1126/science.1533953

Wang, Ping et al. (2013): Mitochondria DNA 4977 bp Common Deletion in Peripheral Whole Blood from Healthy Donors. *Biomedical and Environmental Sciences,* 26(12), 990–993. Online: https://doi.org/10.3967/bes2013.035

Wanga, Lu et al. (2007): Analysis of Common Deletion (CD) and a Novel Deletion of Mitochondrial DNA Induced by Ionizing Radiation. *International Journal of Radiation Biology,* 83(7), 433–442. Online: https://doi.org/10.1080/09553000701370878

Whitehouse, C. A. et al. (2005): Translocation Yields in Peripheral Blood Lymphocytes from Control Populations. *International Journal of Radiation Biology,* 81(2), 139–145. Online: https://doi.org/10.1080/09553000500103082

Yen, Tzu-Chen et al. (1991): Ageing-Associated 5 kb Deletion in Human Liver Mitochondrial DNA. *Biochemical and Biophysical Research Communications,* 178(1), 124–131. Online: https://doi.org/10.1016/0006-291X(91)91788-E

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
18. évfolyam (2023) 4. szám 79–96.
DOI: 10.32567/hm.2023.4.6

István Mihály,[1] Ferenc Varga[2]

An Experimental Study of Smoke Movement in a Pressurised Smoke-Free Staircase

Abstract

Pressurised staircases play an important role in ensuring both safe evacuation and conditions for rescue and firefighting intervention. Occupants may be delayed in getting to safety or extinguishing the fire for unforeseen reasons. In some cases, the pressurised staircase or its lobby may serve as a temporary protected area for persons unable to escape independently, which should ensure the safety of the persons fleeing or being evacuated for a limited period of time. In such cases, the role of effective smoke control should be a priority. The purpose of pressurisation is to prevent the entry of smoke and toxic combustion gases at dangerous levels, but the possibility cannot be excluded. In the present series of studies, the smoke flow in a pressurised staircase was investigated in order to gain experience of the characteristics of smoke movement and propagation under these conditions. This involved a series of experiments with smoke cartridges placed on different staircase levels, supported by ventilation measurements to investigate the smoke flow. Based on the results of the measurements and observations, we proposed possible improvements to the technical solutions.

Keywords: pressurised staircases, differential pressure measurements, Pressure Differential Systems (PDS), smoke movement

Introduction

Restricting smoke ingress into pressurised spaces requires a complex approach and practical considerations. The objective of this research is to investigate the smoke

[1] Certified Fire Protection Specialist, Juridical Expert, CEO, Brandplan Kft.; PhD student, Doctoral School of Military Engineering, Ludovika University of Public Service, e-mail: mihaly.istvan90@gmail.com
[2] Head of Institute of Disaster Management, Faculty of Law Enforcement, Ludovika University of Public Service, e-mail: varga.ferenc2@uni-nke.hu

flow characteristics in an existing pressurised staircase, which requires knowledge of the ventilation characteristics of the staircase. For this purpose the air flow rates, air delivery and air exchange rates into and out of the staircase will be determined prior to the smoke tests.

In the event of fire in mid-rise and high-rise buildings, escape of occupants may be through stairwells or escape windows protected from the effects of the fire. Pressurisation is a common way of preventing smoke from entering stairwells.[3]

An FDS (Fire Dynamics Simulator) simulation study which investigated the effectiveness of pressurisation as a function of the number of open doors, found that in the tested layout, when more than four doors were opened simultaneously, the pressurised smoke venting system was inadequate.[4]

A key challenge in the design of pressurised staircases is the number of stairwell doors that are assumed to be open at one time when determining the fan working point. In this process, the designer has to take into account the design of the building, the evacuation strategy and the impact of firefighter intervention.[5]

In some buildings, the role of smoke control systems may be subordinate to other purposes (e.g. preventing the escape of toxic fumes), in which case they should be designed with special conditions.[6]

In the case of open stairwell doors with pressurisation, outward airflow may also result in backflow in the direction of the stairwell, which can be detected by smoke flow testing.[7]

Two important elements in achieving effective pressurisation are the provision of adequate overpressure and airflow when the windows are closed or open. It is important not only for the evacuation of the building, but also for the efficiency of firefighting intervention and the ability of the firefighters intervening to secure the scene.[8]

According to the definition of the *National Fire Protection Regulations (OTSZ)* issued by the Decree of the Ministry of the Interior 54/2014 (5.XII.), the possibility of smoke and toxic combustion gases formed during a building fire to enter smoke-free stairwells must be limited, which will allow the building to remain suitable for safe evacuation and rescue for a specified period of time. Smoke control itself is defined as a set of measures to prevent the entry of smoke into a sheltered place to an extent that would endanger escape, i.e. not to exclude the possibility of smoke ingress.[9]

According to the Fire Protection Technical Guideline (TvMI) on protection against heat and smoke spread, in staircases without smoke in the absence of fire, the pressure difference between the staircase and the adjacent space may be equalised, and in some cases the pressure in the adjacent space may exceed the staircase overpressure in the absence of pressure relief, which should be prevented by regulation.[10] Most

[3] Alianto et al. 2022: 104224.
[4] Lee–Lau 2023: 132–153.
[5] International Code Council and Society of Fire Protection Engineers 2022: 210.
[6] Kátai-Urbán et al. 2023; Cimer et al. 2021.
[7] Mihály–Bérczi 2023: 47–64.
[8] Varga 2018: 261–276.
[9] Decree 54/2014 (5.XII.) of the Ministry of the Interior.
[10] TvMI 3.4:2022.06.13 2022.

designers and experts use solutions based on TvMI-s. The reason is that these solutions are already proven and meet the level of requirements of the OTSZ.[11]

The Fire Protection Technical Guideline on evacuation provides for the possibility of a smoke-free staircase (pressurised staircase) rest area or smoke-free staircase lobby (pressurised staircase with pressurised lobby) as a temporary protected area. In this case, the staircase or lobby shall be enclosed with fire and smoke barriers appropriate to the risk classification of the building, and shall be protected against fire spread from the facade.[12]

The German VDMA 24188 also differentiates the definition of the minimum air velocity to be provided in the free cross-section of the open door by taking into account the location of the staircase within the building, which is due to the temperature difference between the staircase and the staircase opening in case of fire. In case of some staircase types, where the exhaust air is not extracted or not automatically extracted from the adjacent space, it requires the flushing of the staircase with fresh air at a rate of at least 10 000 m^3/h.[13]

When all stairwell doors are closed, a small amount of airflow is sufficient to maintain a smoke-free stairwell.[14] The sizing should also take into account how many doors are open at the same time.[15]

Description of the subject of the study

The main parameters of the building containing the staircase under study, based on the field survey

The analysed staircase is a pressurised staircase with a pressurised lobby in a mid-rise community building in Budapest, Hungary. The building has a basement level, ground floor, four floors + roof level, the height of the top use level is +21.62 m, and the height of the lowest use level is –3.25 m in relation to the exit level (ground floor). The building is typically occupied by people who are able to escape on their own, but the presence of people who are able to escape with assistance due to their intended use should be expected.

During the last major reconstruction of the monumental building, the provisions of the National Fire Protection Regulations issued by the Ministry of the Interior Decree 2/2002 (23.I.) were applicable.

The main direction of evacuation of the building is the pressurised staircase, which is separated by fire barriers on all floors. Of the two elevators in the pressurised lobby, one is designed as a firefighting lift in accordance with MSZ EN 81-72 and

[11] Bérczi 2021: 32–42.
[12] TvMI 2.5:2022.06.13 2022.
[13] VDMA 24188 2011: 6–15.
[14] Black 2015: 216–230.
[15] NFPA 92 2021: 92-8.

MSZ 9113. When designing smoke-free staircases, it was also necessary to take into account the technical regulation ME-04–132–84 of the building sector.

According to the currently valid, repeatedly amended National Fire Protection Regulations issued by the Ministry of the Interior in Decree 54/2014 (5.XII.), the building's standard risk class is MR (medium risk). Due to the difference in level of more than 14 meters, the staircase of the building considered for evacuation should be designed as a smokeless stairway at present. The current requirement for safe access from a smokeless staircase to a safe space cannot be met by the staircase, but there was no such obligation at the time of the conversion.

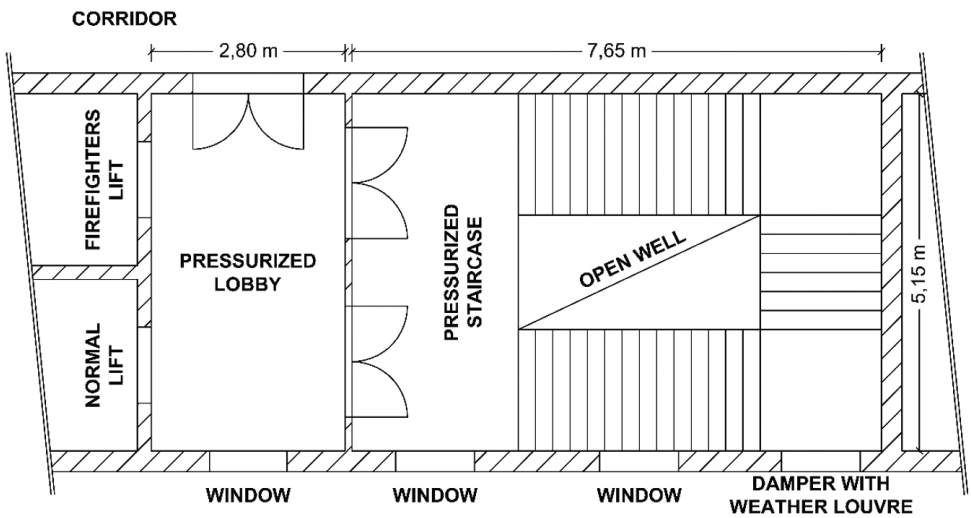


Figure 1: Floorplan of the pressurised stairwell at the 1st floor
Source: compiled by the authors

Main parameters of the pressurisation system based on the on-site survey

The stairwell pressurisation fans are located in a dedicated room on the top floor, with weather louvres on the boundary wall to allow fresh air to be drawn in. The fans supply fresh air to the stairwell at the top level through three openings with a geometric area of 1.44 m^2 per fan. A fan is also installed on the roof level to the pressurised lobbies. The air intake is provided by an air duct with outlets at each level.

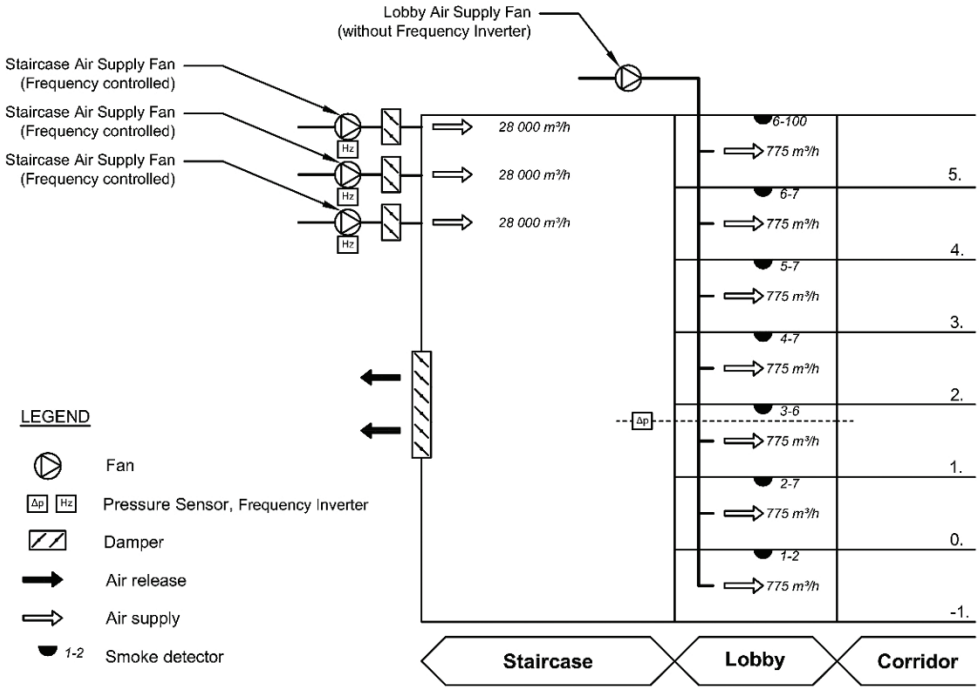


Figure 2: Schematic build of the pressurised stairwell with the designed air volumes of the fresh air
Source: compiled by the authors

The relative overpressure in the staircase is detected by a differential pressure sensor on the first floor between the staircase and the air space of the accommodation. The double-leaf fire doors opening into the staircase have a "non-combustible" flammability rating according to their technical building permit, a certified fire resistance limit value of "TH = 0.5 hours" and an air tightness rating of L4.

The staircase pressure is controlled by PI control with a proportionality factor of 0.5 and an integration time of 10 s, which was not changed during the measurements. The set point was 70 Pa, with a minimum frequency of 10 Hz, which was the same as the start frequency. The designed air volume of each fan was 28 000 m^3/h each, with a total pressure of 350 Pa.

On the external facade wall of the staircase, between the ground floor and the first floor, a 1000 × 1920 mm motorised damper with a weather louvre was installed, which provides a continuous airflow to the open air during the operation of the pressurisation system.

Figure 3: Staircase pressurisation fans on the top floor
Source: compiled by the authors

Ventilation test of the staircase

We have carried out an aerodynamic measurement of the staircase in order to assess the characteristics of the staircase operation. The differential pressure values per level are illustrated in Figure 4. The characteristics of the measuring instruments used in the measurement are summarised in Table 1.

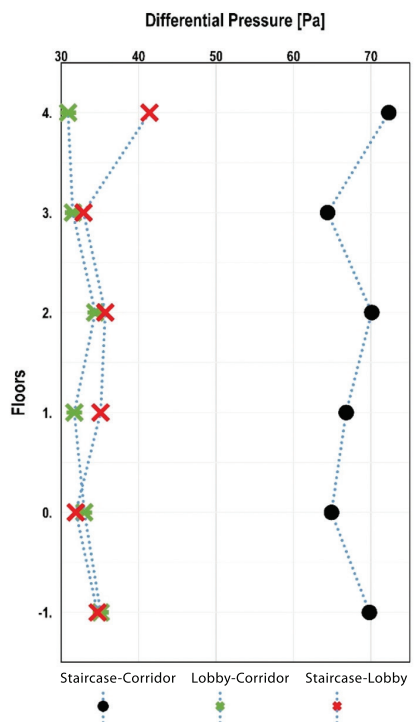


Figure 4: Differential pressure between spaces
Source: compiled by the authors

Table 1: Instruments used in the measurement

No.	Field of measure-ment	Type	Measuring range	Accuracy	Resolution	Date of calibration and certificate No.
1.	differential pressure	0560 0400	0–200 hPa	±(0.3 Pa + 1% of the measured value) ±1 Digit (0 … 25 hPa)	0.001 hPa	10. 10, 2022. 4740014
2.	air velocity	0635 9430	0.3 to 35 m/s	±(0.1 m/s + 1.5% of the measured value) (0.3 to 20 m/s)	0.01 m/s	07. 11, 2022. 224647
3.	temperature	0635 1570	–20 to +70 °C	±0.5 °C (0 to +70 °C)	0.1 °C	04. 11, 2022. 224648
4.	air velocity	0635 1570	0 to 50 m/s	±(0.03 m/s + 4% of the measured value) (0 to 20 m/s)	0.01 m/s	07. 11, 2022. 224649
5.	humidity	0560 6082	2 to 98%RH	±2% RH (2 to 98% RH)	0.1 %RH	07. 11, 2022. 224650
6.	temperature	0560 6082	–10 to +70 °C	±0.5 °C (at +25 °C)	0.1 °C	04. 11, 2022. 224651

Source: compiled by the authors

Based on the pressure measurements, the measured pressure values exceed the current regulations, so we have proposed to control the staircase pressurisation system using a reduced setpoint.

The staircase measured was characterised by a damper located between the ground floor and the 1st floor, opening directly into the open air, providing a continuous air flow from the staircase to the open air, regardless of whether the staircase doors are open or closed. Air velocity measurements were taken when the doors on the ground, 1st and 2nd floors were open, and the resulting air velocities were found to provide airflow rates that meet the requirements at the time of installation. The total measured air flow through the openings was 59 998 m^3/h, of which 11 186 m^3/h escaped through the damper.

Subsequently, the air transport of the staircase air supply system was tested in static condition with closed doors. The aim of the measurements was to obtain data on the amount of air entering the staircase and the amount of air leaving the staircase through the damper before the smoke tests are carried out. The measurements were carried out in three setups. In the first case, the formwork leading to the open air was completely covered with an airtight sheet. Subsequently, further measurements were carried out with uncovered and 25% covered air release opening.

During each series of air measurements, the airflow through the air intakes of the fans was recorded (at 60 points per measurement), the airflow through the outdoor damper (air release opening) when it was not closed (9 and 12 points per measurement), and the relative overpressure between the staircase and the corridor was recorded continuously during the tests, the pressure difference at the damper on the first floor,

the average frequency values displayed by the inverters in the given arrangement. The air velocities measured at the inlet surface as a function of the free surface area of the air release opening and the air volumes calculated from them are summarised in Table 2. The measured values show that the control responded well to the increase in the air release opening surface area, increasing the amount of air introduced. This is confirmed by the values displayed by the frequency inverters (Table 3).

Table 2: Average air velocity at the inlet and the calculated air volume

Free area of the air release opening (%)	**Average air velocity at the inlet [m/s] / calculated air volume [m³/h]**			**Total air volume [m³/h]**
	Fan LB1	**Fan LB2**	**Fan LB3**	
0 (closed)	1.08 5035	0.91 4246	1.03 4795	14 076
25	2.81 13 087	1.48 6884	2.39 11 135	31 107
100	2.76 12 877	1.76 8 196	2.37 11 037	32 110

Source: compiled by the authors

Table 3: Displayed value of frequency on the frequency inverter

Free area of the air release opening (%)	**Displayed value of frequency on the frequency inverter (FI) [Hz]**		
	FI-1 (Fan LB1)	**FI-2 (Fan LB2)**	**FI-3 (Fan LB3)**
0 (closed)	23.6–23.7	24.0	23.6–23.7
25	31.0	35.3	34.6–34.7
100	32.7–32.8	35.5–35.6	34.9–35.0

Source: compiled by the authors

Air measurements on the air release opening to the open air were taken at 12 points in the uncovered configuration and at 9 points with the damper at 25% covered. At each point, one measurement sequence was 30 s, with a recording frequency of 1 Hz. The air velocities measured at each point, and the pressure difference between the two sides of the damper while measuring the air velocity, are illustrated in Figure 5. The free aperture area is taken into account by a factor of 0.8.

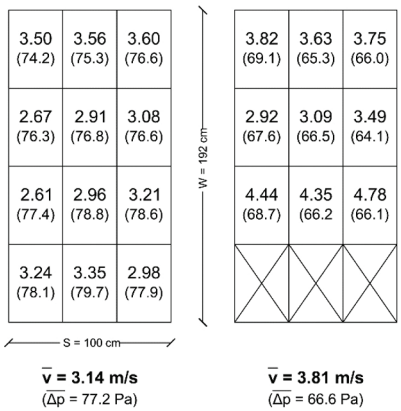


Figure 5: Measured air velocity and pressure difference through the air release opening with 100% and 25% free area of the vent

Source: compiled by the authors

The total gap surface of the staircase was estimated by calculation based on the air volume introduced and the air volume leaving the staircase, which showed a good agreement in the three measurement series even with twice the air volume difference. Its values are summarised in Table 4.

Table 4: Calculated crack area of the staircase

Free area of the air release opening (%)	**Average pressure differential between the staircase and the corridor at 1st floor (deviation) [Pa]**	**Measured air volume at the air release opening [m³/h] (Aeff/A = 0.8)**	**Measured total air volume at the fans [m³/h]**	**Calculated crack area of the staircase without the Area of the air release opening [m²]**
0 (closed)	73.4 (1.89)	≈ 0	14 076	0.354
25	70.6 (1.38)	15 759	31 107	0.393
100	72.9 (1.49)	17 358	32 110	0.372

Source: compiled by the authors

The air measurements show that the staircase is well ventilated even with the doors closed, with an air exchange rate of more than 20 times (23.7 1/h), i.e. about 732 m^3 above the air release opening. The amount of air introduced, the fan speed with the doors closed, is sufficient.

Smoke test observations

The aim of the study was to determine the smoke flow characteristics and properties of a pressurised staircase when ventilated with flush air. For this purpose, we carried out three trials. In all tests, the same smoke candle with the same charge and charge volume was used. We took video footage of the rehearsal from two directions. One of the observation points is the ground floor, from which the damper leading to the open air is clearly visible. The second observation point was the 2nd floor during the first and second tests, and the 3rd floor during the third test. From the selected observation points, the smoke flow was well monitored.

In the first experiment, the smoke candle was placed on the basement level of the pressurised staircase, at the centre of the vertical projection of the open well. In the second experiment, smoke was developed on the rest below the air release opening, and in the third case on the rest above the damper.

The nominal weight of the smoke candles used was 200 g. According to the information provided by the smoke candle manufacturer, the main components of the mixture are 1.4-dihydroxyanthraquinone, potassium chlorate and ammonium chloride. The average time of smoke emission during the tests was 89 seconds.

Smoke candle in the basement

In the first experimental arrangement, the smoke candle was installed at basement level, below the air release opening, about 8 meters below it. Within a few seconds, the developing smoke enveloped the staircase to a height of approximately 3 meters from the floor level. At the same time, an intense flow of smoke was observed from the pressurised space towards the pressurised lobby at basement level. The smoke flowing through the gaps around the door was stirred up and diluted by the air inlet to the hallway. The optical smoke detector located here gave a signal 55 seconds after ignition. The smoke in the lobby airspace then leaked into the lift shafts and towards the accommodations.

In the staircase, smoke was flowing upwards from the lower part of the staircase and smoke was also flowing into the pressurised lobby on the ground floor through the doors from the staircase to the lobby. The optical smoke detector located in the ground floor lobby gave a signal at the 106th second.

During the investigation, there was no significant amount of smoke entering the 1st floor lobby, no fire alarm was received from there, but the presence of smoke was detectable by the senses. The resulting smoke was ventilated very slowly through the damper leading to the open air and through the basement and ground floor lobbies. It could be seen that on the side opposite to the inlet, away from the air release opening, the smoke spread rapidly through the gaps, with significant amounts of smoke entering the lower level lobbies. There was no smoke visible to the senses above the air release opening, although there was smoke entering the lobby on the first floor, which was also not significant. In order to ventilate the stairwell space, it was also necessary to open the doors to the corridor at basement level. Smoke was

seen leaking into the firefighters lift shaft. In the elevator cab waiting on the third floor, the smell of smoke was detectable, while on arrival in the basement lobby, when the lift landing door was opened, the smoke was visible entering the car.

Figure 6: Test 1, observation from the ground floor
Source: compiled by the authors

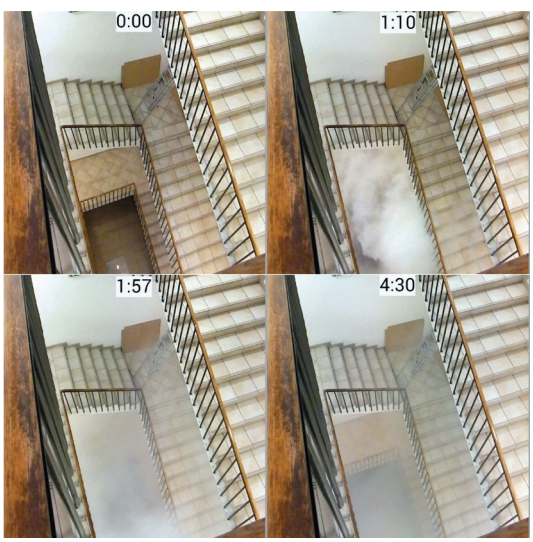


Figure 7: Test 1, observation from the 2nd floor
Source: compiled by the authors

Smoke candle under the air release opening

In the second experimental setup, the smoke candle was installed on the mezzanine rest in front of the air release opening, 2 meters below it. Some of the evolving smoke was released into the open air, but there was a separation in the open well, which caused the smoke to spread towards the lower levels. After the release ceased, the resulting smoke mass descended as a vapour to the lower floors, where a significant amount of smoke was released through the door gaps into the ground floor and basement lobbies.

During the experiment, smoke was observed in the first floor lobby, but not accumulated to the extent that would have been indicated by the optical smoke detector. The optical sensor located in the ground floor lobby was triggered at second 166, while the sensor located in the basement lobby was triggered at second 210. In this experiment, too, there was evidence of smoke in the shaft of the firefighters lift.

Smoke ventilation from the staircase was faster than in the first test arrangement. This is because some of the smoke has already escaped into the open during the development stage. Ventilation of the lower parts was also possible in this case by opening the doors to the corridor.

The investigation showed that the smoke candle placed closer to but lower than the damper created more favourable conditions in the staircase, but still a significant amount of smoke was released into the lower, unflushed area. There was no smoke visible to the senses above the air release opening, but there was smoke leakage into the firefighters lift shaft. The optical smoke detectors gave a later signal than in the first test, due to the fact that part of the smoke from the staircase had escaped through the dampers to the outside, and therefore the smoke concentration in the lobby was slower to develop.

Figure 8: Test 2, observation from the ground floor
Source: compiled by the authors

Figure 9: Test 2, observation from the 2nd floor
Source: compiled by the authors

Smoke candle above the air release opening

In the third experimental setup, the smoke candle installed in the rest area between floors 2-3 was located above the air release opening, about 2 m above it. The smoke initially started to flow down the staircase, and then downward flows were observed in the open well. A significant part of the smoke escaped to the open air through the damper, but the outflow was adversely affected by the fact that the opening to the open air was partially covered horizontally by the stairway. The remainder of the smoke descended down the open well as in the second experiment. In the second floor lobby, smoke ingress was only briefly detectable by the senses. In the lower level lobbies, the optical smoke detectors gave a significantly later signal, which can be explained by the dilution of the smaller amount of smoke. The firefighters lift shaft was leaking a detectable amount of smoke. It can be seen that during the smoke development above the air release opening, a significant part of the smoke generated was vented outdoors through the damper. The remainder descended in the open well, but at a lower volume and density compared to the first and second experiment. The levels above the vents remained smoke-free, but smoke reached the lower levels. The small amount of smoke that entered the lobby slightly penetrated the firefighters lift shaft.

Figure 10: Test 3, observation from the ground floor
Source: compiled by the authors

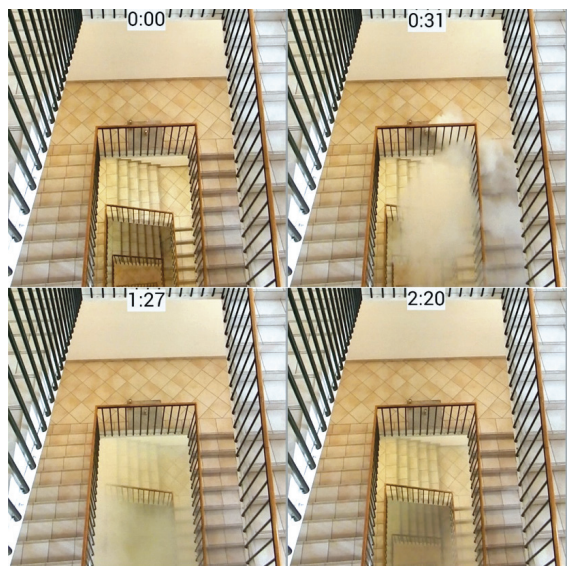


Figure 11: Test 3, observation from the 3rd floor
Source: compiled by the authors

Summary

The levels above the air release opening (damper) remained smoke-free throughout the tests, and with the smoke candle above the damper, smoke did not flow to the area above the smoke candle, meaning that the smoke-free airspace with effective flushing was permanent. This is also due to the roughly 20-fold increase in air exchange in the airspace above the damper, as measured.

In all cases, the smoke was trapped on the levels below the damper, and the smoke flowed through the gaps in the doors into the lower pressure connected spaces. The ventilation of lobbies with lower pressure compared to the staircase stirred up the smoke from the staircase, which in several cases led to the alarm of optical smoke detectors in the lobbies.

A small amount of smoke entered the firefighters lift shaft and the car. This was partly achieved through the gaps around the closed lift landing door, and when the lift landing door was opened, a larger volume was able to flow into both the car and the lift shaft.

Smoke flow into the lift shaft was facilitated by the higher pressure in the lobby compared to the lift shaft. Furthermore, the ventilation opening in the upper part of the lift shaft resulted in a greater chimney effect in the shaft due to the significant temperature difference. During the tests, the outside temperature was 1.9 °C, while the temperature in the staircase was 20.1 °C at the start of the measurements.

Conclusions and recommendations

Based on the tests performed, a fire in the stairwell is a significant risk factor, as the pressurised ventilation will cause smoke to be vented to rooms with stairwell connections away from the fire source, through gaps around the doors.

Smoke can enter a pressurised staircase, even if the installation and use rules are respected, for the following reasons:

- During a simultaneous evacuation, if the staircase for escape is designed as a pressurised staircase, the air velocity required to expel the smoke cannot develop in the door cross-section due to the open condition of the vast majority of the staircase doors
- During a staged evacuation, if the overpressure in a stairwell is briefly or permanently reduced, smoke may leak in through the gaps of closed door(s). This may occur, for example, when evacuating floors above the level affected by fire if evacuation of floors below ground level is also taking place or if more doors than planned are left open
- During the firefighting, for reasons necessary for the intervention, several stairwell doors are open
- Existing staircases open directly into utility spaces (e.g. offices) or other rooms from which air is not or not efficiently ventilated
- Extreme environmental conditions (wind, temperature difference between the staircase and its surroundings)

- Pressurised staircase with overpressure in accordance with point 11.6.6 of the TvMI. In this case, it is proposed to prohibit the creation of temporary protected areas in the pressurised staircase or in its lobby

Smoke or toxic combustion gases can be expected to enter the staircase in the following cases:

- In the event of a fire in a smoke-free stairwell or its lobby (non-compliance with the rules of use)
- Lack of integrity of the building structure enclosing the smoke-free staircase or its vestibule (missing or inadequate sealing of subsequent wall and/or slab penetrations). The wall or slab between the pressurised staircase and the adjacent spaces without pressurised ventilation shall be sealed with a (fire blocking) barrier that cannot withstand static or increased transient overpressure without damage, with particular attention to integrity
- If mechanical heat and smoke extraction and mechanical air supply are used on the fire affected floor, and the failure of the smoke extraction system causes the associated space to become over-pressurised as opposed to the desired balanced or depressurised pressure conditions

Smoke ingress can pose a risk to persons escaping and, in the case of pressurised stairwells designed as temporary protected areas, to persons in the temporary protected area. Smoke penetration that can be felt by the senses can lead to a panic situation.

An air release opening on the opposite side to the intake proved to be effective in removing smoke from the upper floors, but in all cases smoke was able to reach the areas below the air release opening. It is therefore important that the air release opening is located on the opposite side of the airspace to be kept smoke-free from the intake, otherwise smoke can accumulate in areas without effective ventilation.

Article 190 (2) of the National Fire Protection Regulation is correct, according to which all storage is prohibited in the fire lobby, smoke-free stairwell and lobby.

Section 5.1.2 of standard MSZ EN 81-72 refers the design of smoke protection for firefighters' lifts to national regulations and gives criteria for smoke protection in Annex I, point I7.[16] The National Fire Protection Regulations does not prescribe heat and smoke extraction and pressurisations for firefighters lift shafts, but it does specify that the shaft may only be connected to a room or open space protected against the spread of fire. The MSZ 9113 standard requires a ventilation opening in the shaft head with a cross-section equal to 1 or 4% of the horizontal section of the shaft, depending on the design of the firefighting lifts.[17]

The chimney effect created by a standard sized ventilation opening can contribute to smoke ingress into the firefighters lift shaft in case of high temperature differentials, and it is therefore recommended to investigate the need for smoke venting of firefighters lift shafts. It is also important to consider that if the firefighters lift opens into a fire lobby with pressurisation and the lobby pressurisation is only sized to cover

[16] MSZ EN 81-72 2020: 12–13, 45.
[17] MSZ 9113 2003: 4.

the gap losses near the closed doors, there may be a real risk of smoke entering the firefighters lift shaft.

Where a pressurised staircase or pressurised lobby is designed as a temporary protected area to reduce risks, including the risk of panic, it is recommended that smoke-free staircases should have a ventilation surface sized to the air exchange rate to ensure its ventilation. This will remove any smoke from the stairwell. Safety can be further enhanced by locating the temporary protected area in the airspace of the pressurised staircase and creating a pressurised lobby between the staircase and the accommodations (a pressurised staircase with lobby).

Pressurised ventilation of firefighters lift shafts can be used to limit smoke ingress into the lift shaft. Pressurised ventilation of normal lift shafts in the event of fire can reduce the spread of smoke through lift shafts.

Increased emphasis should be placed on the monitoring of compliance with the provisions of Article 190 (2) of the National Fire Protection Regulation during official controls. In addition, it is recommended that the electrical wiring and cables installed in the staircase should be classified as at least class s1 for smoke emission according to MSZ EN 13501-6. The national MSZ 13207:2020 Annex C and the TvMI on electrical installations, lighting protection and protection against electrostatic discharge Annex B.2.6 also contains a requirement for cables, but only for certain types of buildings, and does not include the temporary protected area.[18]

Where open office spaces are connected to a staircase with a pressurised lobby, in addition to the design proposed in the TvMI, consideration should be given to providing an average air velocity of 2 m/s in the free cross-section of the open door to ensure that smoke and other toxic combustion products can be effectively expelled in the event of a full-blown fire.

According to point 5.2.1 of the TVMI on the planning, design and installation of fire alarm systems, the smoke-free staircase and its lobby cannot be considered a low-risk area, i.e. it cannot be excluded from the protection.[19] Based on our investigations, it is recommended, in accordance with Annex C of the TVMI, that the staircase pressurisation system should not be triggered automatically when the first fire alarm is received from the pressurised staircase.

References

Alianto, Beline et al. (2022): High-Rise Building Fire Safety Using Mechanical Ventilation and Stairwell Pressurization: A Review. *Journal of Building Engineering,* 50, 104224. Online: https://doi.org/10.1016/j.jobe.2022.104224

Bérczi, László (2021): The Role of Fire Protection Technical Guideline in the Protection against Heat and Smoke Spread. *Védelem Tudomány,* 6(3), 32–42.

Black, William Z. (2015): Stairwell Pressurization and the Movement of Smoke during a High-Rise Fire. *ASHRAE Transactions,* 121(1), 216–230.

[18] MSZ 13207 2020: 86; TvMI 7.5:2022.06.13: 78–79.
[19] TvMI 5.3:2022.06.13.

Cimer, Zsolt et al. (2021): Application of Chemical Monitoring and Public Alarm Systems to Reduce Public Vulnerability to Major Accidents Involving Dangerous Substances. *Symmetry,* 13(8), 1528. Online: https://doi.org/10.3390/sym13081528

International Code Council and Society of Fire Protection Engineers (2022): *Fire Safety for Very Tall Buildings: Engineering Guide.* The Society of Fire Protection Engineers Series. Cham: Springer. Online: https://doi.org/10.1007/978-3-030-79014-1

Kátai-Urbán, Lajos et al. (2023): Examination of the Fire Resistance of Construction Materials from Beams in Chemical Warehouses Dealing with Flammable Dangerous Substances. *Fire,* 6(8), 293. Online: https://doi.org/10.3390/fire6080293

Lee, Ann – Lau, Ghar Ek (2023): Smoke Control in High-Rise Residential Buildings with Stair Pressurization Systems. *Fire,* 6(4), 132–153. Online: https://doi.org/10.3390/fire6040132

Mihály, István – Bérczi, László (2023): Túlnyomásos füstmentes lépcsőházak légtechnikai méréseinek tapasztalatai II. *Védelem Tudomány,* 8(1), 47–64.

MSZ 9113:2003 Establishment of lifts. Additional requirements for lifts in case of a fire in a building. Magyar Szabványügyi Testület, 2003.

MSZ 13207:2020 Selection, laying and current rating of power cables and control cables with rated voltages from 0.6/1 kV up to 20.8/36 kV. Magyar Szabványügyi Testület, 2020.

MSZ EN 81-72:2020 Safety rules for the construction and installation of lifts. Particular applications for passenger and goods passenger lifts. Part 72: Firefighters lifts. Magyar Szabványügyi Testület, 2020.

NFPA 92: Standard for Smoke Control Systems. National Fire Protection Association, 2021.

TvMI 2.5:2022.06.13. Fire Protection Technical Guideline Protection. Evacuation. 2022.

TvMI 3.4:2022.06.13. Fire Protection Technical Guideline. Protection against heat and smoke spread. 2022.

TvMI 5.3:2022.06.13. Fire Protection Technical Guideline. Planning, design and installation of fire alarm systems. 2022.

TvMI 7.5:2022.06.13. Fire Protection Technical Guideline. Electrical installations, lightning protection and protection against electrostatic discharge. 2022.

Varga, Ferenc (2018): Assessment of the Procedural and Technical Conditions for the Hungarian Fire Investigation System in Line with International Experiences. *Hadmérnök,* 13(4), 261–276.

VDMA 24188:2011-06 (2011): *Rauchschutzmaßnahmen in Treppenräumen – Rauchableitung, Rauchverdünnung, Rauchfreihaltung*. Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA), Frankfurt/Main.

Legal source

Decree 54/2014 (5.XII.) of the Ministry of the Interior on the issuance of the National Fire Protection Regulation

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

18. évfolyam (2023) 4. szám 97–107.
DOI: 10.32567/hm.2023.4.7

István Mészáros[1]

Comparison of the Protection of Critical Healthcare Infrastructures in Germany and Hungary

Abstract

In 2008, the European Union regulated the basics of the protection of critical infrastructures in a directive. The Member States therefore had to ensure that – in addition to the freedom of the method and means of implementation – the provisions of the directive were transposed into their national legal order. Accordingly, some Member States may define different detailed rules. The detailed rules related to the protection of critical infrastructures (e.g. the designation thresholds) are not public in several Member States, but in Germany and Hungary they have been recorded at the legislative level. In my study, I compare the rules related to the protection of critical healthcare infrastructures, including inpatient care institutions, primarily based on legal sources and the experiences of my study tour in Germany, from the selection criteria system to crisis planning. The good practices resulting from the differences and similarities to be discovered can help to revise and standardise the rules and practices related to the protection of critical health infrastructures.

Keywords: critical infrastructure, vital system, health crisis situation, operator security, hospital safety

Regulation of the protection of critical infrastructures in the European Union

The geopolitical and globalisation changes that took place until the 1990s resulted in extremely rapid technical development, which increased society's dependence on infrastructure systems. The proper operation of these systems is of fundamental

[1] PhD student, Ludovika University of Public Service Doctoral School of Military Science and Officer Training, e-mail: meszaros.istvan.mail@gmail.com

importance for the ordinary person, as well as for the economic, commercial, financial, government, and public administration sectors.

Terrorist attacks in the European Union and the United States in the 2000s prompted lawmakers to take action to protect critical system components. When the Green Paper was presented in 2007, it defined the following 11 critical infrastructure areas: energy, information and communication technologies; water supply; food safety; healthcare; financial system; public safety and justice system; public administration system; transport (road, rail and air transport, inland, ocean and sea shipping); chemical and nuclear industry; space and research.[2] Following the submission in 2008, the 2008/114/EC (8 December, 2008) European Council Directive formulated the concept of critical infrastructure and the criteria for classification as critical infrastructure.[3]

The Directive states that "primary and ultimate responsibility for the protection of critical infrastructure rests with the Member States and the owners/operators of the infrastructures".[4]

In addition, the Directive defines the fundamentally critical sectors and horizontal criteria (however, it refers the determination of their threshold values and the sector criteria to the competence of the Member States), as well as the basic rules of identification and designation, the obligation to prepare an Operator Security Plan and employ a Security Liaison Officer for the designated critical infrastructures.

Regulation of the protection of critical infrastructures in Hungary and Germany

The first legislation on critical infrastructures entered into force in Hungary in 2012. This is the Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities (Act of CIP).

The Act defines the concept of a critical infrastructure element, and defines the sectors designated from the point of view of critical infrastructure protection and authorises the Government to designate the sectoral designating authority, the proposing authority, establish the general and sectoral rules for identification and designation, as well as the sectoral and the horizontal criteria.

The Government Decree 65/2013 (8.III.) on the implementation of the Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities defines the rules of designation/withdrawal, the tasks of the security liaison officer and general expectations for its employing, as well as the obligation to prepare the Operator Security Plan.

The Government Decree 246/2015 (8.IX.) on the identification, designation and protection of critical health systems and facilities entered into force in 2016 for the healthcare sector. The decree defines the sub-sectors and designation criteria, the

[2] COM (2005) 576 final.
[3] European Council Directive 2008/114/EC.
[4] European Council Directive 2008/114/EC.

sector-specific rules of the identification procedure and designation, as well as the sector requirements imposed on the security liaison officer.[5]

Sectors and sub-sectors defined for the identification and designation of critical infrastructures from the Act CLXVI of 2012 on the identification, designation and protection of essetial systems and facilities:

- active inpatient care and the services necessary for its operation
- rescue management
- health reserves and blood stocks
- high security biological laboratories
- drug wholesale

In addition to all of this, Act L of 2013 on the electronic information security of state and local government bodies was also extended to cover critical infrastructures. In this law, the legislator regulates the IT security obligations of vital system elements.

In contrast, in Germany, the regulation related to critical infrastructures originates from an information security regulation, the Federal Information Security Office Act (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSIG), which was issued in 2009.

In this law, the legislator authorises the individual ministries to define in a decree the services that are important and are considered critical due to their importance in the given sectors, which facilities, systems or their parts are classified as critical infrastructures under this law, as well as the sectoral thresholds.

In accordance with the above, the Decree on the definition of critical infrastructures according to the BSI Act (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, BSI-KritisV) has been in force since 2016.

The Decree – which has undergone several additions since its publication (e.g. the addition of new sectors) – defines the critical sectors, their sub-sectors and the selection criteria system.

Based on the Decree, sub-sectors within the healthcare sector:

- inpatient care
- delivery of immediate life-sustaining medical devices that are consumables
- supply of prescription drugs and blood and plasma concentrates
- laboratory diagnostics

Operator safety of critical inpatient care infrastructures

Criteria system for designation

Government Decree 246/2015 (8.IX.) on the identification, designation and protection of vital health systems and facilities in Hungary defines the following threshold values:

[5] Mészáros 2023: 43–57.

- has at least 400 active beds
- or the number of persons belonging to its territorial supply obligation reaches or exceeds 1.5 million people

and

- in the event of a breakdown, the nearest hospital cannot be reached by public road within 45 minutes
- or there is a health policy interest in the continued operation of the hospital

The operator prepares an identification report in every four years, which it submits to the Sectoral Decision Committee, where the fulfillment of the horizontal and vertical criteria is examined with the involvement of the specialised authorities. In case of fulfillment, the Sectoral Decision Committee designates the critical infrastructure in a decision.

In Germany, based on the decree on the definition of critical infrastructures according to the BSI Act, that inpatient care facility can be designated as critical infrastructure, where the number of inpatient care cases reaches or exceeds 30,000 cases per year.

Hospitals have to check each year until March 31, whether they meet or exceed this threshold. If fulfilled, the operator sends the appropriate report to the Federal Office for Information Security (BSI) and the hospital is classified as critical infrastructure from the following day (1 April).

Table 1: Selection criteria and review

<table>
<tr><th></th><th colspan="4">Hungary</th><th>Germany</th></tr>
<tr><td rowspan="3">Criteria</td><td>min. 400 beds</td><td>OR</td><td colspan="2">min. supply district of 1.5 million people</td><td rowspan="3">30,000 inpatient care events/year</td></tr>
<tr><td colspan="4">AND</td></tr>
<tr><td>There is no other hospital within 45 minutes</td><td>OR</td><td colspan="2">health policy interest</td></tr>
<tr><td>Review</td><td colspan="4">every 4 years</td><td>annually</td></tr>
</table>

Source: compiled by the author

It can be seen from the above that in Germany a simpler approach was used when determining the threshold, but with an annual review.

The peculiarity of the Hungarian inpatient care system is that within some hospitals, some medical professions have so-called levels of progressivity, which is "a peculiarity of the care system arising from the frequency distribution of diseases, according to which the more frequent – and mostly simpler – cases are organised at a lower level by the care system (according to the patient's place of residence provided in nearby) units. The rarer and mostly more complicated cases, on the other hand, are directed to centralised (territorial, county, regional, national) institutions.

In Hungary, the lowest level is the primary care, and the highest level is the national institutes and university clinics."[6]

In practice, however, it happens that in some hospitals, different professions are at different progressivity levels, as a result of which they have territorial care obligations of different sizes even within certain professional groups. The following tables illustrate the identification of a university clinic (Table 2 and Table 3).

Table 2: Designation criteria and review

Name of department	Profession code	Name of profession	Number of beds	Progressivity level
Obstetrics department	405	Obstetrics	82	2–3
Perinatal Intesive Care Unit	502	PIC	23	1–3
Department of General Gynecology	406	Gynecology	20	1–3
Obstetrics and Gynecology Unit – private	400	Obstetrics Gynecology	15	1–3
Total			140	

Source: compiled by the author

Table 3: Meeting the selection criteria of the same clinic

Criteria	Value	Threshold value	Fulfillment	
A1 (number of beds)	140	400	nov	
A2 (number of persons belonging to its territorial supply)	Progress 1	490 146	1 500 000	no
	Progress 2	1 132 761	1 500 000	no
	Progress 3	3 434 325	1 500 000	YES
B1 (nearest hospital)	Progress 1		It's in 45 minutes	no
	Progress 2		It's in 45 minutes	no
	Progress 3		Not in 45 minutes	YES
B2 (health policy interest)	yes: medical university, research	yes/no	YES	

Source: compiled by the author

The legislator did not specify which level of progressivity should be taken into account, and based on my practical experience, the Sectoral Decision Committee that makes the designation does not take into account the levels of progressivity, but examines the given institution as a whole.

Overall, it can be said that the German designation practice is simpler and somewhat more tangible, and uses a criteria system that adapts more linearly to the horizontal criteria. It is not known to me what kind of changes in the number of care events occur each year for some hospitals compared to the defined threshold.

[6] See: https://fogalomtar.aeek.hu/index.php/Progresszivitási_szintek

However, even if there are changes, the German practice is suitable for hospitals that lose their critical classification overnight to maintain the established operator security practice.

Operator Security Planning

Both Member States have in common that the detailed requirements of the Operator Safety Plan (OSP) are contained in official recommendations, however, a significant difference is that, in accordance with European Union regulations, in Hungary, the legislation defines the obligation to prepare the OSP, and even the sectoral Regulation specifically defines mandatory content elements and that the Health Crisis Plan (HCP) is also part of the institution's Operator Security Plan (OSP). On the other hand, the legal regulations in Germany do not require any obligation to prepare an OSP, and even the official recommendations do not specifically mention OSP, but detail the planning of crisis management measures based on the risk assessment.

In Germany, the law only states that "operators of critical infrastructures are obliged to take the appropriate organisational and technical precautions to avoid disruptions in availability at the latest on the first working day after they are classified as critical infrastructure for the first time or again".[7]

The regulation in Germany can be said to be fundamentally information security-centric. According to the website of the Federal Office for Information Security (BSI) – on the basis of Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical organisations and the repeal of Council Directive 2008/114/EC (CER Directive) – a new legislation, which is expected to enter into force in 2024, will address general operator security issues: "This draft law identifies critical infrastructures at the federal level for the first time and sets minimum standards for physical protection for operators of critical infrastructures. Previously, such federal regulations only existed for the IT security of critical infrastructures. The regulations of the KRITIS-Umbrella law, which concern physical protection, are intended to supplement the existing IT security measures. The aim is to strengthen the resilience of critical infrastructures, the resilience against threats, in Germany as a whole."[8]

In addition to all this, the Federal Office for Civil- and Disaster Prevention (BBK) and the German Hospital Association (DKG) publish recommendations such as:

- Protection of critical infrastructures – Risk and crisis management Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement)
- The hospital as a critical infrastructure – Executive order of the German Hospital Association (Krankenhäuser als kritische Infrastrukturen – Umsetzungshinweise der Deutschen Krankenhausgesellschaft)

These recommendations primarily provide a framework for risk assessment and management, as well as crisis management, without specific calculation requirements,

[7] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSIG.
[8] See: www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html

mainly referring to national and international standards, but using a process-based approach.

In Hungary, in addition to the fact that the law requires the preparation of the OSP with sector-specific obligations, National Directorate General for Disaster Management under the Ministry of the Interior publishes specific recommendations regarding the content and form requirements of the plans, such as:

- risk analysis
- instructions for completing the risk analysis
- OSP assistance

During the risk analysis, meteorological, geological, human, technical, communication, fire, IT risks, as well as risks related to hazardous materials and technologies, are prescribed to analise. The risk analysis can be expanded freely, but it is not process-based. The table is equipped with formulas, and when determining the risk value, it calculates not only the probability of occurrence and the extent of its possible impact, but also the exposure of the institution. During the analysis, the possible risk reduction measures must be indicated and the given risk element must be re-evaluated accordingly.

The OSP assistance defines in detail the content and form requirements of the plan, from the detailed presentation of the infrastructure, through the risk analysis, to the risk management measures.

In summary, it can be said that while German regulation gives operators more freedom for operator security measures, it mostly uses an information security-centric approach. On the other hand, the Hungarian regulations apply a complex approach to the operator's security activities and provide operators with precise, detailed instructions for the performance of these activities.

Crisis planning of inpatient care institutions

In Hungary, the Act CLIV of 1997 on healthcare defines the concept of a health crisis situation, the cooperation and planning obligation for healthcare providers.

Government Decree 521/2013 (30.XII.) on health crisis care details the rules of crisis healthcare, such as the criteria for classifying it as a health crisis situation, detailed rules for the assignment and transfer of healthcare workers, the method of providing the necessary equipment for care, and the tasks of preparation and training. In connection with the latter, the legislator determined that "the minister responsible for health, with the cooperation of the National Chief Medical Officer, can directly order healthcare providers to conduct health crisis exercises or to participate in international exercises", so individual hospitals do not have an obligation to conduct exercises in this sense. The Decree also specifies that the County Government Office must also prepare a Health Crisis Situation Plan for the performance of health crisis tasks, to which the institutional plans of the healthcare providers belonging to the county form an annex.

The Decree 43/2014 (19.VIII.) of the Ministry of Human Resources on the content requirements of the health crisis plans of health institutions and on the amendment of

certain ministerial decrees on health matters determines the rules for the preparation of Health Crisis Plans (HCP). Pursuant to the decree, the healthcare provider must review the plans every year and submit them to the County Government Office for approval. The Decree also defines the exact content and form requirements of the HCP and its sub-plans.

The HCP is actually a plan system consisting of a basic plan and fourteen sub-plans.

"To facilitate structuring, understanding and – obviously – application, plans can be grouped into four categories. These categories are:

- basic information and access to readiness
- reaction to an extraordinary event affecting the given organisation
- responding to an extraordinary event that took place elsewhere, extending the service
- operation of service processes

The implementation and application of the plans can happen separately or simultaneously in different permutations depending on the nature of the event taking place."[9]

It can also be concluded that domestic regulations affecting critical systems are closely related to fire prevention[10] and industrial safety regulations.[11]

In Germany, according to the provisions of the Basic Law, responsibility for the implementation of security measures rests with the individual states. Hospitals are obliged to prepare, update and implement alarm and operation plans for crisis situations. This is governed by the hospital laws or disaster management laws of that federal state.[12]

When creating the individual Hospital Alarm and Response Plan (Krankenhausalarm- und -einsatzplannung) (KAEP) of each hospital, the applicable legal requirements of the federal states must be taken into account. All federal states now have corresponding requirements.[13]

Based on the above, it is regulated at the federal state level in Germany what kind of plans each hospital must prepare and whether they have an obligation to practice these. However, the federal state legislation – as in the case of operator security planning – does not define specific content and form requirements, but generally clarifies the obligation to prepare plans and the responsibility for managing crisis situations.

Recommendations are available regarding the content and form requirements of the plans. An example is the *Handbook of Hospital Alarm and Response Planning (Handbuch Krankenhausalarm- und -einsatzplanung),* which was published by the Federal Office for Civil and Disaster Prevention (BBK) in cooperation with the German Hospital Deployment Planning Working Group (DAKEP) and the German Traumatology Society (DGU).

Based on the manual, a KAEP must cover the following scenarios:

- operational management of the hospital during an extraordinary event

[9] Kátai-Urbán et al. 2019: 48–83.
[10] Érces et al. 2023: 104–128.
[11] Cimer et al. 2021.
[12] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2020.
[13] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2020.

- alarm, deployment, logistics
- crisis communication
- evacuation
- eviction
- mass casualty care
- prevention of chemical, biological and nuclear threats (including pandemics)
- appearance of aggressive persons, bomb threats, appearance of people running amok
- disturbances of the technical infrastructure

The manual also presents case studies of events that occurred in the case of the given scenarios for educational purposes.

By comparing the planning regulations and practices of the two Member States, it can be said that in both cases the planning includes a scenario-based approach, and that each extraordinary event is basically managed based on the establishment of a management structure different from the peacetime one. In Germany's plans, the management of IT incidents has a prominent role, which in Hungary does not appear according to regulations during HCP planning. Hungarian legal regulations define thorough and detailed requirements for healthcare providers, while in Germany, institutions have more freedom in this matter as well, and however, compliance with their responsibilities and obligations is checked in several federal states through mandatory practices.

Summary

Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical organisations and the repeal of Council Directive 2008/114/EC (CER Directive) needs to be transposed into the national legal systems of the Member States in 2024. The Directive takes a new type of approach to protecting vital service providers and thus critical infrastructures by focusing on building and maintaining resilience. With the above study, I would like to highlight that in the regulatory and planning practice of some Member States, there are many professional procedures based on a similar approach beyond the requirements of the Directive, and there are differences that can serve as good examples at the community level in the health sector.

In relation to the sectoral criteria used during the identification and designation of critical infrastructures, it can be said that Hungarian practice uses a more complicated approach, but is based on values that can be said to be permanent, which allow the review to take place only every four years, which provides predictability for the operator during preparation and application. However, in the German regulations, a threshold value based on practice has been defined, subject to an annual review. This practice opens up the possibility for hospitals that lose their certification in the meantime to maintain the already proven operator security practice, thereby contributing to the business continuity of the entire care system.

All in all, it can be said that the regulations in Germany apply a more IT security-oriented approach and give a lot of freedom to hospital operators both in terms of operator security and crisis planning, the implementation of which is monitored through official inspections and the implementation of exercises. On the other hand, the Hungarian regulation uses a fundamentally complex approach, placing great emphasis on physical security, and the legislator regulates in detail the duties of hospital operators, the content and form requirements of the plans, but there are no regulations regarding the maintenance of health care processes in the event of IT security incidents.

In the case of both Member States, the scenario-based approach appears in crisis planning, however, in several cases, they approach certain scenarios from a different direction. While in Hungary the plans describing the individual service processes and related additional scenarios can be applied separately to each scenario, in Germany one scenario accompanies the entire process. In the risk analysis methodology, the process-based approach prevails, as opposed to the Hungarian analysis based on the listing of risks and the examination of their general effects, but in Hungary the measurement of exposures and the evaluation of risk reduction measures appear.

Based on the above comparisons – after further professional discussions and research – in my opinion, a sectoral operator safety and crisis planning framework can be established in the health sector based on uniform guidelines at the community level, which can help beyond local emergencies, in a pandemic similar to the coronavirus pandemic, or in the effective management of the consequences of a potentially raging and escalating conflict in our neighbourhood, and in cooperation between Member States.

References

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) (2020): *Handbuch Krankenhausalarm- und -einsatzplanung* (KAEP). Online: www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/Gesundheit/KAEP/handbuch-kaep.pdf?__blob=publicationFile&v=15

Bundesministerium des Innern (2011): *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement.* Online: www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/bmi-schutz-kritis-risiko-und-krisenmanagement.pdf?__blob=publicationFile&v=12

Bundesministerium des Innern und für Heimat (2023): *Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen.* 28 June, 2023. Online: www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html

Cimer, Zsolt et al. (2021): Application of Chemical Monitoring and Public Alarm Systems to Reduce Public Vulnerability to Major Accidents Involving Dangerous Substances. *Symmetry,* 13(8), 1528. Online: https://doi.org/10.3390/sym13081528

Deutschen Krankenhausgesellschaft (2017): *Krankenhäuser als kritische Infrastrukturen –Umsetzungshinweise der Deutschen Krankenhausgesellschaft.* Online: www.dkgev.

de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/2017_12_19_483_ITSiG_Kritis_Umsetzungshinweise_BSIG_v0.9.pdf

ÉRCES, Gergő et al. (2023): Fire Safety in Smart Cities in Hungary With Regard to Urban Planning. *IDRiM Journal,* 13(2), 104–128. Online: https://doi.org/10.5595/001c.91474

KÁTAI-URBÁN, Lajos – MÉSZÁROS, István – VASS, Gyula (2019): Iparbiztonság, válsághelyzeti tervezés. In MAJOR, László (ed.): *A katasztrófa-készenlét, a reagálás és a beavatkozásbiztonság egészségügyi alapjai.* Budapest: Semmelweis, 48–83.

MÉSZÁROS, István (2023). The Evolution of the Normative Regulation in Hospital Safety and Security. *Hadmérnök,* 18(1), 43–57. Online: https://doi.org/10.32567/hm.2023.1.4

Legal sources

Act CLIV of 1997 on healthcare

Act CLXVI of 2012 on the identification, designation and protection of essetial systems and facilities

Act L of 2013 on the electronic information security of state and local government bodies

Act on the Federal Office for Information Security – BSIG

Commission of the European Communities (2005): *Green Paper on the European Program for the Protection of European Critical Infrastructures.* COM (2005) 576 final

Decree for determining critical infrastructures according to the BSI-Act – BSI-KritisV

European Council Directive 2008/114/EC (December 8, 2008) on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

European Parliament and Council Directive 2022/2557 on the resilience of critical organisations and the repeal of Council Directive 2008/114/EC (CER Directive)

Government Decree 65/2013 (8.III.) on the implementation of the Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities

Government Decree 521/2013 (30.XII.) on health crisis care

Government Decree 246/2015 (8.IX.) on the identification, designation and protection of essential healthcare systems and facilities

Decree 43/2014. (19.VIII.) of the Ministry of Human Resources on the content requirements of the health crisis plans of health institutions and on the amendment of certain ministerial decrees on health matters

HADMÉRNÖK
VÉDELEMINFORMATIKA

18. évfolyam (2023) 4. szám 109–128.
DOI: 10.32567/hm.2023.4.8

Mátyás Ináncsi,[1] Péter Bányász,[2] Máté Dub,[3]
Péter Kugler[4]

Empirical Studies of Russian–Ukrainian War Related Fake News, Part 1[5]

Abstract

The Russian–Ukrainian war, which broke out on February 24, 2022, resulted in several paradigm shifts in cyber warfare. One aspect of these changes is psychological operations. Russia and Ukraine have conducted extensive psychological operation campaigns to fulfil their war objectives, which have since been intense along modified intentions. This series of studies examines the impact of war-related fake news through various empirical research. In the first part of the paper, the authors examine the emergence of psychological operations and related terms in the international academic literature using network analysis methodology. In the second part of the paper, the authors use sentiment and network analysis to investigate the spread of different fake news. In the third study, the authors measure the attitudes toward the perception of the Hungarian Defence Forces from the perspective of the war in the neighbouring country.

Keywords: Russian–Ukrainian war, PSYOPS, cyber warfare, network analysis, sentiment analysis

[1] Ludovika University of Public Service Faculty of Military Science and Officer Training, e-mail: inancsi.matyas@uni-nke.hu
TKP2021-NKTA-51 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NKTA funding scheme.
[2] Ludovika University of Public Service Faculty of Public Governance and International Studies Department of Cybersecurity e-mail: banyasz.peter@uni-nke.hu
[3] Ludovika University of Public Service Faculty of Military Science and Officer Training, e-mail: dub.mate@uni-nke.hu
[4] E-mail: kugler.peti@protonmail.com
[5] ÚNKP (Supported by the ÚNKP-22-4-II-NKE-11, ÚNKP-22-2-I-NKE-79 and ÚNKP-22-1-I-NKE-14 New National Excellence Programs of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund).

Introduction

The Russian–Ukrainian conflict has been dragging on since 2014, and is an unresolved situation affecting our daily lives. Following the Euromaidan protests which began in 2013, and the revolution that led to the ousting of pro-Russian President Viktor Yanukovych in February 2014, pro-Russian unrest broke out in parts of Ukraine.[6]

The two parties finally concluded the Minsk agreements in 2015, however, several disagreements have blocked their full implementation due to both Russia and Ukraine repeatedly violating the treaty, accusing the other. The frozen conflict finally broke out in February 2022, by a military operation launched by Russia on February 24, 2022. This action has surprised the broad public and most experts, even though Ukraine, the NATO, and Russia had conducted large-scale information operations before the war began.[7] The United States, its allies, and Ukraine as a state with increasingly close ties to the United States have regularly accused Russia of preparing a military attack on Ukraine. Meanwhile, Russia has accused – and continues to accuse – Ukraine, using a constantly changing narrative, which is often more and more absurd, to portray itself as a victim of this incident to justify its military aggression.[8] Recurring accusations include that the Nazi Ukrainians (see Figure 1) carried out systematic genocide against the Russian minority, Ukraine is harbouring nuclear weapons to destroy Russia, or that a new type of coronavirus was developed in Ukrainian biological laboratories with U.S. support to build a new world order.

Figure 1: Russian articles about Ukraine that mention Nazism
Source: SMART 2022

[6] The present study does not aim at a detailed description of the war since 2014, but we recommend the studies by József Padányi and János Tomolya, in which they described the events in a complex approach. Padányi–Tomolya 2017a: 63–83. Padányi–Tomolya 2017b: 29–42.

[7] Alekszejeva et al. 2023.

[8] Examples include the history of the Ukrainian bio-labs before the outbreak of the war, and shortly afterwards, or when President Putin and Valery Zorkin together looked at a 400-year-old map on which they claimed there was no Ukraine.

The psychological operations that form part of information operations were significantly intensified on all sides after the start of the war.

The first part of this series of studies aims to define the concepts at the heart of our research, their relative positions, roles, and elements based on military terminology, strategic documents, and the national and international literature.

Methods

In the first half of our study, we reviewed the relevant international and national literature for the following stages of our research. We then searched the Scopus database, looking specifically at how the keywords disinformation, misinformation, or malinformation appear in the relevant international literature.

The results are summarised by year in a chart in the results section. Only a subset of the older scientific papers is recorded in Scopus, so older datasets may, in reality, have more publications than were digitised.

The Scopus system allows the export of up to 20,000 hits at a time, which proved sufficient for the present research. The data were saved in CSV format, and were analysed using VOSviewer version 1.6.19.[9]

Before describing the results of our empirical research, we should consider the relevant concepts.

Hybrid warfare

Although hybrid warfare cannot be considered a directly examined element or part of the narrowed, specific research question, we believe it important to define it in the context of the conceptual outlook. The primary reason for this issue, is that hybrid warfare can be part of information and psychological operations.

In the international literature, there is no consensus on the definition of hybrid warfare, nor on whether it is exclusively attributed to General Valery Vasilievich Gerasimov. Whether he unified the components that already existed and were used, or whether the term "hybrid" as implemented by the West or Gerasimov's original, i.e. the "indirect and asymmetric methods" version, is used in connection with the designation.[10] In this context, the diversity of terminology is illustrated by the fact that the present concept can be referred to as non-linear, next-generation, or fourth-generation warfare or, in some elements, as "grey-zone" activity.[11] However, there is a similarity in terms of the content, i.e., hybrid warfare consists of two main components, military and non-military methods, which contribute to achieving

[9] Comma-separated values is an English abbreviation for a particular separator, usually using a comma or semicolon to separate different values and a row representing a record. For the computer, it is easy to process as a spreadsheet and, because of the lack of formatting, is ergonomic. Its simplicity makes it widely compatible across different operating systems and platforms.

[10] Raychev 2019: 127–151.

[11] Bērziņš 2020: 355–380.

a given objective. In terms of actors, both state and various non-state actors can be identified. General Gerasimov attempts to illustrate with the new rule that non-military means have become more important in achieving political and strategic goals, and often prove more effective than weapons.[12] Regarding non-military means, we can define, among others, political, legal, diplomatic, financial, economic elements, sabotage, social pressure, influence operations, propaganda, and, in the latter case, additional means resulting from cyber capabilities.[13]

Concerning operations in cyberspace, it is important to underline that they can apply to both military (e.g. electronic warfare) and non-military (e.g. psychological operations) components.

NATO defined hybrid threats in its 2014 Wales Summit, specifically in its Closing Declaration, as a set of broad, covert, and overt, military and paramilitary, as well as non-military, procedures and means in the context of a predefined, integrated operational plan.[14]

In 2015, the NATO Parliamentary Assembly's Defence and Security Committee defined hybrid warfare as the use of asymmetric procedures from the attacker's side, whereby non-military means are used to identify and exploit weaknesses and the procedures are tailored to the situation at hand, and then combined with conventional and non-traditional military threats/concrete attacks.[15] In contrast, the EU defines hybrid threats in more detail, as a set of activities that are used by state or non-state actors in a coordinated manner to achieve certain objectives, while not going beyond the officially declared level of warfare. The emphasis is generally on exploiting the vulnerabilities of the target state and creating situations that impede decision-making. Hybrid threat tools also include strong misinformation or disinformation campaigns, whereby attackers use social media platforms to influence the political narrative and to radicalise, recruit and control proxy actors.[16] The social media platforms that are the focus of our research, are defined in the EU terminology and because of their role in information warfare, more specifically in psychological operations, we consider this definition the guiding one.

In summary, hybrid warfare is a coherent and complex system of violent means and threats whereby the attacking party uses a wide range of available assets (military, irregular or non-military) to achieve its objective. In the face of these attacks, it is essential to develop an appropriate defensive methodology, an important element that is to identify the interests, intentions, political objectives and resources of the opposing actor or actors. Knowing the opposing actor's strategy can help refine and improve the effectiveness of defensive solutions and, where appropriate, build consensus or prepare for a possible conflict.[17]

[12] Gerasimov 2013.
[13] Simicskó 2017: 3–16.
[14] NATO 2014.
[15] Kiss 2019: 17–37.
[16] European Commission 2016; Kiss 2019: 17–37.
[17] Van Puyvelde 2015; Kiss–Somodi 2019: 22–28.

The information environment, battlefield and operations

In this section, we discuss the information environment, and more importantly the three dimensions of it. Extending on this, we examine the concept – depending on preferred wording – of information battlefield, information warfare and information operations. We approach this concept from the NATO's definitive perspective.

The information environment

The development of the information environment has accompanied the spread of different ICT tools.[18] The information environment also contributes to the possibility of expanding military operations. The United States of America's Combined Forces Information Operations Doctrine of 2012 (revised in 2014) defines the information environment along the following lines. It is defined as individuals, organisations, and systems which collect, process, and distribute information. According to the document, this environment has three interrelated dimensions that constantly interact with individuals, organisations, and systems. These are the physical, information and cognitive dimensions. The physical dimension includes the leadership and governance systems, key decision-makers and supporting infrastructure that enables individuals and organisations to function effectively. The information dimension defines where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension includes the people who transmit, receive and act on information, and those who act on it.[19]

Going back to Gerasimov's approach, the forces and methods used are more important to coordinate in the information space than in the physical dimension.[20] Regarding the Hungarian definition of terms, the Hungarian *Encyclopaedia of Military Sciences*[21] does not differentiate from the US JP 3-13 regarding essential elements.[22]

Information battlefield, warfare/operations

In the context of the information battlefield, the Hungarian *Encyclopaedia of Military Sciences* defines it as a multidimensional operational space where information activities for military purposes occur. In accordance with the Hungarian interpretation, the information battlefield and the information environment are correlated since they are all physical and online spaces, places, systems, devices, and human resources where information is acquired or produced, used, protected, and stored. This interpretation

[18] Farkas 2023: 11–30.
[19] Joint Chief of Staff 2014.
[20] Rácz 2014.
[21] Under the Hungarian encyclopaedia of military sciences terminology, we refer to Zoltán Krajnc's *Hadtudományi lexikon*. In order to not to break the flow of the English text, we have translated the name of the document, however, the document has no official English name, and we have used a straightforward direct translation. By this reason, English translations of this document in different publications might differ.
[22] Krajnc 2019.

is also complemented by the technological and cognitive information processes and the struggle to acquire and use information as efficiently as possible.[23]

In the Hungarian terminological interpretation, information operations and warfare appear as separate terms in the Hungarian *Encyclopaedia of Military Sciences.* In this interpretation, information warfare can be divided into two main parts. According to one interpretation, information warfare is a new form of warfare in the classical sense, aiming to attack information systems and use information tools to achieve military objectives as an integral part of warfare. The second interpretation, which is also closer to the scope of our research, is that information warfare can be understood in the context of the information environment described above, and refers to the technical and cognitive information activities of an offensive or defensive nature that take place in this environment.[24] It is important to specify, that information warfare is more a Russian or Chinese definition, while the term information operations is more a NATO term.

In the context of NATO's interpretation of information operations (INFOOPS), the following concepts have been defined:[25]

- Information operations are a set of military activities that provide advice and coordination of military information activities to have the predefined, desired impact on and knowledge of the target group(s), adversaries, and their capabilities and to support the activities of the Alliance
- Information operations are activities aimed at influencing information and information systems. Any actor may conduct them and may include protective measures

The document also discusses in detail the relationship between information and the global security environment, strategic management, non-lethal activities, the relevance of information, the role of the media, and the importance of technology and the internet in information operations. The document identifies as relevant to decision-making, the triad of will to act following strategies, the right assessment of the situation, and the capacity to act appropriately, with the desired impact not being achieved even if one of these criteria is missing.[26]

In this context, the main objective is defined as influencing the capabilities and will of the opponent. It is also an important declaration that information operations can be used in the full range of military operations in support of and for their execution.[27]

NATO defines the following categories as areas of application for information activities:

- information activities that focus on changing, influencing, or reinforcing a particular position/situation
- information activities that focus on preserving and protecting the Alliance's room for manoeuvring in the information environment by protecting data and

[23] Krajnc 2019.
[24] Krajnc 2019.
[25] NATO 2009.
[26] Haig 2011: 12–28.
[27] Czeglédi 2017: 74–87.

information that support the Alliance's decision-makers and decision-making processes
- information activities that focus on countering command and control functions and capabilities by influencing data and information supporting adversaries through command and control, intelligence, surveillance, target detection, and weapons systems information[28]

The document's list of capabilities, tools, and techniques used in (and in support of) information operations is considered to be of particular relevance to our research and includes the following categories:
- psychological operations (PSYOPS)
- presence, posture, and profile (PPP)
- operations security (OPSEC)
- information security (INFOSEC)
- deception (MILDEC)
- electronic warfare (E.W.)
- physical destruction
- key leader engagement (KLE)
- computer-network operations (CNO)
- civil-military cooperation (CIMIC)[29]

The Hungarian military terminology of information operations adopts the NATO interpretation and a separate interpretation of information operations. In addition, it emphasises that three main objectives must be applied to support the commander and the mission at the appropriate level, which are:
- to weaken the enemy target group(s)
- strengthening the commitment of the friendly target group(s)
- gaining the support of uncertain or uncommitted target(s)[30]

In addition, it should be noted that the U.S. Joint Forces Information Operations Doctrine (J.P. 3-13) further defines various cyberspace operations (cyber operations)/ cyberspace capabilities as activities supporting information operations. These include but are not limited to influencing decision-making processes, influencing communications or the cognitive dimension of the target, compromising individuals or encrypted messages, and overall reducing the capabilities of the defending party.[31]

[28] NATO 2009.
[29] Pozderka 2016: 131–141.
[30] Krajnc 2019.
[31] Joint Chief of Staff 2014.

The psychological operations

Psychological operations aim to influence the selected target group in the cognitive dimension.[32]

The following main aspects can be identified concerning the diversification of the objectives of psychological operations:

- influence the thinking, feelings, and behaviour of the opposing side
- strengthen the support of friendly and loyal populations in order to achieve political and military objectives
- gain the support and cooperation of uncommitted or undecided target group(s)
- reduce the impact of the adversary's psychological operations on its resources and on groups to be protected

Above all this, the success of these operations depend on the attacker's ability to precisely define the target group and the content of the message, which is being delivered, and the delivery method must not be compromised.[33]

The conceptual interpretation of psychological operations is defined in the Information Operations Doctrine of the Hungarian Defence Forces along the following lines: PSYOPS is a method of influencing a selected target group's behaviour, attitudes, and opinions to achieve predefined PSYOPS objectives agreed upon by the supervisor. To achieve this, PSYOPS activities are designed to trigger or reinforce the desired behaviour of the target group, which will help to achieve the defined long-term objectives. The target of psychological operations may not only be the population of the enemy country but may also be directed at influencing the population of allied or neutral states, and may even be the population of the country or a group of them.[34]

Regarding NATO, it should be added that PSYOPS plans and activities should be consistent with the strategic guidelines for the activities and objectives set out in the Operation Plan. PSYOPS should also maintain direct control over the specific "content" along with its dissemination and, concerning this, the target group. In addition, effective psychological operations are resource-intensive. These resources include adequate intelligence information, language support, dissemination (graphics, print, broadcast, radio, telephone, television, physical press, voice, etc.) mechanisms, appropriate technological tools, and human factors.[35]

When targeting messages or content, the attacker should select credible topics, which should be developed with a particular focus on the vulnerabilities of the target group. The main objective is to ensure that the message/content is credible, receptive to the target group, and influential. Therefore, the topic to be targeted should be real, credible, and verifiable based on appropriate background information. It should also support the objectives of the own action and the psychological operations and set a course of action for the target group that is reasonable and realistic.[36]

[32] Bányász et al. 2019: 111–133.
[33] Haig 2018.
[34] Bányász et al. 2019: 111–133.
[35] NATO 2009.
[36] Haig–Várhegyi 2005.

Concerning the planning of psychological operations, we can identify three methods according to its classical interpretation:

1. Reflexive control: a strategy intended to influence the decision-making mechanism of the commander of an enemy force. The first step in the method is extensive reconnaissance, followed by penetration of the decision-maker's information systems. Here, disinformation is planted in such a way as to support the attackers in making desired decisions.
2. The concept of a social virus: a society can be infected from within if people in a certain position spread fake news. They can be undercover attackers or so-called opinion leaders who can be recruited to influence opinions even under a "foreign flag". They are usually spread among people who are ideologically manipulable, politically aggrieved, and not objectively informed about current events. Opinion leaders and influencers can be easily identified through networks, allowing the preparation of psychological operations and their detection from a defensive point of view.
3. In order to influence the perception of reality and reduce the psychological stability of a person or a group, not only traditional methods such as leaflets or media platforms can be used, but also special methods and tools. Artificial intelligence research is one of the most important branches of such tools. For example, "deepfake" technology uses machine deep learning to deliver audiovisual content in which another person's face or voice is superimposed on real-time content. Fake news on social media can be easily identified by recognising certain patterns, but such technology makes it difficult for even the most experienced person to spot fake news, and technological advances will further reinforce this trend.[37]

Concerning psychological operations, it is also important to explain further concepts. One of the main concept of psychological operations is the use of propaganda. However, it is important to keep in mind that propaganda is a tool that can be used under different psychological operations. The same rule also applies to fake news, disinformation, misinformation and malinformation.

Propaganda

In popular discourse, psychological operations are often confused with propaganda, but propaganda is, in fact, only a part of psychological operations and, contrary to popular terminology, not a condition for promoting a specific political ideology.[38] For grouping, three categories can be defined:

- White propaganda: It has a known intermediary and usually contains truthful information from a credible source. Its tools often include jokes and caricatures to ridicule and discredit the opponent

[37] Bányász et al. 2019: 111–133.
[38] Miller 2015: 163–188.

- Black propaganda is a form of communication that is not truthful, and is usually disguised in order to deceive the target audience. The cover-up can make it appear as if the source of the propaganda is the government rather than the opponent
- Grey propaganda: The source of the news in this category is unknown, and the primary objective is to demoralise the enemy by spreading fake news that is essentially about the enemy. Such propaganda news is used to reduce morale. Fake news often originates from the "hinterland" and can cover topics such as the destruction of soldiers' families or the infidelity of their wives and sweethearts

Propaganda and its content can be defined as reinforcing an over-emphasised point of view by disseminating true or false information to pursue a specific interest. The aim is, therefore, to persuade the target group with the full presence of bias. Propaganda can be used for political, economic, or military purposes, to demoralise the citizens of other countries, to target so-called "soft targets", to reach large masses of people, or to achieve a desired attitude. Historical examples show that the controlled, conscious dissemination of information is a key tool in propaganda campaigns. Among its elements, we can also identify the encouragement to accept a simple statement without criticism, broad formulations, familiar language, slogans, call words, symbols, illustrations, appeals to desire, and various elements of prestige.[39]

In terms of classification of propaganda, we can distinguish, among others, the following categories:

- using mental influence
- bandwagon technique
- plain folk technique
- fear-mongering
- testimonial/reporting
- false dilemma poser
- slogan-based
- statement-type
- operating with fragments of text[40]

Fake news, disinformation, misinformation and malinformation

The term "fake news" is often referred to in everyday language, but from a scientific perspective, it is important to fragment this concept and define exactly what can be included in this interpretation category. In principle, untrue or false news, fake news should be considered a generic term encompassing several approaches and criteria, requiring new definitions to be added, which may not be directly considered fake

[39] Dobák 2022: 93–124.
[40] Betts 2021.

news. From the point of view of the criteria and in order to define them accurately, two main questions need to be answered:

- Are we concerned with true or false information?
- Is the person disseminating the information aware of the consequences of disseminating the information?

By answering the questions, three categories can be identified:

- If the purpose is the deliberate, misleading, malicious dissemination of false/untrue information, then disinformation can be defined. This category can be divided into the group of fake news.
- If false/untrue information is disseminated so that the disseminator is unaware that the information he/she is disseminating is untrue, without deceptive intent or bad faith, misinformation can be defined as misinformation. This category also falls into the category of misinformation since the information is false, even if the person disseminating it is unaware of it.
- If the information is true/true, but its dissemination is misleading and has the wrong intention, it can be defined as "malinformation". (In Hungarian, this term is often called incorrect or bad information.) Unlike the previous ones, this category cannot be classified as fake news because although the dissemination is intentional and the intention is wrong, the information is true.[41]

Researchers have approached the problem of fake news from various perspectives on different topics. These include but are not limited to how governments and international organisations can regulate fake news, specifically disinformation disseminated online. In these activities, the main argument is to defend against challenges to democracy.[42]

In this context, EU terminology includes two additional terms: disinformation and misinformation. The Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on the Action Plan for Democracy in Europe defines the following related terms:

- Information influence operation: means a concerted effort by domestic or foreign actors to influence a target audience by deceptive means, including suppression of independent sources of information and disinformation
- Foreign interference in information space: a set of coercive and deceptive efforts designed to interfere with and prevent the free formation and expression of the political will of individuals by a foreign state actor or its agents[43]

In summary, fake news, disinformation, misinformation, and malinformation pose a particular risk to our security, and these threats include:

- misleading, uncontrolled information that may be a threat to the security of society

[41] Aïmeur et al. 2023.
[42] Jungherr–Schroeder 2021.
[43] European Commission 2020.

- decreasing social trust in the credibility of the media
- foreign interference in economic, political, and social processes and groups
- threats to clean and transparent democratic political processes, such as manipulation of election campaigns
- facilitating decisions based on false information that negatively affects the security of society and individuals
- acceleration of social conflict, anarchy, and extremism[44]

Disinformation in the Russian–Ukrainian conflict

Nowadays, disinformation activities in the online space can spread in a highly sophisticated way. Based on an already analysed previous case (the 2016 U.S. presidential election), fake news accounted for almost 6% of all news consumption in the period under discussion, but it was highly concentrated: only 1% of users were exposed to 80% of fake news, and 0.1% of users were responsible for sharing 80% of fake news, which is a worrying statistic in the academic world in the context of disinformation campaigns and the defence against them.

In addition, recent events have unfortunately seen disinformation campaigns explicitly threatening human lives.[45]

Regarding Russia, they use the opportunities offered by the various online social media platforms. On these platforms, they have two popular and adequate ways of pushing their narrative: the use of so-called "trolls" and botnets.[46]

By trolls, we mean real users who, either out of conviction or for some quid pro quo, advocate a particular point of view in either their own or opposing communities. By botnet, we mean a so-called "robot network", i.e. a collection of interconnected networks that are centrally controlled. The central controller is the one who controls all these interconnected networks. Suppose an attacker decides to attack an organisation or to carry out any activity on various online platforms that he or she has defined; he or she will need a large amount of resources. In that case, botnets are malicious networks, an army, that allows attackers to penetrate web servers by breaking firewall security, conducting large-scale phishing attacks, delivering malware, among other things, and carrying out (distributed) denial of service (D)DoS attacks, but also use so-called "brute force" to compromise devices, user accounts, including their presence on various online platforms. In this regard, botnets can contribute to the success of various psychological operations and disinformation campaigns by delivering the messages and content they want to target very quickly and efficiently to the target group or different layers of users.[47] These possibilities are, of course, also being used in a meaningful way in the Russian–Ukrainian war. In addition to this, it is important to note that Russia relies heavily – albeit undeclared – on cybercriminal

[44] Dobák 2022: 93–124.
[45] Katz 2020: 659–682.
[46] Alieva et al. 2022.
[47] Chen et al. 2022; Sri Skandha Moorthy – Nathiya 2023: 1405–1413; Elliott 2010: 79–103; Srinivasan–Deepalakshmi 2023.

(APT) groups and non-governmental organisations (NGOs) and actors. In terms of its implementation, based on our current knowledge, the Russian government allows/pays no heed to the activities of these criminal groups on the territory of Russia, while certain "tasks" can be outsourced to these group actors.[48]

Along the previously detailed points, we can identify the same objectives for both Russian and Ukrainian disinformation operations:

- promoting their narrative
- gaining the support of its population and the undecided
- convince international opinion
- demoralising, weakening, and influencing the enemy
- drain the enemy's resources
- influence social processes
- create mistrust, provoke conflicts
- support military, political, and economic objectives

Some of the better-known disinformation campaigns:

- The legend of the ghost of Kyiv
- Denial of the Bucha massacre
- Zelensky's flee to the West
- Poland and Finland marched to the Russian border
- The fake news about refugees
- Faking war events
- Failure to acknowledge the fact of war

Countering disinformation

Countering and defending against disinformation and fake news is in the interest of individuals and the community. For individuals and society, and more broadly for a country or even a federal system, obtaining real, credible information is essential to make the right decisions in a wide range of situations and to enable citizens and decision-makers to make decisions in their own and their community's best interests, free from outside influence.

In the fight against disinformation, it is important to remember the need for fact-checking, source-checking, credibility-checking, critical thinking, and sound reasoning (scientific or from multiple, independent, and reliable sources) to minimise the likelihood of falling victim to campaigns.

There is no doubt that education has a key role in fortifying immunity to pseudo-news. Nevertheless, the methodological limitation is that it can take years to build immunity. In many cases, however, there is no time for this; think of the global pandemic caused by Covid–19 or a war. This is why the state has a key role in the fight against the spreaders of pseudo-news. An important tool for this could be the network-theoretic approach in the second part of our article series.

[48] Galeotti 2017.

Results of the analysis of the scientific literature

In this topic, we look at the scientific trends regarding disinformation, misinformation and malinformation keywords.

Firstly, the term malinformation received 37 results. This amount of results compared to other two keywords were much lower, therefore it was excluded from the analysis. Although, it is worth highlighting that the low results indicate a shallow trend regarding this keyword. We suspect the reason for this is that malinformation has a fundamental element compared to the other two keywords. Malinformation, as the name suggests, involves malice act and proving –which is central in a peer-reviewed article – that element is further demanding, compared to it being called misinformation.

If both keywords were found in the same article, the work was included in both analyses for the latter keyword. From the early 2000s onwards, there was a slow increase for each keyword, which started to increase more intensively from 2013 onwards. For the 2023 data, only publications included up to August were processed.

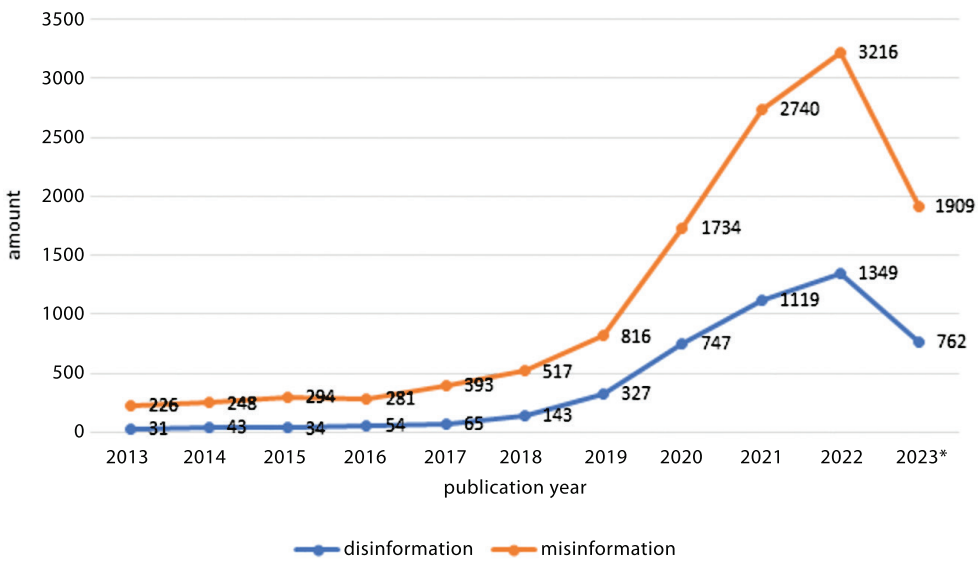


Figure 1: Publication amount comparison by year: disinformation and misinformation 2013–2023
Source: Scopus

Figure 1 shows that the number of publications related to these two terms rose sharply in 2019 and practically quadrupled by 2022. The data suggest that a similar magnitude of publications as in 2022 will be published in 2023. As Figure 1 compares the amount of publications which have the words present, misinformation is more trending. We observe a growth in both words, however misinformation is certainly more popular. From 2019 to 2020 the amount has doubled in both cases. We assume

the reason for this large jump in the trends is connected to the 2020 U.S. Presidential Election, the ongoing Covid–19 crisis, and the Russia–Ukraine conflict. To get a full picture about this assumption, we analysed the top 100 keywords connected to disinformation and misinformation.

Firstly, we highlight the top 100 keywords, and when each keyword started to appear in terms of disinformation is shown in Figure 2. Figure 2 showcases, while disinformation has a major connection to other keywords, it is not clearly in a central position. We can also observe a shift coming from the publishing year. The older articles focus on human aspects, later this transfers to social media and Covid–19. While our initial assumption regarding the Covid–19 connection was right, the U.S. Presidential Election has no connection to the word disinformation in the observed publications.

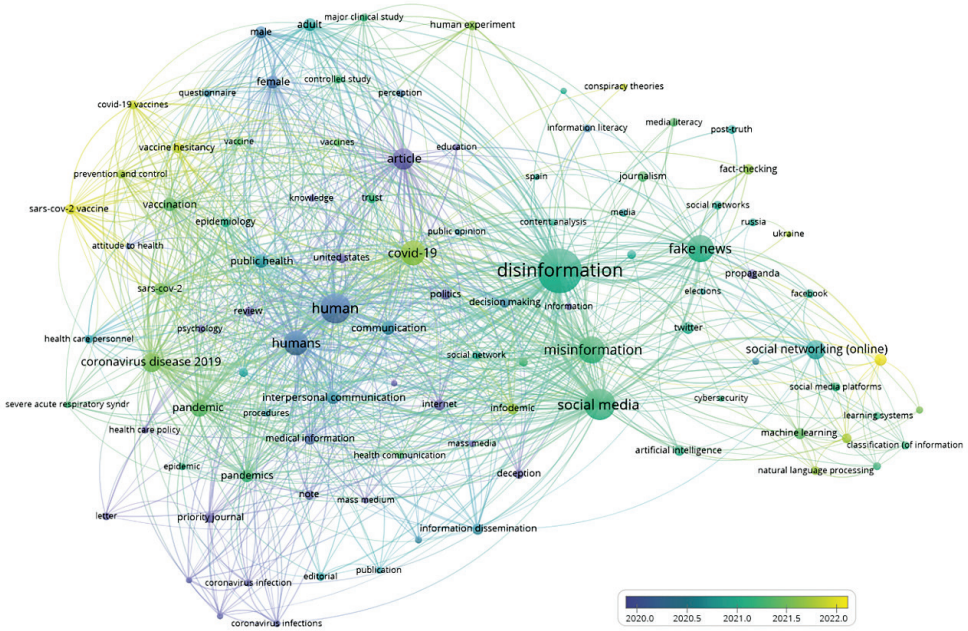


Figure 2: Top 100 keywords in connection with disinformation
Source: Scopus

The only international trend we can witness in Figure 2 is the coronavirus pandemic. The Russia–Ukraine has no presence in the keyword connections, our understanding is that Covid–19 is a way more overwhelming and directly internationally affecting issue. Moreover, for peer-reviewed literature, from the time when the researcher starts working on the article until release more than a year can pass by. For this reason, we assume that the disinformation with Russia–Ukraine related keywords going to be more dominant after 2024.

Figure 3 highlights the top 100 keywords in connection with misinformation. We can already observe compared to Figure 2 that the words are more interconnected.

"Social media" keyword creates a bridge for machine learning, deep learning and fake news topics. This assures an indication that social media plays an important role in these topics. Also looking at the publishing years, we can detect the same shift which we have seen in Figure 2. The older articles showcase mostly human topics, while latest articles focus on Covid–19. Here also the U.S. Presidential Election has no presence in the keyword cloud. The same observation regarding the Russia–Ukraine conflict applies to Figure 3 as well. We assume that due to the research article process topics related to the war going to be more present after 2024.

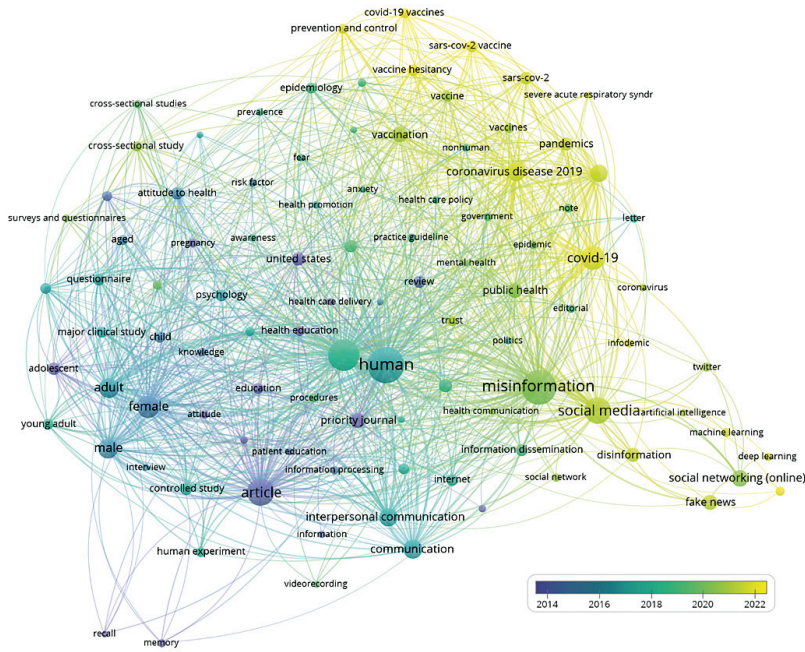


Figure 3: Top 100 keywords in connection with misinformation
Source: Scopus

These three figures give a clear presentation over the current and previous scientific trends. We do observe a delay in topics, which can be connected to the fact that articles take time to create and publish. While Covid–19 as a pandemic started in early 2020, the figures clearly show articles related to this pandemic are mostly from 2022. Based on this observation, we assume that the same will be related to the Russia–Ukraine conflict articles.

It is worth noting and highlighting that the words misinformation, social media, fake news and disinformation are closely bonded. Looking at the shift in time, researchers first approached this question from the individual (human) perspective, but now the focus is on the information itself and platforms, therefore social media, misinformation, disinformation are more dominant in latest articles. We already know that social media plays an important role in the Russia–Ukraine conflict, thus this

trend will very likely to continue. Social media also raises multiple issues regarding fake news, which we open up for discussion in our next chapter.

Discussion

In summary, the operations at the heart of our research (information and psychological operations, disinformation campaigns, dissemination of misinformation and malinformation) represent challenges to the free expression of opinion and political will of the global public, which can be defined as a central, crucial security issue today. In the remainder of our research, we will use sentiment and network analysis to investigate the spread of fake news in war and its impact. As presented in our research, this is not a new issue, but rather an ongoing challenge. If we raise the question of how we tackle fake news, unfortunately there is no clear answer and no clear solution. Creating fake news compared to fact checking information is a relatively cheap and non-time consuming matter. Fake news is often being shared on social media, which further increases the challenge. If traditional media platforms share misleading information, they later can be held responsible for it. There's a clear and established legal process for this, either affected individuals might form a lawsuit towards the media platform, or the government itself can issue a fine. However, if fake news are shared on social by an individual or by a random profile there's a major burden. Firstly resources are required to investigate who is responsible for the fake news. They are also very likely be from a different nation which is lenient in this question. Also governments have no full control over social media platforms, so before any information can be investigated, the platform provider must cooperate. Which is also a burden for governments.

This research is not meant to be deeply analyse how challenging social media is in our modern world, but we feel like in this topic the issue has to be mentioned. Fake news are a constant threat and we see no clear solutions to address them. Moreover, as we have seen from keyword analysis social media is highly connected to fake news. Because it gives a relatively easy option to bad actors to share harmful or misleading information.

As for the information warfare, the spreading of fake news can undermine valuable expensive military operations – especially CIMIC duties in a very cost-effective way. For every military operation, a public support is essential, therefore if we are unable to find a solution to the fake news issue, we anticipate that military operations will be threatened.

References

Aïmeur, Esma et al. (2023): Fake News, Disinformation and Misinformation in Social Media: A Review. *Social Network Analysis and Mining,* 13(30). Online: https://doi.org/10.1007/s13278-023-01028-5

Aleksejeva, Nika et al. (2023): Kremlin Information Operations Before and After Ukraine Invasion. *Atlantic Council,* 22 February, 2023. Online: www.atlantic-

council.org/event/kremlin-information-operations-before-and-after-the-february-2022-invasion

Alieva, I. et al. (2022): How Disinformation Operations against Russian Opposition Leader Alexei Navalny Influence the International Audience on Twitter. *Social Network Analysis and Mining,* 12(1). Online: https://doi.org/10.1007/s13278-022-00908-6

Bányász, Péter et al. (2019): Lélektani műveletek a közösségi médiában. In Auer, Ádám – Joó, Tamás (eds.): *Hálózatok a közszolgálatban.* Budapest: Dialóg Campus, 111–134.

Bērziņš, Jānis (2020): The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria. *The Journal of Slavic Military Studies,* 33(3), 355–380. Online: https://doi.org/10.1080/13518046.2020.1824109

Betts, Jennifer (2021): Examples of Propaganda Done With Different Tactics. Yourdictionary.com, 19 May, 2021. Online: https://examples.yourdictionary.com/examples-of-propaganda.html

Bundtzen, Sara et al. (2022): Hashtag Pairing Is Being Used on Twitter to Facilitate Soviet Propaganda Tactic 'Whataboutism'. *ISD – Institute for Strategic Dialogue (blog),* 15 March, 2022. Online: www.isdglobal.org/digital_dispatches/hashtag-pairing-is-being-used-on-twitter-to-facilitate-soviet-propaganda-tactic-whataboutism

Chen, Long et al. (2022): Social Network Behavior and Public Opinion Manipulation. *Journal of Information Security and Applications,* 64, 103060. Online: https://doi.org/10.1016/j.jisa.2021.103060

Collins, Ben – Korecki, Natasha (2022): Twitter Bans over 100 Accounts that Pushed #IStandWithPutin. *NBC News,* 4 March, 2022. Online: www.nbcnews.com/tech/internet/twitter-bans-100-accounts-pushed-istandwithputin-rcna18655

Czeglédi, Mihály (2017): Az információs műveletek szerepe a korszerű parancsnoki gondolkodásban. *Honvédségi Szemle,* 145(4), 74–87.

Dobák, Imre (2022): A dezinformáció – napjaink kiemelt kihívása. *Katonai Jogi és Hadijogi Szemle,* 10(1), 93–124.

Elliott, Claire (2010): Botnets: To What Extent Are They a Threat to Information Security? *Information Security Technical Report, Computer Crime – A 2011 Update,* 15(3), 79–103. Online: https://doi.org/10.1016/j.istr.2010.11.003

European Commission (2016): *Joint Communication to the European Parliament and the Council – Joint Framework on countering hybrid threats.* JOIN(2016) 18 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018

European Commission (2020): *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European Strategy for Data.* COM(2020) 66 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066

Farkas, Tibor (2023): A kommunikációs és információs rendszerek értelmezése napjainkban: követelmények és kihívások. In Tóth, András (ed.): *Új típusú kihívások az infokommunikációban.* Budapest: Ludovika, 11–30.

Galeotti, Mark (2017): Controlling Chaos: How Russia Manages Its Political War in Europe. *ECFR,* 1 September, 2017. Online: https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe

Gerasimov, Valery (2013): The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military-Industrial Kurier,* 27 February, 2013.

Grinberg, Nir et al. (2019): Fake News on Twitter during the 2016 U.S. Presidential Election. *Science,* 363(6425), 374–378. Online: https://doi.org/10.1126/science.aau2706

Haig, Zsolt (2011): Az információs hadviselés kialakulása, katonai értelmezése. *Hadtudomány,* 21(1–2), 12–28.

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

Haig, Zsolt – Várhegyi, István (2005): *Hadviselés az információs hadszíntéren.* Budapest: Zrínyi.

Joint Chief of Staff (2014): *Joint Publication 3-13: Information Operations.* 20 November, 2014.

Jungherr, Andreas – Schroeder, Ralph (2021): Disinformation and the Structural Transformations of the Public Arena: Addressing the Actual Challenges to Democracy. *Social Media + Society,* 7(1). Online: https://doi.org/10.1177/2056305121988928

Katz, Eian (2020): Liar's War: Protecting Civilians from Disinformation during Armed Conflict. *International Review of the Red Cross,* 102(914), 659–682. Online: https://doi.org/10.1017/S1816383121000473

Kiss, Álmos Péter (2019): A hibrid hadviselés természetrajza. *Honvédségi Szemle,* 147(4), 17–37.

Kiss, Álmos Péter – Somodi, Zoltán (2019): A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban. *Honvédségi Szemle,* 147(6), 22–28. Online: https://doi.org/10.35926/HSZ.2019.6.2

Krajnc, Zoltán ed. (2019): *Hadtudományi lexikon: Új kötet.* Budapest: Dialóg Campus. Online: https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/14688/790_hadtudomanyi_lexikon_2019.pdf?sequence=1&isAllowed=y

Magyar Honvédség (2014): *Ált/57 Információs Műveletek Doktrina.*

Miller, David (2015): Sociology, Propaganda, and Psychological Operations. In Dawson, Matt et al. (eds.): *Stretching the Sociological Imagination: Essays in Honour of John Eldridge.* London: Palgrave Macmillan, 163–188. Online: https://doi.org/10.1057/9781137493644_9

NATO (2009): *NATO AJP-3.10 – Allied Joint Doctrine for Information Operations.* Online: https://info.publicintelligence.net/NATO-IO.pdf

NATO (2014): *Wales Summit Declaration issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Wales.* 5 September, 2014. Online: www.nato.int/cps/en/natohq/official_texts_112964.htm

Nemeth, William J. (2002): *Future War and Chechnya: A Case for Hybrid Warfare.* Naval Postgraduate School, Monterey. Online: https://core.ac.uk/download/pdf/36699567.pdf

Padányi, József – Tomolya, János (2017): Háború és béke Ukrajnában, avagy keleten a helyzet változatlan 1. rész. *Hadtudomány,* 27(1–2), 63–83. Online: https://doi.org/10.17047/HADTUD.2017.27.1-2.63

Padányi, József – Tomolya, János (2017): Háború és béke Ukrajnában, avagy keleten a helyzet változatlan 2. rész. *Hadtudomány,* 27(3–4), 29–42. Online: https://doi.org/10.17047/HADTUD.2017.27.3-4.29

Porkoláb, Imre (2015): Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? *Hadtudomány,* 25(3–4), 36–48. Online: https://doi.org/10.17047/HADTUD.2015.25.3-4.36

Pozderka, Zoltán (2016): Az információs műveletek helye és szerepe a műveletervezésben. *Hadtudomány,* 26(Special ed.), 131–141. Online: https://doi.org/10.17047/HADTUD.2016.26.K.131

Rácz, András (2014): *Oroszország hibrid háborúja Ukrajnában*. KKI-Tanulmányok 2014/1. Online: http://docplayer.hu/6612943-Oroszorszag-hibrid-haboruja-ukrajnaban.html

Raychev, Yavor (2019): Roots of the Concept of Hybrid War in Russian Political and Military Thought. *Balkan Social Science Review,* 13(13), 127–151.

Simicskó, István (2017): A hibrid hadviselés előzményei és aktualitásai. *Hadtudomány,* 27(3–4), 3–16. Online: https://doi.org/10.17047/HADTUD.2017.27.3-4.3

Smart, Charlie (2022): How the Russian Media Spread False Claims About Ukrainian Nazis. *The New York Times,* 2 July, 2022. Online: www.nytimes.com/interactive/2022/07/02/world/europe/ukraine-nazis-russia-media.html

Sri Skandha Moorthy, R. – Nathiya, N. (2023): Botnet Detection Using Artificial Intelligence. *Procedia Computer Science, International Conference on Machine Learning and Data Engineering,* 218, 1405–1413. Online: https://doi.org/10.1016/j.procs.2023.01.119

Srinivasan, Sathiyandrakumar – Deepalakshmi, P. (2023): Enhancing the Security in Cyber-World by Detecting the Botnets Using Ensemble Classification Based Machine Learning. *Measurement: Sensors,* 25, 100624. Online: https://doi.org/10.1016/j.measen.2022.100624

UNHCR [s. a.]: *Situation Ukraine – Refugee Situation.* Online: https://data2.unhcr.org/en/situations/ukraine

Van Puyvelde, Damien (2015): Hybrid war – does it even exist? *NATO Review,* 7 May, 2015. Online: www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html

Legal sources

Government Decree 1163/2020 (21.IV.) on the National Security Strategy of Hungary. Online: https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001

Government Decree 1393/2021 (24.VI.) on the National Military Strategy of Hungary. Online: https://honvedelem.hu/hirek/nemzeti-katonai-strategia.html

HADMÉRNÖK
VÉDELEMINFORMATIKA
18. évfolyam (2023) 4. szám 129–146.
DOI: 10.32567/hm.2023.4.9

Hankó Viktória[1]

Információbiztonság a női munkavállalók aspektusából I.[2]

Information Security from the Perspective of Women Employees I

Absztrakt

A 21. században az információbiztonság, kiberbiztonság kiemelt fontosságú. Ezen területek szakemberállománya vizsgálatának szükségessége is hangsúlyozza a terület aktualitását – különös tekintettel a nemi megoszlásra, bérezés kérdésére, illetve ezek alakulására, okaira. A tanulmány első részében az információbiztonság és az ahhoz kapcsolódó fogalmak ismertetése mellett a szerző bemutatja a már szakmában dolgozó férfiak és nők jelenlegi szakmai helyzetét, motivációit. Ez egy kérdőíves kutatás keretében valósult meg. Emellett a közösségi média egyre növekvő szerepe is megjelenik a tanulmányban. Ehhez kapcsolódóan az aktuális trendek bemutatása történik szentimentanalízis segítségével.

Kulcsszavak: információbiztonság, munkaerőpiac, közösségi média

Abstract

In the 21st century, information security and cybersecurity is a top priority. The need to examine the workforce in these fields also underlines the importance of this area, particularly in terms of gender distribution, pay and its evolution and causes. In the first part of the article, the author describes the current professional situation and motivations of men and women already working in the field, in addition to the concepts of information

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: viktoria.hanko@protonmail.com

[2] A cikk a Innovációs és Technológiai Minisztérium ÚNKP-21-2-II-NKE-46 kódszámú Új Nemzeti Kiválósági Programjának szakmai támogatásával készült.

security and related concepts. This was done through a survey. Besides, the growing role of social media is also reflected in the study. In this context, current trends are presented by means of a sentiment analysis.

Keywords: information security, labour market, social media

Bevezetés

A 21. század az internet, az informatika világa, így az információbiztonság és a kiberbiztonság is a mindennapjaink része. Az elterjedt prekoncepció szerint a számítógépes játékok, illetve a programozás inkább a fiúk érdeklődési körébe tartozik, így számukra vonzóbb lehet a szakma a későbbi pályaválasztás során. Ennek következményeként kialakult egy sztereotípia, amely az informatikai kompetenciákat inkább a férfiakhoz köti, mintsem a nőkhöz – ezzel további kihívásokat állítva a fiatal lányok elé, mint például női példaképek azonosítása az informatika területéről. Egyre több tanulmány és internetes cikk születik, amelynek a témája a nők megjelenése az információbiztonsági szektorban. Ezek között találkozhatunk olyanokkal is, amelyek régebbi sikereket ismertetnek például a programozás területén, valamint olyanokkal is, amelyek az aktuális helyzetet mutatják be felmérések eredményeiként. A statisztikák évről évre jobb eredményt mutatnak, ennek egyik mozgatórugója lehet, hogy világszinten különböző szervezetek működnek mentorálási lehetőséggel azon fiatal vagy éppen idősebb hölgyek számára, akik a pályára lépnének.

A kutatás célja felmérni és feltárni a nők elhelyezkedésének problémáját az információbiztonsági szektorban, illetve azokat a kihívásokat, amelyekkel szembesülnek. Elsősorban a már a szektorban dolgozók motivációját mérem fel. Továbbá kitérek a jelenlegi helyzetükre is, különös tekintettel a bérezésre, illetve a diszkriminációra, valamint kiemelten a bemenetelre, az előmenetelre és a pályaelhagyás alakulására. Ezen kérdések vizsgálatát kérdőíves kutatáson keresztül valósítom meg. Annak érdekében, hogy a másik nem álláspontját is feltárjam a nemek közötti egyenlőség munkahelyi helyzetével kapcsolatban, a kérdőíves kutatás keretében nemcsak női, hanem férfi szakértőket is megkérdeztem. Emellett a közösségi médiában megjelenő különböző nemzetközi kulcsszavak vizsgálatát végzem el, hogy feltárjam a téma megítélést.

Kutatási módszertan

Elsődlegesen a releváns a hazai és nemzetközi szakirodalmat dolgoztam fel. Ezekben az információbiztonság, kiberbiztonság és informatikai biztonság terminológiai különbségeinek meghatározása mellett megjelenik az információbiztonsági terület fejlődése, jelenlegi tendenciái, valamint szakmai összetétele – hazai és nemzetközi szinten. A cikk második pillérét a kérdőíves kutatás képezi. A feltett kérdések elemzését az IBM SPSS szoftver segítségével végzem el. A vizsgálat során kiválasztott kérdések közötti kapcsolat vizsgálata pedig kereszttábla-elemzéssel, illetve klaszterelemzéssel történt. Továbbá a közösségi médiában megjelenő trendek is fókuszba kerülnek a szentimentanalízis keretében.

Információbiztonság mint munkaerőpiaci szakterület

A nemzetközi szakirodalom szinonimaként használja az információbiztonság, a kiberbiztonság és az informatikai biztonság szavakat. Valóban van átfedés és hasonlóság a fogalmak között, azonban nem teljesen ugyanazt jelentik. A NIST 800-59 irányelve alapján az információbiztonság az információk és információs rendszerek védelmét jelenti a jogosulatlan hozzáféréstől, felhasználástól, nyilvánosságra hozataltól, megzavarástól, módosítástól vagy megsemmisítéstől a bizalmasság, sértetlenség és rendelkezésre állás biztosítása érdekében.[3] Muha Lajos és Krasznay Csaba úgy fogalmaz, hogy az információbiztonság alatt a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben vagy bármilyen más módon kezelt információk védelmét értjük.[4] Jeremy Hilton és Yulia Cherdantseva megfogalmazásában az információbiztonság általános definíciójában öt pontot szükséges kiemelni, amelyek a következők:

1. Nincsenek korlátozások az információ típusára vonatkozóan. Tág értelemben az információbiztonság bármilyen formájú vagy típusú (például elektronikus, papír, verbális, vizuális) információval foglalkozik.
2. Tartalmazza az információk védelmét szolgáló összes műveletet. Így nemcsak a technikai műveletekkel foglalkozik, hanem az információfeldolgozás, -tárolás vagy -továbbítás során szükséges védelmi műveletek sokféleségével is.
3. A nemkívánatos események listája széles és nyitott. A definíció kifejezetten felsorolja a lopást, kémkedést és az információ megrongálását, de nem korlátozódik ezekre.
4. Az általános definíció nem tartalmaz olyan biztonsági célokat, mint a bizalmasság, sértetlenség, rendelkezésre állás vagy bármi más. A tudományág fő célja tehát – a harmadik ponttal összhangban – az átfogó információvédelem, és nem csupán több, előre meghatározott biztonsági cél elérése.
5. Az információbiztonság magában foglalja az előre megtett intézkedéseket. Ezért nemcsak a már megtörtént nemkívánatos események elemzésével kell foglalkoznia, hanem az ilyen események előrejelzésével és azok valószínűségének felmérésével is.[5]

Ennek egy részterületét képezi az informatikai biztonság, amely az informatikai rendszerekben kezelt adatok és az azokat kezelő rendszer(ek) védelmét jelenti, ebből kifolyólag nem a teljes információs rendszerre, csupán annak valamennyi elemére terjed ki.[6]

Mindemellett a kiberbiztonság a NIST megfogalmazása alapján kibertérben megjelenő támadókkal szembeni védekezés képességét jelenti.[7] Ezzel szemben Magyarország Nemzeti Kiberbiztonsági Stratégiájában

[3] Barker 2003.
[4] Krasznay–Muha 2014.
[5] Cherdantseva–Hilton 2014.
[6] Muha 2008.
[7] Paulsen–Byers 2019.

„a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez, működtetéséhez"

definícióval találkozhatunk.[8] Mindkét fogalom a kiberteret említi, amely a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét foglalja magában.[9] A fogalmi evolúció párhuzamosan zajlott a NATO kiberbiztonsággal kapcsolatos stratégiai fejlődésével, amelyben a szakemberképzés hangsúlyos elemként jelenik meg.[10] A magyar kibervédelem rendszeréről elmondható, hogy rendkívül szerteágazó, amelyben meg kell teremteni egy tudásbázist, amely különböző kérdésköröket kell tartalmazzon: stratégiai, jogi, vagy akár szervezeti, működési ismereteket.[11]

A fent említett definíciókból látható, hogy valóban van átfedés a fogalmak között, azonban az információbiztonság egy szélesebb terület, amely mind az informatikai biztonság, mind pedig a kiberbiztonság elemeit lefedi.

A munkaerőpiac bemutatása

Az előző fejezetben feltártak alapján elmondható, hogy igen széles területről van szó, amelynek fő eleme – annak elnevezéséből is adódóan – a biztonság és a védelem megteremtése, fenntartása. Ennek megvalósítása a területen dolgozó szakemberállomány – vagy legalább egy részének – a feladata. Elmondható továbbá, hogy az információbiztonság az utóbbi években mind a tudományos kutatásban, mind az ipari gyakorlatban előtérbe került. A hatékony biztonsági műveletek támogatásához többre van szükség, mint pusztán technikai megoldások sokaságára. Az emberi tényezőt kulcsfontosságúnak kell tekinteni ebben az iparágban.[12] Emellett fontos megjegyezni, hogy az információbiztonsági szektorban nem feltétlenül mindenki biztonsági tesztelő, valamint a területen dolgozók közül sem mindenki tölti minden idejét a biztonsággal kapcsolatos problémákkal.[13] Ebből fakadóan multidiszciplináris területről beszélhetünk, és az emberek gyakran több kalapot viselnek (remélhetőleg mindenki fehéret[14]), miközben ugyanazt a szerepet töltik be. Lehet a munkakör oktató, aki megtanítja az irodai dolgozókat, illetve további munkatársakat hogyan végezzék el a feladataikat anélkül, hogy szükségtelen biztonsági kockázatoknak tennék ki a szervezetet, mint például az utcán talált pendrive vállalati számítógépbe helyezése.

[8] Magyarország Nemzeti Kiberbiztonsági Stratégiája 2013.
[9] Magyarország Nemzeti Kiberbiztonsági Stratégiája 2013, 3. pont.
[10] Bányász–Krasznay–Tóth 2021: 130–149.
[11] Krasznay 2017.
[12] Hámornik–Krasznay 2017.
[13] Tóth 2022: 224.
[14] Angolul „white hat hacker", vagyis etikus hacker.

Mellettük jelen vannak a programozók, akiknek idejük nagy részét a kódok áttekintése teszi ki, amellyel szerencsés esetben a potenciális támadók előtt fedezik fel a biztonsági réseket. Továbbá lehet a szektorban valaki újságíró is, aki az aktuális kockázatok leírása mellett elemzéseket készít az iparági trendekről.[15] Vannak továbbá a biztonsági műveleti központok, azaz a Security Operation Center-ek vagy SOC-ok, ahol a csapatok a technológiát használják a feladatok közös elvégzésére, céljaik elérésére.[16]

A munkahelyek, foglalkozások, készségek és profilok esetében különféle hivatkozásokat találhatunk a munkaerőpiacon. Ezek közül a legismertebbek a European Skills, Competences, Qualifications and Occupations, azaz a készségek/kompetenciák, képesítések és foglalkozások európai osztályozása (a továbbiakban: ESCO), az Európai Unió (a továbbiakban: EU), új munkaerő-osztályozás, az e-CF vagy az 16234-es európai szabvány. Az ESCO osztályozásán belül az információs és kommunikációs technológiai (a továbbiakban: IKT) foglalkozások között találhatjuk meg az információbiztonság, kiberbiztonság területén megjelenő munkaköröket, amely a következőképpen alakul.

1. táblázat: Munkakörök megnevezése, leírás

Munkakör megnevezése	**Munkakör leírása**
Biztonsági tesztelő	Behatolásvizsgálatot, valamint biztonsági sebezhetőségi értékeléseket hajt végre az elfogadott módszereknek és protokolloknak megfelelően. Különböző biztonsági szempontok alapján elemzi a rendszereket.
IKT-audit menedzser	Felügyeli az információs rendszerek, platformok és működési eljárások ellenőrzéséért felelős IKT-auditorokat a hatékonyság, a pontosság és a biztonság érdekében kialakított vállalati normákkal összhangban. Felméri és értékeli a szervezet IKT-infrastruktúráját kockázati szempontból, valamint ehhez kapcsolódóan ellenőrzéseket vezet be. Továbbá a jelenlegi rendszerváltozások/frissítések végrehajtására vonatkozóan, illetve a kockázatkezelési ellenőrzésekre javaslatot tesz.
IKT-auditor	Információs rendszerek, platformok, valamint üzemeltetési eljárások ellenőrzését végzi, összefüggésben a vállalat által meghatározott hatékonysági, pontossági és biztonsági szempontokkal. Emellett az IKT-audit menedzserhez hasonlóan ő is ellenőrzi az IKT-infrastruktúrát és ellenőrzéseket vezet be, valamint javaslatokat tesz.
IKT biztonsági adminisztrátor	Megtervezi és végrehajtja azokat a preventív intézkedéseket, amelyek hiánya szándékos támadás, lopás vagy korrupcióból származó információk és adatok kiszivárgásához vezethetne.

[15] Hughes 2019.
[16] Hámornik–Krasznay 2017.

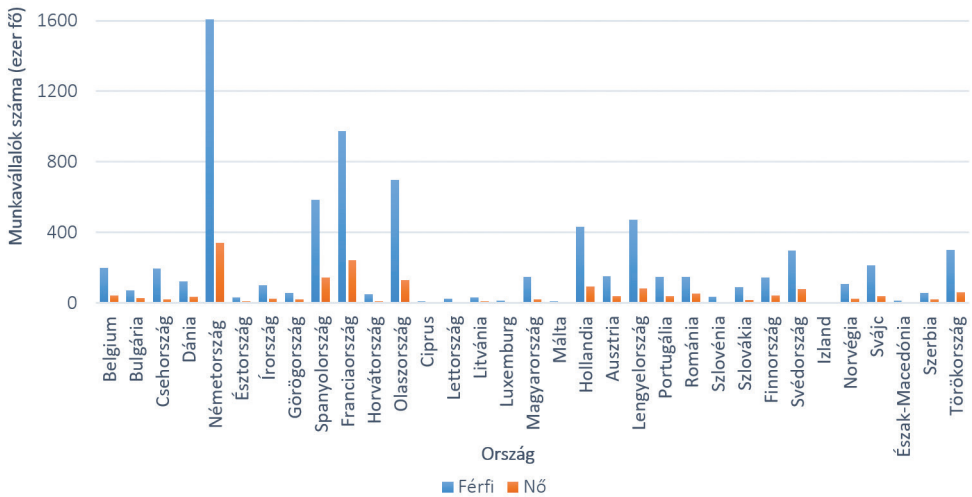
Munkakör megnevezése	Munkakör leírása
IKT biztonsági igazgató	Védi a céginformációkat, valamint a munkavállalók adatait a jogosulatlan hozzáféréssel szemben. További feladata az információs rendszer biztonságpolitikájának meghatározása. Kezeli a biztonságos telepítést az információs rendszerekben, és az információk rendelkezésre állását is biztosítja. CISO néven is ismert.
IKT biztonsági menedzser	Javasolja és végrehajtja a szükséges biztonsági frissítéseket. Emellett a tanácsadás, támogatás, valamint tájékoztatás is a munkája részét képezi a képzés és tudatosítás mellett.
IKT biztonságtechnikai tanácsadó	Javaslatot tesz és hajt végre, amelynek célja az adatokhoz és programokhoz való hozzáférés ellenőrzése. Továbbá a biztonságos információcserét is elősegíti.
IKT katasztrófaelhárítás menedzser	A szervezet kiberbiztonságának, ellenálló képességének és egy katasztrófa utáni helyreállítás képességének fejlesztése érdekében modelleket, irányelveket, módszereket, technikákat és eszközöket kutat, tervez és fejleszt.
IKT-tanácsadó	Tanácsot ad a meglévő eszközök és rendszeres használatával kapcsolatban optimalizálás szempontjából amellett, hogy ajánlást tesz üzleti projektek, technológiai megoldás fejlesztésére, illetve megvalósítására. Továbbá részt vesz az IKT-megoldások kiválasztásában és értékelésében is.
Szoftvermenedzser	Felügyeli a rendszer beszerzését és annak fejlesztését amellett, hogy a végrehajtott szoftvermegoldások és projektek eredményét, minőségét is nyomon követi.

Forrás: az ESCO alapján a szerző szerkesztése

A munkakörök meghatározása után szükséges nevesíteni azt is, hogy hány emberről beszélhetünk ebben a szektorban, illetve a nemek közötti arányok bemutatása további, különböző kérdéseket vethet fel.

2020-ban az EU-ban mintegy 8 400 000 fő dolgozott IKT-szakemberként. A legtöbben (1 900 000 fő) Németországban vállaltak munkát, ahol az uniós szakemberek több mint egyötödét (23,1%) foglalkoztatták. A sorban második Franciaország, ahol 1 200 000 főt tett ki a szakemberállomány (az EU létszámának 14,5%-a), ezt követte Olaszország, ahol 800 000 fő (9,8%) dolgozott IKT-szakemberként. Magyarország esetében 319 200 főről beszélhetünk, ez az EU-s szakemberállomány 3,8%-át teszi ki.[17]

[17] Eurostat é. n.



1. ábra: az IKT-szektorban dolgozók száma 2020-ban
Forrás: az Eurostat alapján a szerző szerkesztése

Kiemelendő – ahogy az az 1. ábrán látható –, hogy az EU-ban IKT-szakemberként foglalkoztatottak túlnyomó többsége férfi, arányukat tekintve 2020-ban 81,5% volt, ami 1,5 százalékponttal alacsonyabb, mint 2011-ben. Csehországban (89,7%), Máltán (89,0%) és Magyarországon (87,7%) 2020-ban 10 IKT-szakemberből 9 férfi volt. Míg a többi uniós tagállam többségében 10 IKT-szakértőből körülbelül 8 férfi volt, addig Bulgária (71,8%), Görögország (73,5%) és Románia (73,8%) voltak azok a kivételek, ahol a férfiak aránya nem érte el a 75%-ot. Bulgáriában az IKT-szakemberek 28,2%-a 2020-ban nőkből állt, ami a legmagasabb arány az uniós tagállamok között. Görögországban és Romániában az összes IKT-szakember körülbelül egynegyedét, 10 másik uniós országban pedig az összes IKT-szakember egyötödét vagy annál is többet tettek ki a nők. Abszolút értékben számolva Németországban 2020-ban több mint negyedmillió női IKT-szakembert (340 400 fő) foglalkoztattak. Ez messze a legmagasabb női foglalkoztatási szint, mivel Franciaország (244 500 fő), Spanyolország (144 500 fő) és Olaszország (130 500 fő) voltak azok a tagállamok, ahol 100 000 fő vagy annál több a női IKT-szakember.[18]

A területen dolgozók motivációja, tapasztalatai – empirikus vizsgálat

Egy afrikai kutatás[19] során gyűjtött adatokból három domináns szempont rajzolódott ki az IKT-szektor mellett döntő dél-afrikai nők körében. Ezek a következők voltak:

[18] Eurostat é. n.
[19] Makola–Kgosinyane 2020.

- tudatos választás és szerencsés véletlen: ebben az esetben saját döntésről számoltak be a résztvevők, illetve a munkáltatóik által biztosított foglalkoztatási lehetőségeket említették, valamint néhány résztvevő jelezte, hogy véletlenül került az IKT-ágazatba;
- érdeklődés és szenvedély: a résztvevők ebben az esetben azt jelezték, hogy az IKT iránti érdeklődésük, amely a szenvedélyükké vált, ösztönözte őket arra, hogy belépjenek az ágazatba;
- társadalmi és családi befolyás: a résztvevők fele arról számolt be, hogy a család és a társadalom befolyásolta őket abban, hogy belépjenek az iparágba – ez magában foglalta szüleik foglalkozását is. A családtagok és a kortársak hatása mellett többen a média befolyását is említették.

Ez a kategorizálást vettem alapul a kérdőíves kutatásom adatainak csoportosítására.

A kérdéssor alapját a BCS, The Chartered Institute for IT 2014 májusában indított kampányának kérdőíve adta. A kampány célja az volt, hogy több nőt ösztönözzenek az információbiztonsági területre való belépésre. A felmérést a szervezet online végezte, személyre szabott meghívás alapján. Ennek során az Egyesült Királyságban élő mintegy 5000 szervezeti tag (véletlenszerűen kiválasztva), illetve szintén az országban működő BCSWomen tagjai voltak jogosultak a kitöltésre. Ebből összesen 771 válasz érkezett a kitöltési időszakban, amely 2014. január 2-től 2014. február 15-ig tartott – tehát 12%-os válaszadási arányról beszélhetünk.

A kitöltők 79%-a úgy érezte, hogy előnyös lenne, ha több nő lenne a szektorban. Emellett a válaszadók több mint fele úgy gondolta, a nőknek nehezebb visszatérni a pályára. Bérezés és előmenetel tekintetében a megkérdezettek nagy része úgy vélte, hogy a férfiak számára jobb lehetőségek adottak. Az információbiztonsági karrierhez a válaszadók szerint leginkább technológia iránti érdeklődés, logikai szemléletmód és általános IT-ismeretek szükségesek.[20]

Az általam reprezentált kérdőív arra a kérdésre ad választ, hogy hazai szinten a szektorban dolgozók milyen tapasztalatokkal rendelkeznek, és mi motiválta őket a pályaválasztás során, valamint ők hogyan motiválnának fiatalokat, hogy ezt a területet válasszák. Ennek megválaszolásához a kérdőív első részében a demográfiai adatok mellett a beosztásra és a munkakörre is rákérdeztem. A felmérés második részében a munkával kapcsolatos motivációval kapcsolatban tettem fel kérdéseket, végül a harmadik részben a hangsúly a foglalkoztatottak munkakörülményeire került. Az adatfelvétel 2021. november 30. és 2022. március 30. közötti történt. Eddig a dátumig 52 (n = 52)[21] kitöltés érkezett. A kitöltők száma az adattisztítási folyamatot követően 52 fő maradt, ebből 15 nő volt (28,8%). Ez alapján a férfiak 71,2%-os arányt képviselnek.

A kitöltők által megnevezett munkakörök alapján megalkottam a következő szakmatérképet:

[20] BCS 2014.

[21] Az alacsony kitöltésszámot vélhetően az indokolja, hogy a célcsoport privacyérzékenysége magas. Több megkeresés is érkezett, hogy többek szerint a demográfiai adatok alapján könnyen profilozhatók, így nem töltötték ki a kérdőívet.

2. ábra: Szakmatérkép
Forrás: a szerző szerkesztése

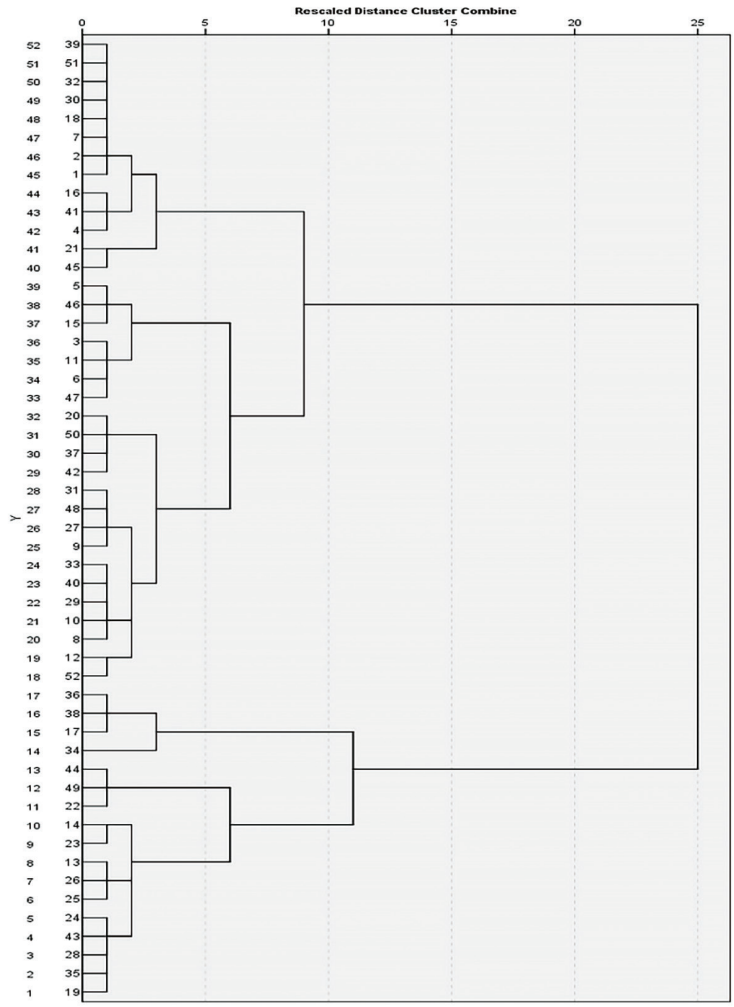
Az ábráról leolvasható, hogy a kitöltők között a férfiak tekintetében – kék és lila színű feliratok – az IBF,[22] CISO[23] és a Tanácsadó volt a legtöbbet említett pozíció, a nők esetében – fekete színű feliratok – az IBF, a Security Tester és Analyst,[24] valamint a Tanácsadó, Információbiztonsági szakértő volt a legnépszerűbb.

Ezt követően Spearman-féle korrelációs vizsgálatot folytattam le, amely azt mutatja meg, hogy az egyik változó nagysága milyen mértékben határozza meg a másik változó nagyságát, valamint az összefüggés irányát és erősségét.[25] Ennek során a legtöbb kérdés között közepesnél erősebb szignifikáns kapcsolat volt kimutatható. A klaszterelemzés az adatok csoportosítását jelenti úgy, hogy figyelembe veszi az egyedek egy meghatározott ismérvrendszerben felvett értékeit. Ennek alapján csak azon változók vonhatók be, amelyeknél közepesnél gyengébb kapcsolat nem mutatható ki.[26] Így a klaszterelemzésbe az alábbi három változót vontam be:

1. Általánosságban mennyire érzi magát motiváltnak a munkahelyén?
2. Mennyire érzi biztosnak (hosszú távon) a jelenlegi munkahelyét?
3. Ön szerint mennyire könnyű vagy nehéz a nők számára visszatérni az IT-/információbiztonsági/kiberbiztonsági munkakörbe a karrier megszakítása vagy szüneteltetése után?

Elméleti megfontolások alapján úgy tűnhet, hogy az 1. és 2. változó között erős kapcsolat van, azonban az elvégzett korrelációs vizsgálat alapján megállapítható, hogy 0,515, ami közepesen erős kapcsolatot mutat.

[22] Elektronikus információs rendszer biztonságáért felelős személy.
[23] IKT biztonsági igazgató.
[24] Biztonsági tesztelő és elemző.
[25] *Spearman korreláció* é. n.
[26] Mitev–Sajtos 2007.



3. ábra: Kapott dendogram
Forrás: a szerző szerkesztése

Ezután az alacsony kitöltési szám okán hierarchikus klaszterelemzést végeztem Ward-eljárással[27] és négyzetes euklideszi távolságmérték[28] alkalmazásával. A kapott dendogram[29] alapján három klasztert azonosítottam, ezek elnevezését és jellemzőit a 4. ábra tartalmazza.

[27] Minden egyes klaszterre kiszámolják az összes változó átlagát, majd minden megfigyelési egységre kiszámítják az euklideszi távolságot. Mitev–Sajtos 2007: 295.

[28] Távolságmérő eljárás, amelyben két pont távolsága, a pontok különbségének négyzetének gyökével egyezik meg. Lásd: http://mialmanach.mit.bme.hu/fogalomtar/euklideszi_tavolsag

[29] A dendogram a klaszterelemzés eredményét grafikus formában ábrázoló diagram. Láthatók rajta a csoportosulási pontok, amelyek a hozzájuk tartozó klaszterekkel beazonosíthatók. Mayer 2016.

Elégedetten biztosak	Középutasok	Elégedetlen bizonytalanok
□ általánosságban motiváltnak érzi magát a munkahelyén; □ biztosnak érzi (hosszú távon) a jelenlegi munkahelyét; □ inkább nehéz visszatérni a nőknek a karrier megszakítása/szünetel-tetése után.	□ közepesen motiváltnak érzi magát a munkahelyén; □ közepesen biztosnak érzi (hosszú távon) a jelenlegi munkahelyét; □ inkább nehéz visszatérni a nőknek a karrier megszakítása/szünetel-tetése után.	□ nem igazán érzi motiváltnak magát a munkahelyén; □ nem érzi feltétlen biztosnak (hosszú távon) a jelenlegi munkahelyét; □ inkább nehéz visszatérni a nőknek a karrier megszakítása/szünetel-tetése után.

4. ábra: Klasztereket és jellemzőiket összefoglaló táblázat
Forrás: a szerző szerkesztése

A kialakított klaszterekben az „elégedetten biztosak" 13 főt, a „középutasok" 22 főt, míg az „elégedetlen bizonytalanok" 17 főt számláltak. A csoportok kialakítását követően további változókat vontam be, úgymint a kitöltő neme, valamint arra a kérdésre adott válasza, hogy szerinte előnyös lenne-e, ha több nő dolgozna a területen. Klaszterek tekintetében 6-6 nő a „középutasok", illetve az „elégedetlen bizonytalanok", míg 3 nő az „elégedetten biztosak" csoportjába tartozik. Emellett az is elmondható, hogy a legmagasabb arányban a „középutasok" és az „elégedetten biztosak" tagjai tartanák előnyösnek, hogy több nő dolgozzon a területen. A nők esetében arányait tekintve többségben vannak, akik szerint előnyös lenne, mindazonáltal azt is ki kell emelni, hogy a női válaszadók arányát tekintve 20% egyáltalán nem támogatja, 26,6% pedig nem biztos benne, hogy kívánatos lenne, ha többen lennének a területen.

Ezt követően kereszttábla-elemzést végeztem, amely során a nemek és a bérezés véleménye közötti kapcsolatot vizsgáltam. Ez arra ad választ, hogy a kitöltők meglátása szerint van-e különbség a férfi és a női munkavállalók bérezése között. A *khi-négyzet-próba* két minőségi változó közötti kapcsolat vizsgálatát teszi lehetővé, azaz arra ad választ, hogy van-e szignifikáns kapcsolat a két változó között.[30] Ennek során a nullhipotézis az, hogy a két változó között nincs szignifikáns összefüggés, ezt akkor fogadjuk el, ha a kapott érték nagyobb, mint 0,05. Az alternatív hipotézis az, hogy van a két változó között kapcsolat, ez akkor igazolódik be, ha a kapott érték kisebb vagy egyenlő, mint 0,05. Az elemzés lefuttatását követően a kapott eredmény 0,222, így nincs kapcsolat. Ebből következik, hogy a nemek és a bérezési, juttatási körülmények között nem mutatható ki összefüggés a vizsgált minta válaszai alapján. A vélemények alapján megállapítható, hogy a férfiak és nők szerint nincs különbség a bérezési, juttatási feltételek között a szektorban.

[30] *Khi-négyzet-próba jelentése és alkalmazása az SPSS-ben* é. n.

Az általam készített kérdőív válaszai alapján két csoportba tudom besorolni a válaszokat:

- Tudatos választás és szerencsés véletlen: a válaszadók között többen írták, hogy a hivatástudat vezérelte a választás során, illetve a saját karriercélok is megjelentek a már korábbi szakmai tapasztalatok mellett.
- Érdeklődés és szenvedély: a válaszok nagy része ebbe a kategóriába tartozik – informatika, szabványok, valamint a rendvédelmi érdeklődés is motivációs tényező.

Emellett fontos kiemelni, hogy a válaszok nagy részében megjelent az újszerűség, illetve a folyamatos tanulás, fejlődés tényezőként. Pár válaszadó a „jó fizetés"-t is megemlítette.

Közösségi média

A webdesign és a motiváció kapcsolata fentebb már szóba került, azonban nem érdemes elmenni a közösségi média jelentősége mellett sem. Érdemes kitérni rá, hogy a közösségi média használatát háromféleképpen osztályozzák. Elsősorban a barátok, rokonok és kollégák közötti kapcsolattartásra használják, másodsorban pedig az öröm és az érzelmi élmények affektív szükségletkielégítésére. A harmadik a kognitív használat, amikor az emberek a közösségi médiát arra használják, hogy információt, tudást gyűjtsenek.[31] Számos közösségi hálózati alkalmazás áll rendelkezésre – amelyet szervezetek hivatalos célokra használhatnak –, mint például a Facebook, a WhatsApp, a YouTube, a Twitter, a blogok, a Skype és a fényképmegosztó oldalak. Ezen túlmenően néhány speciális és privát közösségi hálózatot is használhatnak a szervezetek kommunikációjára,[32] mint például a „Yammer", míg a szervezetek kis része podcastot, second life-ot és Pinterestet használ.[33] Ezek a médiumok nemcsak a munkavállalók közötti kommunikációra használhatók, hanem a nyilvánosság számára is elérhetőséget is biztosíthatnak a szervezet felé – platformot kínálva a különböző tevékenységek, valamint mentorprogramok bemutatására is. Az elemzésnél figyelembe lehet venni az eszközök közötti kapcsolatokat is.[34]

Hatékonyságot tekintve egy tanulmány[35] megállapításai szerint az informatikai szektorban a belső toborzás, a közösségi média, az állásközvetítő tanácsadók és a munkaerő-vadászat a mérsékelten hatékony toborzási formák. A vállalatok toborzási stratégiáit és gyakorlatát befolyásoló belső tényezők közül a vállalat imázsa és a munkahelyi élet minősége a legjelentősebb tényezők. A külső tényezők közül a társadalmi-gazdaságiak befolyásolják leginkább a toborzási gyakorlatot, amelyet a gazdaságban a foglalkoztatási ráta követ. A válaszadók többsége elégedett az informatikai vállalatoknál alkalmazott toborzási gyakorlatokkal és eljárásokkal.

[31] Ali-Hassan – Nevo – Wade 2015: 65–89.
[32] Farkas 2023: 11–30.
[33] Macnamara–Zerfass 2012: 287–308.
[34] Bederna–Szádeczky 2021: 51–66.
[35] Singh–Kamal 2019.

Ez azt jelenti, hogy a kiválasztott vállalatok – TCS, Infosys, Wipro, HCL Technologies and Cognizant Technology Solutions Corporation – pozitív és hatékony toborzási gyakorlatokat követnek.

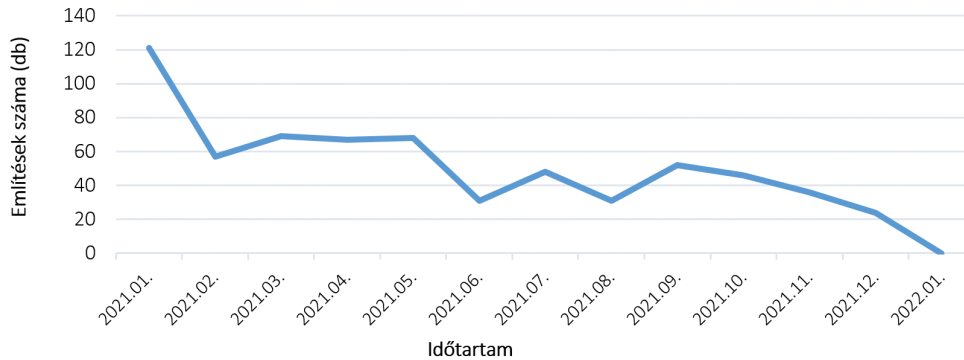
Ezzel szemben egy másik tanulmány[36] eredményei mást mutatnak. Ebben az esetben a toborzási folyamat során olyan innovatív eszközöket vettek igénybe vállalatok, mint például a Facebook, Twitter vagy a LinkedIn. A felmérés eredményeként kiderült, hogy a toborzók 94%-a nagyon kedveli a közösségi oldalakon való hálózatépítést annak érdekében, hogy a tehetségeket hatékonyan kutassák fel. Ettől eltekintve a toborzási szoftverek, illetve a pályázókövető rendszer is segít a folyamat hatékonyságának növelésében. Ennek eredménye, hogy az informatikai vállalatok 70%-a alkalmazza a pályakövetési rendszert a jelölt önéletrajzának elemzéséhez. Ez a szoftver segíthet a tehetségek kiválasztásában, felkutatásában azáltal, hogy elemzi a jelentkezők dokumentumait, keresve a kapcsolatot az előírt feltételek, tapasztalatok, valamint a korábbi munkavállalói tevékenység között. Ezáltal ellenőrizhető a jelentkező tapasztalata, illetve biztosítható a törvényeknek való megfelelőség is.

Trendek és megítélés

Az említett platformokon megjelennek különböző trendek, amelyhez szorosan kapcsolódnak a közösségimédia-adatok (például a követők vagy like-ok számának alakulása) összegyűjtésének, mérésének és értelmezésének folyamata, azaz a közösségimédia-elemzés. Ez a social listening, vagyis a közösségimédia-figyelés egy része, amely során az online beszélgetések nyomon követése folyik annak érdekében, hogy egy adott személyről, márkáról stb. való vélemény, megítélés kiderüljön.[37] Ehhez a SentiOne szoftvert használtam, amely 70 nyelven beszélő, az egész világot lefedő szöveganalitikát alapul vevő social listening szoftver. Hasonló módszertan alkalmazásával vizsgálta Bányász Péter, Tóth András és László Gábor tanulmánya a koronavírus-oltásokkal kapcsolatos állampolgári attitűdöt.[38] A keresett kulcsszót valós időben, vagy akár 3 évre visszamenőleg monitorozza, elemzi a különböző platformokon – internetes fórumok, blogok, közösségi média, weboldalak – közzétett szövegekben. Több mint 20 milliárd adat érhető el, ennek két nagy csoportját a cikkek, valamint a felhasználók által készített tartalmak adják. Ez utóbbiakhoz automatikusan érzelmi besorolást rendel a rendszer – pozitív, negatív vagy semleges besorolás a saját fejlesztésű algoritmus által. Az eredményeket különböző diagramok formájában ábrázolja a szoftver, valamint lehetőséget biztosít a tartalmak, posztok, cikkek és az említések egyenkénti vizsgálatára és kategorizálására.[39]

A #womeninit kifejezést futtattam 2021. január 1. és 2022. január 1. közötti időszakban. Ez idő alatt 650 releváns poszt jelent meg, ebből 163 pozitív, 11 negatív és 476 semleges besorolással. Ezek időszakos megoszlását a következő ábra tartalmazza:

[36] Jose–Asha 2019.
[37] *A social listening alapjai* é. n.
[38] Bányász–Tóth–László 2022: 99–125.
[39] SentiOne é. n.

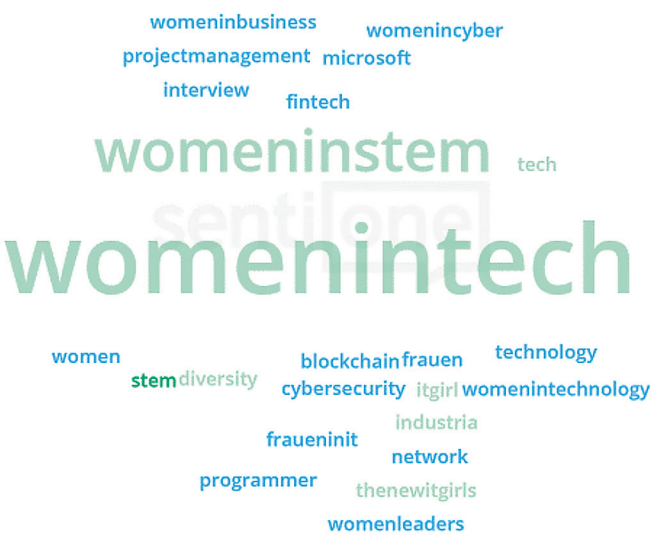


5. ábra: #womeninit kifejezés említésének alakulása
Forrás: a SentiOne alapján a szerző szerkesztése

A kiugró pontok esetében egyrészt a Dell Technologiesnál a nemzetközi nőnap alkalmából írtak egy posztot, amelyben egy sokszínűbb és egyenlőbb világ teremtését említik. Emellett kiemelkedő, amikor Franciaországban az Oracle, az IBM, a Salesforce és a Microsoft élén női vezetőket említenek. Megjelenési platform tekintetében elmondható, hogy a legtöbb poszt a Twitteren született (70,77%), valamint az Instagram (16,46%) és a Facebook (12,62%) mellett egyéb weboldalakon (0,15%) is találkozhatunk ezzel a taggel.

Kiemelendő, hogy a megosztó nemét tekintve a férfiak vannak többségben, ennek megoszlását a következő ábra mutatja:

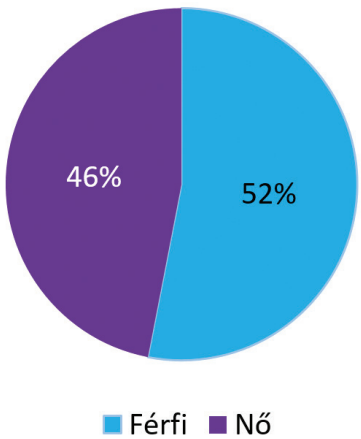
Jól látható, hogy a férfi tartalommegosztók vannak többségben, ennek oka valószínűsíthetően az, hogy az oldalt kezelő neme férfi.



6. ábra: Tartalmat megosztók nemi megoszlása
Forrás: a szerző szerkesztése a SentiOne alapján

A program további legfontosabb 25 kulcsszót is megjelenít az eredeti #womeninit tag keresése mellett. Így minél gyakoribb a megjelenés, valószínűsíthetően annál fontosabb. Ezeket a következő szófelhő tartalmazza.

Az ábra alapján elmondható, hogy a korábbi fejezetekben megjelenő kifejezésekkel gyakran találkozhatunk, úgymint a STEM, vagy éppen a kiberbiztonság, azaz a cybersecurity. Emellett a Microsoft vállalat vagy a női vezetők (womenleaders), vagy egyszerűen a nők a technológiai szektorban (womenintechnology) kéz a kézben járnak.



7. ábra: Kapcsolódó kifejezések
Forrás: SentiOne

Összegzés

Összegezve a leírtakat, elmondható, hogy egy igen szerteágazó és kihívásokkal teli területről van szó. Érdeklődéstől függően találhatunk műszaki vagy akár kevésbé műszaki munkaköröket is. A nemek arányát tekintve a nők továbbra is kisebb arányban vannak jelen az információbiztonság, kiberbiztonság területén. Több felmérésben, cikkben olvashatók ennek különböző okai, az egyik jellemző a nem azonos bérezési, juttatási körülmények.

Ebből fakadóan egy kérdőíves kutatás keretében vizsgáltam a hazai információbiztonsági, kiberbiztonsági szektorban dolgozók motivációját és tapasztalatait – többek között – ezzel a kérdéssel kapcsolatban. A kitöltők nemi megoszlásának aránya már jelzésértékű ebben az esetben – jelentősen kevesebb nő válaszadó volt. Az eredmények alapján elmondható, hogy a klaszterekbe való besorolást követően hozzáadott változók – válaszadó neme, előnyös lenne-e, ha több nő dolgozna a területen – azt mutatják, hogy akik elégedettek és hosszú távon biztosnak érzik a jelenlegi munkahelyüket, inkább támogatják a nők bevonását, mint azok, akik kevésbé elégedettek és biztosak a jelenlegi munkahelyükben. A bérezési, juttatási körülmények tekintetében elmondható, hogy a válaszadók meglátásai szerint a nők és a férfiak azonos díjazással

rendelkeznek – a kereszttábla-elemzés eredményei szerint. Mindemellett a terület választásának motivációját vizsgálva megfigyelhetők azonosságok az említett afrikai tanulmány kategorizálásával, azonban a társadalmi és családi befolyás a kitöltők esetében nem releváns tényező. A minta nagysága miatt általános következtetés nem vonható le, azonban további kiterjesztett kutatás során megfelelő alapként szolgálhat. Elmondható, hogy a közösségi média platformjainak is egyre növekvő szerepe van, amelyet a gyakran alkalmazott kapcsolattartás mellett akár toborzásra is használhatnak egyes vállalatok. Mindemellett a népszerűsítés, információátadás is megjelenik a különböző oldalakon. A trendek szorosan kapcsolódnak egymáshoz, így a #womeninit kulcsszó kapcsán találkozhatunk a #womenintehcnology vagy akár a #womenleaders kifejezésekkel is. A semleges értékeket leszámítva a megítélése inkább pozitív ezeknek a kifejezéseknek a platformokon, amelyek közül a legjellemzőbb a Twitter, mellette pedig az Instagram és a Facebook.

Irodalomjegyzék

A social listening alapjai [é. n.]. Online: https://sentione.com/hu/eroforrasok/social-listening

Ali-Hassan, Hossam – Nevo, Dorit – Wade, Michael (2015): Linking Dimensions of Social Media Use to Job Performance: The Role of Social Capital. *The Journal of Strategic Information Systems,* 24(2), 65–89. Online: https://doi.org/10.1016/j.jsis.2015.03.001

Bányász Péter – Krasznay Csaba – Tóth András (2021): A NATO kibervédelmi szakpolitikája. In Szenes Zoltán (szerk.): *A mai NATO: A szövetség helyzete és feladatai.* Budapest: HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 130–149.

Bányász Péter – Tóth András – László Gábor (2022): A koronavírus oltással kapcsolatos állampolgári attitűd vizsgálata szentimentanalízis segítségével. *Információs Társadalom,* 22(1), 99–125. Online: https://doi.org/10.22503/inftars.XXII.2022.1.6

Barker, William C. (2003): Guideline for Identifying an Information System as a National Security System. *National Institute of Standards and Technology,* 2003. augusztus. Online: https://doi.org/10.6028/NIST.SP.800-59 ; DOI: https://doi.org/10.6028/NIST.SP.800-59

BCS (2014): *Women in IT Survey.* Online: www.bcs.org/media/4446/women-it-survey.pdf

Bederna, Zsolt – Szádeczky, Tamás (2021): Modelling Computer Networks for Further Security Research. *Security and Defence Quarterly,* 36(4), 51–66. Online: https://doi.org/10.35467/sdq/141572

Cherdantseva, Yulia – Hilton, Jeremy (2014): Information Security and Information Assurance: Discussion about the Meaning, Scope, and Goals. In Portela, Irene Maria – Almeida, Fernando (szerk.): *Organizational, Legal, and Technological Dimensions of Information System Administration.* Hershey: IGI Global, 167–198. Online: https://doi.org/10.4018/978-1-4666-4526-4.ch010

Eurostat [é. n.]: *ICT Specialists in Employment.* Online: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment

Farkas Tibor (2023): A kommunikációs és információs rendszerek értelmezése napjainkban: Követelmények és kihívások. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban.* Budapest: Ludovika, 11–30.

Hámornik, Balázs Péter – Krasznay, Csaba (2017a): A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers. In Nicholson, D. (szerk.): *Advances in Human Factors in Cybersecurity.* [H. n.]: Springer, Cham. 224–236. Online: https://doi.org/10.1007/978-3-319-60585-2_21

Hámornik, Balázs Péter – Krasznay, Csaba (2017b): Prerequisites of Virtual Teamwork in Security Operations Centers: Knowledge, Skills, Abilities and Other Characteristics. *Academic And Applied Research In Military And Public Management Science,* 16(3), 73–92. Online: https://doi.org/10.32565/aarms.2017.3.5

Harpeet, Singh – Kamal, Roop (2019): Recruitment Practices in IT Sector: A Study of Employees Perspective. *Pramana Research Journal,* 9(1), 318–323.

Hughes, Matthew (2019): *Women Are Only 24% of the Infosec Workforce. Now Go Follow Them on Twitter.* Online: https://thenextweb.com/news/women-are-24-of-the-infosec-workforce-now-follow-some-of-them

Jose, Sajin – Asha, P. (2019): Innovation in Recruitment and Talent Acquisition: A Study on Technologies and Strategies Adopted for Talent Management in IT Sector. *International Journal Of Marketing & Human Resource Management,* 10(2), 1–8. Online: https://iaeme.com/MasterAdmin/Journal_uploads/IJMHRM/VOLUME_11_ISSUE_2/IJMHRM_11_02_002.pdf

Khi-négyzet-próba jelentése és alkalmazása az SPSS-ben [é. n.]. Online: https://spssabc.hu/ketvaltozos-elemzes/khi-negyzet-proba/

Krasznay Csaba (2017): A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. *Nemzet és Biztonság,* 10(3), 38–53.

Krasznay Csaba – Muha Lajos (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem.

Macnamara, Jim – Zerfass, Ansgar (2012): Social Media Communication in Organizations: The Challenges of Balancing Openness, Strategy, and Management. *International Journal of Strategic Communication,* 6(4), 287–308. Online: https://doi.org/10.1080/1553118X.2012.711402

Makola, Sizile – Kgosinyane, Esther (2020): How Women End Up in the Information Technology Sector: The Perspectives of South African Women. *Academy of Strategic Management Journal,* 19(4).

Mayer Annamária (2016): *A dendogram fogalma, jellemzői.* Online: https://spssabc.hu/diagram-keszitese/dendogram

Mitev, Ariel – Sajtos László (2007): *SPSS kutatási és adatelemzési kézikönyv.* Budapest: Alinea.

Muha Lajos (2008): Az informatikai biztonság egy lehetséges rendszertana. *Bolyai Szemle,* 17(4), 137–156.

Paulsen, Celia – Byers, Robert (2019): Glossary of Key Information Security Terms. *National Institute of Standards and Technology.* Online: https://doi.org/10.6028/NIST.IR.7298r3

SentiOne [é. n.]: *Tudásbázis.* Online: https://sentione.com/hu/tudasbazis

Spearman korreláció [é. n.]. Online: https://spssabc.hu/ketvaltozos-elemzes/spearman-korrelacio/
TÓTH András (2022): *A digitális állam információbiztonsági kihívásai.* Budapest: Ludovika.

Jogi forrás

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Online: https://njt.hu/jogszabaly/2013-1139-30-22.1

HADMÉRNÖK
VÉDELEMINFORMATIKA

18. évfolyam (2023) 4. szám 147–158.
DOI: 10.32567/hm.2023.4.10

Szeleczki Szilveszter[1]

A metaverzum értelmezése és katonai célú meghatározása 2. rész – rendszerszintű értelmezés[2]

Interpreting the Metaverse and Its Definition for Military Purposes Part 2 – System Interpretation

Absztrakt

Az infokommunikációs hálózatok fejlődését mi sem tükrözi jobban, mint azok sokrétű képességei. A katonai célú infokommunikációs kihívások közé sorolható a metaverzum kérdésköre, s vele aktuálissá vált a virtuális információs környezetekkel szemben támasztott kérdések megválaszolása. Az aktualitás megkérdőjelezhetetlen még akkor is, ha egy már a múltban is létező fogalomról van szó, a technológia jelenleg nem áll készen a kapcsolódó négydimenziós teret megjelenítő hálózatok megvalósítására. A katonai metaverzum egyértelműen sok kérdést felvet mind funkcionális, mind biztonsági szempontból. Célom a katonai metaverzum rendszerszintű értelmezése, a szükséges szemléletmóddal megvizsgálva annak főbb aspektusait. Az elvárható képességek megvalósítása érdekében szükségessé vált ezen infokommunikációs hálózat mélyebb tanulmányozása. A katonai metaverzum hálózatalapú rendszere speciális információs környezet elképzelését követeli meg.

Kulcsszavak: metaverzum, virtuális, infokommunikáció, hálózat, katonai

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtudományi Doktori Iskola, e-mail: Szeleczki.Szilveszter@uni-nke.hu

[2] Ez a publikáció a Kulturális és Innovációs Minisztérium Kooperatív Doktori Program doktori hallgatói ösztöndíj programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Abstract

The evolution of infocommunication networks is no better illustrated than their various capabilities. One of the challenges of infocommunications for military purposes is the issue of metaverse, and with it the need to answer the questions posed by virtual information environments. The relevance is clear even if it is a term that has already used in the past, the technology is now ready to implement networks that represent the associated four-dimensional space. The military metaverse clearly raises many questions, both from a functional and security point of view. My goal is to understand the military metaverse at a systems level, examining its main aspects with the necessary perspective. A deeper study of this infocommunication network has become essential in order to realise the expected capabilities. The network-based system of the military metaverse requires a specific information environment.

Keywords: metaverse, virtual, infocommunication, network, military

Bevezetés

Az infokommunikációs hálózatok kihívásainak vizsgálata egyértelműen aktuális kutatási területnek mondható.[3] A korszerűségre való törekvés megállíthatatlan, a csúcstechnológiákban rejlő lehetőségek feltárása is folyamatos. Manapság az egyik leginkább közkedvelt és széles körű lehetőséggel kecsegtető terület az immerzív technológiák[4] kutatása. Bárki, aki kicsit is érdeklődik ezen technológiák iránt, számos elméleti és gyakorlati orientáltságú szakirodalmat találhat. Mindez azon egyszerű oknál fogva lehetséges, mert ezen csúcstechnológiák társadalmunk számára mind civil, mind katonai célok megvalósítása vonatkozásában egyaránt relevánsak. A különböző szervezetek, óriási technológiai cégek mellett a magánszemélyek otthoni alkalmazása is szóba kerül a terület kapcsán. Természetesen a virtuális terek integrációjának számos funkcionális és biztonsági aspektusa létezik, amelyek aktuális, megválaszolandó kérdéseket vonnak maguk után. Az immerzív technológiák közül kiemelkedik a kibővített valóság, amely gyakorlatilag lefedi az ezen technológiákkal kapcsolatos sokrétű lehetőségeket.

Minden bizonnyal nem véletlen, hogy a manapság közismertnek tekinthető metaverzum lényegében egyenrangú a kibővített valóság képességi halmazával. Jómagam is érdeklődöm mind a kibővítettvalóság-technológia, mind pedig a metaverzumok koncepcionális kérdései iránt. Úgy vélem, ha a civil és katonai célok nyomán akarok foglalkozni a kutatási területtel, akkor a lehetséges fogalmi meghatározás mellett a metaverzum rendszerszintű értelmezése elengedhetetlen. Jelen publikációval célom a metaverzum mint egységes rendszer lehetséges alkotóelemeit és hálózatalapú szegmenseit feltárni. Úgy gondolom, hogy az alábbiakban felvetett kérdéseim is ezen

[3] Farkas 2023: 12–14.

[4] Szeleczki 2023b: 41. A *Directions in the Development of Virtual Reality and Its Military Applicability* című könyvem ezen oldalától ismertetem és részletezem az immerzív technológiák főbb típusait.

célokhoz kapcsolódnak. Ehhez részben felhasználom a már korábbi publikációmat,[5] amelyben a metaverzum fogalmi értelmezésével foglalkoztam. Emellett természetesen további szakirodalmat is felhasználok, amelyben a civil és a katonai alkalmazási lehetőségekre koncentrálok, immár a rendszer szintjén. Kiemelném Matthew Ball[6] munkásságát a témában, akinek sajátos nézetét leíró dokumentumai mindenképpen releváns szakmai anyagnak számítanak. A metaverzumok fejlesztése sokrétű követelményrendszer létrehozásával jár, amelynek eredményeképpen bonyolult, mégis hatékony infokommunikációs hálózat működtethető.

Véleményem szerint a digitális katonai koncepcionális kérdéseknek a metaverzumok fejlesztésében fontos szerepe van. A következőkben célom, hogy ennek jelentőségére felhívjam a figyelmet a kutatók, fejlesztők számára. A metaverzumok egyfajta információs rendszerként írhatók le, a rájuk speciálisan jellemző virtuális és valós terek általi információs környezeti fuzionálásával. Jómagam a metaverzum rendszerszintű értelmezésében gondolkodva a következő főbb kérdéskörökkel foglalkozom:

- A metaverzumoknak milyen egységes, általános alkotóelemei írhatók le?
- Meghatározható-e a metaverzumok felépítése, struktúrája?
- Mi alapján célszerű megkülönböztetni a metaverzumok hálózatos felépítését?
- Összehasonlítható-e valamilyen szempont szerint a civil és a katonai metaverzumok felépítése?

A rendszerszintű elképzelések főbb aspektusai

Lehetséges alkotóelemek nyomában

A metaverzum történeti előzményeivel, valamint lehetséges fogalmi meghatározásával már korábban foglalkoztam, amely vizsgálatok során arra jutottam, hogy nincsen egységesen elfogadott definíció. Többen foglalkoztak már a kérdéssel – közülük is kiemelném Matthew Ballt, akinek könyve is jelent meg a metaverzum témájában. A metaverzumok jövőre tekintő irányainak (mondhatni fejlesztési céljainak), valamint főbb követelményeinek vizsgálata során megalkottam a saját fogalmamat, amely szerint a metaverzum a következő:

„A valós tér virtuális elemekkel kibővített világa, melyben az emberek, a termékek, a szolgáltatások és egyéb tartalmak fizikai megjelenése mellett azok digitális reprezentációi is interakcióba lépnek egymással a mindennapokban, biztosítva ezáltal immerzív és más többdimenziós technológiák és platformok infokommunikációs hálózatokban történő alkalmazásának lehetőségét."[7]

A metaverzum kétséget kizáróan egyfajta információs környezet, amelyet lényeges és szükségszerű részletesebben kibontani. Mindez a könnyebb megértés és a hozzá

[5] Szeleczki 2023a. A publikáció a metaverzum fogalmi értelmezésével foglalkozik, amely egyúttal a rendszerben való gondolkodást és kapcsolódó vizsgálatot közvetlen megelőző kutatásom.

[6] Matthew Ball az Epyllion cég vezérigazgatója. A cég különböző befektetésekkel, tanácsadásokkal, többek között televíziós műsorok, filmek és videójátékok gyártásával foglalkozik.

[7] Szeleczki 2023a: 184.

köthető célok megvalósulása, továbbá a mindehhez tartozó technológiai fejlesztési lehetőségek pontosabb meghatározása érdekében is fontos. Ahogyan az 1. ábrán látható, a metaverzumnak hat főbb alkotóelemét határoztam meg. Az alkotóelemek meghatározásakor figyelembe vettem, hogy még nem volt kidolgozott hasonló felsorolható elemzés, és elkezdtem vizsgálni a főbb befolyásoló tényezőket, a függőségi viszonyokat a katonai metaverzum üzemeltetése kapcsán. Olyan kérdéseket tettem fel magamnak, mint például a kik, mit, hol, hogyan és mi alapján.

1. ábra: A metaverzum általános alkotóelemei
Forrás: a szerző szerkesztése

A metaverzum alkotóelemeinek kérdése összefügg a célok megvalósításához vezető lépésekkel, lényegi összetevőkkel. A metaverzum számos tekintetben visszavezethető az információ igényére, amelyet így az elsődleges alkotóelemnek tekintek. Az információk áramlását, az információcserét mindenképpen szükséges valamilyen szabályozás alá venni, amelyből kifolyólag úgy vélem, a következő fontos alkotóelem a szabályzói háttér (például nemzeti vagy szövetségi, EU vagy NATO által leírt szabályzók).[8] A szabályzók mellett természetesen szükséges a metaverzumhoz köthető technológiai háttér, amely szintén kétséget kizárólag az alkotóelemek közé sorolható. Az immerzív technológiák megítélésem szerint központi helyet foglalnak el a metaverzum elképzelésében.

Tovább haladva a célok megvalósulása mentén egyértelműen fontosak a kapcsolatok. Ezalatt nem csupán a gépi (hardveres és szoftveres kérdések és a kapcsolódó úgynevezett interoperabilitási megoldások tartoznak), hanem az emberi kapcsolatok (magánjellegű, szervezeti és állami szintű együttműködések) is egyaránt értendők.[9] A metaverzumok hálózatai különfélék, akár centralizáltak, akár decentralizáltak is lehetnek. A hálózatok létrehozásához a következő főbb alkotóelemként a mindezeket megvalósító fizikai egységet, az eszközöket nevezem meg. Az eszközök kapcsán például

[8] Tóth 2020: 310.
[9] Tóth 2021: 26.

nyilvánvalóan az immerzív technológiát megvalósító szemüvegek az elsődlegesek, de ugyanúgy fontosak a csatlakoztatott számítógépek vagy egyéb érzékelők (például kéz- vagy lábgesztusok, mozdulatok érzékelése) stb.

A metaverzum komplex rendszerében a kapcsolatokhoz hasonlóan a gépi és emberi entitásokat tudni kell azonosítani. Szükséges definiálni minden, különösen az információcserékben részt vevő entitást. A metaverzum alkotóelemeként tehát az entitásokat tartom még fontosnak felsorolni. Az alkotóelemek zárásaként kétséget kizárólag szót kell ejteni arról is, hogy a metaverzum hol is van jelen, azaz miként nevezhető annak környezete. A technológiáknak köszönhetően virtuális terek hozhatók létre, viszont ehhez elengedhetetlen az, hogy a valós, fizikai tér is igénybe legyen véve. Nagyszerű példa erre a kiterjesztettvalóság-technológia felhasználása.

A metaverzumok hálózatos felépítésének lehetséges elképzelése

Ahogy az a fogalmi meghatározásom kapcsán is olvasható, a metaverzumban a fizikai megjelenés mellett már a digitális reprezentációk is kapcsolatba léphetnek egymással. A hálózatos gondolkodásban fontos figyelembe venni, hogy a metaverzum nem tekinthető egy vállalatban eddig megszokott adatbázisnak, sokkal inkább egy komplex rendszerben működő entitások halmazának (legyen szó digitális avatárokról vagy létező személynevekről), számos kapcsolódási ponttal, funkcionális és biztonsági aspektussal. A metaverzumok fejlesztése nem véletlenül kapcsolódik rendkívül szorosan a kibővítettvalóság-technológiához. Ahogy egy kapcsolódó cég forrásában is írja: „Üdvözöljük a kibővített valóságban, a holnap metaverzumát alakító, konvergáló technológiák új határán."[10] A metaverzumok struktúrája meghatározható a kapcsolódó célok tekintetében, lehet például szervezeti és magánszemélyeket érintő hálózatokról is beszélni. Jómagam a hálózatok kiterjedése alapján tartom fontosnak a strukturális meghatározást, amely véleményem szerint nagyszerű kiindulási alapja a metaverzumokkal szembeni célok elméleti meghatározásához. A számítógépes hálózatok sémáját némileg követve, a következő főbb metaverzumokat határozom meg:

- személyi metaverzum;
- kis kiterjedésű metaverzum;
- közepes kiterjedésű metaverzum;
- nagy kiterjedésű metaverzum;
- globális metaverzum.

A személyi metaverzum az adott felhasználó közvetlen infokommunikációs hálózatát jelenti, amely a sajátos eszközeit, rendszerét tartalmazza, egyúttal önálló kibővített információs környezetként működik. A kis kiterjedésű metaverzumok vonatkozásában szóba jöhet a személyes metaverzumok összekapcsolása, ezzel kialakíthatók például lokális, otthoni hálózatok is. A kis kiterjedés alatt városon belüli hálózat értendő, amely épületeket, telephelyeket, különböző irodákat is magában foglalhat. A városokon túli hálózatokból építhető fel az úgynevezett közepes kiterjedésű metaverzum, amelyek

[10] KPMG 2022.

városok, sőt megyék infokommunikációs hálózatát tartalmazza. Ezen hálózattípusra lehet példa egy civil vállalkozás vagy akár egy katonai szervezet sajátos, országon belüli információs környezete. Egy adott állam vagy nagyobb szervezet sajátos célú fejlesztése lehet egy nagy kiterjedésű metaverzum, amely már országokat is összeköthet a sajátos célok elérése érdekében. Végezetül mindezen valós és virtuális tereket tartalmazó (a célok érdekében akár szuperszámítógépeket is felhasználó), fuzionált infokommunikációs hálózatokból épülhet fel a globális metaverzum, amely a világunkat ezen a technológiai területen összefoghatja. Globális szinten földrészek, kontinensek információs környezete értendő, amelyek bolygónk különböző, egymástól meglehetősen nagy távolságra lévő pontjait is összeköti.

Katonai rendszerszemlélet

A korábbiakban meghatározott hálózati elképzelésemből kifolyólag a katonai célra megvalósítható metaverzum egy adott helyet jelöl meg egy lehetséges globális metaverzum koncepciójában.[11] Ezt a metaverzumot a maga egyszerűségében katonai metaverzumnak nevezem, amely a sajátos infokommunikációs technológiai igényeknek megfelelően valósulhat meg. A korábban meghatározott metaverzum alkotóelemei katonai perspektívából is érvényesek, amelyek szükségesek a speciális célú, kibővített információs rendszer létrehozásához. A katonai metaverzumban minősített információk továbbítódnak az infokommunikációs hálózatokon, épp ezért ezen hálózatok funkcionális és biztonsági kérdésekben nyilvánvalóan bővelkednek. A katonai metaverzumok struktúrájában gondolkodva, hasonlóan az előzőekben történt elméleti megközelítéshez, a hálózati kiterjedésű besorolási lehetőségeit mindenképpen fontos kiinduló alapnak tekintem. A katonai metaverzum egy információs környezet, amelyet adott szervezet vonatkozásában műveleti és intézményi információs környezetre célszerű felosztani. Az információs környezet olyan környezet, amely magából az információból, az információt fogadó, feldolgozó és továbbító egyénekből, szervezetekből és rendszerekből, valamint abból a kognitív, virtuális és fizikai térből áll, amelyben mindez történik.[12] A katonai műveletek többféle szempont szerint felosztathatók,[13] ilyenek többek között a népszerű, művelet szintjeinek megfelelő felsorolás, amelyhez fontosnak tartom hozzáadni az egyéni, személyes felszereltségű katonai metaverzumot is. Mindezek alapján úgy vélem, hogy a katonai metaverzumok egy lehetséges hálózatalapú felosztása a következő:

- digitális katonai metaverzum (egyéni infokommunikációs hálózat);
- harcászati szintű katonai metaverzum (csoportos infokommunikációs hálózat);
- hadműveleti szintű katonai metaverzum (csoportos infokommunikációs hálózat);

[11] A metaverzumok hálózatos elképzelése többféle szervezetet is magában foglalhat, amely globálisan is kialakítható. A katonai szervezetek akár civil szervezetekkel együttműködve (betartva a kapcsolódó szabályokat) is kiépíthetnek globális méretű metaverzumot. A katonai célú metaverzumok egy adott helyet jelölhetnek meg egy, a társadalmunkat jelentős mértékben összefogó, az internethez hasonlítható hálózati elképzelésben, a világot összekötő globális metaverzum koncepciójában.

[12] NATO 2021: 68.

[13] Értve ezalatt a katonai műveletek rendszerét, amely kapcsán releváns Szendy István 2017-ben, *Hadügy és hadviselés* címmel megjelent könyvének 107. oldala.

- stratégiai szintű katonai metaverzum (csoportos infokommunikációs hálózat).

A digitális katonai metaverzum vonatkozásában egy önálló rendszert értek, amely az adott személy virtuális térrel kibővített egyéni információs környezetét jelenti. A további, már magasabb szintű struktúrákban egyre nagyobb jelentősége van a korábban általam meghatározott alkotóelemeknek, az információknak, a szabályzóknak, a technológiáknak, a kapcsolatoknak, az eszközöknek és az entitásoknak. Figyelembe véve a katonai vezetés és irányítás (C2[14]) rendszerét, információcsere szempontjából össze van kötve a vezető parancsnokkal, viszont önálló információs környezetet használ fel a parancs végrehajtása során.[15]

Ezek a rendszerek többféle feladat ellátását támogathatják a védelmi szektorban, amelyek minden esetben önálló alrendszerrel rendelkeznek speciális funkciókkal kiegészítve,[16] valamint kapcsolódnak a műveletek vezetését végrehajtó parancsnoki rendszerhez.[17] Onnantól kezdve, hogy több egyéni metaverzum össze van kapcsolva, szóba jöhet a legkisebb, harcászati szintű katonai metaverzum. A harcászatra jellemző paramétereknek és információcseréknek megfelelően ez a metaverzum már kiterjedésében, funkcionális és biztonsági vonatkozásokban is sokrétű. Ugyanez még inkább igaz a hadműveleti és különösen a stratégiai szintű katonai metaverzum elképzelésére.

A felsorolt metaverzumok egyre szélesebb infokommunikációs hálózatot jelentenek, s a korábban felvázolt alkotóelemek skálája is kiszélesedik. A katonai metaverzumok tehát érezhetően sokrétűek lehetnek, amelyekben a vezetés és irányításhoz tartozó releváns infokommunikációs képességek természetszerűleg kerülnek előtérbe a követelmények meghatározása vonatkozásában.

A katonai metaverzumok a műveletek főbb jellemzői alapján rendszerezhetők. Különböző szempontrendszerek szerint tehát kialakíthatók az egyes katonai metaverzumok képességei. Véleményem szerint itt jöhet szóba a katonai műveletek szintjein túl az azok jellegéből adódó szempontrendszer, amely szerint a következő képességcsoportok alakíthatók ki:

- harci erők metaverzumainak képességei;
- harci támogató erők metaverzumainak képességei;
- harci támogató kiszolgáló erők metaverzumainak képességei;
- különleges műveleti erők metaverzumainak képességei.[18]

A katonai metaverzumban nagyon fontos meghatározni a különböző katonai beosztásoknak megfelelő képességekkel szemben támasztott követelményeket. Nem véletlen, hogy a korábban általam a katonai metaverzum vonatkozásában meghatározott fogalomba is mindenképpen beillesztettem a kapcsolódó szegmenseket.

[14] Command and Control (C2).
[15] Farkas–Hronyecz 2017: 355.
[16] Farkas–Hronyecz 2016: 153–156.
[17] Farkas–Hronyecz 2015: 53–61.
[18] Szeleczki 2023b: 124. A *Directions in the Development of Virtual Reality and Its Military Applicability* című könyvem 124. oldalán szót ejtek az immerzív technológiák kapcsán létrehozható képességcsoportokról, amelyek a katonák feladatrendszere szerint is felosztható.

„A katonai metaverzum egy a civil szférától eltérő, speciális fejlesztési és üzemeltetési célokkal létrehozott, a valóságot virtuális térrel kibővített világ, amely többdimenziós intézményi és műveleti térben, a szervezet egészére kiterjedő infokommunikációs hálózatokban, digitális reprezentációk és interoperábilis információcserék által biztosít interakciós lehetőségeket a harcoló, a harci támogató, a harci kiszolgáló támogató, a különleges műveleti erők és egyéb honvédelmi alkalmazottak tevékenységeinek sikeres megvalósításához."[19]

Véleményem szerint a katonai metaverzumok alapkövei a katonák egyéni feladataikhoz köthető képességekben rejlik. Minden, akár műveleti területen, akár irodai környezetben végzett tevékenységekhez tartozó metaverzum az egyéni követelményrendszer meghatározásából indul ki. Kialakíthatók az adott szervezet nagyobb kiterjedésű, hálózatba kapcsolt metaverzumai is: ez egy globális méretű katonai metaverzum megvalósulását is eredményezheti.

Egy korábban publikált cikkemben már foglalkoztam a digitális katonákkal szemben támasztható főbb funkcionális követelményekkel, amelyek az alábbiak:

- helymeghatározó, célmegjelölő rendszer;
- digitális hang- és adatkommunikáció;
- vezetést és irányítást támogató rendszer;
- energiaellátó rendszer;
- szenzoros állapot felügyeleti rendszer;
- fegyverrendszer;
- egységes információs rendszer;
- modernegyenruha-megoldások.[20]

Itt kiemelném a szóban forgó immerzív technológiákat, amelyek több tekintetben is beleillenek a felsorolásba. Az említett képességcsoportokat egységes követelményrendszerben szükséges kidolgozni. A digitális katonai elképzelésekhez tartozó kibővített információs rendszer a szenzoros érzékeléstől kezdve a fegyverrendszeren át érinti a vezetés és irányítást is. A közös képességeken felül a katonai beosztásnak megfelelő egyéni (például harcoló erők esetében a lövészek vagy harci támogató erők esetében a felderítők), funkcionális és biztonsági követelményei is a katonai metaverzum megvalósításához szükséges specifikáció részét képezik.

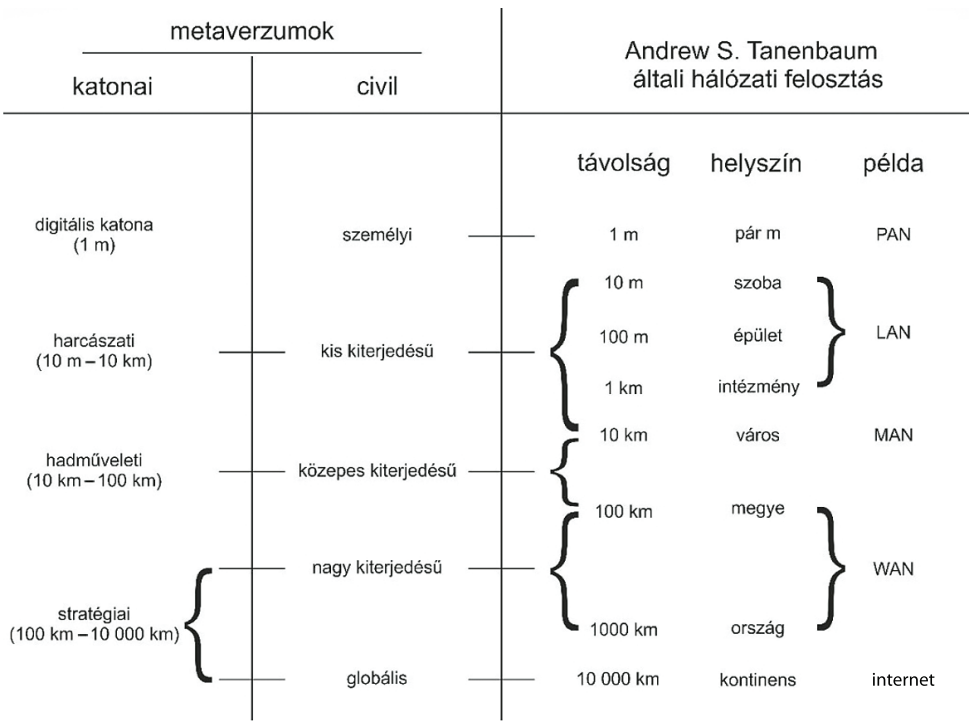
Civil és katonai metaverzumok hálózatos rendszerszemléletének logikai hasonulása

Meglátásom szerint a metaverzum civil és katonai rendszerszemlélete valamelyest logikailag összeköthető egymással, úgy is mondhatnám, hogy a kétféle struktúra felépítésének valamilyen formában hasonulni célszerű egymáshoz. Az előzőekben a hálózati megközelítés, azon belül is a kiterjedés szerinti csoportosítás alapján történt a metaverzumok rendszerszintű leírása. Mivel ugyanazon szempontrendszert

[19] Szeleczki 2023a: 185.
[20] Szeleczki 2020: 102.

használtam, így egyértelműen összehasonlítható a két rendszer. A katonai műveletek szintjeit és sokrétűségét figyelembe véve kissé képlékenyek a határok, de egy megközelítő elméleti behatárolás mindenképpen kezdeményezhető. A 2. ábrán látható az általam vélt civil és katonai metaverzumok hálózatalapú, elméleti megközelítésű logikai összekötése. Mindehhez felhasználtam Andrew S. Tanenbaum kapcsolódó, a témában alapműnek számító dokumentumát.[21]

Mindkét esetben a hálózat lehetséges méretét vettem figyelembe, amelyben a legkisebb a személyes hálózat. A civil oldalról meghatározott személyi metaverzum remekül illik az egyéni, digitális katonai elképzeléshez tartozó metaverzumhoz. A kis kiterjedésű metaverzumok, úgy vélem, közel állnak a legkisebb, harcászati szintű katonai műveletekhez. Abból indultam ki, hogy adott katonai erő harc során például egy városnyi területet könnyedén el is foglalhat. Harcászati szinten tehát olyan alapvető infokommunikációs hálózatról van szó, amely már jelentős katonai állomány közös információs környezetét teheti hatékonnyá, s amelyre a nagyobb struktúrák építhetők.



2. ábra: A civil és katonai metaverzumok méretbeli hasonulása
Forrás: a szerző szerkesztése

A katonai műveletek hadműveleti szintje minden bizonnyal a közepes kiterjedésű metaverzum hálózatához köthető, amely vonatkozásában városokról és vele több

[21] Tanenbaum 2011: 18.

tíz kilométernyi információs környezetről van szó. A hadászati vagy más nevén stratégiai szintű műveletek már kissé nehezen köthetők a civil metaverzumokhoz. Stratégiai szinten egyértelműen a nagy kiterjedésű metaverzumról lehet beszélni, fontos azonban e szint nagyságát a globális metaverzum vonatkozásában is elhelyezni. Ugyan az ábrán nem részleteztem, véleményem szerint a nagy kiterjedésű metaverzum összehasonlítható a nemzeti szinten folyó stratégiai műveletekkel, míg a globális metaverzum már a többnemzeti és szövetségi stratégiai műveletekkel vonható párhuzamba.

Összegzés

A metaverzumok struktúrája sokféleképpen meghatározható, amelyek közül jómagam a hálózatok kiterjedésének lehetőségeit vettem alapul. A metaverzumok fontos fejlesztési irányvonala a kapcsolódó infokommunikációs hálózat nagyságának tervezhetősége. A számítógépes hálózatokhoz hasonlóan tehát a metaverzumok struktúrája is behatárolható, még akkor is, ha kissé szokatlan, speciális módon is történik. A metaverzumok rendszerszintű értelmezése közben kulcsfontosságúvá vált a civil és katonai alkalmazás összehasonlító vizsgálata. Bizonyítottam, hogy a két fő szegmens hálózat alapján történő strukturális elképzelése összeköthető egymással. Legyen szó személyi vagy globális szinten értelmezett metaverzumról, meghatároztam annak civil és katonai célú hálózatának megfelelőjét. A korábban behatárolt, metaverzumok általánosnak ítélt alkotóelemei részletes kidolgozása által bármely metaverzum infokommunikációs hálózatának követelményrendszere leírható, legyen szó civil vagy katonai alkalmazásról.

Következtetések

A metaverzumhoz kapcsolódó követelmények a fogyasztói kör által pontosítást igényelnek. Robbanásszerű változás helyett szerintem folyamatos fejlődésre célszerű törekedni, sajátos célú metaverzumokban. Mindent összevetve a fejlesztések jelenlegi álláspontja szerint az elméletben elképzelhető, társadalmi szinten értelmezett globális metaverzum jelenleg nem létezik. A jövőben, úgy vélem, szükségessé válik valamilyen módszertan létrehozása a metaverzumok vonatkozásában. A katonai műveletek rendszeréből célszerű lehet alapul venni a műveletek jellegéből és a műveleti szintekből adódó, továbbá a haderőnemi és összhaderőnemi (beleértve a nemzeti, többnemzeti, szövetségi műveleteket is) feladatokból származó követelményrendszerek felállítását. A digitális katonai koncepciókhoz egyértelműen aktuálissá válik a kibővítettvalóság-technológia integrálása és vele a különböző harci, harci támogató, harci kiszolgáló támogató és a különleges műveleti erők kapcsolódó képességei. Az elvárt képességek, követelmények rendszerszintű meghatározása tehát a jelenkori katonai infokommunikációs kihívásai közé sorolandó!

Szükséges egyfajta keretrendszer felállítása annak érdekében, hogy a kibővített információs rendszerek és vele a metaverzumok fejlesztése is megkezdődhessenek. E célból a NATO kapcsolódó dokumentumában is napirendre tűzték a kibővített

technológia fejlesztését.[22] Mindezek példaként a szárazföldi erők metaverzuma rendszerszintű kidolgozásának remek alapkövei lehetnek. A katonai metaverzumok egyik legfőbb fejlesztési irányvonala szerintem a vezetési és irányítási rendszer megvalósítása. Mind civil mind katonai tekintetben célszerű a legkisebb hálózati szegmensből, az egyéni képességekből kiindulni, azt részletesen kidolgozni és fokozatosan nagyobb rendszert alkotni. A bevezetésben feltett kérdésekre válaszolva arra jutottam, hogy az alkotóelemek egyértelműen leírhatók, s vele a strukturális elképzelés is. A katonai metaverzumok hálózatát célszerű a civil életben bevált minták alapján felépíteni (lásd például Tanenbaum-féle internetfelosztást). A civil felhasználási célú metaverzum tehát egyértelműen összehasonlítható a katonai elképzelésekkel, amelyek közös metszete maga a kapcsolódó infokommunikációs hálózat, s a hozzá tartozó funkcionális és biztonsági szegmensek. A képességekkel szemben állítható követelményrendszer meghatározása kezdeti lépés a katonai metaverzum megvalósításában.

Irodalomjegyzék

Ball, Matthew (2020): *The Metaverse: What It Is, Where to Find it, and Who Will Build It.* Online: www.matthewball.vc/all/themetaverse

Ball, Matthew (2021): *Framework for the Metaverse.* Online: www.matthewball.vc/all/forwardtothemetaverseprimer

Ball, Matthew (2022): *The Metaverse: And How It Will Revolutionize Everything.* New York: WW Norton.

Farkas, Tibor – Hronyecz, Erika (2015): The Info-Communication System Requirements of the Deployable Rapid Diagnostic Laboratory Support 'Sampling Group' II. *AARMS,* 14(1), 53–61. Online: https://doi.org/10.32565/aarms.2015.1.5

Farkas, Tibor – Hronyecz, Erika (2016): Basic Information Needs in Disaster Situations (Capabilities and Requirements). In Bitay Enikő (szerk.): *A XXI. Fiatal Műszakiak Tudományos Ülésszaka előadásai.* Kolozsvár: Erdélyi Múzeum Egyesület, 153–156.

Farkas, Tibor – Hronyecz, Erika (2017): Info-Communication Areas of Modernizing Field C2 Systems and Command Posts in the interest of Successful Home Defense- Peace Operations- and Disaster-Management Tasks. In *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY).* Subotica, Serbia, 000353–000358. Online: https://doi.org/10.1109/SISY.2017.8080582

Farkas Tibor (2023): A kommunikációs és információs rendszerek értelmezése napjainkban: Követelmények és kihívások. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban*. Budapest: Ludovika, 11–30.

KPMG (2022): *The Future of the Metaverse and Extended Reality.* Online: https://kpmg.com/th/en/home/insights/2022/04/the-future-of-the-metaverse.html

NATO (2015): *Allied Joint Doctrine for Information Operations.* AJP-3.10.

NATO (2020): *Glossary of Abbreviations Used in NATO Documents and Publications.* AAP-15.

NATO (2021): *Glossary of Terms and Definitions.* AAP-06.

[22] NATO 2022: 45.

NATO (2022): *2022 Collaborative Programme of Work.* NATO Science & Technology Organization.

Pierpont, Morgan John (2022): *Opportunities in the Metaverse. How Businesses Can Explore the Metaverse and Navigate the Hype vs. Reality.* Online: www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf

Szeleczki, Szilveszter (2020): Outlining a Set of Theory-based Requirements for the Future Digital Soldier. *AARMS,* 19(1), 95–108. Online: https://doi.org/10.32565/aarms.2020.1.8

Szeleczki Szilveszter (2023a): A metaverzum értelmezése és katonai célú meghatározása. I. rész.: fogalmi-szintű értelmezés, *Hadmérnök,* 18(3), 177-187. Online: https://doi.org/10.32567/hm.2023.3.12

Szeleczki, Szilveszter (2023b): *Directions in the Development of Virtual Reality and Its Military Applicability.* Budapest: Ludovika.

Szendy István (2017): *Hadügy és hadviselés.* Budapest: Dialóg Campus.

Tanenbaum, S. Andrew (2011): *Computer Networks.* Boston: Prentice Hall.

Tóth, András (2020): Information-Sharing Challenges and Issues in Multinational Operations, Part 1. *Land Forces Academy Review,* 25(4), 307–316. Online: https://doi.org/10.2478/raft-2020-0037

Tóth, András (2021): Information-Sharing Challenges and Issues in Multinational Operations. Part 2. *Land Forces Academy Review,* 26(1), 22–30 (2021) Online: https://doi.org/10.2478/raft-2021-0004

HADMÉRNÖK
FÓRUM
18. évfolyam (2023) 4. szám 159–175.
DOI: 10.32567/hm.2023.4.11

Molnár Ákos Ádám[1]

Az álhírekkel kapcsolatos informálás és az oltakozás közötti összefüggések empirikus vizsgálata

Empirical Investigation of the Relationship Between Fake News Information and Vaccination

Absztrakt

2019. decemberben Vuhanban jelent meg a napjainkra már mindenki által ismert és azóta világjárvánnyá nyilvánított Covid–19. A vírussal együtt azonban felerősödtek az álhírek és az ezzel kapcsolatos dezinformálás. Az álhírek és azok terjedése több csatornán is meg tud valósulni, azonban napjainkban ez a legerőteljesebben az online térben történik. 2020 tavaszán a World Health Organization az „infodemic" kifejezéssel, azaz amikor túl sok információ, köztük rengeteg megtévesztő jelenik meg egy járvánnyal kapcsolatban, mutatott rá, hogy nemcsak a vírus, de a vele kapcsolatos dezinformáció, vagyis félreinformálás is ugyanolyan mértékben terjed a világon. Jelenleg még mindig ebben a korszakban élünk, a „post truth" árnyékában, amikor a különböző híreket gyakrabban hisszük el az érzelmi töltöttségük alapján, mintsem valóságtartalmuk vagy forrásuk alapján, jelentősen befolyásolva a társadalom informáltságát. Kutatásom fő célja a koronavírussal kapcsolatos álhírek és érzelmek vizsgálata. Ezen belül az álhírek fajtáit, terjedését és hallgatóságra tett hatásait vizsgáltam. Online felületeken végzett kulcsszóelemzést alkalmazva az álhírek terjedését, annak ütemét és miértjét kutattam. Továbbá kérdőíves elemzést alkalmazva vizsgáltam a világjárvánnyal kapcsolatos álhírek elfogadását, illetve az aggodalmat, fenyegetettséget és fogékonyságot – utóbbi hármat összesítve észlelések néven elemeztem. A kapott adatokat később különböző statisztikai módszerekkel vizsgáltam az IBM SPSS nevű programban. Az adatok alapján megállapítottam, hogy a vakcinákkal kapcsolatos álhírek kivételével, azok a Covid–19-cel kapcsolatos álhírek, amelyek a vírus megjelenésekor voltak

[1] Hallgató, Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Államtudományi Szak, e-mail: molnar.akos.adam@uni-nke.hu

a legnépszerűbbek, az első hullám idején voltak a legelterjedtebbek, szemben a többivel. Bebizonyítottam, hogy a vírus ellen megalkotott ellenanyagok megjelenésével és tömeges használatával az álhírek online megjelenése ismét megerősödött. Statisztikai elemzés során bebizonyítottam, hogy az álhírekben való hiszékenység alapján képzett csoportok összefüggést mutatnak a vírussal kapcsolatos érzékeléseikkel. Megállapítottam, hogy a különböző álhírekre adott válaszok összefüggenek az adott személyek oltakozási hajlandóságával.

Kulcsszavak: koronavírus, kérdőíves felmérés, Covid–19, oltás

Abstract

The well-known Covid-19 virus emerged in Wuhan, a province of China, in December 2019 and has since been declared a pandemic. World Health Organization used the term „infodemic" in the spring of 2020, which means too much information, including a lot of misinformation, is published about an epidemic, to point out that not only the virus but also the disinformation about it is spreading around the world at the same rate. We are still living in this era, in the shadow of „post-truth", where news is more often believed on the basis of its emotional content than its veracity or source, significantly affecting the information of society. The main aim of my research is to explore the fake news and emotions related to the crown virus. In this context, I investigated the types and spread of fake news and the impact on audience. Using a keyword analysis on online platforms, I investigated the spread of fake news, its pace and why. A survey was launched for exploring thebeliefs as well as concerns, threats and susceptibility to pseudo-news related to pandemics. The latter three was analysed collectively as perceptions. The data obtained were later analysed using various statistical methods in the IBM SPSS program. Based on the data, I found that, except for vaccine-related pseudo-news, the Covid-19-related pseudo-news that were the most popular at the time of the virus' release was the most prevalent during the first wave, compared to the others. I coulddemonstrate that with the emergence and mass use of antiviral antidotes to the virus, the online emergence of fake coronavirus news has been reinvigorated. In a statistical analysis, I show that groups formed based on the beliefs in fake news are correlated with their perceptions of the virus. I found that responses to different pseudo-news are associated with individuals' propensity to vaccinate.

Keywords: coronavirus, survey, covid–19, vaccination

Bevezetés

2019 decemberében Kína egyik városában, Vuhanban felbukkant a mai napig mindenki által ismert és azóta világjárvánnyá nyilvánított Covid–19. A vírus nyomán azonban az álhírek és a dezinformációk is terjedni kezdtek. Ezek különösen hatékonyan terjednek az online térben, amely lebontja a határokat és lehetővé teszi, hogy szinte bármilyen információ tömegeket érjen el napok vagy akár órák alatt. Jelenleg a világ még mindig a pandémia árnyékában él, és az „infodemic" kifejezéssel vált világossá, hogy a járványhoz kapcsolódó dezinformáció éppolyan gyorsan terjed, mint maga

a vírus. Az álhírek terjedése komoly károkat okozhat, történjen az közvetlen vagy közvetett módon.[2] Közvetlenül vezethet például olyan esetekhez, mint a „pizzagate" vagy az 5G-s rádiótornyok lerombolása, de közvetve akár tragikus következményekkel is járhat, például az oltások elmulasztása és az ebből fakadó következmények.[3] Az álhírek miatt sokan a legelemibb tényeket is kétségbe vonják, ami gyakran eredményezi, hogy nem tesznek eleget állampolgári kötelességeiknek, és olyan cselekedetekre buzdítanak másokat, amelyek megzavarják a társadalmi rendet.

Az álhírek terjedésének megállítása jelentős emberi, technikai és pénzügyi forrásokat igényel.[4] Az információs technológia nyújtotta lehetőségek segíthetik a védekezést, például kontaktkövetésekkel, de kockázatot is jelenthetnek.[5] A dezinformációk különösen komoly problémát jelentenek a vírus ellen kifejlesztett védőoltások megjelenésével.[6] Ezért kiemelten fontos a helyes tájékoztatás és az álhírek megfékezése, hogy hatékonyan kezeljük a járványt és minimalizáljuk a károkat, amelyeket a dezinformáció okozhat a társadalomban. A dolgozatomban kérdőív alapján tanulmányozom a kitöltők járvánnyal kapcsolatos tájékozottságát és érzelmeiket, továbbá azt, hogy a különböző álhírek milyen irányban befolyásolják az oltakozási hajlandóságot. Ennek vizsgálatához a következő hipotéziseket fogalmaztam meg:

H1: Az álhírekre vonatkozó kérdésekre adott válaszok alapján képzett klaszterek szignifikáns összefüggést mutatnak az aggodalom, fenyegetés és fogékonyság kérdéseiben.

H2: Az általam vizsgált álhírekre adott válaszok összefüggenek az adott személy oltakozási hajlandóságával.

Kérdőíves felmérés bemutatása

Kérdőívem az álhírek és az oltakozási hajlandóság között keres összefüggést. Több nemzetközi szakirodalom áttekintése alapján választottam ki Ahmed Naoras Bitar és szerzőtársainak kutatását, amelyet reprodukáltam, mégpedig azért, mert a hipotéziseim vizsgálatához megfelelő módszertant és kérdéseket használt, továbbá jó alapot nyújtott a járvánnyal kapcsolatos kérdőívem kidolgozásához.[7] A kérdéseket átfogalmaztam, több helyen módosítottam. Ennek oka, hogy az eredeti kérdőív még a védőoltások megjelenése előtt készült, és 2020. április 12-e és 26-a között töltették ki a jemeni lakossággal. Ezzel szemben az első oltás csak 2020. december 8-án történt meg, míg a tömeges oltakozások csak 2021 első harmadában indultak el.[8] A második ok a változtatásra a jemeni és a magyar kulturális különbségekben keresendő: míg Jemenben a *katcserjét* a lakosság nagy része fogyasztja különböző addiktív mellékhatásai miatt, addig idehaza a lakosság jelentős része még csak hallani sem hallott róla.[9]

[2] Farkas 2023; Bányász 2019.
[3] Bányász 2022; Bányász 2023.
[4] Ináncsi–Farkas 2022.
[5] Németh–Magyar 2020.
[6] Bányász 2022.
[7] Bitar et al. 2021.
[8] *Google adatvédelmi irányelvek* é. n.
[9] Annoni Manghi 2011.

Jemenben jelentős társadalmi probléma a szer fogyasztása az addiktív hatásai és egyéb káros mellékhatási miatt.

A kérdőívvel azt vizsgáltam, hogy az oltakozási hajlandóság kapcsolatban áll-e a vizsgált értékek bármelyikével, mint demográfiai adatok, Covid–19-cel kapcsolatos tájékozottság és félreinformáltság. A kérdőív kitöltése anonim módon történt a Google jelenleg hatályos (2021. július 1.) adatvédelmi szabályai szerint.[10]

A kérdőívemet összesen 202 ember töltötte ki 2021. szeptember 7-e és 2021. szeptember 16-a között. A kérdőívet a Google Form szolgáltatással készítettem és a Facebook különböző platformjain osztottam meg.

A kérdőív szerkezete és az elemzés módszerei

A kérdőív szerkezete

A kérdőív több részből épül fel. Első részben a demográfiai adatokat vizsgáltam. Ilyen adatok voltak a nem, életkor, iskolai végzettség, lakhely, rendelkezik-e egészségbiztosítással, mennyi a havi nettó jövedelme, milyen a kapcsolati státusza, illetve, hogy szenved-e bármilyen krónikus betegségben.

A második szekcióban az álhírekkel kapcsolatos ismereteiket vizsgáltam hét darab álhír állításával. Ezekre az állításokra egy ötös skálán tudtak válaszolni, egyáltalán nem ért egyet, nem ért egyet, részben egyetért, egyetért és teljes mértékben egyetért válaszok közül válogatva. A válaszlehetőségeket kitáblázva majd 1-től 5-ig számokat rendelve hozzájuk, minden kitöltőnél kaptam egy eredményt 7 és 35 között. Az SPSS program segítségével mediánt alkalmazva a skálán 1–19-ig pontszámot kapó emberek jól informáltnak számítanak a Covid–19-cel kapcsolatos álhírekkel kapcsolatban, míg 19-es pontszám felettieket a félreinformált személyek táborába soroltam.

A harmadik szekció a Covid–19-cel kapcsolatos észlelések volt. Ezt a fejezetet további három részre osztottam, ezekre a kérdésekre egy négyes skálán tudtak válaszokat megadni. Az első rész az észlelt fogékonyságot vizsgálja, hogy mennyi esélyt lát rá, hogy a járvány ismét elkezd terjedni, vagy hogy egy közeli ismerőse elkapná a közeljövőben. Ebben a részben négy kérdésre összesen 4 és 16 között lehetett pontot elérni. Második része a fejezetnek az észlelt fenyegetés, amelynek lényege megtudni, hogy a kitöltő mennyire tartja veszélyesnek a járványt magára és környezetére.

A kérdőív utolsó részében az észlelt aggodalmat vizsgálva kutattam a válaszadó aggodalmát a járvánnyal kapcsolatban. Utóbbi két szekcióban 5-5 kérdés alapján négy válaszlehetőségből összesen 5 és 20 pont között tudtak elérni a kitöltők. Az észlelések című rész összpontjait összesítve szintén az SPSS program használatával mediánt alkalmazva osztottam fel a megkérdezetteket, a 29 pont alatt végzett személyek az alacsony érzékelési, míg a 29 pontot vagy többet elérő személyek a magasabb érzékelési csoportba tartoznak.

[10] *Google adatvédelmi irányelvek* é. n.

Az elemzés során használt statisztikai eljárások

A kérdőívemre kapott válaszokat először Excel-táblázatokban összegeztem és kódoltam. Az adatok elemzését az IBM SPSS statisztikai programcsomag segítségével végeztem el, majd az eredményekből a dolgozatban bemutatott diagramokat Excel segítségével készítettem el. Az SPSS-ben lefuttatott elemzések során elsősorban Sajtos László és Mitev Ariel[11] útmutatása alapján jártam el.

A szoftverben a különböző válaszokhoz különböző számkódokat párosítottam, a szoftver gördülékenysége érdekében (például nő = 1, férfi = 2), majd a változókat csoportosítottam, attól függően, hogy azok nominálisak, ordinálisak vagy intervallum-alapúak. Nominális skála esetén a válaszok között nincs értékváltozás (például nem, nemzetiség), ordinális skála esetében van rangsor a válaszok tekintetében, azonban nem tudni, mekkora (például egy betegség előrehaladtának mérése). Intervallum-skáláról, pedig akkor beszélhetünk, ha az értékek közti különbséget tudjuk értelmezni is (például testmagasság, hőmérséklet).[12]

A szoftver ezeket a bonyolult matematikai módszereket magától futtatja le, nekünk csak a megfelelő elemeket kell kijelölni hozzá,[13] az eredmények értelmezhetőségének biztosítása azonban megköveteli az adatok jellegéhez igazodó eljárás megválasztását. Az alkalmazott eljárások a következők:

A *kereszttábla* egy adattáblázat, ahol az adatokat sorokban és oszlopokban egymással összevetve egyesével tudtam megvizsgálni a különböző eredményeket. A két változó közti összefüggések vizsgálata azonban csak százalék- és számértékeket ad meg. A kereszttábla-elemzéshez a szignifikanciaszint meghatározásához *khi-négyzet próbát* alkalmaztam. A próba során kapjuk meg a *szignifikanciaszint* értékét. Ha ez az érték 0,05 alá esik ($s < 0,05$), akkor beszélhetünk szignifikáns összefüggésről, tehát van kapcsolat két változó között. Ugyanakkor, ha ez a szám egyenlő vagy nagyobb, mint 0,05 ($s = 0,05$ vagy $s > 0,05$), akkor nem beszélhetünk szignifikáns összefüggésről, tehát megállapítjuk, hogy nincs, vagy csak véletlenszerű a kapcsolat a változók között. Fontos kitétel ugyanakkor, hogy a kereszttábla mátrixának celláiban 5-nél több értéknek kell lennie, amennyiben a cellák minimum 20%-ában a mennyiségre utaló adatok nem érik el az 5 darab/főt, akkor a khi-négyzet próba adatait nem vehetjük figyelembe. A kereszttábla-elemzés során kiszámítottam a *Cramer's V mutató* értékét is, ami a legmegbízhatóbb mutató a szignifikanciaszint erősségének vizsgálatára. A teszt megmutatja, milyen erős két változó közötti szignifikáns kapcsolat. Az értéke 0 és 1 között terjedhet, amennyiben az értéke 0,5 alatti, akkor gyenge kapcsolatról beszélhetünk, 0,5-ös értéknél közepes erősségű kapcsolatról, míg 0,5 és 1 között erős kapcsolatról.[14]

Kruskal–Wallis-teszt segítségével vizsgálatam különböző csoportképző ismérvek szerinti különbözőségeket, Likert-skálán mért változók esetében. A Likert-skálák az egyén attitűdjét vizsgálják egy kérdés kapcsán, s ezt az attitűdöt később számértékkel

[11] Sajtos–Mitev 2007.
[12] Sajtos–Mitev 2007.
[13] Csallner é. n.
[14] Sajtos–Mitev 2007; Csallner é. n.

láttam el, a mérés lefuttatása érdekében.[15] Az elemzés során két dolgot vizsgáltam. Egyrészt a csoportok és változók közötti szignifikanciaszintet, másrészt a *rangszámok átlagait.* A rangszámátlagok azt mutatják meg, hogy a csoporthoz való tartozás milyen magatartást mutat a vizsgált kérdések tekintetében (minél magasabb, annál inkább értenek egyet az adott kérdéssel a csoport tagjai).[16]

A vélemények és az eredmények további csoportosításához *klaszterelemzést* alkalmaztam. A csoportok számát *Ward-féle eljárással* határoztam meg, így olyan csoportokat tudtam elkülöníteni, amelyek belső szóródása a legkisebb. A klaszterelemzés során különböző homogén csoportokat hoztam létre az elemzésbe bevont kérdések és az azokra adott válaszok alapján.[17] Ezeket a csoportokat azonban a Kruskal–Wallis-teszt során elvégzett egyéb változókkal való összevetés után tudtam elnevezni a kapott rangátlagok segítségével (például jól informáltak, kevésbé informáltak stb.). Az elemzés során az elnevezett csoportokat vizsgáltam tovább egyéb kérdésekre adott válaszokkal és demográfiai adatokkal.[18]

A kérdőíves felmérés eredményei

Ahogy az első táblázaton látható, a kitöltők több mint fele (64,4%) nő volt. A válaszadók 76,7%-a 16 és 24 éves kor közötti, míg 9,9%-uk 25 és 34 éves, a maradék 13,4% 35 éves kor felett van. Iskolai végzettség alapján a mintaalanyok 67,3%-a rendelkezik középfokú végzettséggel, 10,4%-uk általános iskolás bizonyítvánnyal és csupán a kitöltők 22,3%-nak van felsőfokú végzettsége. A településforma megoszlását figyelembe véve 43,1% lakik életvitelszerűen a fővárosban, 31,7% városokban, 12,9% megyei jogú városban és 12,4% községekben. A válaszadók továbbá 63,4%-a egyedülálló, özvegy vagy elvált, és 55%-nak 80 000 forint alatt van a havi nettó bevétele. A megkérdezettek 88,1%-a nem szenved semmilyen krónikus betegségben, továbbá 86,6%-uk be van oltva valamilyen Covid–19 elleni védőoltással. A megkérdezettek 43,1%-a fizetne nagyjából ötezer forintot egy Covid–19 elleni szérumért, míg 39,1%-uk nem, 17,8% nem tudja. Ezen számok alapján a kérdőívet kitöltő személyek oltottsági szintje közel 40%-ot esne, ha ötezer forintba kerülne és nem ingyenes volna.

Khi-négyzet-elemzés során, összevetve a férfiak és nők válaszait, szignifikáns összefüggés jelent meg (s = 0,017) a nemek közt abban a tekintetben, hogy fizetne-e egy nagyjából ötezer forintos vakcináért, ugyanebben az esetben a kapcsolati státusz is összefüggést mutat (s = 0,070). Ezen eredmények alapján, tehát a nem és a kapcsolati státusz olyan változók, amelyek befolyásolják a fizetős vakcinára feltett kérdések válaszait. A Cramer's V mutató megfigyelt értéke azonban 0,201 és 0,162, ami alapján gyenge az összefüggés az értékek között. Ugyanakkor, az életkor (s = 0,431), iskolázottság (s = 0,866), lakhely (s = 0,949), jövedelem (s = 0,377) és a krónikus betegségben szenvedők (s = 0,297) esetében már nem beszélhetünk szignifikáns

[15] Mayer 2018.
[16] Statistics é. n.
[17] Sajtos–Mitev 2007.
[18] Sajtos–Mitev 2007.

összefüggésről, mivel a kapott szignifikanciaértékek 0,05 alá esnek. A kérdőív első részére adott válaszokat az 1. táblázat jól mutatja.

1. táblázat: A kérdőívet kitöltők demográfiai adatai

		Fő	Megoszlás
Nem	nő	130	64,4%
	férfi	72	35,6%
Életkor	16–24	155	76,7%
	25–34	20	9,9%
	35 vagy idősebb	15	7,4%
Iskolai végzettség	általános iskolai bizonyítvány	21	10,4%
	középfokú végzettség	136	67,3%
	felsőfokú végzettség	45	22,3%
Lakóhely	főváros	87	43,1%
	város	64	31,7%
	község	25	12,4%
	megyei jogú város	26	12,9%
Kapcsolati státusz	kapcsolatban van	74	36,6%
	egyedülálló	128	63,4%
Havi nettó jövedelem	80 ezer forint alatt	111	55,0%
	80 ezer forint felett	91	45,0%
Krónikus betegség	Igen	24	11,9%
	Nem	178	88,1%
Covid–19-védőoltással rendelkezik	Igen	175	86,6%
	Nem	27	13,4%

Forrás: a szerző szerkesztése

A második fejezetben a kitöltők Covid–19-cel kapcsolatos informáltságukat elemeztem (lásd 2. táblázat). A hét kérdésre az „egyáltalán nem ért egyet" értéktől a „teljes mértékben egyetért" értékig lehetett választani. A megkérdezettek közel fele (49,7%) részben vagy teljesen egyetért azzal az állítással, hogy a Covid–19 vírus egy emberek által alkotott vírus, amely a gyógyszeripari cégek pénzügyi növekedését segíti elő. Ennél a számnál magasabb eredményt ért el a következő állítás, miszerint a Covid–19 egy ember által alkotott biológiai fegyver. Ezzel az állítással a megkérdezettek több mint a fele, 118 fő valamennyire egyetért, a megkérdezettek 10,9%-a (22 fő) pedig teljes mértékben egyetért. A következő két kérdésre, miszerint a vírus nem terjed át melegebb éghajlatokra és a gyerekek nem tudják elkapni a vírust, a megkérdezettek majdnem teljes része nem ért egyet valamilyen formában, 91,6%-kal és 92,5%-kal. A tesztet kitöltők továbbá kevesebb mint egyharmada (63 fő) hiszi azt, hogy az antibiotikumok

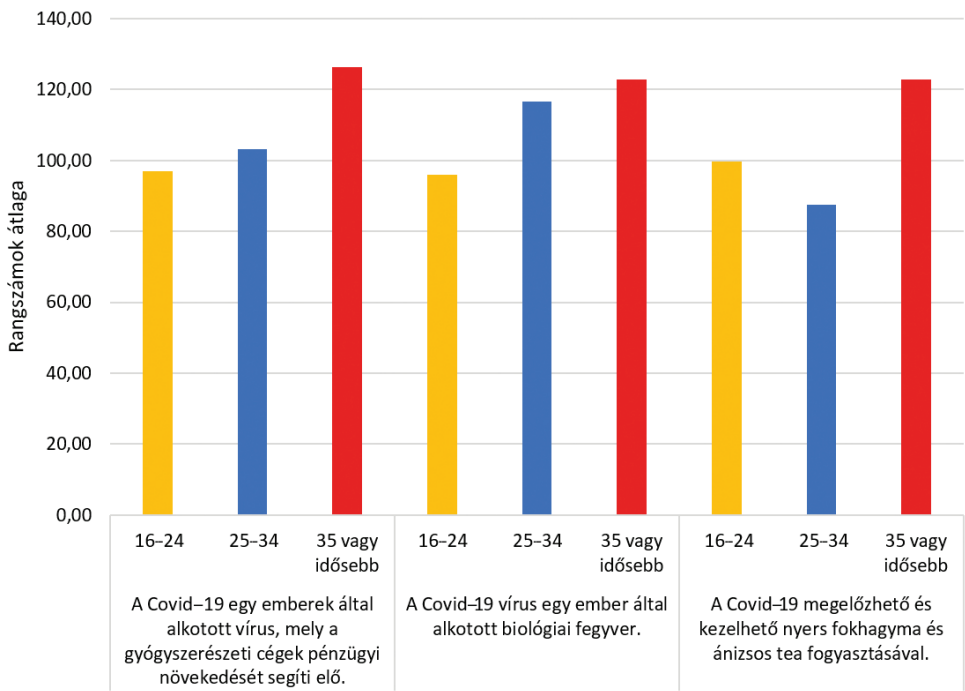
hatásosak a Covid–19 vírus ellen. Ezenfelül az utolsó két kérdésre adott válaszok alapján a kitöltők szintén megközelítőleg 90%-os arányban cáfolták, hogy az ánizsos tea és nyers fokhagyma fogyasztása hatásos lenne a Covid–19 ellen, vagy azt, hogy az emberek legnagyobb része, aki elkapja, bele is hal a vírusba. Ezen adatok alapján kimondhatjuk, hogy a megkérdezettek közel 90%-a jól informált a koronavírussal kapcsolatban (190 fő), míg összesen 12 főről beszélhetünk csak, akik hajlamosabbak a Covid–19-cel kapcsolatos álhíreket elhinni.

2. táblázat: A kitöltők álhírekkel kapcsolatos válaszai

Álhírekkel kapcsolatos egyetértés	**Egyáltalán nem ért egyet**		**Nem ért egyet**		**Részben egyetért**		**Egyetért**		**Teljes mértékben egyetért**	
A Covid–19 egy emberek által alkotott vírus, amely a gyógyszerészeti cégek pénzügyi növekedését segíti elő.	55 fő	27,2%	46 fő	22,8%	65 fő	32,2%	23 fő	11,4%	13 fő	6,4%
A Covid–19 vírus egy ember által alkotott biológiai fegyver.	50 fő	24,8%	34 fő	16,8%	64 fő	31,7%	32 fő	15,8%	22 fő	10,9%
A Covid–19 vírus nem tud átterjedni a melegebb éghajlatú területekre.	115 fő	56,9%	70 fő	34,7%	13 fő	6,4%	1 fő	0,5%	3 fő	1,5%
A gyerekek nem tudják elkapni a Covid–19-et.	132 fő	65,3%	55 fő	27,2%	9 fő	4,5%	5 fő	2,5%	1 fő	0,5%
Az antibiotikum hatásos a Covid–19 megelőzésében és kezelésében.	72 fő	35,6%	67 fő	33,2%	51 fő	25,2%	12 fő	5,9%	0 fő	0,0%
A Covid–19 megelőzhető és kezelhető nyers fokhagyma és ánizsos tea fogyasztásával.	122 fő	60,4%	54 fő	26,7%	24 fő	11,9%	1 fő	0,5%	1 fő	0,5%
A legtöbb ember, aki elkapja a Covid–19 vírust, bele is hal.	110 fő	54,5%	70 fő	34,7%	16 fő	7,9%	5 fő	2,5%	1 fő	0,5%

Forrás: a szerző szerkesztése

A Kruskal–Wallis-tesztet használva az álhírekre kapott eredményekre és az életkor vizsgálatánál megállapítható, hogy több kérdésnél is mérvadó, hogy az adott személyek mely korosztályba tartoznak. Az első álhírre adott válaszok alapján 0,045-ös szignifikanciaszint mellett megállapítható, a rangátlagadatokat megfigyelve, hogy a korosztályok felfelé haladtával egyre magasabbak a kapott értékek. A második kérdésre adott válaszok alapján szintén szignifikáns összefüggésekről beszélhetünk (s = 0,34), szintén a korosztály felfelé haladtával emelkedve a rangátlagokat. Ugyanakkor a harmadik szignifikáns állításnál, miszerint a Covid–19 megelőzhető és kezelhető nyers fokhagyma és ánizsos tea fogyasztásával (s = 0,040), ez már nem mondható el, mivel a 25 és 34 éves kor közöttiek rangátlaga alacsonyabb, mint a fiatalabb korosztályé. Ezen adatok függvényében azonban kimondható, hogy az alábbi kérdéseknél a 35 év vagy afeletti csoport rangátlaga a legmagasabb, tehát ők értenek legnagyobb mértékben egyet az álhírekkel a három vizsgált korcsoport közül (1. ábra).



1. ábra: Életkor és az álhírekkel kapcsolatos hiszékenység vizsgálata
Forrás: a szerző szerkesztése

A harmadik táblázat mutatja, hogy külön kérdéscsoporttal vizsgáltam részben a vírussal kapcsolatos különböző magatartásokat. Az észlelt fogékonyság alapján a megkérdezettek 59,4%-a nem lát rá esélyt, hogy a közeljövőben elkapná a koronavírust, míg szintén 52,5% nem látja valószínűnek, hogy egy rokona elkapná. Ugyanakkor, a kitöltők 79,2 és 88,1%-a hiszi, hogy a közeljövőben egy újabb, koronavírushoz köthető járvány

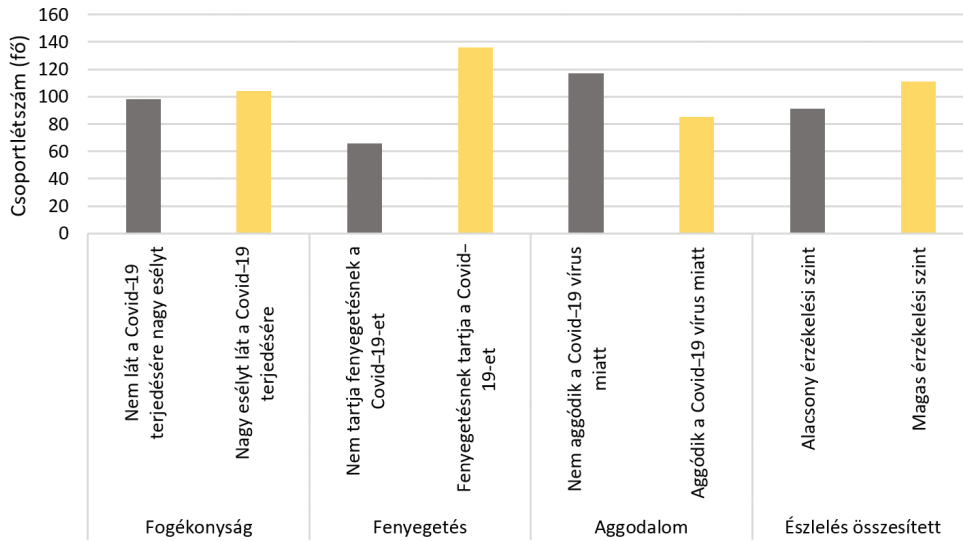
fog kialakulni a városukban vagy az országban. Az adatokat összesítve a megkérdezettek 48,5%-a nem lát esélyt a vírus ismételt elterjedésére, míg 41,5%-uk igen. Az észlelt fenyegetés alapján a megkérdezettek több mint 63,3% tartja veszélyesnek a koronavírust, azonban a saját szervezetükre már csak 26,8%-uk. A kitöltők hasonló arányban válaszoltak meg az utolsó három kérdésre a szekcióban. Közel kétharmados arányban választották a veszélyes vagy nagyon veszélyes lehetőséget, összesen 132, 145 és 168 fő. Ezen adatokat összesítve megállapítható, hogy a kitöltők 20,3%-a nem tartja fenyegetésnek a vírust, míg 79,3%-a igen. A fejezetben ezt követően az észlelt aggodalmat vizsgáltam. Annak ellenére, hogy a megkérdezettek nagy arányban tartották veszélyesnek a vírust, az aggodalmuk szintje már sokkal alacsonyabb volt. A vírus miatt csak 49-en (24,3%), míg amiatt, hogy el is kapja az adott személy 31-en (15,4%) aggódnak csak. Arra, hogy közeli rokonaik elkapják a közeljövőben a vírust, már a minta 58,4%-a aggódik valamilyen formában. Végül amiatt, hogy egy újabb Covid-járvány miatti korlátozásoknak a következményeként elhagyni sem tudja majd a házát, a kitöltők több mint a fele (57,9%) aggódik valamilyen módon. A mintát e szempontból is két részre osztva megállapítottam, hogy 67 főt (33,2%) tölt el aggodalommal, míg 135 főt (66,8%) nem tölt el aggodalommal a Covid–19 vírus (2. ábra).

3. táblázat: A kitöltők észlelésekre adott válaszai

Észlelt fogékonyság	**Nem lát rá esélyt**		**Kevésbé lát rá esélyt**		**Lát rá esélyt**		**Nagy esélyt lát rá**	
Mennyire látja valószínűnek, hogy az elkövetkezendő hónapokban elkapja a Covid–19 vírust?	39 fő	19,3%	81 fő	40,1%	75 fő	37,1%	7 fő	3,5%
Mennyire látja valószínűnek, hogy az elkövetkezendő hónapokban egy családtagja elkapja a Covid–19 vírust?	30 fő	14,9%	76 fő	37,6%	85 fő	42,1%	11 fő	5,4%
Mennyire látja valószínűnek, hogy az elkövetkezendő hónapokban egy újabb Covid–19 járvány fog kitörni a városában?	6 fő	3,0%	36 fő	17,8%	112 fő	55,4%	48 fő	23,8%
Mennyi esélyt lát rá, hogy az elkövetkezendő pár hónapban egy újabb Covid–19 hullám fog kitörni Magyarországon?	4 fő	2,0%	20 fő	9,9%	107 fő	53,0%	71 fő	35,1%
Észlelt fenyegetés	Egyáltalán nem veszélyes		Nem igazán veszélyes		Veszélyes		Nagyon veszélyes	

Észlelt fogékonyság	**Nem lát rá esélyt**		**Kevésbé lát rá esélyt**		**Lát rá esélyt**		**Nagy esélyt lát rá**	
Mennyire tartja veszélyesnek a Covid–19 vírust?	5 fő	2,5%	49 fő	24,3%	125 fő	61,9%	23 fő	11,4%
Mennyire lenne veszélyes a vírus a saját szervezetére nézve Ön szerint?	31 fő	15,3%	117 fő	57,9%	47 fő	23,3%	7 fő	3,5%
Mennyire lenne veszélyes Ön szerint, ha a Covid–19 vírus elkezdene terjedni az Ön közösségében?	6 fő	3,0%	63 fő	31,2%	105 fő	52,0%	28 fő	13,9%
Mennyire lenne veszélyes a vírus a saját városára nézve, ha elkezdene terjedni Magyarországon?	7 fő	3,5%	50 fő	24,8%	115 fő	56,9%	30 fő	14,9%
Ön szerint mennyire lennének veszélyesek egy újabb Covid–19 járvány következményei Magyarországra tekintve?	3 fő	1,5%	31 fő	15,3%	101 fő	50,0%	67 fő	33,2%
Észlelt aggodalom	Egyáltalán nem aggódik		Kevésbé aggódik		Aggódik		Nagyon aggódik	
Mennyire aggódik a Covid–19 miatt jelenleg?	55 fő	27,2%	98 fő	48,5%	43 fő	21,3%	6 fő	3,0%
Mennyire aggódik amiatt, hogy elkapja a Covid–19 vírust az elkövetkezendő hónapokban?	90 fő	44,6%	81 fő	40,1%	27 fő	13,4%	4 fő	2,0%
Mennyire aggódik amiatt, hogy egy közeli ismerőse vagy rokona elkapja a vírust az elkövetkezendő hónapokban?	19 fő	9,4%	65 fő	32,2%	81 fő	40,1%	37 fő	18,3%
Mennyire aggódik amiatt, hogy esetleg egy új Covid–19-hullám tör ki a városában	25 fő	12,4%	75 fő	37,1%	81 fő	40,1%	21 fő	10,4%
Mennyire aggódik amiatt, hogy nem fog tudni kimenni a házából sem egy új Covid–19-hullám érintő korlátozás miatt?	45 fő	22,3%	40 fő	19,8%	54 fő	26,7%	63 fő	31,2%

Forrás: a szerző szerkesztése

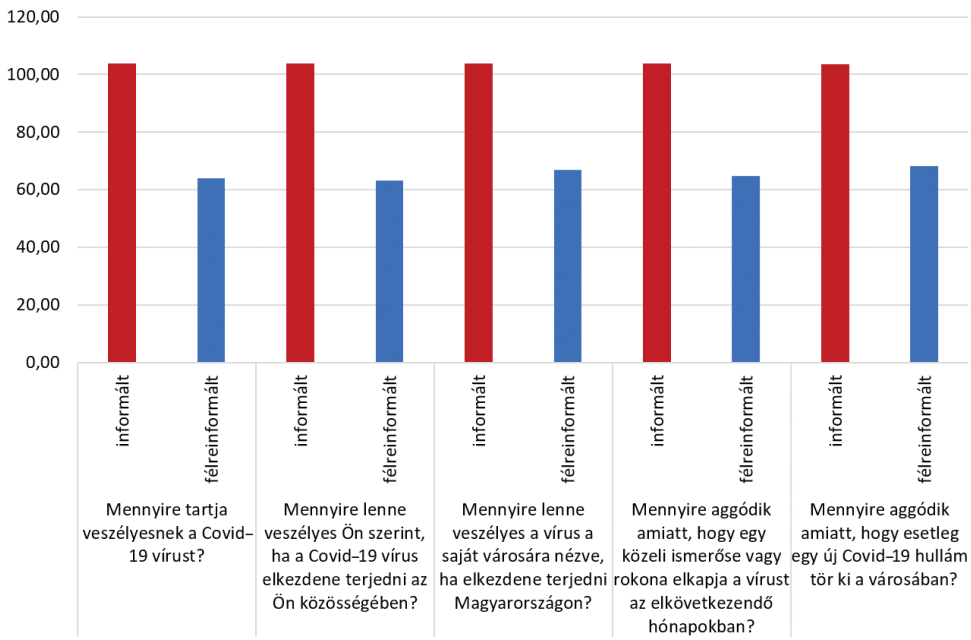


2. ábra: Az „Észlelések" fejezet kitöltői főben megadva
Forrás: a szerző szerkesztése

A válaszok alapján Khi-négyzet próbában összevetve az észlelési szinteket és az álhírekre adott válaszokat, semmilyen szignifikáns összefüggés nem található az álhírekkel kapcsolatos hiszékenység és aközött, hogy mennyire fogékony vagy mennyire aggódik a koronavírus miatt. Ugyanakkor több esetben is megállapítható szignifikáns összefüggés abban a tekintetben, hogy valaki fenyegetésnek tartja-e a vírust, és hogy mennyire hiszi el az álhíreket. A „Covid–19 egy emberek által alkotott vírus, amely a gyógyszeripar pénzügyi növekedését segíti elő" állítás és aközött, hogy az adott illető mennyire tartja fenyegetésnek a járványt, kisebb mint 0,001-es szignifikancia található, tehát van kapcsolat a két változó között, azonban lefuttatva a Cramer's V tesztet, kiderül, hogy ez az összefüggés nem erős, 0,274-es értékkel. Ugyanebben az esetben arra, hogy a Covid–19 vírus egy ember által alkotott biológiai fegyver, 0,023-as szignifikanciaszint állapítható meg, és a Cramer's V teszt alapján egy még gyengébb, 0,157-es erősségű összefüggés. Végül abban a kérdésben állapítható még meg szignifikáns összefüggés, hogy a Covid–19 megelőzhető és kezelhető fokhagyma és ánizsos tea fogyasztásával. Ebben az esetben szintén Khi-négyzet próbát alkalmazva 0,44-es erősségű szignifikancia állapítható meg, és a Cramer's V teszttel 0,142-es erősségű összefüggés a változók között. A többi kérdés esetén semmilyen szignifikáns összefüggés nem volt található a változók között. Ezen adatok alapján megállapítható, hogy a Covid–19-álhírek és a vírussal kapcsolatos észlelések között csekély, összesen három esetben beszélhetünk szignifikáns összefüggésről.

A Kruskal–Wallis-tesztet lefuttatva az észlelések és az összesített álhírhiszékenység között, megállapítható, hogy több hírnél is szignifikáns összefüggés van aközött, hogy a válaszadók összességében jól vagy rosszul informáltak a koronavírussal kapcsolatban. A fogékonyság rész és az álhírek hiszékenysége között nem található szignifikáns

összefüggés (s > 0,05), tehát nem is hatnak egymásra, ellenben a „fenyegetettség" és az „aggodalom" résznél megállapítható több esetben is. A 3. ábrán látható kérdések és az álhírrel kapcsolatos hiszékenység között minden esetben szignifikáns összefüggés állapítható meg, azaz s < 0,05. A kapott adatok alapján szintén megállapítható, hogy az alábbi kérdéseknél minden esetben magasabb a rangszámok átlaga azoknál a személyeknél, akik nagyobb mértékben informáltak a Covid–19 vírussal kapcsolatban, tehát összességében veszélyesebbnek és aggasztóbbnak is találják magát a járványt és annak következményeit, mind magukra mind a környezetükre, mint a kevésbé informált társaik.

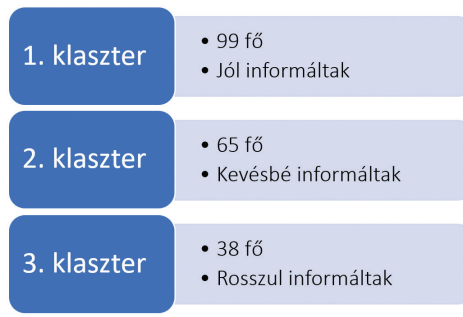


3. ábra: Informált és félreinformált csoportok rangátlagai különböző álhírek esetében
Forrás: a szerző szerkesztése

A kérdőívvel kapcsolatos hipotézisek vizsgálata

H1 hipotézisem arra a feltevésre épül, hogy klaszterelemzés során az álhírekre adott válaszok alapján csoportosítva az egyéneket, szignifikáns összefüggés található az elemzett érzékelések kérdéskörökben adott válaszaikra. Könyökelemzés során megvizsgálva a válaszokat, a hármas számú klaszterezést találtam a legmegfelelőbbnek. Ezt követően Kruskal–Wallis-elemzést alkalmazva, a rangátlagokat figyelve megállapítottam, hogy az egyes számú csoportba kerülő 99 fő azok a személyek, akik az álhírekkel legkevésbé értettek egyet, második csoportba az a 65 személy, akik kevésbé értettek egyet az álhírekkel és a harmadik klaszterbe azon kitöltők, akik leginkább egyetértettek azokkal.

Megvizsgálva a kapott csoportokat, az aggodalmak kérdéskörével összesen két kérdésnél található szignifikáns összefüggés a csoportok között. A „mennyire aggódik amiatt, hogy egy rokona vagy közeli ismerőse, illetve, hogy saját maga elkapja a Covid–19 vírust a közeljövőben" kérdésekre adott válaszoknál volt megfigyelhető összefüggés. Megnézve szintén a rangátlagokat, az első csoportnál a legkiemelkedőbb, míg a harmadik csoportnál a legkisebb az érték. Ennek a mértéke azt mutatja, hogy mennyire aggódik, tehát minél magasabb, annál inkább. Emiatt elmondható a klasztercsoporttagság alapján, hogy azon személyek, akik a leginkább hisznek az álhírekben, azok hiszik legkevésbé, hogy rokonaik vagy maguk elkapnák a vírust, míg a legjobban informált klaszterbe tartozók látják rá a legnagyobb valószínűséget.



4. ábra: Klasztercsoportok
Forrás: a szerző szerkesztése

A klasztereket összevetve a fenyegetés kérdéskörében, mind az összesített értékekre, mind a kérdéseket egyesével tekintve, szignifikáns összefüggés található. Egyedül annál a kérdésnél nem volt található szignifikáns összefüggés, hogy mennyire lenne veszélyes a Covid–19 az egyén szervezetére. Így – a Kruskal–Wallis-teszt alapján figyelve a rangszámok átlagát – kimondható, hogy szignifikáns összefüggés van az álhírekre adott válaszok alapján képzett klaszterek és a fenyegetettség mérése során használt kérdésekre adott válaszok között. Elmondható, hogy a csoporthoz való tartozás megmutatja, milyen mértékben tartják veszélyesnek a vírust a környezetükre és magukra nézve.

Végül a csoportokat összevetve a vírusra való fogékonyság mérésére alkalmazott kérdések eredményeivel összesen két kérdésnél volt szignifikáns összefüggés a csoportok között. Azoknál a kérdéseknél, hogy az adott személy vagy családtagja elkapja-e a Covid–19 vírust, kétoldali szignifikancia állapítható meg. Emiatt kimondható, hogy a klaszterekbe való tartozás alapján, egy egyén mennyire hiszi el az álhíreket, összefügg azzal, hogy mennyire tartja valószínűnek, hogy maga vagy rokonai elkapják a vírust. A rangszámok átlagát elemezve pedig az következtethető, hogy attól függően, az álhírekkel kapcsolatos hiszékenység alapján milyen klaszterbe tartoznak, fordított arányos mértékben mutatja, mekkora esélyt lát arra, hogy rokona vagy maga megfertőződne a közeljövőben.

A kapott eredményeket tekintve mind az aggodalomnál, mind a fogékonyság kérdéscsoportnál, a saját és rokonai egészségére feltett kérdésekre adott válaszok összefüggenek a klasztercsoporthoz tartozással, méghozzá fordítottan arányosan. Attól függően tehát, hogy az adott személy mennyire aggódik vagy tartja valószínűnek, hogy a közeljövőben saját maga vagy rokona elkapja a Covid–19 vírust, ellentétes mértékben nő az álhírekben való hiszékenysége és ez alapján a klasztercsoporthoz való tartozása.

A H2 hipotézisem alapján az álhírekre adott válaszok összefüggenek az adott személy oltakozási hajlandóságával. Ezt több szempontból és módszerrel is megvizsgálom. Az álhírekre adott válaszokat két csoportra osztottam. Az első csoportba azok a személyek kerültek, akik az adott kérdésre „egyáltalán nem ért egyet" vagy „nem ért egyet" választ adtak. Második csoportba pedig azokat a kitöltőket, akik a részben egyetért, egyetért és teljesen egyetért válaszokat adtak meg. Ezután megvizsgáltam – Kruskal–Wallis-teszttel –, hogy mely álhírrel kapcsolatos kérdéseknél van összefüggés abban a tekintetben, hogy az illető beolttatta-e már magát. Minden kérdésnél, amelynél szignifikáns kapcsolat található, a rangszámok átlaga magasabb volt azoknál a személyeknél, akik nem olttatták be magukat a vírus ellen. Esetünkben ez a szám minél magasabb, annál jobban értett egyet a csoport az adott álhírrel. Ezt követően kereszttábla-elemzés során két esetben tudtam Khi-négyzet próbát alkalmazni és Cramer's V teszttel megvizsgálni az eredményeket a kitöltők alacsony száma miatt. Ebben a kettő esetben is kétoldali szignifikanciát találtam, illetve a Cramer's V teszt alapján mindegyik kérdésnél egy gyenge nullához közeli értéket kaptam, ami alapján kimondható, hogy nem erős a két változó közötti kapcsolat. Ezeket az eredményeket összefoglalva a 4. táblázat mutatja.

4. táblázat: Egyes álhírek és az oltakozás közti különbségek

Kruskal–Wallis-elemzés	**Szignifikancia**		**Klaszter V**	
Álhírek	Oltott személyek	Fizetős vakcina	Oltott személyek	Fizetős vakcina
A Covid–19 egy emberek által alkotott vírus, amely a gyógyszerészeti cégek pénzügyi növekedését segíti elő.	0,000	0,648	0,00	X
A Covid–19 vírus egy ember által alkotott biológiai fegyver.	0,009	0,036	0,09	0,35
A Covid–19 vírus nem tud átterjedni a melegebb éghajlatú területekre.	0,043	0,972	X	X
A gyerekek nem tudják elkapni a Covid–19-et.	0,018	0,512	X	X
Az antibiotikum hatásos a Covid–19 megelőzésében és kezelésében.	0,797	0,157	X	0,796
A Covid–19 megelőzhető és kezelhető nyers fokhagyma és ánizsos tea fogyasztásával.	0,030	0,674	X	X
A legtöbb ember, aki elkapja a Covid–19 vírust, bele is hal.	0,199	0,749	X	X

Forrás: a szerző szerkesztése

A vizsgálatot elvégeztem azzal a kérdéssel is, hogy fizetnének-e nagyjából 5000 forintot egy vakcináért. Az alábbi összevetést tekintve azonban már csak egy kérdés esetén volt szignifikáns kapcsolat (s = 0,036). Ezt követően kereszttábla-elemzés során Khi-négyzet próbát alkalmazva és Cramer's V teszttel vizsgálva 0,36-os szignifikanciaszint állapítható meg, valamint és 0,182-es erősségű kapcsolat a két változó között (4. táblázat).

Összegzés

A kérdőívet kitöltők és válaszaik alapján több eredményt is sikerült megállapítani. A kitöltők jelentős része (86,6%) már rendelkezik Covid–19 elleni védőoltással. A válaszok alapján az elemzett minta több mint fele 16 és 24 éves kor közé tehető, középfokú végzettséggel rendelkezik és városi lakos.

Vizsgálva a kitöltők álhírekkel kapcsolatos egyetértését megállapítottam, hogy a 202 főből 190 fő összességében jól informált, azonban vannak kérdéskörök, amelyeknél a megkérdezettek több mint fele bedőlt az álhíreknek (a koronavírus egy ember által alkotott biológiai fegyver, a gyógyszeripar pénzügyi növekedése érdekében alkották meg).

Összevetve az álhírekre adott válaszokat és a korosztályokat, szignifikáns összefüggést fedeztem fel aközött, hogy minél idősebb korosztályba tartozik az egyén, annál inkább hiszi, hogy a Covid–19 ember által alkotott. Továbbá a 35 vagy annál idősebb korosztálynál a legmagasabb minden szignifikáns kérdésnél a rangátlag, ami alapján kimondható, hogy ők a leghiszékenyebbek.

Megvizsgálva a vírussal kapcsolatos különböző észlelésekre adott válaszokat, mint a fogékonyságra, fenyegetésre és aggodalomra, a mintát külön csoportokra tudtam osztani, fogékonyság szempontjából nagyjából 50-50%-ban oszlanak meg, de fenyegetés szempontjából már jelentős különbség van. A kitöltők közel 80%-a tartja fenyegetésnek a járványt, azonban 117 fő összességében nem aggódik miatta.

H1 hipotézisemet vizsgálva a klaszterelemzés alapján arra az eredményre jutottam, hogy az álhírekre adott válaszok alapján létrehozott klasztereket összevetve a különböző érzékelésekre adott válaszok eredményeivel, a fogékonyság kérdésénél, illetve az aggodalomnál is meghatározók voltak a rokonok, illetve saját egészségünkre vonatkozó kérdésekre adott válaszok. A fenyegetés kérdéskörnél ugyanakkor minden kérdés meghatározó volt a klasztertartozást tekintve, kivéve, hogy mennyire tartja saját magára tekintve veszélyesnek a vírust. Tekintve a szignifikanciaszinteket az adott csoportok és kérdések között, illetve a rangátlagok értékét, H1 hipotézisem beigazolódott.

H2 hipotézisem vizsgálatának eredményeként elmondható, hogy vannak olyan álhírek, amelyeknél az adott személy informáltsága és az oltakozási hajlandósága szignifikáns kapcsolatot mutat. Ugyanakkor, lefuttatva a Cramer's V teszteket, kiderül, hogy egyik kérdésnél sem erős a kapcsolat. Általánosságban nem mondható ki tehát, hogy a félreinformáltság összefüggésben van az oltakozási hajlandósággal, azonban vannak olyan kérdések, amelyeknél összefüggenek.

Irodalomjegyzék

Annoni Manghi, Rita et al. (2011): Khat Use: Lifestyle or Addiction? *Journal of Psychoactive Drugs,* 41(1), 1–10. Online: https://doi.org/10.1080/02791072.2009.10400669

Bányász Péter (2022): A Covid-oltásokkal kapcsolatos érzelmek vizsgálata Magyarországon. *Magyar Tudomány,* 133(5), 601–609. Online: https://doi.org/10.1556/2065.183.2022.5.6

Bányász Péter et al. (2019): Lélektani műveletek a közösségi médiában. In Auer Ádám – Joó Tamás (szerk.): *Hálózatok a közszolgálatban.* Budapest: Dialóg Campus, 111–133.

Bányász, Péter – Nagy, Gréta – Molnár, Ákos (2023): Empirical Studies of COVID-19 Related Fake News. *Hadtudomány,* 33(E-szám), 20–36. Online: https://doi.org/10.17047/Hadtud.2023.33.E.20

Bányász Péter – Tóth András – László Gábor (2022): A koronavírus oltással kapcsolatos állampolgári attitűd vizsgálata szentimentanalízis segítségével. *Információs Társadalom,* (22)1, 99–125. Online: https://doi.org/10.22503/inftars.XXII.2022.1.6

Bitar, Ahmad Naoras, et al. (2021): Misinformation, Perceptions Towards COVID-19 and Willingness to Be Vaccinated: A Population-Based Survey in Yemen. *Scientific Communication and Education,* 2021. február 25. Online*:* https://doi.org/10.1101/2021.02.25.432838

Csallner András Erik [é. n.]: *Bevezetés az SPSS statisztikai programcsomag használatába.* Online: www.jgypk.hu/tamop15e/tananyag_html/spss/

Farkas Tibor (2023): Kommunikációs és információs rendszerek értelmezése napjainkban: Követelmények és kihívások. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban.* Budapest: Ludovika, 11–30.

Google adatvédelmi irányelvek [é. n.]. Online: https://policies.google.com/privacy?hl=hu

Ináncsi Mátyás – Tibor Farkas (2022): Álhírek ellenőrzése a közösségi médiafelületeken a COVID-19 járvány alatt. *Hadtudomány,* 32(E-szám), 42–53. Online: https://doi.org/10.17047/Hadtud.2022.32.E.42

Mayer Annamária (2018): *A Likert-skála fogalma és 3 fajta módszer az elemzésére.* Online: https://spssabc.hu/kutatasmodszertan/likert-skala-fogalma-elemzese/

Németh, András – Magyar, Sándor (2020): An Investigation of Data Used to Support Contact Tracing to Curb the Spread of Covid-19 Pandemic from the Aspect of Possible National Security Application (Part 1). *National Security Review,* 6(2), 52–64.

Németh, András – Magyar, Sándor (2021): An Investigation of Data Used to Support Contact Tracing to Curb the Spread of Covid-19 Pandemic from the Aspect of Possible National Security Application (Part 2.). *National Security Review,* 7(1), 218–231.

Sajtos László – Mitev, Ariel (2007): *SPSS kutatási és adatelemzési kézikönyv.* Budapest: Alinea.

Statistics [é. n.]: *Kruskal-Wallis H Test using SPSS Statistics.* Online: https://statistics.laerd.com/spss-tutorials/kruskal-wallis-h-test-using-spss-statistics.php

HADMÉRNÖK
FÓRUM
18. évfolyam (2023) 4. szám 177–188.
DOI: 10.32567/hm.2023.4.12

Torda Péter[1]

A légierő-elméletek és a stratégiai kommunikáció összefüggései

The Relationship Between Airpower Theories and Strategic Communication

Absztrakt

Jelen tanulmány feltárja a stratégiai kommunikációval kapcsolatos összefüggéseket a légi hadviselés alaptételeit lefektető klasszikus teoretikusok, illetve a légierő-elméletek korszakváltását fémjelző gondolkodók hadelméleteiben. A tanulmány rámutat, hogy a stratégiai kommunikáció koncepciói a kezdetektől fogva részét képezik a légierő-elméleteknek, illetve arra, hogy a légierő teoretikusai rendkívül erős stratégiai kommunikációs hatást tulajdonítanak a légi hadviselésnek. A légierővel kapcsolatos teóriák egyik alapfeltevése, hogy a légicsapások olyan lélektani hatást váltanak ki az ellenséges lakosság, illetve az ellenséges vezetés tudatában, amely kulcsfontosságú az ellenség akaratának megtöréséhez és a támadó fél akaratának érvényesítéséhez, vagyis a háború politikai céljának eléréséhez. Ez a feltételezés ugyanúgy jellemzi a klasszikus, mint a modern légierő-elméleteket. Ugyanakkor, sem a klasszikus, sem a modern teóriák nem állapítanak meg általános érvényű összefüggéseket arra a hatásmechanizmusra, amely a légicsapástól az ellenség megadásra kényszerítéséig vezet.

Kulcsszavak: stratégiai kommunikáció, légierő-elmélet, Giulio Douhet, Hugh M. Trenchard, William L. Mitchell, John R. Boyd, John A. Warden III, David A. Deptula

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: torda.peter@stud.uni-nke.hu

Abstract

The present article explores strategic communication-related aspects in the military theories of classical thinkers who have laid out the foundational theses of air warfare and in the military theories of thinkers who have hallmarked the new era of airpower theories. This article demonstrates that the concepts of strategic communication have been integral to airpower theories from the outset as well as that airpower theorists attribute an exceptionally strong strategic communication impact to air warfare. One of the basic assumptions of airpower theories is that airstrikes impose a psychological impact in the minds of enemy populations and of enemy leadership which is key to breaking the enemy's will and to enforcing the will of the attacking party, and ultimately to achieving the political objective of warfare. This assumption is equally characteristic of classical as of modern airpower theories. However, neither classical, nor modern theories lay out findings of a general validity when it comes to the mechanisms which lead from airstrikes to forcing the enemy to surrender.

Keywords: strategic communication, airpower theory, Giulio Douhet, Hugh M. Trenchard, William L. Mitchell, John R. Boyd, John A. Warden III, David A. Deptula

Bevezetés

Az elmúlt évtizedekben a stratégiai kommunikáció egyre meghatározóbb szerepet tölt be a hadelméletben és a hadviselésben egyaránt. Nem létezik egységesen elfogadott definíció a stratégiai kommunikációra, de a tudományos irodalom két alapvető kommunikációs modell mentén értelmezi a koncepciót. Szűkebb értelmezési keretben, a szakirodalomban klasszikus referenciapontként használt definíció alapján,[2] a szervezet által tudatosan és küldetése elérése érdekben folytatott kommunikációt tekinthetjük stratégiai kommunikációnak. Tágabb értelmezési keretben, a szervezet maga is kommunikációs mozzanatokból épül fel,[3] és a szervezet bármely tagjának bármely cselekvése, vagy annak hiánya, kommunikál, és akarva vagy akaratlanul is kiválthat stratégiai hatást.

A stratégiai kommunikáció katonai összefüggéseit vizsgálva, a NATO definícióit tekinthetjük jellemzőnek, mivel ezek valamennyi szövetséges állam egyetértését tükrözik. A NATO fogalomkészlete egyaránt átfogja a stratégiai kommunikáció tágabb és szűkebb értelmezési kereteit. A tágabb értelemzési mezőre a Szövetség stratégiai kommunikációs doktrínájában találunk példát, amely így fogalmazza meg a NATO stratégiai kommunikációs megközelítését.

„Minden, amit a NATO és partnerei tesznek és mondanak, vagy elmulasztanak megtenni es elmondani, akaratlagos és akaratlan következményekkel jár. Üzenetet közvetít minden

[2] Hallahan et al. 2007: 3.
[3] Torp 2015.

cselekvés, szó és kép, és a fegyveres erők minden tagja üzenetek hordozója, a műveleti területen tevékenykedő egyes katonától a hadszíntérparancsnokig."[4]

A szűkebb értelmezési mezőből merít a NATO definíciója a stratégiai kommunikációra:

„a NATO kommunikációs tevékenységeinek és képességeinek koordinált és megfelelő alkalmazása, ideértve szükség szerint a nyilvános diplomáciát,[5] közkapcsolatokat,[6] katonai közkapcsolatokat,[7] információs műveleteket[8] és lélektani műveleteket,[9] a Szövetség szakpolitikáinak, műveleteinek és tevékenységeinek támogatása, illetve a NATO céljainak előmozdítása érdekében".[10]

Habár a stratégiai kommunikáció kortárs fogalom, a kommunikáció mindig is központi és kritikus kérdése volt a háború megvívásának.[11] A stratégiaikommunikáció-tanulmányok érdeklődési körébe tartozó kutatási objektumok a kezdetektől fogva részét képezik a hadtudományi gondolkodásnak. Ezek közé tartoznak a hadviselés erkölcsi és lélektani aspektusai, köztük a meggyőzés, befolyásolás, megtévesztés, elrettentés, megfélemlítés, az ellenfél akarata megtörésének kategóriái. A léghadviseléssel kapcsolatos teóriák fejlődése során ezek az aspektusok folyamatosan és hangsúlyosan jelennek meg az elméletekben.

A légierő-elméletek kezdetektől jelen lévő és meghatározó jelentőségű problémája a csapásmérés lélektani hatásainak, illetve a lélektani hatásokból következő stratégiai és politikai hatások előrejelzése. A teóriák fejlődése során a hangsúly a polgári lakosság és a létfontosságú infrastruktúrák megkülönböztetés nélküli pusztításától az ellenség megbénításához szükséges mértékű precíziós légicsapások felé tolódott el. Ugyanakkor az egymást követő elméletek mögött változatlan formában maradt meg az az alapfeltevés, hogy a légicsapások olyan hatásokat keltenek az ellenséges lakosság, illetve politikai vezetés tudatában, amelyek végső soron aláássák a háborús erőfeszítést. A kérdés rendszerezett formában történő elemzése a II. világháború végét követő időszakban vette kezdetét,[12] de azóta sem vált ismertté általános érvényű összefüggés az ellenségre mért légicsapások és az ellenséges társadalom morális állapotában vagy az ellenséges vezetés döntéshozatali folyamatában elérni kívánt hatás között.[13]

Kutatásomhoz azt a hipotézist vettem alapul, hogy a légierő-elméletek magukban foglalják a légi hadviselés és a stratégiai kommunikáció összefüggéseit, és tanulmányomban azt a tudományos problémát kívánom feltárni, hogy pontosan milyen összefüggések állapíthatóak meg a légierő-elméletek és a stratégiai kommunikáció között. Tanulmányom célja a légierő hadelméleteiben megvizsgálni a stratégiai kommunikáció helyét és szerepét, valamint elemezni annak feltételezett hatását

4 NATO 2023: 20.
5 Public Diplomacy.
6 Public Affairs.
7 Military Public Affairs.
8 Information Operations.
9 Psychological Operations.
10 Althuis et al. 2023: 10.
11 Németh 2013: 130.
12 Mueller 2010: 10.
13 Henriksen 2008: 850.

a háború céljának elérésére. Vizsgálatom a hagyományos fegyverekkel folytatott légi hadviseléssel kapcsolatos elméleti anyagra fókuszál, jóllehet a mai fogalomhasználattal tömegpusztító fegyvernek nevezett eszközök alkalmazása már a légi hadviselés első teoretikusainak műveiben is megjelenik, például Douhet vegyi fegyverek alkalmazásával kapcsolatos elképzeléseiben. Ugyanakkor a tömegpusztító fegyverek alkalmazásától való általános tartózkodás, illetve azok egy részére vonatkozó nemzetközi jogi tilalmak, olyan speciális összefüggéseket vetnek fel a stratégiai kommunikáció szempontjából, amelyeket jelen tanulmányban nem indokolt vizsgálni. A tömegpusztító fegyvereken belül külön kategóriát képeznek a nukleáris fegyverek, amelyek hadrendbe állításuk óta egyértelmű és szoros összefüggést mutatnak a stratégiai kommunikációval: elég, ha a nukleáris doktrínák középpontjában álló elrettentés fogalmára gondolunk. Ennek az összefüggésnek a feltárása azonban szintén túlmutat jelen tanulmány keretein.

Feltevésem igazolása vagy megcáfolása érdekében áttekintettem a stratégiai kommunikációval kapcsolatos összefüggéseket a légierő klasszikusainak, valamint modern teoretikusainak munkáiban. A klasszikusok közül a két világháború közötti időszakban a légi hadviselés alaptételeit lefektető[14] legbefolyásosabb gondolkodók, Giulio Douhet, Hugh M. Trenchard és William L. Mitchell, hadelméletét vizsgálom. A légierő modern teoretikusai közül a légierő-elméletek korszakváltását fémjelző amerikai gondolkodók, John R. Boyd, John A. Warden III és David A. Deptula hadelméletét dolgoztam fel.

A kutatómunkát a légi hadviselés elméletével kapcsolatos tudományos irodalom feltárásával végeztem el, részben elsődleges, részben másodlagos forrásokra támaszkodva. A szakirodalmi forrásokat tudományos adatbázisokban, tárgyszavas keresés útján kutattam fel. A kutatási területet érintő tudományos művek döntő többsége angol nyelvű forrásokból, különösen angol nyelvű tudományos folyóiratokból férhető hozzá.

A stratégiai kommunikáció és a légierő-doktrínák általános összefüggései

A stratégiai kommunikáció felértékelődése a hadművészetben átfedést mutat a légierő haderőnem előtérbe kerülésével, különösen az elmúlt évtizedek fegyveres konfliktusaiban. „A modern világban a legierő vált a katonai erő kivetítésének elsődleges formájává",[15] és a modern légierő-doktrínákban helyet kapnak a stratégiai kommunikációval kapcsolatos összefüggések. Az Amerikai Egyesült Államok (USA) légierejének doktrínája megállapítja, hogy a „légierő a világ minden pontján kommunikálja a közönségek számára az USA képességeit és eltökéltségét".[16] A doktrína leírja továbbá a légierő kritikus szerepét az információs térben végrehajtott műveletekben. „A légierő minden cselekvése […] kommunikál valamilyen üzenetet vagy szándékot […]. Ezeknek az üzeneteknek a megformálása és kiaknázása központi része a műveleti és tervező munkának."[17] A NATO légi és világűrműveleti doktrínája rögzíti a légiműveletek

[14] Csengeri 2017: 48.
[15] Olsen 2018: 12.
[16] U.S. Air Force 2021: 8.
[17] U.S. Air Force 2021: 9.

stratégiai kommunikációs szempontjait, ideértve, hogy a „katonai tevékenységek, különösen, amelyek erő alkalmazásával járnak, stratégiai szinten kommunikálhatnak és a közönségek széles körében befolyásolhatják a percepciókat".[18] Az Egyesült Királyság légierő-doktrínája már az előszóban kiemeli a légierőnek azt a jellemzőjét, hogy mind a puha hatalom, mind a kemény hatalom eszközeivel képes befolyásolni a közönségeket, és ezáltal hozzájárulni az események gyors értékeléséhez és az azokra történő határozott reagáláshoz.[19] A brit doktrína emellett leírja a légierő szerepét az integrált fellépésekben, amelyek a katonai és nem katonai tevékenységek összehangolásán keresztül befolyásolják a célközönségek attitűdjét és magatartását a kívánt hatások elérése érdekében.[20] A Magyar Honvédség Légi Művelet Doktrínája[21] nem nevesít kommunikációs aspektusokat. A légierő alkalmazásának elveit felsorolva azonban elsők közt említi az erődemonstrációt, amely összefügg a stratégiai kommunikációval. Összegezve, az USA, NATO és az Egyesült Királyság doktrínái is számolnak a légierő stratégiai kommunikációs célú alkalmazásával, beleértve az információs környezet értékelését és a közönségek tájékoztatását és befolyásolását.

Stratégiai kommunikáció a légierő klasszikus teoretikusainak gondolkodásában

Giulio Douhet, a légierő hadelméletének talán legismertebb úttörője, *A légiuralom* című munkájában a háború menetét egyedül is eldönteni képes, az ellenség anyagi és erkölcsi ellenállását szakadatlan légitámadásokkal megtörő légierő képét festi le.[22] Douhet légiuralom-koncepciójának lényeges eleme az ellenség lakott területeinek pusztítása és ezáltal olyan lélektani hatások kiváltása, mint pánik, kilátástalanság, a társadalom demoralizálása, amelyek a háború ellen fordítják a lakosságot. Douhet szerint a légierő közvetlen romboló tevékenysége által „sokkal könnyebben érhető el az anyagi-erkölcsi összeomlás",[23] az ellenfél erkölcsi ellenállóerejének „megsemmisítése vagy legalábbis súlyos megrongálása meggyorsítja majd a döntést és a jövő háborúinak időtartamát jelentősen megrövidíti".[24] Douhet elutasít minden korlátozást a légierő alkalmazását illetően, beleértve a civil lakosság bombázásával kapcsolatos önmérsékletet.

Hugh M. Trenchard, akire a „Brit Királyi Légierő atyjaként" is hivatkoznak, Douhet-t megelőzve kezdte megalkotni légierő-elméletét. Douhet nézeteit megelőlegezve, Trenchard sokkal pusztítóbbnak vélte a levegőből mért pusztítás lélektani hatását, mint annak fizikai hatását.[25] Trenchard híressé vált, habár tudományosan nehezen alátámasztható számítása szerint a bombázás erkölcsi hatásai hússzorosan haladják meg annak fizikai hatását.[26] Erre a meggyőződésre épül Trenchard „erkölcsi hatású

[18] NATO 2016: 1–18.
[19] UK MoD 2022: 14.
[20] UK MoD 2022: 70.
[21] MH 2015: 1–2.
[22] Douhet 1971.
[23] Douhet 1971: 37.
[24] Douhet 1971: 37.
[25] Szűcs–Krajnc 2014: 19.
[26] Gurantz 2022: 125.

bombázás" elmélete, amely azzal kalkulál, hogy „az ellenség létfontosságú hadiipari központjainak támadása erősen aránytalan mértékű pszichológiai hatással jár majd a dolgozók körében, amely nagymértékben aláássa az ellenséges nemzet katonai erejét".[27] Trenchard azonban bizonyos korlátozások mellett tartotta csak elfogadhatónak a lakosság moráljának megtörését célzó légitámadásokat, illegitimnek minősítve a polgári lakosság megkülönböztetés nélküli terrorbombázását.

Az amerikai William L. Mitchell, Trenchardhoz hasonlóan, a nemzeti légierő alapító atyjaként vonult be a köztudatba. Mitchell is úgy vélekedett, hogy

> „az ellenséges nemzet lakossága szempontjából létfontosságú központok (nagyvárosok, ellátócentrumok, közlekedési csomópontok stb.) ellen végrehajtott bombázásokkal elérhető, hogy az adott országban polgári elégedetlenség, vagy felkelés »elsöpörje« a kormányon levőket és így a célzott politikai események bekövetkezzenek".[28]

Mitchell, illetve az általa képviselt iskola azonban ellenezte a polgári lakosság közvetlen támadását, „az infrastrukturális és ipari létfontosságú központok támadásában látta a civil morál és az ellenség ellenállása megtörésének hatékonyabb módját".[29] Mitchell felfogásában a légierő nemcsak intenzívebbé és gyorsabb lefolyásúvá teheti a háborút, de a légierő olyan erős fenyegetést jelenthet, amely eltántoríthat egy ellenséges államot attól, hogy háborúba lépjen.[30]

Megjegyzendő, hogy a két világháború között megjelent munkáikban a gépesített háború más teoretikusai is erős jelentőséget tulajdonítottak az erkölcsi és lélektani szempontoknak a légierő hadművészetében. Liddel Hart úgy vélekedett, hogy a repülőgép képes arra, hogy „ráugorjon" az ellenség „akarati és politikai központjára", néhány órán vagy napon belül megbénítsa „a harcoló ország idegrendszerét".[31] Fuller úgy vélte, hogy a légierő és a szárazföldi erők gépesítésének hatására „a fizikai pusztítás, amely az első világháborúban érte el csúcspontját, egyre növekvő mértékben átadja a helyét az ellenség demoralizálásának és ez nemcsak a hadseregekre, hanem a polgári lakosságra is vonatkozik".[32] Ez utóbbi összefüggés rajzolódik ki Fuller gépesített háborúval kapcsolatos nézeteinek vezérfonalaként: a küzdelem intellektuális és erkölcsi dimenziója lép a „pusztítás dogmájának" helyébe, a lélektani támadás veszi át a fizikai harc, az emberi test megsemmisítéséért vívott küzdelem helyét.[33]

A légierő hadelméletének úttörői arra számítottak, hogy a civil lakosság és a létfontosságú infrastruktúrák ellen irányuló bombatámadások megtörik az ellenséges társadalom morálját, és végső soron megadásra kényszerítik az ellenséget. Ezt a várakozást végül nem váltották be a II. világháború tapasztalatai. A II. világháborúban jellemző stratégiai légibombázási műveletek, amelyeket a területbombázás vagy terrorbombázás fogalmaival is leírhatunk, nem kényszerítették térdre a szemben álló

[27] Muller 2014: 25.
[28] Krajnc 2014: 199.
[29] Jenei–Szűcs–Krajnc 2014: 33.
[30] Davis Biddle 2019: 20.
[31] Liddel Hart 1972: 30.
[32] Fuller 1972: 54–55.
[33] Fuller 1972: 54–55.

feleket, sem a tengelyhatalmak, sem a szövetségesek oldalán. Douhet, Trenchard és Mitchell teóriái mind arra a feltételezett ok-okozati összefügésre építenek, amely a légibombázás, a polgári lakosság morális összeomlása, az ellenség akaratának megtörése és a háború politikai céljának elérése között húzódik. Jóllehet a klasszikus gondolkodók különbözőképpen vélekedtek a civil lakosság bombázásának megengedhetőségéről, illetve annak felételeiről, légibombázással kapcsolatos feltételezéseik osztoznak abban az alaptézisben, hogy a légicsapások az ellenséges lakosság tudatának befolyásolásán keresztül a háborús győzelem irányába hatnak.

Stratégiai kommunikáció a légierő modern teoretikusainak gondolkodásában

A II. világháború tapasztalatait tükrözik vissza a hidegháború időszakában végrehajtott stratégiai légibombázási műveletek is. Különösképpen az amerikai területbombázási stratégia sem a koreai háborúban nem kényszerítette megadásra az ellenséget, sem a vietnámi háborúban nem omlasztotta össze az ellenség morálját. A II. világháború utáni időszak első, az ellenség morálját igazolhatóan megrendítő légihadjárata az 1990–91-es öbölháborúban a szövetséges támadás első fázisában végrehajtott amerikai légibombázási művelet volt. Az öbölháborúban sikeresnek bizonyult koncepció segítette győzelemre a NATO-t az 1999-ben Jugoszlávia ellen folytatott légihadjáratban is, habár nincs tudományos konszenzus abban a kérdésben, hogy a háborút a légierő egyedül nyerte meg,[34] esetleg a NATO szárazföldi támadás fenyegetése és/vagy az orosz diplomácia bírta kapitulációra Milošević elnököt.[35] Az öbölháborús koncepció alapozta meg a kezdeti stratégiai és politikai sikereket az USA afganisztáni és iraki műveleteiben a 2000-es évek elején. A NATO által 2011-ben Líbia ellen végrehajtott légihadművelet a repüléstilalmi zóna kiterjedt alkalmazására jelent példát, amely magában foglalja a szárazföldi csapatmozgások és csoportosítások tilalmát is, és ezáltal megakadályozza az ellenséges csapatok felfejlődését.[36] A NATO légihadműevelete hozzájárult a felkelők területszerzéséhez,[37] és végső soron kulcsfontosságúnak bizonyult a Kadhafi-ellenes koalíció győzelmében.[38]

A légierő-elméletek megújításában kulcsszerepet betöltő, a koreai és vietnámi háborúk tapasztalataiból merítő, John R. Boyd, amerikai légierő-teoretikus, „koncepcionális megközelítése az ellenség pszichológiai megbénításán alapul […], elméletei a konfliktus kognitív és erkölcsi szféráira helyezik a hangsúlyt".[39] Boyd hadelméletének központ fogalma az OODA,[40] amely az angol megfigyelni, eligazodni, dönteni, cselekedni igékből alkotott betűszó. Boyd ciklikusan ismétlődő folyamatkét írta le az OODA-t, amelyet nemcsak a légiküzdelem taktikai szintjén, hanem a hadviselés magasabb

[34] Olsen 2015: 15.
[35] Henriksen 2008: 824.
[36] Stephens 2015: 283.
[37] Petersson 2023.
[38] Stephens 2015: 285.
[39] Olsen 2015: 20.
[40] Observe – Orient – Decide – Act.

szintjén is érvényesnek tartott. Stratégiai értelemben az eligazodás válik a folyamat központi fázisává, amelynek sikere a helyzetelemzés eredetiségén és a gondolkodás kreativitásán múlik.[41] Boyd olyan stratégia mellett szállt síkra, amely az ellenség vezetésének tudatát célozza meg.[42] Jóllehet Boyd az általános érvényesség igényével fogalmazta meg teóriáját, „a sebességre és az ellenség dezorientáló hatású meglepésére helyezett hangsúly […] különösen a légihadviselés területén tűnik érvényesnek […]".[43] Boyd manőverrel kapcsolatos elgondolása alapvetően kognitív meghatározottságú,[44] magában foglalja a „meglepés, sokkhatás, megtévesztés és kétértelműség fogalmait, megtöri az ellenség kohézióját, zűrzavart és pánikot okoz.[45]

Az 1990–91-es öbölháborúban az amerikai légihadjárat[46] stratégiai koncepcióját megalkotó John A. Warden a felszínen szkeptikus volt a polgári lakosság moráljának megtörését illetően.[47] Hadelméleti gondolkodásának középpontjában az ellenség stratégiai megbénítása állt, és jóllehet Warden felismerte ennek fizikai és pszichológiai összetevőit, ez utóbbiakat rendkívül nehezen mérhetőnek vagy beazonosíthatónak ítélte meg.[48] Ugyanakkor Warden koncepciója mégiscsak erősen lélektani jellegű, amennyiben „ellentmondást nem tűrő fókuszt helyezett a vezetésre, az ellenséges elit tudatára".[49] Warden a vezetés elpusztítását vagy elszigetelését tartotta az ellenséges állam feletti győzelem leghatékonyabb és leghatásosabb módjának.[50] Az ellenség súlypontjainak, különösen a kulcsfontosságú gazdasági, kommunikációs és vezetési struktúráinak, egyidejű, precíz, célzott támadásán keresztül igyekezett az ellenfelet megbénítani és megadásra kényszeríteni.[51] Warden ez irányú gondolkodásáról sokat elmond az a kijelentése, miszerint „meg kell szabadulnunk attól a gondolattól, hogy a háború központi jellemzője a katonai erők összecsapása".[52] Habár az öbölháborús légihadjárat tényleges hatásmechanizmusát illetően nincs teljes egyetértés, a hadjárat mégis széles körben sikeres megítélés alá esik.[53] Ennek egyik oka, hogy az amerikai légicsapások aláásták az iraki szárazföldi erők erkölcsi ellenálló képességét: az iraki frontcsapatok 20-40%-a dezertált a szárazföldi támadás megindítása előtt.[54] Warden elbeszélésében[55] az iraki kommunikációs rendszerek megbénítása többek között azt a célt akarta elérni, hogy aláássa Szaddám Husszein imázsát és jelenlétét a lakosság hétköznapjaiban. Warden abban bízott, hogy az Irak ellen folytatott légihadjárat előidézi a Szaddám-rendszer összeomlását, de elgondolása nem adott választ arra az alapvető jelentőségű kérdésre, hogy az ellenség megbénítása pontosan hogyan vezet

41 Mellinger 2001: 142.
42 Mellinger 2001: 142.
43 Mellinger 2001: 142.
44 Davis Biddle 2019: 43.
45 Davis Biddle 2019: 44.
46 „Instant Thunder" kódnevű légi hadjárat.
47 Ward 2006: 11.
48 Stephens 2015: 268.
49 Stephens 2015: 268.
50 Ward 2006: 11.
51 Hunter Ward 2020: 31.
52 Ward 2006: 11.
53 Gurantz 2022: 125.
54 Davis Biddle 2019: 49.
55 Warden 1997: 182.

majd el az ellenséges nemzet küzdeni akarásának megtöréséhez.[56] Utólag Warden azzal magyarázta a kívánt hatás elmaradását, hogy nem került sor a Szaddám-rendszer ellenajánlatát megfogalmazó stratégiai lélektani műveleti kampányra, amely ugyanolyan fontos lett volna, mint a légibombázási műveletek. Warden felidézi, hogy épp erre tett javaslatot a szövetséges erők parancsnokának, Schwartzkopf tábornoknak, de egy ilyen erőfeszítésre nem mutatkozott fogadókészség a politikai vezetés részéről.[57]

A hatásalapú műveletek teoretikusaként ismertté vált[58] David A. Deptula részt vett az öbölháborús amerikai légihadjárat megtervezésében, és a bombázás megkezdésekor személyesen üzente meg az iraki civil lakosságnak a nemzetközi médiában, hogy „amint megszabadultok Szaddámtól, újra lesz áram".[59] Deptula hatásalapú műveletek koncepciója arra a felismerésre épít, hogy egy légicsapás sikerét nem feltétlen a pusztítás mértéke, hanem annak hatása határozza meg. Az öbölháborús légihadjárat példájából kiindulva, egy iraki erőmű lerombolása helyett bizonyos rendszerelemek kiiktatása is elégségesnek bizonyult annak a hatásnak az eléréséhez, hogy Bagdad egyik körzetében átmenetileg szüneteljen az áramszolgáltatás.[60] Deptula teóriájának központi – és a háború lezárása szempontjából kritikus – eleme a lakosság akaratának és a vezetésbe vetett bizalmának megtörése, és az ilyen irányba ható műveleteket hatékonyabbnak ítélte a katonai célpontok támadásánál.[61] A hatásalapú műveletek koncepciójához kapcsolódik a párhuzamos hadviselés elgondolása, amelynek lényege, hogy számos repülőgép egyidejűleg mér csapást a teljes hadszíntéren, az ellenség megbénításának, nem pedig megsemmisítésének céljából.[62] A hatásalapú műveletek „végrehajtása olyan kifinomult megfigyelési és precíziós csapásmérő képességeken múlik, amelyek alkalmasak az ellenség döntéshozatali képességének összeomlasztására, zavart, félelmet és a reménytelenség érzését keltik, ami pedig fatális ballépéshez, megadáshoz vagy bénító hatású akaratvesztéshez vezet".[63]

Összegezve, Boyd, Warden és Deptula légierő-elméleteinek közös szála az ellenség megbénítása, amely közvetve vagy közvetlenül, a légierő kognitív dimenzióban gyakorolt hatásából ered. Boyd elmélete elsősorban az ellenség lélektani, míg Warden és Deptula elmélete elsősorban az ellenség fizikai megbénítását célozza.[64] Ugyanakkor Warden és Deptula elméletei azt feltételezik, hogy az ellenség fizikai megbénítása, amely a minimálisan szükséges mértékű rombolást foglalja csak magában, az ellenséges társadalom vagy vezetés körében olyan kognitív hatást vált ki, amely ellehetetleníti a háborús erőfeszítés fenntartását, ezáltal győzelemre vezet.

[56] Henriksen 2008: 850.
[57] Warden 1997: 182.
[58] Davis Biddle 2019: 50.
[59] Graham 2006: 182.
[60] Mellinger 2018: 41.
[61] Ward 2006: 12.
[62] Olsen 2018: 16.
[63] Tomes 2006: 54.
[64] Olsen 2015: 20.

Következtetések

A lefolytatott vizsgálat igazolta a kutatómunka alapját képező hipotézist, vagyis azt, hogy a légierő-elméletek magukban foglalják a légihadviselés és a stratégiai kommunikáció összefüggéseit. A vizsgált elméletek mindegyike megfogalmaz olyan összefüggéseket a légierő alkalmazásával, különösen a légibombázással, kapcsolatban, amelyek a stratégiai kommunikáció értelmezési keretébe esnek. Ezek közül legjellemzőbb az ellenséges ország polgári lakosságának és vezetésének olyan jellegű tudati befolyásolása, amely a támadó fél háborús sikerének irányába hat.

A légierő-elméletek a kezdetektől fogva rendkívül erős stratégiai kommunikációs hatást tulajdonítottak az új haderőnemnek, feltételezve, hogy a légicsapások lélektani hatása felülmúlja azok fizikai hatását. A klasszikus teoretikusok a hadban álló társadalom erkölcsének megtörését tekintették annak a kritikus kapocsnak, ami a fizikai pusztítást az ellenség vereségbe kényszerítésével köti össze. E hatásmechanizmus beindítására pedig különösen alkalmasnak találták a légierőt. Hasonló feltételezés fut végig a modern légierő-elméleteken is: az ellenség megbénítása, a szükséges mértékű és célzott fizikai rombolás útján, olyan kognitív hatást vált ki a társadalomban és az ellenséges vezetésben, amely összeomlást okoz. Mind a klasszikus, mind a modern légierő-elméletek elemzéséből arra következtetünk, hogy a légierő alkalmazásának feltételezett stratégiai kommunikációs hatása kulcsfontosságú a háború céljának eléréséhez, vagyis akaratunk rákényszerítéséhez a szemben álló félre.

Ugyanakkor a légierő-elméletek adósak maradnak annak magyarázatával, hogy a stratégiai kommunikációs hatások és kölcsönhatások milyen láncolata vezet a légicsapástól az ellenség ellenállásának megtöréséig. Ebben a tekintetben további tudományos kutatás tárgyát képezheti az ok-okozati összefüggéslánc két csomópontja: a légicsapás nyomán az ellenség körében kiváltott kognitív hatásra vonatkozó általános érvényű összefüggések, valamint az előidézett kognitív hatás és a háborús cél elérése között feltárható törvényszerűségek.

Irodalomjegyzék

Althuis, J. et al. (2023): *Understanding Strategic Communications: NATO Strategic Communications Centre of Excellence Terminology Working Group Publication No. 3*. Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/pdfjs/?file=/publications/download/Terminology-Report-No3-DIGITAL.pdf?zoom=page-fit

Berkland, David (2011): Douhet, Trenchard, Michell and the Future of Airpower. *Defence & Security Analysis,* 27(4), 389–393. Online: https://doi.org/10.1080/14751798.2011.632256

Csengeri János (2017): A légierő, mint a geostratégiai törekvések egyik meghatározó eszköze. *Repüléstudományi Szemelvények,* 31–66. Online: https://repulestudomany.hu/kiadvanyok/RepSzem-2017.pdf

Davis Biddle, Tami (2019): *Air Power and Warfare: A Century of Theory and History.* [H. n.]: United States Army War College Press. Online: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1377&context=monographs

Douhet, Giulio (1971): *A Légiuralom. Szemelvények a burzsoá katonai teoretikusok műveiből*. Ford. Tandori Dezső. [H.n.]: Zrínyi Miklós Katonai Akadémia.

Fuller, J. F. C. (1972): Előadások. In Száva Péter (szerk.): *A páncélos háború elméletének képviselői. Szemelvények a burzsoá katonai teoretikusok műveiből 3*. Budapest: Zrínyi Miklós Katonai Akadémia, 49–103.

Graham, Stephen (2006): Switching Cities Off. *City,* 9(2), 169–194. Online: https://doi.org/10.1080/13604810500196956

Gurantz, Ron (2022): Does Punishment Work? Selection Effects in Air Power Theory. *Comparative Strategy,* 41(2), 123–134. Online: https://doi.org/10.1080/01495933.2022.2039005

Hallahan, Kirk et al. (2007): Defining Strategic Communication. *International Journal of Strategic Communication,* 1(1), 3–35. Online: https://doi.org/10.1080/15531180701285244

Henriksen, Dag (2008): Inflexible Response: Diplomacy, Airpower and the Kosovo Crisis, 1998–1999. *Journal of Strategic Studies,* 31(6), 825–858. Online: https://doi.org/10.1080/01402390802373131

Heuser, Beatrice (2013): Misleading Paradigms of War: States and Non-State Actors, Combatants and Non-Combatants. *War & Society,* 27(2), 1–24. Online: https://doi.org/10.1179/072924708791329190

Hunter Ward, Robert (2020): Fewer Civilian Casualties: Trending Toward a Constraint on the Use of Force. *Comparative Strategy,* 39(1), 29–40. Online: https://doi.org/10.1080/01495933.2020.1702345

Jenei Imre – Szűcs Pál – Krajnc Zoltán (2014): William Mitchell Légierő Értelmezése (2.) (Műveleti és Szervezeti Elképzelései, Hatása a Légi Hadviselés és a Légierő Ügyére). *Repüléstudományi Közlemények,* 26(1), 31–38. Online: https://repules-tudomany.hu/folyoirat/2014_1/2014-1-04-Jenei_I-Szucs_P-Krajnc%20Z_2.pdf

Krajnc Zoltán (2017): A légierő eszmerendszerként való értelmezése. In Krajnc Zoltán (szerk.): *A katonai vezetői-parancsnoki (harcászati vezetői) kompetenciák fejlesztésének lehetséges stratégiája (tanulmánykötet).* Budapest: Nemzeti Közszolgálati Egyetem, 192–212.

Liddel Hart, B. H. (1972): Emlékiratok. In Száva Péter (szerk.): *A páncélos háború elméletének képviselői. Szemelvények a burzsoá katonai teoretikusok műveiből 3*. Budapest: Zrínyi Miklós Katonai Akadémia, 5–47.

Magyar Honvédség (MH) (2015): *Légi Műveletek Doktrína*. 1. kiadás. MH DOFT kód: MD 3.3 (1).

Mellinger, Phillip S. (2001): *Airmen and Air Theory. A Review of the Sources.* Alabama: Air University Press, Maxwell Air Force Base. Online: www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0013_MEILINGER_AIRMEN_AIR_THEORY.PDF

Mellinger, Phillip S. (2018): Air Power Theory. In Olsen, John Andreas (szerk.): *Routledge Handbook of Air Power* [ePub]. Abingdon: Routledge, 35–46. Online: https://doi.org/10.4324/9781315208138

Mueller, Karl P. (2010): *Air Power.* Online: www.rand.org/pubs/reprints/RP1412.html

Muller, Richard R. (2014): The Origins of Mad: A Short History of City-Busting. In Sokolski, Henry D. (szerk.): *Getting Mad: Nuclear Mutual Assured Destruction, Its Origins and Practice.* [H. n.]: Strategic Studies Institute, US Army War College, 15–50. Online: www.jstor.org/stable/resrep12035.5.

NATO (2016): *AJP 3.3 – Allied Joint Doctrine for Air and Space Operations*. Edition B Version 1. NATO Standardization Office (NSO), NATO. Online: https://assets.publishing.service.gov.uk/media/5a82d7bc40f0b62305b94a32/doctrine_nato_air_space_ops_ajp_3_3.pdf

NATO (2023): *AJP-10 Allied Joint Doctrine for Strategic Communications*. Edition A Version 1. With UK National Elements. NATO Standardization Office (NSO), NATO. Online: https://assets.publishing.service.gov.uk/media/6525459d-244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf

Németh József Lajos (2013): A (stratégiai) kommunikáció és a háború kapcsolata napjainkban. *Hadtudomány,* 23(1–2), 129–139. Online: www.mhtt.eu/hadtudomany/2013/1_2/HT_2013_1-2_Nemeth_Jozsef.pdf

Olsen, John Andreas (2015): Introduction. Airpower and Startegy. In Olsen, John Andreas (szerk.): *Airpower Reborn* [ePub]. Annapolis: Naval Institute Press, 13–28. Online: www.scribd.com/read/362570562/Airpower-Reborn-The-Strategic-Concepts-of-John-Warden-and-John-Boyd#

Olsen, John Andreas (2018): Understanding Modern Airpower. *The RUSI Journal,* 163(3), 12–20. Online: https://doi.org/10.1080/03071847.2018.1494350

Petersson, Emil (2023): Looking to the Skies: Operation Unified Protector and the Strategy of Aerial Intervention. *International Interactions,* 49(5), 813–844. Online: https://doi.org/10.1080/03050629.2023.2250901

Stephens, Alan (2015): Fifth-Generation Startegy. In Olsen, John Andreas (szerk.): *Airpower Reborn* [ePub]. Annapolis: Naval Institute Press, 243–293. Online: www.scribd.com/read/362570562/Airpower-Reborn-The-Strategic-Concepts-of-John-Warden-and-John-Boyd#

Szűcs Pál – Krajnc Zoltán (2014): Hugh Trenchard Légierő Értelmezése. *Repüléstudományi Közlemények,* 26(1), 18–24. Online: https://repulestudomany.hu/folyoirat/2014_1/2014-1-02-Szucs_P-Krajnc_Z.pdf

Tomes, Robert (2006): Schlock and Blah: Counter-insurgency Realities in a Rapid Dominance Era. *Small Wars & Insurgencies,* 16(1), 37–56. Online: https://doi.org/10.1080/0959231042000322558

Torp, S. M. (2015): The Strategic Turn in Communication Science: On the History and Role of Strategy in Communication Science from Ancient Greece Until the Present Day. In Holtzhausen, D. R. – Zerfass, A. (szerk.): *The Routledge Handbook of Strategic Communication.* New York: Routledge, 34–52.

United Kingdom (UK) Ministry of Defence (MoD) (2022): *Joint Doctrine Publication 0-30. UK Air Power.* Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1116428/UK_Air_Power_JDP_0_30.pdf

United States (U.S.) Air Force (2021): *Air Force Doctrine Publication One. The Air Force.* Online: www.doctrine.af.mil/Portals/61/documents/AFDP_1/AFDP-1.pdf

Tartalom