HADMÉRNÖK

Kiemelt közlemények

18. évf. (2023)
3. 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: Gergely Zsuzsánna, Nagy Judit, Resofszki Ágnes

Tartalom

Védeleminformatika

Fórum

Könyvismertető

HADMÉRNÖK
KATONAI MŰSZAKI INFRASTRUKTÚRA

18. évfolyam (2023) 3. szám 5–17.
DOI: 10.32567/hm.2023.3.1

Ember István[1]

Additív eljárással készült lineáris vágótöltetek működésének vizsgálata[2]

Performance Testing of Additive Linear Cutting Charges

Absztrakt

Napjaink egyik rohamosan fejlődő területe a 3D nyomtatás, amely több évtizedes múltra tekint vissza, mégis csak most lett széles körben elterjedt. Az additív eljárások sok lehetőséget biztosítanak alkatrészek készítésére. Az egyik ilyen terület, ahol alkalmazni lehet ezt a gyártási módszert, a robbantástechnika. Az egyedi töltetek és a kumulatív robbantási feladatok területén jelentős mozgásteret ad ez a technológia, azonban az alacsony sűrűségű alapanyagok esetében nem minden részterületen rendelkezünk kellő tapasztalattal. A bemutatott tesztben sikerült több ilyen töltet működését megvizsgálni robbantás után a céltárgyak elemzésével. Többek között az optimális vágáshoz szükséges távolságot is sikerült azonosítani, ami hasznos ismeret lesz a további töltetek tervezésénél.

Kulcsszavak: hatásvizsgálat, 3D nyomtatás, vágótöltet, robbantás, PLA

Abstract

3D printing is one of today's fast-growing fields, with a history stretching back decades, yet it is only now becoming a widespread solution. Additive processes offer many possibilities for the manufacture of components. One of the areas where this manufacturing method

[1] Egyetemi tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Műveleti Támogató Tanszék; doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtudományi Doktori Iskola, 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.

can be applied is the blasting technology. For customized charges and cumulative blasting tasks, this technology offers considerable scope, but for low-density materials, we do not always have sufficient experience in these areas. In the study presented, it was possible to investigate the performance of several such charges by analysing targets after blasting. Among others, the optimal distance for cutting was identified. This will be useful knowledge for the design of further charges.

Keywords: efficiency trial, 3D printing, cutting charge, blasting, PLA

Bevezetés

Az additív gyártás alkalmazása széles körben elterjedt napjainkban. Egyre több háztartásban jelenik meg 3D nyomtatásra képes technikai eszköz, amely megkönnyíti a hétköznapokat, és eddig pótolhatatlannak gondolt alkatrészek és tárgyak válnak olcsón és gyorsan[3] elérhetővé általa.

A katonai alkalmazás területén is egyre nagyobb teret hódít magának[4] ez a korántsem új, de jelenleg még felfutó módszer. Az oktatást támogató eszközöktől[5] egészen az egyedi és nagy teherbírású alkatrészekig szinte minden elkészíthető 3D nyomtatással. Az additív gyártásra képes eszközök alkalmazása éppen ezért illeszkedik a hadtudományok tekintetében kijelölt fő kutatási irányokhoz.[6] Meg kell említeni, hogy vannak kihívói ennek a területnek, ugyanis a mesterséges intelligencia alkalmazásának katonai módozatai, lehetőségei[7] szintén nagy figyelemnek örvendenek napjainkban.

Nem mehetünk el a gondolat mellett, hogy az eljárás és annak széles körben elterjedt módozatai kifejezetten olcsó megoldást biztosítanak egy-egy problémára, azonban ez esetenként némi tervezési, gyártási tapasztalatot, ismeretet igényel. Előbbire főleg abban az esetben van szükség, ha a nyomtatásra tervezett tárgy már elkészült 3D modellje nem elérhető az internet valamelyik letöltőplatformján ingyenes vagy fizetős formában.

Természetesen a haditechnikai vagy robbantástechnikai vonatkozású sablonok nem hozzáférhetők a fenti módszerrel, éppen ezért tervezni és kivitelezni egyaránt szükséges őket egy-egy kutatáshoz. Az általam vizsgált kumulatív nyújtott töltetek, vagy közismertebb nevükön vágótöltetek esetében is ez a helyzet. A tervezési nehézségek és a kialakítatlan gyártási menet ellenére azonban szükséges, hogy a robbantástechnikába is bekerüljön az eljárás.

A fent nevezett vágótöltetek általánosságban valamilyen brizáns,[8] bináris[9] robbanóanyaggal készülnek el. A robbanás energiájának fókuszálásával[10] képesek főleg fémből készült tárgyak darabolására, anyagfolytonosságuk részleges vagy teljes megszüntetésére.

[3] Gál–Németh 2019: 233.
[4] Végvári–Hegedűs–Zentay 2022: 58–62.
[5] Gyarmati–Hegedűs–Gávay 2022: 125–126.
[6] Boda et al. 2016: 1–23.
[7] Németh–Virágh 2022: 21; Fazekas 2022: 51–52; Tóth–Vég 2022: 114.
[8] Lukács 2017: 26.
[9] Kugyela 2020: 58–75.
[10] Lukács 2010: 175–185.

A bemutatott vizsgálatban az additív gyártás egyik módszerével készült vágótöltetek működését fogom megvizsgálni, kifejezetten azok vágásmintáját. Elvárásaim szerint sikerül majd megállapítani egy értéket, amely tükrözi, hogy a töltet gyutacsoldali végén milyen távolságban fut fel a detonáció a robbanóanyagban olyan szintre, hogy kialakuljon a töltet optimális vágóhatása. Mindezt olyan töltetek esetében, amelyek nem tartalmaznak fém komponenst, kizárólag alacsony sűrűségű anyagokból készülnek.

A fő cél megvizsgálni a töltetek általános működési hatékonyságát és adatokat gyűjteni a vágás méretéről a céltárgyakon. Ez adatot szolgáltat majd további kumulatív idomtöltetek tervezéséhez, amelyek esetében kifejezetten az optimális vágáshoz szükséges felfutási távolság lesz majd fontos. Ez utóbbira feltételezésem az, hogy 20 mm körüli értékkel kell majd számolni.

A vizsgált töltetek

Ebben a vizsgálatban politejsav (PLA[11]) alapanyagból készült töltetekkel végeztem empirikus teszteket. Több szempontból is praktikus ez az anyag. Valamennyivel könnyebben bomlik, mint a polimerek általában, könnyen beszerezhető, könnyen nyomtatható, és mivel elterjedt az additív gyártásban, nagy tapasztalat áll rendelkezésre vele kapcsolatban. Korábban már volt szerencsém az alapanyagot hasonló kutatási projektnél alkalmazni.[12]

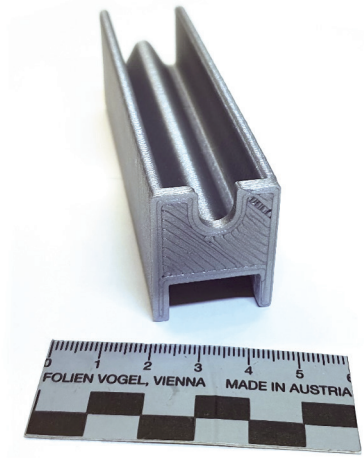
A vágótölteteket lineáris formában alakítottam ki. A falvastagságuk egyaránt 3 mm a teljes test esetében. Ezt az adatot korábbi eredményeimre alapozva határoztam meg, amelyeket kumulatív töltetek hatékonyságának vizsgálatakor értem el.[13] A hivatkozott kutatás azt mutatja, hogy ennél akár vékonyabb is lehet a kumulatív béléstest jobb hatékonysággal,[14] de ezt az eredményt egyelőre nem találtam teljesen megalapozottnak.

Az indított végén a gyutacs behelyezésére egy zárólapot terveztem, amely központi helyzetben tartja a gyújtási lánc első elemét. A központi helyzet kifejezetten fontos szempont, mert így ideális körülmények mellett fut fel a detonációs sebesség a robbanóanyag teljes keresztmetszetében.

A béléstest egy egészet képez a töltetházzal. A vizsgált változatoknál a vágóél két hajlítási szögben készült: 60° és 90°. Ezzel szeretnék átfogóbb képet kapni az esetleges további fejlesztési irányokhoz. A hajlított vágóélek nyílástávolságát 10 mm-ben határoztam meg mindkét változat esetében.

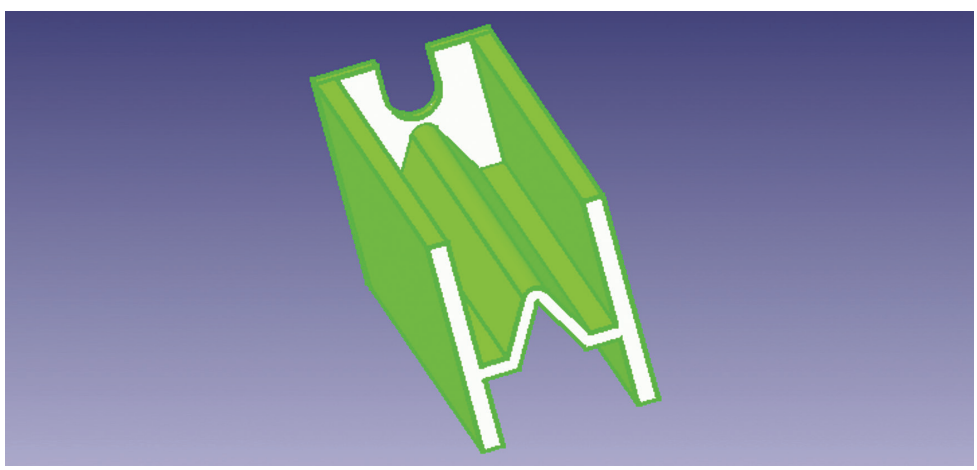
Az 1. ábrán egy 60°-os változatot mutatok be, amelynek felületén jól láthatók az additív gyártás rétegei.

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



1. ábra: 60°-os lineáris vágótöltet
Forrás: a szerző felvétele

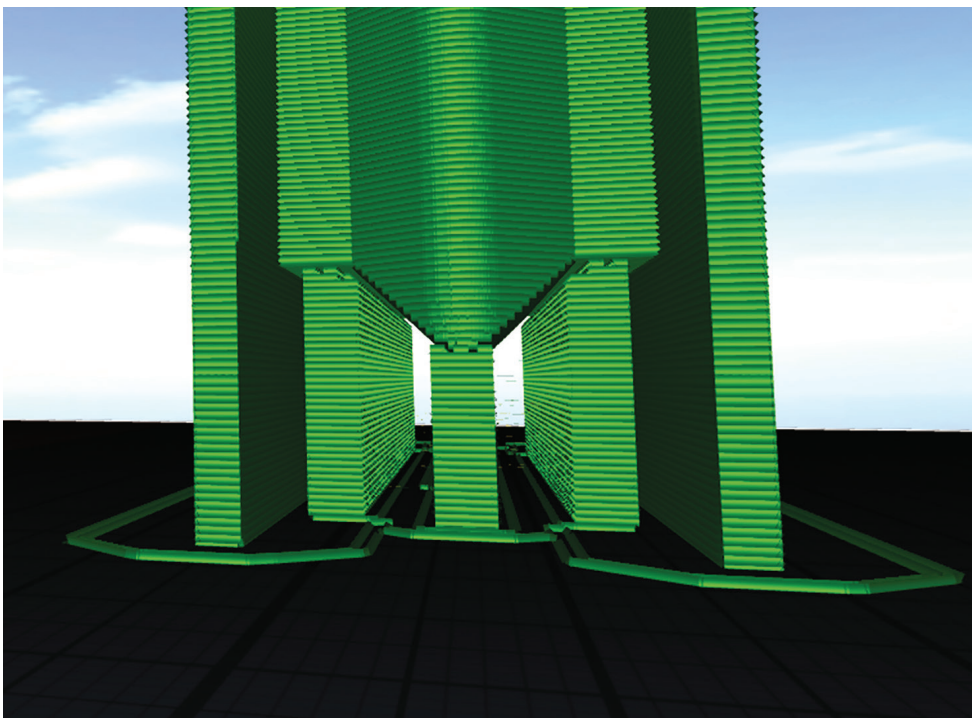
A 3D modellek elkészítésére számítógéppel támogatott tervezési formát (CAD[15]) választottam, amely elengedhetetlen az additív gyártás általam alkalmazott módszeréhez. A számítógépes modelleket (2. ábra) FreeCAD 0.19 szoftverrel készítettem. A töltetek elkészítéséhez használt 3D nyomtató „duál extruderes"[16] CraftBot 3 típus volt, amelyet 0,8 mm-es fúvókával szereltem a feladathoz. Ez utóbbi lehetővé tette, hogy viszonylag gyorsan, de kevésbé sima felülettel készüljenek el a munkadarabok. A gyártáshoz ugyanazon gyártó egyező színű és paraméterekkel rendelkező termékét használtam fel alapanyagként.



2. ábra: 60°-os lineáris vágótöltet CAD-modellje a tervezőszoftver felületén
Forrás: a szerző szerkesztése

[15] Angolul: computer-aided design.
[16] Két nyomtatófej egyidejű vagy váltott alkalmazására képes.

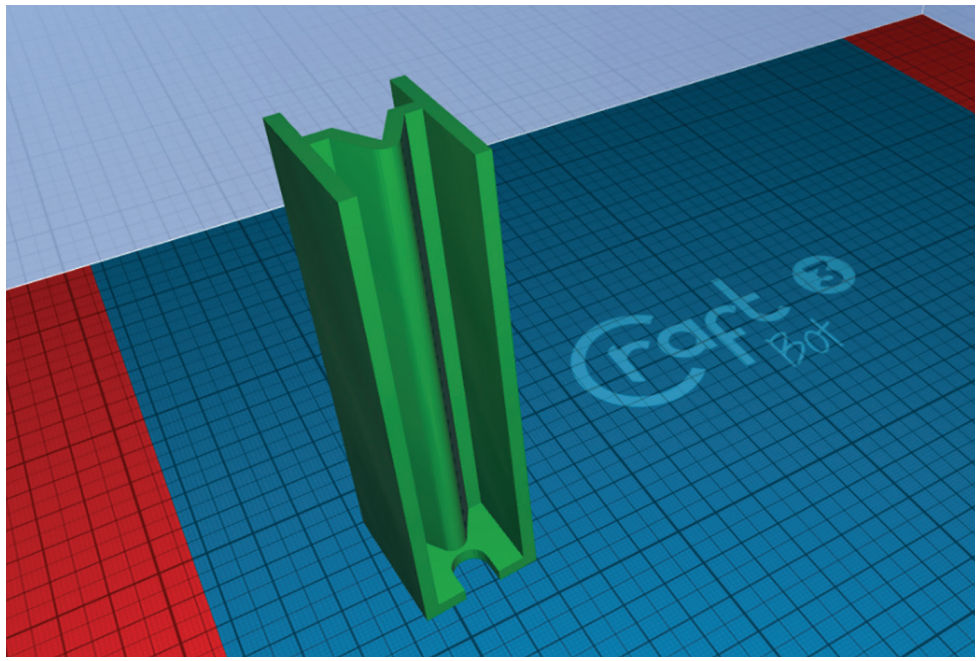
Mivel a fent nevezett nyomtató szálhúzásos vagy szálolvasztásos (FDM[17]) rendszerű gyártást tesz lehetővé, a modell kialakítása és szeletelése is ehhez a folyamathoz lett optimalizálva. Ennek keretében több dologra is figyelmet kellett fordítani, de a támaszok elhelyezkedéséből és mennyiségéből adódó szempontok voltak a legfontosabbak. A támaszok elengedhetetlenek egy bizonyos építési szög felett vagy a modell „lebegő" részei esetében (3. ábra), viszont eltávolításuk esetenként érdes felületeket hagy maga után, ritkábban akár rongálhatja is az alkatrészt.



3. ábra: Gyártási támasz egy idom vágótöltet esetében
Forrás: a szerző szerkesztése

A gyártás időszükséglete nem volt jelentős. Állított pozícióban (4. ábra) a 60°-os töltet elkészítése a szoftver előrejelzése alapján 1 óra és 14 perc, míg a kisebb, 90°-os változatnál ez 1 óra és 2 perc volt. A jelzett adatok a valóságban nem voltak pontosak, a tárgyak hozzávetőleg 10%-os időtöbblettel készültek el. A felhasznált filament hosszát 13, valamint 11,2 m-re kalkulálta g-code[18] előállításakor a CraftWare szoftver.

[17] Angolul: fused deposition modelling.
[18] A 3D nyomtató számra feldolgozásra alkalmas fájl, mely tartalmazza a szükséges gyártási paramétereket.



4. ábra: 60°-os lineáris vágótöltet megjelenítése a CraftWare szoftverben
Forrás: a szerző szerkesztése

A vizsgálat körülményei

A tesztrobbantásra Táborfalván került sor a Magyar Honvédség (MH) robbantási területén, a végrehajtásban pedig a MH 1. Tűzszerész és Folyaműr Ezred (MH 1. TFE) szakállománya segédkezett és biztosította feltételeket.

A robbantási feladatot villamos gyújtóhálózattal hajtottam végre, amelyben a gyutacsok soros kapcsolásba voltak rendezve. A vágótölteteket Semtex-H típusú robbanóanyaggal töltöttem fel, amely kiváló tulajdonságokkal rendelkezik a katonai robbantásokhoz.[19] A tölteten kialakított nyílásba helyeztem a villamos gyutacsokat, amelyek pontosan 10 mm-t hatoltak be a töltet belsejébe. A robbantás során a tölteteket olyan térközzel helyeztem el, hogy azok egymásra ne lehessenek az eredményt befolyásoló hatással. Mivel a robbantásoknál a legfontosabb tényező a biztonságos végrehajtás,[20] egy 150 cm mély árok alján kialakított 30 × 30 cm-es alapterületű és 30 cm mély üregekben helyeztem el a céltárgyakat a rájuk rögzített töltetekkel.

A kialakított töltetek tömegének adatait az 1. táblázatban láthatjuk, amely azt is megmutatja, hogy típusonként 3–3 db robbantásával hajtottam végre a teszteket. Minden változat 100 mm hosszúságú volt, az eltartást a vágóél szélességében

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

(10 mm) határoztam meg. Mindegyik rövidítésekből álló elnevezést kapott, amely a vágóél belső szélességéből mm-ben, a vágóél hajlási szögéből és a töltet alakjának jelzéséből tevődött össze.

1. táblázat: A felrobbantott töltetek paraméterei

Fsz.	Típus	Töltetház tömege (g)	Robbanóanyag tömege (g)	Szerelt tömege (g)
1.	10–60–LIN	15	63	78
2.	10–60–LIN	15	63	78
3.	10–60–LIN	15	63	78
4.	10–90–LIN	15	54	69
5.	10–90–LIN	15	54	69
6.	10–90–LIN	15	54	69

Forrás: a szerző szerkesztése

A töltetházak tömegének adatai teljesen egységes képet adtak. A gyártásnál és a feltöltésnél sem volt probléma az egyező tömeg elérése. A robbanóanyag esetében ez kifejezetten fontos szempont lehet, bár kismértékű eltérés vélhetően nem befolyásolná mértékadó módon az eredményeket.

A céltárgyak mindegyike szabványos 50 mm-es, melegen hengerelt „U" szelvény volt. Ezeket egy teljes, 6 m hosszú szálból vágtam 150 mm-es darabokra. A tölteteket a szelvény hossztengelyében helyeztem el, azokat pontosan a végéhez igazítva, hogy mérhető eredményt kaphassak a hatékony vágás kialakulásának távolságáról. A rögzítést szigetelőszalaggal oldottam meg, ami kellően stabilnak bizonyult.

A robbantás előkészítésének a folyamata az alábbi lépésekből állt:

- a töltetek feltöltése plasztikus robbanóanyaggal;
- a töltetek tömegének ellenőrzése digitális mérleggel;
- a töltetek rögzítése a céltárgyakhoz ragasztószalaggal;
- a céltárgyak és a töltetek behelyezése a robbantásra kialakított gödrökbe;
- a villamos gyutacsok behelyezése a töltetekbe.

A vizsgálati eredmények

Az 1. töltet (5. ábra) esetében a céltárgy felületén 105 mm-es szakaszon látható vágás, és további 30 mm-en folytatólagos repedés található a felületen. A vágott rész szélessége 16–48 mm közötti értéket mutat. A vágás első 10–20 mm-es szakasza egyenetlen, tépéses felületet mutat, ami arra utal, hogy ezen a szakaszon a töltet vágó hatása még nem érvényesült teljesen, az anyagfolytonosságot vélhetően a további erőhatások szüntették meg, nem pedig az alapfunkció.

5. ábra: Az 1. töltet a céltárgyon és a vágás eredménye
Forrás: a szerző felvétele

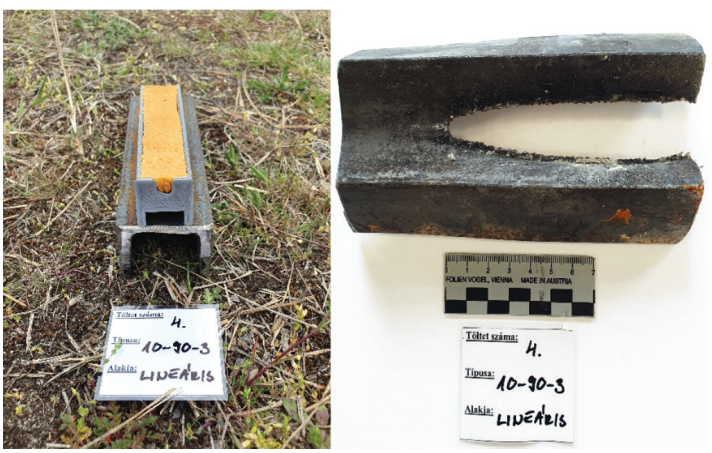
A 2. töltet (6. ábra) esetében a céltárgy felületén 102 mm-es szakaszon azonosítható vágás, és a teljes felület folytatólagosan elrepedt. A vágás első 10 mm-es szakasza egyenetlen, és itt is tépéses felületet mutat.

6. ábra: A 2. töltet a céltárgyon és a vágás eredménye
Forrás: a szerző felvétele

A 3. töltet (7. ábra) esetében a céltárgy felületén 108 mm-es szakaszon látható vágás, és további 13 mm-en folytatólagosan elrepedt a felület. A vágás szélessége 10–30 mm között változik. A vágott szakasz első 10–20 mm-es szakasza ebben az esetben is egyenetlen, szakadásos felületet mutat.

7. ábra: A 3. töltet a céltárgyon és a vágás eredménye
Forrás: a szerző felvétele

A 4. töltet (8. ábra) esetében a céltárgy felületén 106 mm-es szakaszon azonosíthatunk vágást, amely további 13 mm-en repedést okozott a felületen. A vágás szélessége 5–20 mm között változik. A vágott szakasz elején 10–15 mm hosszan tépett felület látható.



8. ábra: A 4. töltet a céltárgyon és a vágás eredménye
Forrás: a szerző felvétele

Az 5. töltet (9. ábra) esetében a céltárgy felületén 110 mm-es szakaszon látható vágás és további 12 mm-en repedés, amely folytatólagos a vágás irányára. A vágott szakasz szélessége 3–27 mm közötti. A vágott szakasz 22 mm hosszan szakadással kezdődik.

9. ábra: Az 5. töltet a céltárgyon és a vágás eredménye
Forrás: a szerző felvétele

A 6. töltet (10. ábra) esetében a céltárgy felületén 107 mm-es szakaszon azonosíthatunk vágást és további 11 mm-en repedést, amely folytatólagos a vágás irányára. A vágott szakasz szélessége 6–22 mm közötti. A vágott szakasz 20–22 mm hosszan szakadással indul.

10. ábra: A 6. töltet a céltárgyon és a vágás eredménye
Forrás: a szerző felvétele

Összegzés

Az elvégzett tesztek alapján kialakult egy jól látható kép az additív eljárással készített vágótöltetekről. Ezek a robbantások bemutatták, hogy lehetséges olyan hatékonyan működő töltetet készíteni, amely képes az 5 mm vastag homogén acélt elvágni. A céltárgyak mindegyikénél bekövetkezett a vágás, és viszonylag hasonló eredményt mutatott a hossz tekintetében, amely 102–110 mm közötti volt. A vágott felületek között már ennél nagyobb volt a szórás a nyílás méretének esetében, de ezt nem vizsgáltam tüzetesebben, hiszen a legkisebb méret is megfelel az elvárásoknak. A vágott szakaszok után minden esetben folytatólagos repedés volt tapasztalható, amely 11 mm-től a teljes hosszig terjedt. A vágott szakaszok elején 10–22 mm intervallumban volt tapasztalható tépett perem, ami arra utalt, hogy a vágás még nem alakulhatott ki, a felület vélhetően a robbanás egyéb erőhatásaitól vált el.

Ezek az adatok alátámasztják a feltételezésemet, amely szerint az 1 cm-re behelyezett gyutacs és további 1 cm szükséges ahhoz, hogy a robbanóanyagra jellemző detonációs sebesség kialakuljon, ezzel megteremtve a kumulatív hatás optimumát. Mivel azonban egy esetben ennél 10%-kal magasabb adatot is mértem, a továbbiakban a feljebb említett optimális teljesítmény kialakulása érdekében a vágandó objektum kezdetétől 3 cm-rel távolabb szükséges a folyamatot elindítani. Ez a kiegészített hossz a fenti eredmények alapján biztosítja majd, hogy a detonáció a céltárgy felületét elérve már képes legyen hatékonyan elvágni azt.

Sikerült tehát meghatározni azt az adatot, amely alapvető a 3D nyomtatással készített kumulatív idomtöltetek tervezésekor, legalábbis abban az esetben, ha alacsony sűrűségű anyagot alkalmazunk a vágóél készítésére.

Az ilyen eljárással készült töltetek tehát képesek hatékony vágásra, amellyel tartószerkezeteket semmisíthetünk meg, de különleges esetben akár improvizált robbanótestek[21] vagy nagy méretű hagyományos robbanótestek – mint a légibombák[22] – hatástalanításában is szerepet kaphatnak. A témakör még természetesen további vizsgálatokat követel, de jól látható, hogy a civil robbantástechnikában és a műszaki támogatás rendszerén[23] belül végzett robbantási feladatoknál egyaránt adódik lehetőség az alkalmazásukra.

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

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

[21] KOVÁCS 2012a: 37–52; KOVÁCS 2012b: 35–44; DARUKA–KOVÁCS 2013: 384–389.
[22] DARUKA 2014: 70–78.
[23] KOVÁCS 2002: 30–35.

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

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.

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

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 (2002): Gondolatok a műszaki támogatás és a műszaki zárás alapjairól. *Nemzetvédelmi Egyetemi Közlemények,* 6(1), 30–35.

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

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

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

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
18. évfolyam (2023) 3. szám 19–32.
DOI: 10.32567/hm.2023.3.2

Ács Éva,[1] Bíró Tibor,[2] Béres Deák László,[3]
Duleba Mónika,[4] Grigorszky István,[5] Kiss Keve Tihamér,[6]
Németh Zoltán,[7] Papp András,[8]
Vadkerti Edit[9]

Alkalmas-e a kavitációs vízkezelés az algavirágzások csúcsainak letörésére?[10]

Is Cavitation Water Treatment Suitable for Breaking the Peaks of Algal Blooms?

Absztrakt

Egy kísérleti kavitációs berendezés tervezésével, létrehozásával és kisüzemi alkalmazásával a szennyezett vizek egyik lehetséges tisztítási módját vizsgáltuk. A kísérleti berendezés mobil kivitelű, és alkalmas különböző szennyezettségű vizek tisztítására. Bemutatjuk a kavitáció hatását különböző mikroszkopikus méretű élőlényekre. Először egy hígított zöldalgatenyészetet vizsgáltunk, megállapítottuk, hogy 16–32 perces kavitáció több mint 10–20%-kal csökkenti a klorofillkoncentrációt és az ép sejtek arányát. Biológiailag bontható szennyvízzel kevert algás halastóvízben, kavitáció hatására a cianobaktériumok, ostoros

[1] Nemzeti Közszolgálati Egyetem VTK Vízellátási és Csatornázási Tanszék, e-mail: acs.eva@uni-nke.hu
[2] Nemzeti Közszolgálati Egyetem VTK Vízépítési Tanszék, e-mail: biro.tibor@uni-nke.hu
[3] GAMMA ANALCONT Kft., e-mail: beresdeak@gmail.com
[4] Nemzeti Közszolgálati Egyetem VTK Vízellátási és Csatornázási Tanszék, e-mail: duleba.monika@uni-nke.hu
[5] Debreceni Egyetem TTK Hidrobiológia Tanszék, e-mail: grigorszky.istvan@science.unideb.hu
[6] Nemzeti Közszolgálati Egyetem VTK Vízellátási és Csatornázási Tanszék, e-mail: kiss.keve.tihamer@uni-nke.hu
[7] GAMMA ANALCONT Kft., e-mail: info@gammaanalcont.hu
[8] GAMMA ANALCONT Kft., e-mail: info@gammaanalcont.hu
[9] Nemzeti Közszolgálati Egyetem VTK Vízellátási és Csatornázási Tanszék, e-mail: vadkerti.edit@uni-nke.hu
[10] A kutatásokat a K-KFI-16-1-2017 0159558 számú projekt támogatta, a Hernád hullámterében elvégzett hordgásztavi vizsgálatokat pedig a Széchenyi Terv Plusz RRF-2.3.1-21-2022-00008 program keretében végeztük.

algák mennyisége 40–80%-kal csökkent, a zöldalgáknál minimális volt a csökkenés. Ezeknél a méréseknél síkszelepes, nagynyomású kavitációgenerátort alkalmaztunk. Bizonyítottuk, hogy a hajók ballasztvize és a szennyvizek mikrobiótája mennyiségének csökkentésére a kavitációs vízkezelés ígéretes megoldásnak tekinthető, de figyelemmel kell lenni arra, hogy csak elpusztul a mikrobióta, de nem tűnik el a vízből.

Kulcsszavak: kavitáció, vízkezelés, algatenyészet, halastóvíz, szennyvíz, ballasztvíz

Abstract

An experimental cavitation equipment was designed, built and applied on a small scale to investigate a possible method of purifying contaminated water. The experimental unit is mobile and suitable for the purification of water with different contaminations. The effect of cavitation on organisms of different microscopic sizes is demonstrated. First, a diluted culture of green algae was tested and it was found that 16–32 minutes of cavitation reduced chlorophyll concentration and intact cell percentage by more than 10–20%. In fishpond water mixed with biodegradable wastewater, cavitation reduced cyanobacteria and flagellate algae by 40–80%, with minimal reduction in green algae. For this purpose a flat type HP cavitation generator has been used. Evidence has been provided that cavitation water treatment is a promising solution for reducing the microbiota in ships' ballast water and wastewaters, but care must be taken to ensure that the microbiota is only destroyed, but not removed from the water.

Keywords: cavitation, water treatment, algae cultivation, pond water, wastewater, ships' ballast water

Bevezetés

Az élővizek szennyezése és a szennyező anyagok eltávolítása korunk egyik legnagyobb problémája. Jelen kutatásunk eredményeképp a természetes vizekben, szennyezett vizekben, szennyvizekben élő, ott elszaporodó, túlnyomórészt mikroszkopikus méretű élőlények eltávolításának, mennyiségük csökkentésének egyik lehetséges módját, a kavitációs vízkezelés eredményességét mutatjuk be.

A felszíni vizekben, ha azok jó ökológiai állapotúak, mikroszkopikus méretű élőlények nem szaporodnak el olyan mértékben, hogy az kedvezőtlen lenne a víziélőlény-együttesek vagy a vízhasználat szempontjából. Ha a vízben a növényitápanyag-kínálat (N, P) nagy, az első lépésként a fitoplankton gyors szaporodását eredményezheti, vízvirágzások alakulhatnak ki. Ezeket esetenként toxikus cianobaktériumok okozhatják, mint ahogy a Balatonon,[11] a Velencei-tóban[12] is előfordult. Hasonló vízvirágzások folyóvizek mellékágaiban, horgászvizekben, halastavakban is gyakoriak.[13]

[11] Vörös 2019.
[12] Reskóné Nagy – Törökné Kozma 2000: 554–557.
[13] Vasas 2011: 107–109.

Nagy egyedszámú mikrobióta (baktériumok, egysejtű eukarióták és többsejtű mikroszkopikus élőlények) jellemzi a szennyvizeket, legyenek akár nagyvárosi, kistelepülési, vagy akár egy-egy lakóházhoz tartozó szennyvíztisztítók elfolyó tisztított szennyvizei.

Az utóbbi években került az érdeklődés homlokterébe a mikróbák és egyéb kisebb élőlények, vagy azok szaporító képleteinek eltávolítása a hajók ballasztvizéből. A ballasztvíz a hajó egyensúlyának biztosítására szolgál, kirakodáskor feltöltik a hajó tartályait jellemzően tengervízzel, amely persze rengeteg mikróbát és tengeri élőlényt tartalmaz. Ezek a többnapos vagy többhetes út során nagymértékben elszaporodnak, majd a fogadó kikötőben a ballasztvízzel együtt kijutnak a vízbe a világ egy másik pontján. Az új környezetben a behurcolt élőlények jelentős része invazív fajként elszaporodhat és megváltoztathatja az élővilág összetételét.[14] Ezek eltávolításának, ártalmatlanná tételének egyik ígéretes lehetősége a kavitáció alkalmazása a ballasztvíz kieresztésekor.

Dular és szerzőtársai (2016) hidrodinamikus kavitációval végzett kísérletek során elsősorban gyógyszerek (klofibrinsav, ibuprofén, ketoprofén, naproxén, diklofenák, karbamazepin), mérgező cianobaktériumok *(Microcystis aeruginosa),* zöld mikroalgák *(Chlorella vulgaris),* baktériumok *(Legionella pneumophila)* és vírusok *(Rotavírus)* vízből és szennyvízből való eltávolítására fektették a hangsúlyt. Megállapították, hogy a hidrodinamikus kavitáció rutin víztisztítási módszerként való alkalmazásához még hosszú az út, de a közelmúltban elért eredmények reményt keltők arra, hogy alacsony energiafogyasztású víz- és szennyvíztisztítási módszert lehessen kidolgozni.[15] Song és szerzőtársai (2022) véleménye szerint a kavitációt a szennyvíztisztításban is fel lehet használni, ahol a kavitáció termikus, mechanikus és kémiai hatása egyaránt hasznosul a szerves anyagok lebontása során.[16]

Wu és szerzőtársai (2012) toxikus cianobaktérium-sejtek *(Microcystis aeruginosa)* eltávolítására hidrodinamikus kavitációs kezelést alkalmaztak, ózonnal kombinálva. Azt tapasztalták, hogy kavitációval az algasejtek 15%-át, ózonos kezeléssel 35%-át sikerült eltávolítani.[17] Hidrodinamikus kavitáció és ózonozás kombinált alkalmazásával 99%-os hatásfokot értek el. Jelentősen eltérő célú alkalmazási lehetőség például a mikroalgákból származó bioaktív anyagok kinyerése kavitáció segítségével.[18]

A kutatás során vizsgált kavitációs berendezés a fenti példákban szereplő mikrobióta szaporodásának csökkentését, eltávolítását teszi lehetővé. Ilyen kis méretű, a kutatásunk során jól használható és hatékony berendezés tervezése, megépítése és kisüzemi tesztelése is részét képezte munkánknak. A mérések során síkszelepes kavitátort és hidrodinamikus (Venturi-elven működő) kavitációs berendezést használtunk.

A kutatás során arra kerestük a választ, hogy 1. az általunk tervezett kis méretű kavitációs berendezés a kísérleti üzemeltetés során hatékonyan működtethető-e; 2. zöldalga- (Chlorococcales) tenyészetekben sikeresen csökkenthető-e az algák

[14] Carlton–Geller 1993: 78–82.
[15] Dular et al. 2016: 577–588.
[16] Song 2022: 302–320.
[17] Wu et al. 2012: 152–158.
[18] Mittal–Ranade 2023: 1129–1161.

mennyisége, szaporodása kavitációs kezeléssel; 3. biológiailag bontható szennyvízzel kevert algás halastóvízben csökkenthető-e az algák mennyisége kavitációs kezeléssel; 4. alkalmas-e a kavitációs vízkezelés az algavirágzások csúcsainak letörésére.

A kísérleti kavitációs berendezés bemutatása

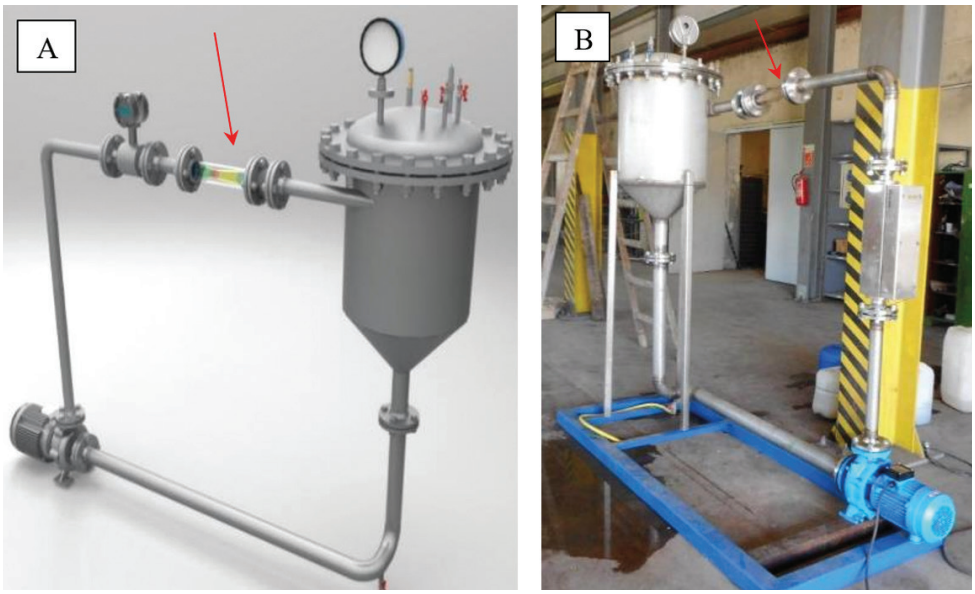
A kavitáció klasszikusan egy csatornában való folyadékáramlásban lép fel akkor, ha a nyomás esése következtében, jelenleg a kezelendő víz, folyadékfázisból hirtelen gázfázisba megy át. Ezt nevezzük hidrodinamikus kavitációnak. A buborékképződés jelensége a folyadékban akkor lép fel, amikor az áramlás egy adott pontjában a nyomás olyan mértékben csökken, hogy eléri az adott folyadék hőmérsékletéhez tartozó telített vízgőz nyomásának értékét. A folyadék ekkor forrni kezd és a buborékképződés miatt gőz- és folyadékfázis heterogén keveréke lesz. A buborékban uralkodó nyomást a buborék mérete és a folyadék-gőz felületén fellépő felületi feszültség határozza meg.

Az így létrejött többfázisú áramlás viselkedése lényegesen eltér a tiszta folyadék esetén várható áramlástól, a folyadék „tejszerű" lesz, gőzzel teli buborékok tömege, esetleg gőzzel telt üreg jelenik meg. A gőzös kavitációnak van roncsoló hatása.[19] Felismerve azt, hogy a kavitációnak nemcsak hátránya, hanem előnye is lehet, a kutatók többféle módszert, illetve szerkezetet (kavitációgenerátort) dolgoztak ki abból a célból, hogy a folyamatot kézben lehessen tartani és intenzitását szabályozni.[20] Több berendezés kipróbálása után egy Venturi típusú kavitátort valósítottunk meg. Szabad és nyílt forráskódú GNU/GPL licensszel rendelkező szoftverrel (Open Source Field Operation and Manipulation) végeztük a kavitációs szimulációkat különböző Venturi-cső-keresztmetszetek esetére. Azt kaptuk, hogy a Venturi legszűkebb keresztmetszetének 31 mm-nek kell lennie, a belépő szűkítő dőlésszöge 22°, a kilépőoldali szűkítő dőlésszöge 10°, és 700 liter/perc szállítóteljesítmény mellett be fog indulni a kavitáció.

Tervezésekor fontos szempont volt, hogy a berendezés egyszerű kialakítású rendszer legyen, a rendszerben található szűkítő cserélhető legyen, és különböző geometriák tesztelésére adjon lehetőséget, amennyiben kedvező mérési eredményeket kapunk, egyszerűen adaptálható legyen különböző tartályokba, víztárolókba, önhordó szerkezetű legyen. A berendezés 200 liter folyadékkal tölthető fel.[21]

A berendezés frekvenciaváltóval van ellátva, amellyel az áramlás intenzitását szabályoztuk. Emellett fontos szempont volt, hogy a berendezés, legalább bizonyos mértékek között, de mobilis legyen, tehát saját kerekeivel gurítható, és amennyiben szükség van rá, átmenetileg fixálható (1. ábra).

[19] Könözsy 2000.
[20] Promptov 2017.
[21] Németh 2018.



1. ábra: A: a kavitációs berendezés 3D modellje, B: a kísérleti kavitációs berendezés
Forrás: a szerzők szerkesztése

Anyag, módszer

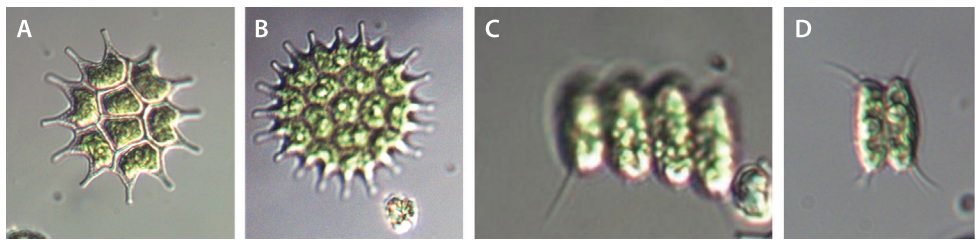
A Venturi-elven működő kavitációgenerátoron a szennyvizet folyamatosan keringettük, és 1, 2, 3, 4, 8, 16 és 32 percnyi kavitálás után vettünk mintát, 12,5–50 Hz kavitációs frekvencia alkalmazásával (16 perctől az 50 Hz-cel). Minden minta esetében a laboratóriumban BBE AlgaeLabAnalyser műszerrel klorofillkoncentráció- (összes klorofill, aktív klorofill) és BBE TenCells műszerrel sejtszám-meghatározást végeztünk, mintánként 3 ismétlésben. Emellett fordított rendszerű fénymikroszkóppal (OLYMPUS IX71) számláló-ülepítő kamrában megvizsgáltuk az algák morfológiai változását, esetleges pusztulását is. Az algasejtekről fényképeket készítettünk a sérülés mértékének, módjának demonstrálására.

Eredmények

Kavitációs kísérletek zöldalgatenyészettel

A kavitációs kísérleteknél fontosnak tartottuk, hogy olyan mikroorganizmusokkal végezzük azokat, amelyek tavakban, folyókban, azok mellékágaiban, horgászvizekben, szennyezett vizekben élő szervezetek.

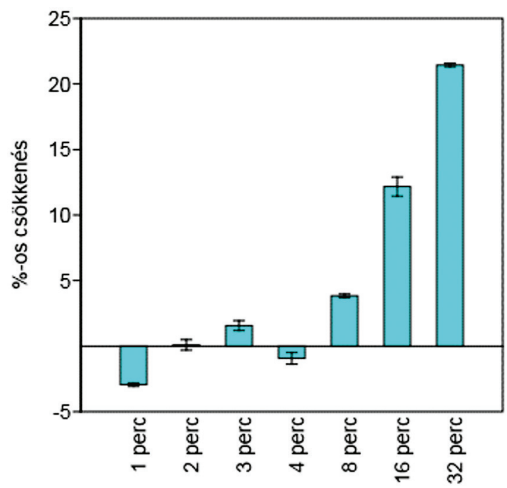
Először olyan hígított zöldalgatenyészettel végeztük a kísérleteket, amelyek természetes vizekben gyakori fajokat tartalmaznak. Ebben a *Pediastrum boryanum* (Turpin) Meneghini 8, illetve 16 sejtes a *Desmodesmus spicatus* W. & G.S. West 2, illetve 4 sejtes cönóbiumokat (sejtcsoportok – ezeket tekintjük egy-egy individuumnak) alkotott (2. ábra, A)–D) fénymikroszkópos felvételek). A hígított algatenyészetben a két faj egyedszáma 10 500 ind/ml volt. Ezzel töltöttük fel a kavitációs berendezés tartályát, a kavitációt 32 percen keresztül végeztük, s közben 1, 2, 4, 8, 16, 32 perckor mintákat vettünk klorofill- és fénymikroszkópos vizsgálatra.



2. ábra: Hígított zöldalgatenyészetből készült fénymikroszkópos felvételek (kavitáció előtt)
A) 8 sejtes Pediastrum cönóbium; B) 16 sejtes Pediastrum cönóbium; C) 4 sejtes Desmodesmus cönóbium; D) 2 sejtes Desmodesmus cönóbium
Forrás: a szerzők felvételei

Algapigment-vizsgálatok

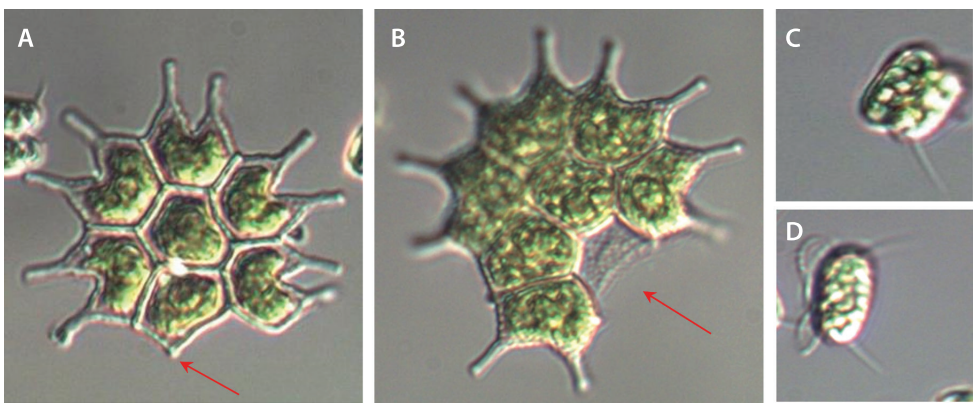
Az algapigment-vizsgálat eredménye alapján elmondható, hogy 32 perces kavitáció már számottevően csökkenti a tenyészetben az algák mennyiségét (3. ábra).



3. ábra: A tenyészet összklorofill-koncentrációjának százalékos változása a kavitáció előtti koncentrációkhoz viszonyítva a kavitálás során (kavitációs idő percben)
Forrás: a szerzők szerkesztése

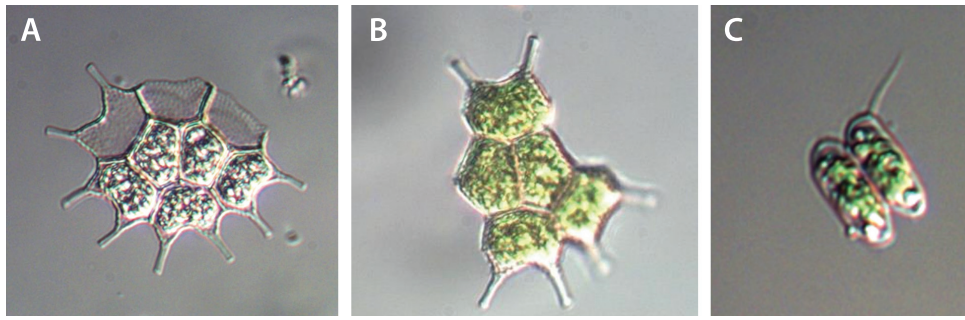
Fénymikroszkópos algológiai vizsgálatok

A fénymikroszkópos algológiai vizsgálatok bizonyították (8, 16, 32 perces kavitáció után vizsgáltuk a mintákat és készítettünk képeket), hogy 8 perc után a *Pediastrum* cönóbiumok túlnyomó része ép. Az osztódás alatt álló telepek aránya nem változott. A telepek 5%-ánál mechanikai sérülést figyeltünk meg, ahol a széli sejteken vagy a külső nyúlvány tört le (vagy sérült – 4. ábra, A) kép), vagy a külső sejtek ívéből 1-3 sejt üres és/vagy törött sejtfalú volt (4. ábra, B) felvétel). A *Desmodesmus* cönóbiumok 50%-a 4 sejtes volt, közel 50% pedig 2 sejtes (ez arra utal, hogy a kavitációs erők hatására a 4 sejtes cönóbiumok egy része kettétört – 4. ábra, C) felvétel). Az ép cönóbiumok között már néhány sérült volt (a cönóbium széli sejtjének sejtfala sérült és üres – D. felvétel).



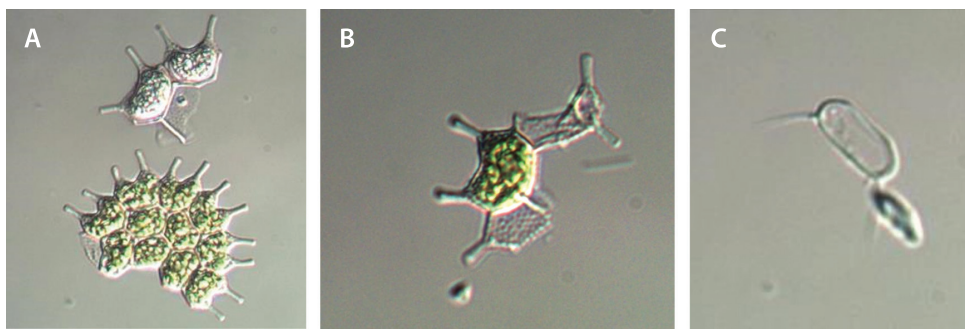
4. ábra: Hígított zöldalgatenyészetből készült fénymikroszkópos felvételek 8 perces kavitáció után (további magyarázat a szövegben)
A) felvétel: sérült Pediastrum sejt; B) felvétel: üres Pediastrum sejt; C–D) felvétel: sérült Desmodesmus cönóbium
Forrás: a szerzők felvételei

16 perc kavitáció után a *Pediastrum* cönóbiumok túlnyomó része még ép. Az osztódás alatt álló telepek aránya nem változott. A telepek ~8%-ánál mechanikai sérülést figyeltünk meg, ahol a külső sejtek ívéből 2-3 sejt üres és/vagy törött sejtfalú volt (5. ábra, A) felvétel), vagy a széli sejtek egy része letört a cönóbiumból (5. ábra, B) felvétel). A *Desmodesmus* cönóbiumok 40%-a 4 sejtes volt, közel 60% pedig 2 sejtes. Az ép cönóbiumok között ~2%-nál mechanikai sérülést figyeltünk meg (a cönóbiumok széttöredeztek, a széli sejtek tüskéje sérült, 5. ábra, C) felvétel).



5. ábra: Hígított zöldalgatenyészetből készült fénymikroszkópos felvételek 16 perces kavitáció után (további magyarázat a szövegben)
A) felvétel: sérült külső Pediastrum sejtek; B) felvétel: sérült Pediastrum cönóbium; C) felvétel: sérült Desmodesmus cönóbium
Forrás: a szerzők felvételei

32 perc kavitáció után a *Pediastrum* cönóbiumok nagyobb része még ép. Az osztódás alatt álló telepek aránya nem változott. A telepek ~10%-ánál mechanikai sérülést figyeltünk meg, ahol a széli sejteken vagy a külső nyúlvány tört le (vagy sérült), vagy a külső sejtek ívéből 2-3 sejt üres és/vagy törött sejtfalú volt. A 16 sejtes telepek között volt olyan, ahol a telep sejtjeinek harmada–fele sérült (6. ábra, A)–C) felvételek). A *Desmodesmus* cönóbiumok 20%-a 4 sejtes volt, közel 80% pedig 2 sejtes. Az ép cönóbiumok között ~7%-nál mechanikai sérülést figyeltünk meg, sérült volt a cönóbium széli sejtjének sejtfala, és üres.



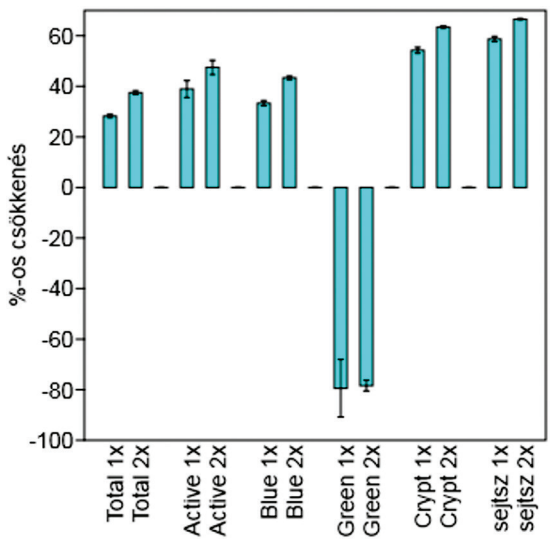
6. ábra: Hígított zöldalgatenyészetből készült fénymikroszkópos felvételek 32 perces kavitáció után (további magyarázat a szövegben)
A) felvétel: sérült Pedistrum cönóbiumok; B) felvétel: sérült Pediastrum cönóbium; C) felvétel: üres Desmodesmus sejt
Forrás: a szerzők felvételei

Kavitációs kísérletek halastóvíz-szennyvíz „keverékkel"

A zöldalgatenyészettel végzett kísérleteket követően egy jellegzetes élővíztípussal, halastóvízzel folytattuk kutatásainkat. Ebben az esetben a Kaposvár térségéből származó halastóvizet a Kométa gyár (Kaposvár) üzemének nagy baktériumtartalmú szennyvizével kevertük 50-50%-ban és ezt egy- és kétszeres kavitációval kezeltük, síkszelepes kavitátorral. A kezeletlen mintákat, valamint az egyes kavitációs fázisok végén gyűjtött mintákat vizsgáltuk.

Algapigmentmérések

Az algapigment-vizsgálat alapján megállapítottuk, hogy a zöldalgák (Green) kivételével a többi vizsgált csoportra hatással volt a kavitáció, az érzékenyebb Cryptophyta (Crypt) csoportra nagyobb mértékben (7. ábra).

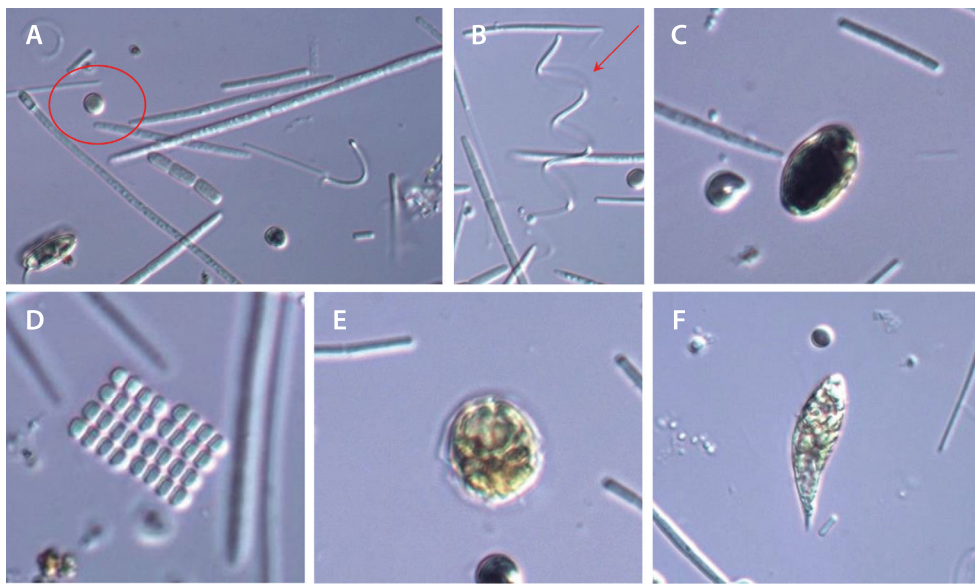


7. ábra: A halastóminták algapigment-koncentrációjának és -sejtszámának százalékos változása a kavitáció előtti koncentrációkhoz viszonyítva egyszeres és kétszeres kavitálás után (Total: összklorofill-koncentráció, Active: aktív algák összklorofill-koncentrációja, Blue: cianobaktériumok, Green: zöldalgák, Crypt: Cryptophyta és Dinophyta algák pigmentkoncentrációja, sejtsz: a minta sejtszáma 1x: egyszeres, 2x: kétszeres kavitáció)

Forrás: a szerzők szerkesztése

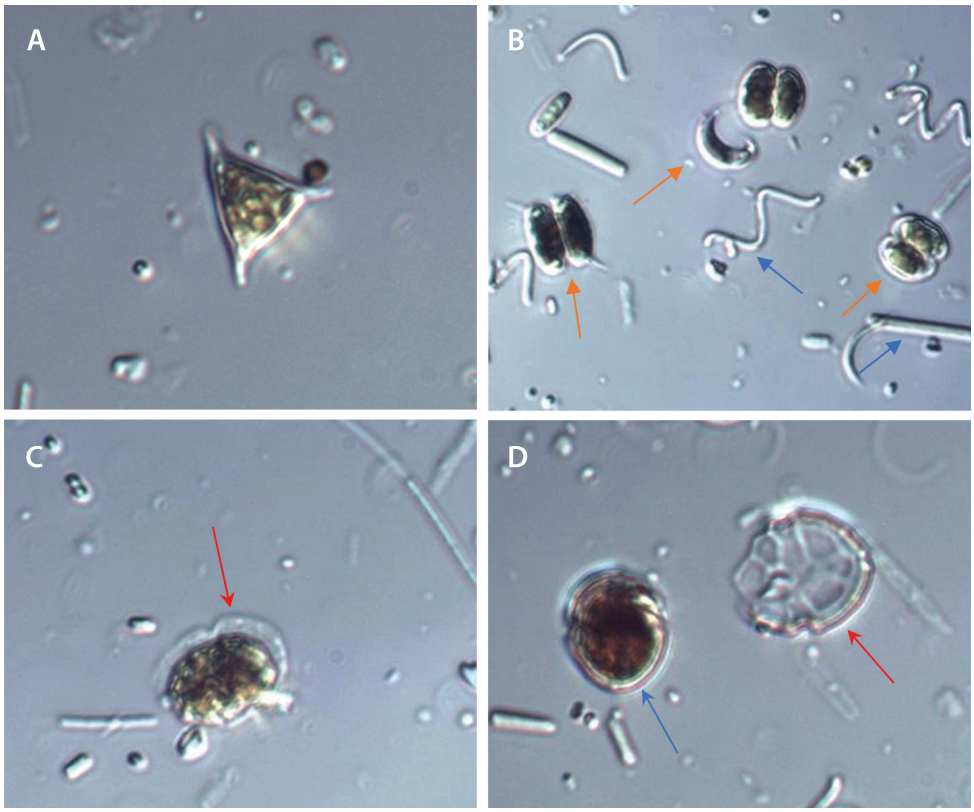
Fénymikroszkópos algológiai vizsgálatok

A kezeletlen, túlnyomórészt halastóvizet tartalmazó mintában legnagyobb számban cianobaktériumok *(Cyanobacteria),* kisebb mennyiségben zöldalgák *(Chlorophyceae)* voltak, és rendszeresen találtunk ostorosalgafajokat (Cryptophyta – *Cryptomonas,* Dinophyta – *Peridinium,* Euglenophyta – *Euglena*). A cianobaktériumok között egysejtű, kis sejtszámú telepes és fonalas alakok fordultak elő. A fonalas fajok 20-100 µm hosszú, egyenes vagy spirális fonalakat alkottak (8. ábra, A)–B) felvétel). A többi csoportba tartozó algafaj egysejtes volt, illetve 4, 8, 16 sejtes cönóbiumot alkotott (8. ábra, C)–F) felvételek).



8. ábra: Kezeletlen halastavi mintából készült fénymikroszkópos felvételek (további magyarázat a szövegben)
A) felvétel: rövidebb-hosszabb fonalas, bal oldalon egy nagyobb kerek cianobaktérium-sejt (piros kör); B) felvétel: középen egy spirális cianobaktérium-fonál (piros nyíl); C) felvétel: ovális alakú Cryptomonas sejt; D) felvétel: 32 sejtes cianobaktérium-telep; E) felvétel: kerekded Peridinium; F) felvétel: fűzfalevél alakú Euglena
Forrás: a szerzők felvételei

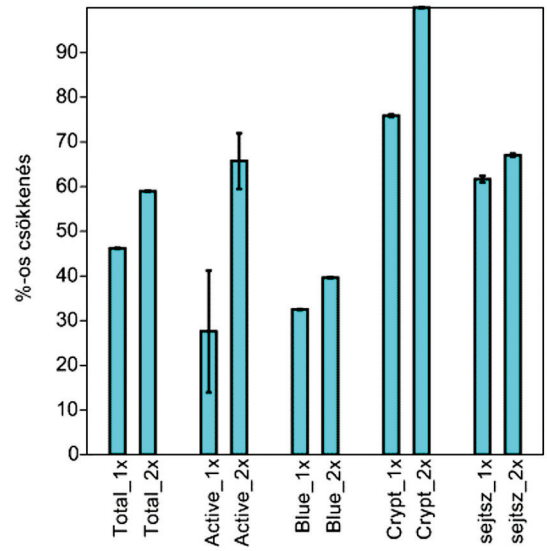
Az 1-szeres és 2-szeres kavitáció hatása hasonló volt, de a második esetben nagyobb volt a roncsolódott sejtek aránya. Mind az egyenes, mind a spirális cianobaktérium-fonalak széttöredeztek, bár ez utóbbiak kevésbé. A Dinophyta sejtek cellulóz páncélja széttört (összetett szerkezetű sejtfal – 9. ábra, C)–D) felvételek), benne a sejtek elpusztultak, egyes esetekben még benne maradtak a törött páncélban, más esetekben kiszabadultak abból és teljesen szétestek. A Cryptophyta és Euglenophyta sejtekkel ugyanez történt. A zöldalgasejtek többségükben épek maradtak (9. ábra, A)–B) felvételek).



9. ábra: Kavitációval kezelt halastavi mintából készült fénymikroszkópos felvételek (további magyarázat a szövegben)
A) felvétel: Tetraedron zöldalgasejt épen maradt; B) felvétel: ép Chlorococcales (piros nyíl) és cianobaktérium-sejt (kék nyíl); C) felvétel: Peridinium sejt félig levált páncélja; D) felvétel: egy ép Peridinium sejt (kék nyíl) és külön egy letört páncél (piros nyíl)
Forrás: a szerzők felvételei

Halastóvízzel hígított csirkefarmi szennyvíz vizsgálatai

A halastavi mintával hígított csirkefarmi szennyvízmintában BBE AlgaeLabAnalyser és BBE TenCells műszerrel kimutatható mennyiségben cianobaktériumok és Cryptophyta divízióba tartozó algák voltak. A mérési eredmények alapján jól látszik, hogy már az 1-szeres kavitáció jelentősen csökkentette a klorofillkoncentrációt, ez 2-szeres kezeléssel 60% fölé emelkedett. A cianobaktériumok mennyiségének csökkenése 30–35%-os volt, a Cryptophyta fajok esetében ez 1-szeres kavitáció után 70% volt, 2-szeres kavitációt követően megközelítette a 100%-ot (10. ábra).

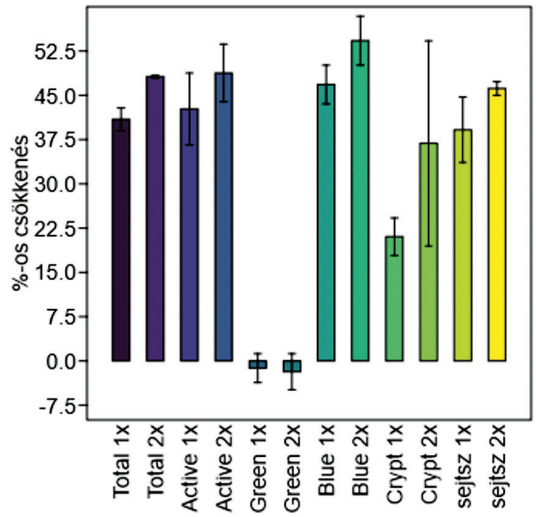


10. ábra: Halastó vizével hígított csirkefarmi szennyvízminták algapigment-koncentrációjának és -sejtszámának százalékos változása a kavitáció előtti koncentrációkhoz viszonyítva egyszeres és kétszeres kavitálás után
(Total: összklorofill-koncentráció, Active: aktív algák összklorofill-koncentrációja, Blue: cianobaktériumok, Crypt: Cryptophyta és Dinophyta algák pigmentkoncentrációja, 1x: egyszeres kavitáció, 2x: kétszeres kavitáció)
Forrás: a szerzők szerkesztése

Aranykavics-horgásztó

A Hernád 97-98-as folyókilométer jobb parti szelvényében található Aranykavics-horgásztóból gyűjtött mintákban vízszíneződést okozott a fitoplankton, amelyben a cianobaktériumok domináltak (*Aphanizomenon* és *Pseudolyngbya* spp.). Mellettük néhány Cryptophyta (*Cryptomonas, Chroomonas*) faj volt említésre méltó mennyiségben, a Chlorococcales *(Desmodesmus)* mennyisége elenyésző volt.

A horgásztavi mintában a BBE AlgaeLabAnalyser és BBE TenCells műszerrel kimutatott klorofill- és sejtszámértékek alapján jól látszik, hogy már az 1-szeres kavitáció is számottevően csökkentette a klorofillkoncentrációt és a sejtszámot, ami 2-szeres kezeléssel tovább csökkent (11. ábra). A cianobaktériumok mennyiségének csökkenése volt a legnagyobb, 50% fölötti, ezt követte a Cryptophyta fajoké, a zöldalgákra gyakorlatilag hatástalan volt, ez elsősorban azzal magyarázható, hogy a *Desmodesmus* fajok sejtfala erős fölépítésű.



11. ábra: Az Aranykavics-horgásztó vize algapigment-koncentrációjának és -sejtszámának százalékos változása a kavitáció előtti koncentrációkhoz viszonyítva egyszeres és kétszeres kavitálás után (Total: összklorofill-koncentráció, Active: aktív algák összklorofill-koncentrációja, Green: Chlorophyceae, Blue: cianobaktériumok, Crypt: Cryptophyta és Dinophyta algák pigmentkoncentrációja, 1x: egyszeres kavitáció, 2x: kétszeres kavitáció)

Forrás: a szerzők szerkesztése

Összegzés

Egy Venturi típusú kísérleti kavitációs berendezés tervezésével, létrehozásával és kisüzemi alkalmazásával a szennyezett vizek egyik lehetséges tisztítási módját vizsgáltuk. Kísérleteink eredményei azt mutatták, hogy a kavitációs kezelés kimutatható mértékben roncsolja a vizsgált vízi szervezeteket, azonban az egyes élőlénycsoportokra ugyanolyan mértékű kavitációs kezelés más-más mértékben hat. Megállapítható, hogy a mikroszkópos megfigyelés fontos kiegészítője a kezelések hatása vizsgálatának, de a hatékonyság megállapítására a vízi szervezetek mennyiségi detektálására van szükség. Az eddigi kezelések alapján még nem tudjuk azt mondani, hogy 100%-ban elpusztítja a kavitáció a vízi szervezeteket, azonban az eredmények bíztatók, a kísérletek folytatása szükséges. Az előzetes eredmények alapján arra a következtetésre jutottunk, hogy a kavitáció erősségének a fokozása hatékonyabb, mint a kavitációs idő növelése. Ugyanakkor figyelemmel kell lenni arra a megállapításra, hogy az egyes élőlénycsoportok eltérő mértékben károsodnak. Az eddigi eredmények alapján nem lehet általánosítani, és csak óvatos következtetéseket szabad levonni. A jövőben mindenképpen érdemes volna megvizsgálni a spórákat, petéket, cisztákat, egyéb szaporító és áttelelő képleteket tartalmazó mintákat is. Nem szabad elfelejtkezni arról a tényről, hogy a kavitáció hatására csak elpusztul a mikrobióta, de anyagai nem tűnnek el a vízből, emiatt az algavirágzások csúcsainak letörésére a módszer nem alkalmas. Ugyanakkor viszont, mivel képes elpusztítani a sejteket, a hajók ballasztvizében való

idegenhonos fajok behurcolása elleni védekezés hatékony eszköze lehet a jövőben, mivel a kezelés maga nem juttat káros anyagot a vízbe.

Irodalomjegyzék

Carlton, James T. – Geller, Jonathan B. (1993): Ecological roulette: the global transport of nonindigenous marine organisms. *Science,* 261(5117), 78–82. Online: https://doi.org/10.1126/science.261.5117.78

Chu, Ka Hou et al. (1997): A Biological Survey of Ballast Water in Container Ships Entering Hong Kong. *Hydrobiologia,* 352, 201–206. Online: https://doi.org/10.1023/A:1003067105577

Dular, Matevž et al. (2016): Use of Hydrodynamic Cavitation in (Waste) Water Treatment. *Ultrasonics Sonochemistry,* 29, 577–588. Online: https://doi.org/10.1016/j.ultsonch.2015.10.010

Könözsy László (2020): *A kavitációs áramlások szimulációja. A létező modellek, módszerek ismertetése, kritikai elemzése.* Szakirodalom-kutatás. Beszámoló. Miskolc: Miskolci Egyetem, Áramlás- és Hőtechnikai Gépek Tanszéke. Kézirat.

Mittal, Rochak – Ranade, Vivek (2023): Bioactives from Microalgae: A Review on Process Intensification Using Hydrodynamic Cavitation. *Journal of Applied Phycology,* 35, 1129–1161. Online: https://doi.org/10.1007/s10811-023-02945-w

Németh Zoltán (2018): *Kavitációs folyamatok.* Szakdolgozat. Budapest: Budapesti Műszaki Egyetem.

Promptov, M. A. et al. (2017): *Szennyvízkezelés kavitációval.* Tambovi Műszaki Egyetem közleményei.

Reskóné Nagy Mária – Törökné Kozma, Andrea (2000): Toxic Microcystis aeruginosa in Lake Velencei. *Environmental Toxicology,* 15, 554–557. Online: https://doi.org/10.1002/1522-7278(2000)15:5<554::AID-TOX28>3.0.CO;2-Y

Song, Yongxing et al. (2022): Hydrodynamic Cavitation as an Efficient Water Treatment Method for Various Sewage: A Review. *Water Science & Technology,* 86(2), 302–320. Online: https://doi.org/10.2166/wst.2022.201

Vasas Gábor (2011): Hatóanyagok, speciális anyagcseretermékek fotoszintetizáló algaszervezetek tömegprodukcióiból. *Hidrológiai Közlöny,* 91(6), 107–109.

Vörös Lajos (2019): *Fecskemoszat és cianobaktérium invázió 2019 nyarán a Balatonban*. Balatoni Limnológiai Kutatóintézet, 2019. szeptember 11. Online: www.blki.hu/rendkivui_balatoni_vizviragzas

Wu, Zhilin et al. (2012): Removal of Blue-Green Algae Using the Hybrid Method of Hydrodynamic Cavitation and Ozonation. *Journal of Hazardous Materials,* 235–236, 152–158. Online: https://doi.org/10.1016/j.jhazmat.2012.07.034

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

18. évfolyam (2023) 3. szám 33–44.
DOI: 10.32567/hm.2023.3.3

Györki Gábor[1]

Szennyvízkezelés a múltban és a jelenben[2]

Wastewater Management through History

Absztrakt

Az emberiség történelmében több ezer éve fontos szerepet játszik a szennyvíz kezelése. Kezdetben csak a higiéniai feltételek biztosítása miatt volt rá szükség, a népesség és az ipari termelés növekedésével azonban a szennyezők kibocsátása már a természetes környezetet is fenyegeti. Amióta érzékelhetők a szennyezés hatásai, illetve kifejlődtek megbízható analitikai módszerek, mind a kutatás-fejlesztés, mind a törvényhozás egyre nagyobb figyelmet szentel a környezetvédelemnek, a szennyvíztisztításnak, a szennyvíz-újrafelhasználásnak. Jelen tanulmány a releváns szakirodalom áttekintésével szeretne átfogó képet adni arról, hogyan jutott el a szennyvízkezelés a történelem során a pillanatnyi állapotába.

Kulcsszavak: decentralizált szennyvíztisztítás, higiénia, környezetvédelem, makroszennyezők, szennyvízkezelés, történelem

Abstract

Wastewater management has played a crucial role in the history of mankind for thousands of years. Initially, it was necessary to ensure sanitary conditions, but since the rapid increase in population and industrial production, the high amounts of discharged pollutants are threatening the environment. Since the effects of pollution can be detected using modern, reliable analytical methods, both research and development, as well as legislation are paying

[1] Nemzeti Közszolgálati Egyetem Víztudományi Kar Vízellátási és Csatornázási Tanszék, 6500 Baja, Bajcsy-Zsilinszky u. 12–14., e-mail: gyorki.gabor@uni-nke.hu
[2] Víztudományi és Vízbiztonsági Nemzeti Laboratórium, Nemzeti Közszolgálati Egyetem Víztudományi Kar, 6500 Baja, Bajcsy-Zsilinszky u. 12–14.

attention to environmental protection, wastewater treatment, and wastewater reuse. By reviewing the relevant literature, this study aims to provide a comprehensive picture of how wastewater management changed throughout history, and reached its current state.

Keywords: decentralised wastewater treatment, sanitation, environmental protection, macropollutants, wastewater management, history

Bevezetés

Napjainkban a környezetbiztonság és a környezetvédelem fogalma az élet szinte minden területén megjelenik. Ahogy a mindennapokban, különböző szakterületeken is figyelembe kell venni e szempontok érvényesülését. A környezetvédelem jól definiálható: azokat a tevékenységeket és szabályokat foglalja magában, amelyek az emberi tevékenységek által a természetes és épített környezetnek okozott károk kiküszöbölését szolgálják. Ezzel szemben a környezetbiztonság (vagy környezeti biztonság) egy folyamatosan változó, összetett fogalom.[3] Többek között olyan ismert tevékenységek tartoznak ide, mint a hulladék mennyiségének általános csökkentése, az újrahasznosítás, a megújuló energiaforrások használata, valamint a biodiverzitás megőrzése.

A „szennyvíz" szó önmagában több nyelvben arra utalhat, hogy egy hulladékról van szó, amelytől egyszerűen meg kell szabadulni (hulladékvíz jelentése van például az angol waste water vagy az olasz acque reflue kifejezésnek is). A legmodernebb szennyvíztisztítási technológiák alkalmazása mellett nem csak a tisztítás és az emberi egészség megőrzése teljesül, egyszerre meg lehet felelni a környezetvédelem és a környezetbiztonság összes fent említett pontjának is. Az utóbbi években megjelent technológiák és találó újrafelhasználási módok lehetővé teszik, hogy az eddig hulladékként kezelt használt vizet pozitív hatások elérésére használjuk fel, így egyszerre védjük az emberi egészséget, segítjük a gazdaságot és csökkentjük a környezetterhelést. Egyre gyakrabban jelenik meg továbbá a „lineáris" gazdaságról az úgynevezett „cirkuláris" gazdaságra való átállás, vagyis a regeneratív vízgazdálkodás. Optimális esetben megszüntethető a szennyvíz befogadókba való kibocsátása, ezt a szakirodalom Zero Liquid Discharge (ZLD)-nak nevezi.[4]

Történeti áttekintés

Jelentős mennyiségű kutatás és tanulmány született arról, hogy a történelem során hogyan alakult a vízfelhasználás és a vízkezelés. Sok esetben írásos emlékek alapján állítható össze pontos kép, más esetekben csak a megmaradt vagy régészek által feltárt építmények és eszközök utalnak ezekre. Az is ismert továbbá, hogy kezdetben az emberi egészség védelme követelte meg a hulladék-, víz- és szennyvízkezelés fejlesztését. Az ipari forradalmak és a népességnövekedés hihetetlen felgyorsulása

[3] Hankó–Földi 2009: 24–38.
[4] Yaqub–Lee 2019: 551–563.

exponenciálisan megnövelte a környezetszennyezés mértékét, így a 19–20. századra már elkerülhetetlen volt erre is figyelmet fordítani. A 21. században a népesség méretének és a vízkészletek mennyiségének aránya miatt még egy lépést kellett tenni, ennek legfőbb pontjai a folyamatos átállás a víz minél nagyobb mértékű újrahasznosítására és az értékes nyersanyagok visszanyerésére.[5]

Egyes vélemények szerint a vízkezelés történetét vizsgálni lényegtelen, a múlt és a jelen közötti jelentős különbségekből adódóan, viszont a civilizáció fejlődése végigkísérhető az elveken és az alkalmazott technológiákon keresztül.[6] A politikus és regényíró Victor Hugo szerint az emberiség történelme a csatornák történelmében tükröződik.[7]

A vízkezelés és a szennyvízkezelés több mint 5000 évvel ezelőttre nyúlik vissza, az ókori görög és szanszkrit írások alapján.[8] Az emberek már ekkor felismerték a tiszta ivóvíz fontosságát: ismerték a szűrést, a homokszűrést, valamint a forralás jelentőségét. Természetesen a mikroorganizmusok jelenlétéről, valamint a kémiai szennyeződésekről még nem tudhattak. A környezetvédelem ekkor még ismeretlen fogalom volt, az emberek életmódjából adódóan nagyon sokáig nem is volt rá szükség. Az egyik legfőbb indok, hogy az emberiség népességsűrűsége kisebb volt, az elszórt közösségek nem tudtak jelentős környezeti károkat okozni. A nomád életmódot követő letelepedett, termelő életmód vonta maga után a közösségek körüli tér folyamatos szennyeződését.[9] Egy másik kézenfekvő indok, hogy a ma ismert és szabályzott szennyezők jelentős részét vagy nem tudták kimutatni, vagy még nem is léteztek.[10] Közel 5500 éve Mezopotámiában néhány lakóháznak már volt lefolyója és szennyvíztározója. Az Indus-völgyi civilizációban hasonlóképp nem engedték valamilyen kezelés (leginkább szűrés, ülepítés) nélkül elfolyni a szennyvizet. Később Egyiptomban a társadalom felső rétegének már elérhető volt a fürdőszoba kezdetleges formája. Az ókori Görögország élen járt mind a vízkezelésben, mind a szennyvízkezelésben, latrinák alatt épített csatornák gyűjtötték össze a szennyvizet és szállították el a városból, többnyire a termőföldeken való felhasználásra.[11] Ezeket a találmányokat később a Római Birodalom tökéletesítette, kiterjesztve a vízellátást, a csatornázást és az általános higiéniát a társadalom szegényebb rétegeire, valamint elterjedten alkalmaztak kezdetleges emésztőgödröket is.[12]

Az egyik legkorábbi szennyvízfelhasználási eljárás a mezőgazdasági területeken való alkalmazás volt, amelyre már a bronzkorban is találunk példát. A nitrogénben és foszforban gazdag szennyvíz így az emberektől viszonylag távol került, természetes módon trágyázta a termesztett növényeket. Ez a megoldás azonban egészségügyi kockázatot (mikroorganizmusok) és környezeti kockázatot is (eutrofizáció, a talaj minőségének romlása) jelentett. A Római Birodalom bukása után a középkorban szinte teljesen eltűntek ezek a higiéniát szolgáló megoldások, és az ipari forradalomig szinte

[5] Torre et al. 2021.
[6] Sarma 2018.
[7] Lofrano–Brown 2010: 5254–5264.
[8] Sarma 2018.
[9] Lofrano–Brown 2010: 5254–5264.
[10] Sarma 2018.
[11] Lofrano–Brown 2010: 5254–5264.
[12] Jaramillo–Restrepo 2017.

vissza sem tértek.[13] A szennyvíz összegyűjtésére és mezőgazdasági felhasználására ezután volt néhány példa (London, 1189-től), de széles körben csak az újkor elején terjedt el ismét, főleg Európában.[14]

Az emberek a higiénia és a környezetvédelem fontosságára csak a 19. században jöttek rá, ezelőtt a szennyvizet szinte sehogy nem kezelték, sok esetben el sem vezették. Ezt támasztja alá a több európai járványhullám is, amelyek az iparosodás és a városiasodás során kialakuló higiéniai problémák miatt törtek ki.[15] Ezenfelül a gőzgép és a szivattyú feltalálása után csaknem korlátlan mennyiségben állt rendelkezésre a víz a lakosságnak, az iparnak és a fellendülő vegyiparnak, az innen származó agresszív szennyvizek kezelés nélkül kerültek a befogadókba. Londonban a lakosság és az ipar által termelt szennyvíz a Temzét olyannyira zavarossá, koszossá és kellemetlen szagúvá tette, hogy a folyó gúnyneveket is kapott (The Great Stench – A Nagy Bűz; Monster Soup – Szörnyleves). Ennek ellenére a folyó hígító hatását még mindig elegendőnek gondolták a tisztításhoz.[16] Az 1830-as és 1850-es években szinte megállíthatatlanul terjedő kolera- és hastífuszjárványok több tízezer ember életét követelték. Ezután vált nyilvánvalóvá a betegségek vízzel való kapcsolata, így mérnöki megoldásokat hívtak segítségül, és még a 19. században modern csatornarendszereket építettek ki a szennyvíz biztonságos elvezetésére.[17] A világon először egy 1861-es törvény mondta ki, hogy a szennyvizet tisztítani szükséges a befogadóba vezetés előtt. Először azonban csak fizikai tisztítást (rácsokat, később ülepítőket) alkalmaztak, a „modernebb" technológiák megjelenésére még fél évszázadot kellett várni. Az első eleveniszapos telep (akkoriban úgynevezett szellőztetéses biológiai rendszer) 1914-ben épült Manchesterben, ami mérföldkőnek számított, ugyanis lerakta az alapját a környezetvédelmi ipar kialakulásának. Németországban már 1904-ben létrejött Európa első vízvédelmi szervezete, amely a folyók szennyezettségi állapotát vizsgálta. Ebben az időben definiálták a szennyvíz egy fontos paraméterét is, a biokémiai oxigénigényt, amely a biológiailag bontható szénforrások lebontásához szükséges oxigénmennyiség.[18] A környezeti és egészségügyi problémák kezelésének módját ebben az időben jelentősen befolyásolta a politika, a tudományos felfedezések, valamint olyan társadalmi-gazdasági történések, mint a világháborúk.[19]

A 20. században a nagyvárosok folyamatosan fejlesztették ki az egyre újabb, jobb és költségesebb rendszereket: az ipari szennyezés jelentős problémává nőtte ki magát, aminek hatására több országban fogadtak el víztisztítással kapcsolatos törvényeket. Budapest jelentős eredményeket ért el a nagy fokú csatornázással, ezek hiányában pedig pöcegödrök és derítők alkalmazásával. Tisztítóművek épültek továbbá Pécsen és Debrecenben is. Hatékonyan alkalmazták már az iszap elgázosítását, valamint a klóros kezelést is, amelynek eredményeként a mikrobiológiai problémák lényegesen ritkábbak lettek. A második világháború után jelentős lassulás volt megfigyelhető,

[13] Lofrano–Brown 2010: 5254–5264; Jaramillo–Restrepo 2017.
[14] Lofrano–Brown 2010: 5254–5264; Angelakis–Snyder 2015: 4887–4895.
[15] Lofrano–Brown 2010: 5254–5264.
[16] Juhász 2011.
[17] Sarma 2018.
[18] Juhász 2011.
[19] Lofrano–Brown 2010: 5254–5264.

majd a kutatások fellendülésével a vízminőségi problémák kezelése is újra felgyorsult.[20] Először az olyan, könnyen észlelhető vízminőségi paramétereket és eseményeket azonosították, mint az oxigénegyensúly, az eutrofizáció, a nehézfémek jelenléte, a savasodás, a talajszennyezés, majd az antropogén anyagok jelenléte. Fontos megjegyezni, hogy az ipar mindennap újabb és újabb szennyező anyagokat produkál, amire a tisztítási technológiák csak fáziskéséssel tudnak reagálni. Ez utóbbi szennyezők típusukat tekintve leginkább a mikroszennyezők közé tartoznak.[21]

Eltávolítandó szennyezők

A szennyvíztisztításban az ipari forradalom óta a makroszennyezők eltávolítása elengedhetetlen környezetvédelmi szempontból,[22] a hagyományos fizikai, kémiai és biológiai úton működő szennyvíztisztító telepek és berendezések képesek ezeket megfelelő mértékben eltávolítani. Ide tartoznak olyan, relatíve nagy (általánosan az 1 mg/l feletti) koncentrációjú szennyezők, mint a lebegőanyagok, szerves anyagok és növényi tápanyagok.[23]

A szennyvízben a nitrogén jelen lehet ammónia, nitrit, nitrát formájában és szerves anyagokban kötött nitrogénként, az esetleges szennyeződések típusától és korától függően. Felszíni vizekben friss szennyezésre utal a magas ammónia- és nitrittartalom, a nitrát az előrehaladott nitrifikáció folyamatára utal. A foszfor jellemzően ortofoszfát, polifoszfát, valamint szerves anyagokban kötött foszfor formájában van jelen a vizekben. Gyakori jelenség, hogy a szennyvíztelepekről kijutó nitrogén- és foszforformák mint növényi tápanyagok feldúsulnak a befogadókban.[24] Ezek felszíni vizekbe jutása eutrofizációt (vízvirágzást) okozhat, amely során megnő a fotoszintetizáló szervezetek (algák/vízi növények) mennyisége, aránya és diverzitása, ami hatással lehet a táplálékláncra és a környező ökoszisztémára is. A jelentős tápanyag-feldúsulás miatt az algák gyorsan elszaporodnak, nehezen bontható anyagokat, esetleg toxinokat állítanak elő, az elburjánzó növényzet sok esetben a víz felszínét beteríti, így árnyékolja a víz alsóbb rétegeit. Az emésztőgödrökből is kiszivároghatnak a tápanyagok, így nem körültekintő elhelyezés esetén a talajvízen keresztül eljuthatnak a felszíni víztestekhez, eutrofizációt idézve elő.[25]

A szerves széntartalmú vegyületek (*total organic carbon,* TOC) jelentős része könnyen felhasználható szénforrást jelent a mikroorganizmusoknak, amelyek elszaporodásukkal anyagcseréjük révén befolyásolják a vízi élettereket, többek között az oxigénszint csökkentésével. Egyes vegyületek továbbá káros melléktermékeket képezhetnek az ivóvíztisztítás során alkalmazott vegyszerekkel. A TOC mellett a kémiai oxigénigény (KOI), valamint a biológiai oxigénigény (BOI) további fontos mérőszámai a vizeknek és a szennyvizeknek, amelyek az oxigénfogyáson keresztül

[20] Juhász 2011; Lofrano–Brown 2010: 5254–5264.
[21] Juhász 2011.
[22] Juhász 2011.
[23] Knisz 2020.
[24] Smith 2009: 61–73.
[25] Herren et al. 2021.

adnak információt a szervesanyag-tartalomról. A szennyvíz szerves széntartalma jelentősen csökkenthető már ülepítés során is, nagyobb mértékű eltávolítás pedig a biológiai lépésekben történik.[26]

A lebegőanyagok (*total suspended solids,* TSS) és oldott anyagok (*total dissolved solids,* TDS) további fontos jellemzők, amelyek jelentős változatosságot mutatnak nemcsak a szennyvíztelepek között, de adott telepen belül is. A lebegőanyagok lehetnek szerves, illetve szervetlen eredetűek. A vizekben magas koncentráció esetén zavarosságot okoznak, valamint elnyelik a fényt, ezáltal a vízhőmérséklet megemelkedhet, az oldott oxigénszint pedig csökkenhet. A szennyvíztisztítás során a fertőtlenítésre használt UV-fényt is elnyelhetik, ezzel csökkentve annak hatékonyságát. Ezekből kifolyólag a lebegőanyagokat szűrők és rácsok segítségével, illetve flotálással, ülepítéssel eltávolítják.[27] Az oldott anyagok közé tartoznak az ásványi anyagok, oldott sók, fémek és néhány szerves anyag. A sók, valamint a fémek természetes mennyiségben nem okoznak gondot a természetben. A szerves anyagok (amelyek a víztestekbe kerülve megnövelnék azok oxigénigényét) jelentős részét biológiai úton könnyen el lehet távolítani, amennyiben biodegradálhatók és nem toxikusak. A káros szerves anyagok eltávolítása általában nem ilyen egyszerű, az utóbbi időkben azonban ezek eltávolítására is nagy hangsúlyt fektetnek.[28]

A mikroszennyezők, a makroszennyezőkhöz képest, jelentősen alacsonyabb koncentrációban vannak jelen a vízben, és kis koncentrációban is mérgezők lehetnek. Általában az 1 mg/l-es szint alatt határozzák meg ezeket a komponenseket. Megkülönböztethetünk szerves és szervetlen mikroszennyezőket is. Olyan anyagok tartoznak ide, mint a gyógyszermaradékok, peszticidek, ipari vegyszerek, nehézfémek, kozmetikai és testápolási szerek.[29] A legelterjedtebb szennyvíztisztítási eljárások nem képesek teljes mértékben eltávolítani néhány ilyen mikroszennyezőt, így a kezelt szennyvíz továbbra is veszélyt jelenthet a környezetre és az emberi egészségre.[30]

A szennyvíztisztítás egyik célja a patogén ciklus megállítása, a patogén mikroorganizmusok eltávolítása általában meg is történik. A tisztítás úgynevezett harmadlagos fokozata felelős többek között a patogén baktériumok eltávolításáért, például UV-fertőtlenítés segítségével, ozonizálással vagy oxidatív reagensek adagolásával. Eleveniszapos rendszerek esetén az iszap dúsulhat a patogénekben, ami szintén nem elhanyagolható.[31] Gyakran vizsgált és eltávolítani kívánt indikátorbaktériumok például az *Escherichia coli*, a *Salmonella* és a *Clostridium perfringens.* Ezek mellett fontos megemlíteni a patogén vírusokat (például adenovírusok), a férgeket (például galandférgek), valamint a protozoákat (például *Giardia lamblia*).[32]

[26] Karches 2020.
[27] Karches 2020.
[28] Nemerow 2007: 105–148.
[29] Knisz 2020.
[30] Elgarahy et al. 2021.
[31] Knisz 2020.
[32] De Sanctis et al. 2017.

Centralizált és decentralizált rendszerek

A szennyvíztisztítás több mint 150 éves múltjában[33] számtalan különböző megoldást találunk, kisebb-nagyobb hatékonyságokkal, ezenkívül minden módszernek és berendezésnek megvan az előnye és a hátránya. A történeti áttekintésből világosan látszik, hogy a kezdetben emberi egészséget szolgáló megoldások egyre inkább olyan irányba fejlődnek, amely a környezetvédelmet is lényeges pontnak tekinti.

A rendszerek két nagy csoportba sorolhatók: ezek a centralizált telepek és a decentralizált megoldások. A centralizált kezelés során a szennyvizet összegyűjtik, majd elvezetés után nagy léptékben, a keletkezéstől távol tisztítják meg, a befogadóba jutás előtt. A decentralizált berendezések ezzel szemben definíció szerint a szennyvizet a keletkezés helyén, általában kis léptékben kezelik. Ez utóbbi rendszerek jelentős változatosságot mutatnak mind méret, mind felépítés és működési elv szerint.[34] A legkorábban alkalmazott emésztőgödrök szigorúan véve decentralizált rendszernek számítanak, bár kialakulásuk idején ez a kifejezés még nem létezett.

A centralizált rendszerek a 20. században jelentek meg, amikor szükségessé vált a nagy mennyiségű, koncentrált szennyvizet tisztítani. A nagyvárosok fejlődésével terjedtek el a szennyvíztisztító telepek, az épületek jelentős részét pedig csatlakoztatták a csatornarendszerhez.[35] Napjainkban is ilyen telepek látják el a nagyobb, illetve sűrűn lakott települések szennyvizének tisztítását. A kistelepüléseken csatornázás hiányában még mindig előfordulhat, hogy esetenként kezelés nélkül folyik el a szennyvíz az épületektől, ami jelentős terheket róhat a környezetre. Azokon a településeken és településrészeken, ahol a csatornahálózat kiépítése gazdaságilag nem indokolt, ott az egyedi szennyvízkezelés valamely változatának használata kötelező a talaj, talajvíz és felszíni víz szennyezésének elkerülésére. A 174/2003. (X. 28.) Korm. rendelet szerint az egyedi szennyvízkezelés három eszköze egyedi szennyvízelhelyezési kislétesítmény, egyedi szennyvíztisztító kisberendezés vagy egyedi zárt szennyvíztároló létesítmény lehet.[36] Az első megoldáshoz tartozik például a gyökérzónás tisztítás, míg az utóbbihoz az emésztőgödrök vagy szikkasztók alkalmazása.

Napjainkban viszont egyre népszerűbbek az olyan, modernebb technológiákat alkalmazó decentralizált rendszerek, mint az eleveniszapos reaktorok és a membrán bioreaktorok.[37] Ezeket leggyakrabban pénzügyi okokból, vagy csatornák hiányában kényszerből alkalmazzák, és a szennyvíztisztító telepekhez hasonlóan védik az emberi egészséget, valamint a környezetet, megállíthatják a felszíni vizek minőségromlását.[38] A kialakításból és működésből adódó különbségek miatt közvetlenül nehezen hasonlíthatók össze a centralizált és decentralizált rendszerek, ezt tovább nehezíti az eltérő mintavételezés, legfőképp pedig a beérkező szennyvíz összetételében rejlő eltérések. Míg a decentralizált rendszerek 1-1 ház, épület vagy gyár szennyvizét kezelik, a centralizált telepekre gyakran az esővíz, a lakossági és különféle ipari szennyvizek is

[33] Juhász 2011.
[34] Bernal–Restrepo 2012.
[35] Juhász 2011.
[36] Karches 2020.
[37] Bába–Karches 2020: 103–111.
[38] Libralato – Volpi Ghirardini – Avezzù 2012; Torre et al. 2021.

befolynak, rendkívül összetetté téve a kezelendő vizet.[39] Az eutrofizáció megelőzését tekintve a jelenleg legjobb centralizált és decentralizált rendszerek hasonló eltávolítási hatásfokkal rendelkeznek, a befogadó vizekben megakadályozzák a tápanyag-feldúsulást.[40] A decentralizált rendszereknek megfelelő üzemeltetés esetén több működésbeli előnyük is van, amelyek közvetlenül hatnak a természetes környezetre, az energiaigényeken keresztül pedig indirekt módon az éghajlatváltozásra. A szennyvíz a keletkezés helyén szétválasztható, a frakciók pedig célzottan kezelhetők. A feketevíz kezelhető granulált iszapos anaerob rendszerben (például Upflow Anaerobic Sludge Blanket, UASB), a szürkevíz pedig eleveniszapos reaktorban vagy membrán bioreaktorban (MBR). Az UASB rendszerekben oxigén hiányában nem megy végbe a nitrifikáció és denitrifikáció, amely nitrogéngázt eredményezne; a biológiai többletfoszfor-eltávolítás pedig váltakozó anaerob és anoxikus terek kialakításával megoldható. Így megvalósítható a nagy fokú nitrogén- és foszforvisszanyerés, amely akár négyszer, illetve harmincszor hatékonyabb lehet egyes kisberendezések esetén. Így csökken az N_2O-kibocsátás,[41] és indirekt módon csökkenthető a műtrágya-előállítás szükségessége. A centralizált telepeken a nitrifikáció során a nitrogén nagy része a légkörbe kerül, így nem nyerhető ki.[42] A kémiai oxigénigényt vizsgálva megállapították, hogy a szerves anyagok eltávolítása és biogázzá alakítása is hatékonyabb a különböző szennyvizek szétválasztását alkalmazó rendszereknél. A biogázból energia nyerhető vissza, amely csökkenti az ilyen rendszerek jelentős energiafelhasználását, tovább csökkentve a környezeti terhelést.[43] A keletkezett iszap is kevesebb gondot okoz kisberendezések esetén: egyrészt a kisebb vegyszerhasználat miatt több lehetőség van annak felhasználására, másrészt nincs szükség magas költségű szállításra, kezelésre és elhelyezésre.[44] A nagyobb iszapkor és az eltérő mikrobiális összetétel miatt hatékonyabban történhet egyes szerves anyagok lebontása, egy kutatás szerint pedig 13 olyan anyagot is sikerült eltávolítani, amelyet a centralizált rendszerek nem tudtak, többek között például 3-metil-akridin, p-(2-metilallil)-fenol.[45]

A kisberendezések legnagyobb előnyei a centralizált telepekkel szemben azonban nem a hatékonysággal függenek össze. Egy 2012-es kutatás részletesen ismerteti az azt megelőző, több mint 10 év pozitív tapasztalatait.[46] Jelentős pénzügyi előnynek számít, hogy nem kell egy kiterjedt csatornarendszert építeni és karbantartani, a berendezések kis helyet igényelnek, több változatban elérhetők, és dinamikusan üzemeltethetők. Ebből kifolyólag alkalmas megoldás az elszigetelt vagy kis létszámú települések kiszolgálására, megkönnyítheti a városok tervezését, viszont a megfelelő berendezést körültekintően kell kiválasztani.[47] Továbbá, nincs szükség a természetes vagy épített környezet megzavarására csatornák telepítésével. Odafigyelő szennyvízkezelés mellett kevesebb anyagi terhet ró a lakosságra, ami a gazdaságilag elmaradottabb

[39] Libralato – Volpi Ghirardini – Avezzù 2012; Bernal–Restrepo 2012.
[40] Torre et al. 2021.
[41] Bencsik–Karches 2015.
[42] Torre et al. 2021.
[43] Besson et al. 2021; Estévez et al. 2022.
[44] Torre et al. 2021.
[45] Mladenov et al. 2022.
[46] Libralato – Volpi Ghirardini – Avezzù 2012.
[47] Boguniewicz-Zabłocka – Capodaglio 2017.

területeken kiemelten fontos. A centralizált telepek mint kritikus infrastruktúrák működését befolyásoló természeti katasztrófák (földrengés, viharok) és esetleges szándékos szabotázsok (terrorista támadások) jelentős kockázatot jelentenek. Ezzel szemben a decentralizált rendszerek kis méretükből, biztonságosabb működésükből és elszórt elhelyezkedésükből adódóan kevésbé kitettek ezeknek a veszélyeknek.[48] A legígéretesebb előnyük továbbá, hogy lehetővé (és kedvezővé) teszik a kezelt szennyvíz helyben történő újrahasznosítását. Korszerű és összetett módszerekkel ez felhasználható ivóvízként, toalettöblítésre, viszont a leggyakoribb mód az öntözésre való felhasználás. A kitermelendő víz mennyisége és a víztestek terhelésének csökkentése mellett a tulajdonosoknak is megtakarítást jelenthet.[49] Fontos megemlíteni, hogy az elégtelenül kezelt szennyvízben maradt patogén baktériumok jelentős egészségügyi kockázatot jelentenek felszíni öntözésre való felhasználás esetén.[50] Egy 2012-es tanulmány összefoglal több olyan esetet, ahol a decentralizációval jelentős sikereket értek el: az Egyesült Államokban a kezelt szennyvizet több helyen használják kertek, golfpályák és közterületek öntözésére. Pekingben a nagyobb intézmények rendelkeznek saját decentralizált szennyvíz-újrahasznosító rendszerrel, Velence szigetein pedig 4493 kisberendezés látja el a szennyvízkezelést.[51]

A kutatások alapján a decentralizált rendszerek mindenképpen előnyösebbek a környezetre és az emberi egészségre nézve, mint a szennyvizek közvetlen befogadókba engedése, bármilyen típusú vagy koncentrációjú szennyvízről legyen is szó. A centralizált rendszerekkel szemben viszont a felsorolt előnyök mellett néhány hátrány is jelentkezhet. Először is, szennyvíz-térfogategységre lebontva a modern kisberendezéseknek nagyobb az energiaigényük,[52] ez nagyobb nyersanyag-felhasználást von maga után. Ez önmagában kedvezőtlen, de a korábban tárgyalt előnyökkel a környezeti hatások összességében csökkenthetők.[53] A meghibásodások miatti esetlegesen környezetbe kerülő kezeletlen szennyvíz a kisebb hígítás miatt lokálisan nagyobb károkat okozhat.[54] Ennek kiemelt jelentősége van, tekintve, hogy a kisberendezések karbantartása nem minden országban megoldott.

Összefoglalás

Ez a tanulmány a releváns szakirodalom feldolgozásával vette sorra az ókortól napjainkig tartó fejlődést és változásokat a szennyvízkezelés témakörében, és hasonlította össze az aktuálisan alkalmazott két legfontosabb technológiai megoldást. A történelmi események és az utóbbi idők jogszabályai alapján jól követhető, hogyan kap egyre nagyobb jelentőséget a természetes környezet védelme. A történelem során többször is előfordult, hogy a háborúk és konfliktusok miatt a környezetvédelem háttérbe került,

[48] Libralato – Volpi Ghirardini – Avezzù 2012.
[49] Libralato – Volpi Ghirardini – Avezzù 2012.
[50] Knisz et al. 2021.
[51] Bernal–Restrepo 2012.
[52] Karches 2022.
[53] Besson et al. 2021; Torre et al. 2021.
[54] Torre et al. 2021.

azonban minden esetben igazolódik ennek rendkívüli fontossága. Az utóbbi néhány évtized kutatásai rávilágítottak azokra a pontokra, ahol van lehetőség fejleszteni a szennyvíztisztításon, a kapcsolódó publikációk egyre növekvő száma pedig igazolja, hogy egy releváns, intenzíven kutatott témáról van szó. A folyamatosan megjelenő innovatív megoldások közelebb vihetik az emberiséget ahhoz, hogy az erőforrások megvédésével biztosíthassa saját fejlődését. Mindazonáltal törekedni kell arra, hogy a különböző technológiák alkalmazása során a gazdaságosság és az egészségvédelem mellett mindig központi szerepet kapjon a környezetvédelem.

Köszönetnyilvánítás

A cikkben bemutatott kutatás a Széchenyi Terv Plusz program keretében az RRF-2.3.1-21-2022-00008 számú projekt támogatásával valósult meg.

Felhasznált irodalom

Angelakis, Andreas N. – Snyder, Shane A. (2015): Wastewater Treatment and Reuse: Past, Present, and Future. *Water (Switzerland),* 7(9), 4887–4895. Online: https://doi.org/10.3390/w7094887

Bába, Barnabás – Karches, Tamás (2020): Sizing of a Decentralized Wastewater Treatment Unit Supported by Biokinetic Modeling. *Pollack Periodica,* 15(1), 103–111. Online: https://doi.org/10.1556/606.2020.15.1.10

Bencsik, Dániel – Karches, Tamás (2015): Estimation of GHG Emissions of a Fixed Bed Biofilm Reactor Cascade in Wastewater Treatment. *Journal of Environmental Science and Engineering A,* 4(11). Online: https://doi.org/10.17265/2162-5298/2015.11.001

Bernal, Diana P. – Restrepo, Inès (2012): Key Issues for Decentralization in Municipal Wastewater Treatment. In *12th edition of the World Wide Workshop for Young Environmental Scientists.* Online: https://hal-enpc.archives-ouvertes.fr/hal-00731140

Besson, Mathilde et al. (2021): Environmental Assessment of Urine, Black and Grey Water Separation for Resource Recovery in a New District Compared to Centralized Wastewater Resources Recovery Plant. *Journal of Cleaner Production,* 301. Online: https://doi.org/10.1016/j.jclepro.2021.126868

Boguniewicz-Zabłocka, Joanna – Capodaglio, Andrea G. (2017): Sustainable Wastewater Treatment Solutions for Rural Communities: Public (Centralized) or Individual (On-Site) – Case Study. *Economic and Environmental Studies,* 17(44), 1103–1119. Online: https://doi.org/10.25167/ees.2017.44.29

De Sanctis, Marco et al. (2017): Removal of Pollutants and Pathogens by a Simplified Treatment Scheme for Municipal Wastewater Reuse in Agriculture. *Science of the Total Environment,* 580, 17–25. Online: https://doi.org/10.1016/j.scitotenv.2016.12.002

Elgarahy, A. M. et al. (2021): A Critical Review of Biosorption of Dyes, Heavy Metals and Metalloids from Wastewater as an Efficient and Green Process. *Cleaner Engineering and Technology,* 4, 100209. Online: https://doi.org/10.1016/j.clet.2021.100209

Estévez, Sofía et al. (2022): How Decentralized Treatment Can Contribute to the Symbiosis Between Environmental Protection and Resource Recovery. *Science of the Total Environment,* 812. Online: https://doi.org/10.1016/j.scitotenv.2021.151485

Hankó Márta – Földi László (2009): Életterünk környezetbiztonsági kérdései. *Hadmérnök,* 4(4), 24–38. Online: http://hadmernok.hu/2009_4_hanko1.pdf

Herren, L. W. et al. (2021): Septic Systems Drive Nutrient Enrichment of Groundwaters and Eutrophication in the Urbanized Indian River Lagoon, Florida. *Marine Pollution Bulletin,* 172. 112928. Online: https://doi.org/10.1016/j.marpolbul.2021.112928

Jaramillo, María F. – Restrepo, Inés (2017): Wastewater Reuse in Agriculture: A Review about Its Limitations and Benefits. *Sustainability (Switzerland),* 9(10), 1734. Online: https://doi.org/10.3390/su9101734

Juhász Endre (2011): *A szennyvíztisztítás története.* Budapest: Magyar Víziközmű Szövetség.

Karches Tamás szerk. (2020): *Kis kapacitású szennyvíztisztító létesítmények.* Budapest: Ludovika.

Karches, Tamás (2022): Fine-Tuning the Aeration Control for Energy-Efficient Operation in a Small Sewage Treatment Plant by Applying Biokinetic Modeling. *Energies,* 15(17). Online: https://doi.org/10.3390/en15176113

Knisz Judit szerk. (2020): *Szerves mikroszennyezők a vizekben.* Budapest: Ludovika.

Knisz, Judit et al. (2021): Genome-level Insights into the Operation of an On-site Biological Wastewater Treatment Unit Reveal the Importance of Storage Time. *Science of the Total Environment,* 766. Online: https://doi.org/10.1016/j.scitotenv.2020.144425

Libralato, Giovanni – Volpi Ghirardini, Annamaria – Avezzù, Francesco (2012): To Centralise or to Decentralise: An Overview of the Most Recent Trends in Wastewater Treatment Management. *Journal of Environmental Management,* 94(1), 61–68. Online: https://doi.org/10.1016/j.jenvman.2011.07.010

Lofrano, Giusy – Brown, Jeanette (2010): Wastewater Management through the Ages: A History of Mankind. *Science of the Total Environment,* 408(22), 5254–5264. Online: https://doi.org/10.1016/j.scitotenv.2010.07.062

Mladenov, Natalie et al. (2022): Persistence and Removal of Trace Organic Compounds in Centralized and Decentralized Wastewater Treatment Systems. *Chemosphere,* 286. Online: https://doi.org/10.1016/j.chemosphere.2021.131621

Nemerow, Nelson L. (2007): Removal of Organic Dissolved Solids. In *Industrial Waste Treatment.* Burlington, MA: Butterworth-Heinemann, 105–148. Online: https://doi.org/10.1016/B978-012372493-9/50043-0

Sarma, Bornali (2018): Evolution of Waste Water Treatment Technology and Impact of Microbial Technology in Pollution Minimization during Natural Fiber Processing. *Current Trends in Fashion Technology & Textile Engineering,* 3(5), 555621. Online: https://doi.org/10.19080/CTFTTE.2018.03.555621

Smith, V. H. (2009): Eutrophication. In Likens, Gene E. (szerk.): *Encyclopedia of Inland Waters.* Amsterdam: Elsevier, 61–73. Online: https://doi.org/10.1016/B978-012370626-3.00234-9

Torre, Andre et al. (2021): Wastewater Treatment Decentralization: Is This the Right Direction for Megacities in the Global South? *Science of the Total Environment,* 778, 146227. Online: https://doi.org/10.1016/j.scitotenv.2021.146227

Yaqub, Muhammad – Lee, Wontae (2019). Zero-liquid Discharge (ZLD) Technology for Resource Recovery from Wastewater: A Review. *Science of the Total Environment* 681, 551–563. Online: https://doi.org/10.1016/j.scitotenv.2019.05.062

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
18. évfolyam (2023) 3. szám 45–56.
DOI: 10.32567/hm.2023.3.4

Lilla Horváth[1]

Physiological and Psychological Stress Effects on the Rescue Units Involved in the Earthquake Rescue Operation in Turkey, with Particular Regard to the HUNOR Rescue Team

Abstract

The purpose of this article is to present all the impacts on rescue teams that occur during rescue operations. The HUNOR rescue team, which searched for survivors for a week after the earthquake in Turkey, will be presented. The physiological and psychological strain is not negligible, so the article also makes a short detour about aftercare. At the end of the article, all the development directions that can contribute to the enhanced protection of a rescue team will be discussed, both in terms of personal protective equipment and organisational and health preparedness.

Keywords: earthquake, rescue, survivor, rescue team, personal protective equipment

Introduction

On 6 February 2023, several earthquakes occurred in the south of Turkey and the north of Syria (first a 7.8 on the Richter scale, then a 7.5), during which many buildings collapsed and several tens of thousands died.[2] The damage is incalculable. After the disaster, rescue teams from several countries arrived in search of survivors, as did the Hungarian HUNOR SAR team, who set off on the same day.[3]

[1] University of Public Service, Doctoral School of Military Engineering, e-mail: lilla.horvath@katved.gov.hu
[2] KAWOOSA 2023.
[3] HUNOR s. a.

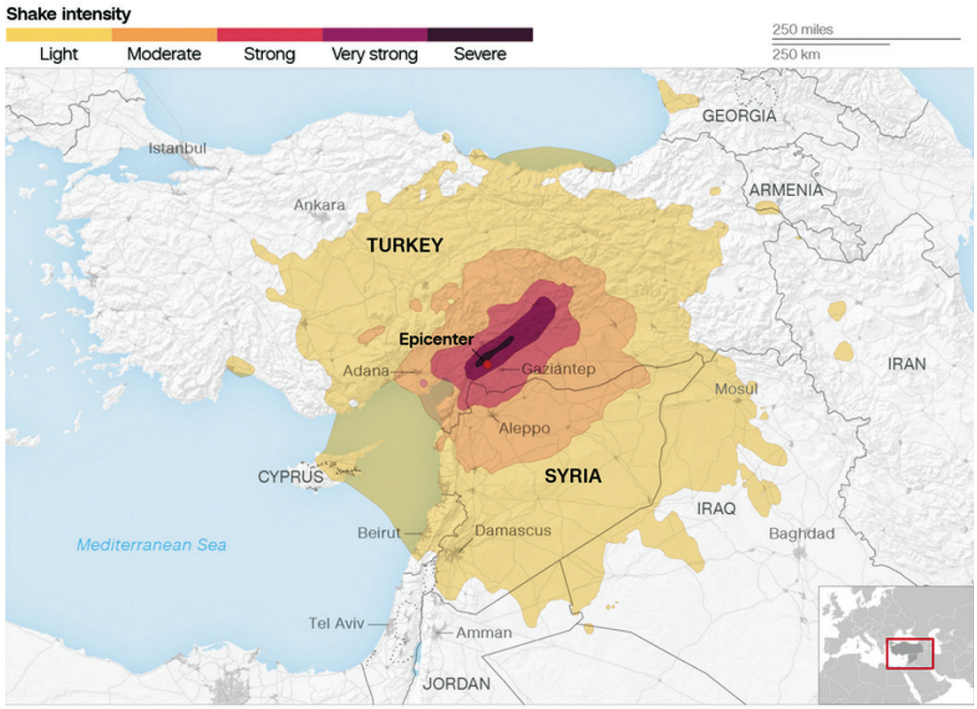


Figure 1: Shake intensity
Source: Mogul et al. 2023a.

After such an event, the members of the rescue organisations must be strong not only physically, but also mentally, since in addition to the sight of dead people, they also have to cope with the fact that they cannot save everyone, even though they know and hear that they are lying there under the ruins. In addition, they must be able to reassure the relatives of the victims and, if necessary, take them to a safe place. After the 6 February earthquake, several earthquakes of lesser intensity occurred, which also made the rescue work more difficult.[4]

The rescue organisation HUNOR arrived at the scene with a total of 50 people (6 people from the staff of the National Rescue Service and 44 firefighters) and two rescue dogs, and during their six-day stay outside, they rescued 17 adults and three children from under the ruins.[5] Their competence and professional knowledge deserve all recognition. The units of the rescue organisations of the other aid-giving countries also worked tirelessly to rescue as many survivors as possible.

But how could the earthquake have developed and what kind of professional background is required to conduct a rescue in a dangerous environment? In the next section, the author tries to answer these questions.

[4] Hallam et al. 2023b.
[5] National Directorate General for Disaster Management 2023a.

Earthquakes

Earthquakes were already written down in ancient times, as shown by the quote below, which comes from the pen of Phlegon, an ancient historian:

"Huge skeletons have come to light from the cracks in the earth. The local inhabitants were so terrified that they did not dare to move them, but a tooth was sent to Rome as a specimen, the length of which even exceeded a foot."[6]

Their formation can be explained by plate tectonics reasons. There used to be a continuous landmass on Earth, and then the continents we know today were formed, and in the case of plates sliding next to and on top of each other and straining against each other, tension arises, which beyond a certain extent can be balanced in the form of kinetic energy. There are areas where earthquakes occur more often, these are called earthquake zones.[7]

A natural disaster in a given region, especially an earthquake, causes not only environmental but also economic damage. In addition to buildings, it also causes serious losses in infrastructure, and it also poses a threat to the lives of the population. In industrially developed areas, mainly high-rise buildings and skyscrapers are built, as this allows more people to live and work in a given area. Nowadays, the provision of electricity (critical infrastructure), along with water supply and district heating, has become a vital element of everyday life. As a result of an earthquake, the number of victims in a given area is also higher. In addition, we can count on the release of dangerous substances into the open, famine and the occurrence of epidemics, so a complex disaster situation can develop in such an event.[8] Reducing the effects of post-disaster conditions and preventing further damage is event-specific in each case. Major accidents can also happen in risky plants during manufacturing, processing or storage, when the release of harmful substances can have a disastrous effect on human health, as well as pollute surface and ground water and the built environment.[9] The given communication or health insurance procedure depends on the scope of the event, the data of the residents of the given area, the critical infrastructure, or the endangered environmental elements.[10]

A major earthquake (Izmit Earthquake) occurred in Turkey earlier, on 17 August 1999, during which 17,000 people died and 250,000 became homeless.[11] During the 6 February 2023 earthquake, nature caused a similar destruction. But why is it that in some countries this type of event occurs relatively often, while in others it is rare? This question is answered by the Global Seismic Hazards Assessment Project (GSHAP), which was carried out from 1992 to 1998. The GSHAP Global Seismic Hazard Map shows which areas are highly or lightly affected by earthquakes.[12]

6 Németh 2015: 19–22.
7 Hornyacsek 2011: 276–295.
8 Hábermayer–Muhoray 2021: 94–110.
9 Cimer et al. 2021: 1–16.
10 Antal–Révai 2014: 60–69.
11 PreventionWeb s. a.
12 Giardini et al. 1999: 1225–1230.

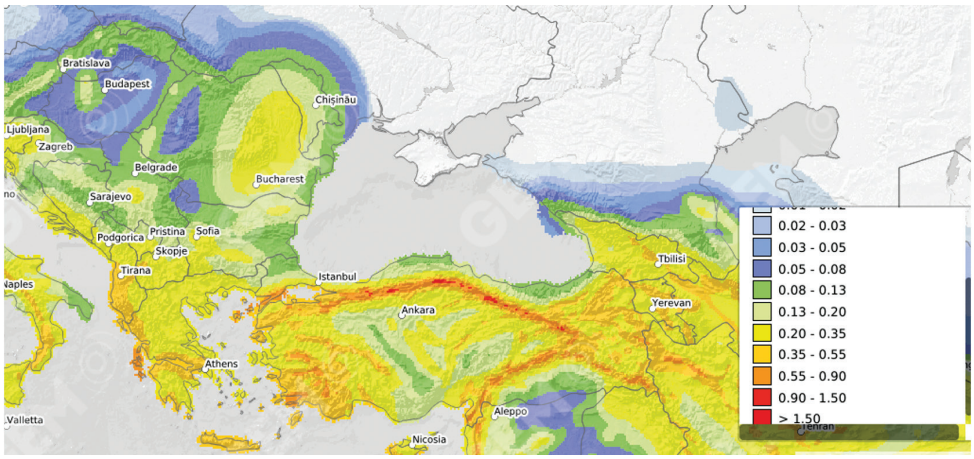


Figure 2: Global Seismic Hazard Map
*Source: **OpenQuake Map Viewer s. a.***

The relationship between the earthquake risk assessment and the infrastructure of the buildings is given by the peak ground acceleration value (PGA) measured on the ground. Figure 2 shows that Turkey and its region are exposed to a high risk in this respect, while in Hungary, for example, this risk is low.[13] This is also shown by the scale on the right side of the figure.

The earthquake that occurred in Turkey on 6 February 2023, caused enormous damage. According to estimates, the number of dead exceeds 47,000 people, and the number of destroyed or damaged buildings is in the hundreds of thousands.[14] It could take years to repair the damage due to the extent of the destruction. The infrastructure, such as the road network or public utility network, has been significantly damaged, and damage liquidation and restoration will require significant costs. In addition, many people's housing and jobs have become insecure, and ensuring this will also places an additional burden on the state coffers. In addition to the financial damage, it is also worth mentioning the mental strain and trauma experienced by many survivors, they lost relatives, children and parents. For them, psychological help in the coming months is extremely important.

Presentation of HUNOR

The HUNOR Hungarian National Organization for Rescue Services was established in 2012 and in the same year, it was awarded heavy urban search and rescue qualification by the United Nations (UN) International Search and Rescue Advisory Group (INSARAG). The purpose of its establishment is to perform urban search and rescue

[13] Irwansyah et al. 2013.
[14] CNBC 2023.

tasks in the event of an emergency, or threat of disaster. The Director General of the National Directorate General for Disaster Management (NDG DM) can order its mobilisation. It can intervene in unexpected and serious situations with a quick response, the logistics staff and members arrive at the designated meeting place within 3 hours of the alarm, and the rest within 6 hours. Its members may include the following: members of the professional staff of disaster management agencies, full-time professional experts of partner agencies, and volunteers, such as disaster specialists, nurses, paramedics, dog handlers, static engineers and psychologists. It is also important to mention the K9 dog unit, which has an internationally certified rescue dog, and the International Rescue Dog Organization (IRO) deployability and ruin investigation exam. The NDG DM regularly provides the staff of the rescue organisation with further professional training, to ensure that their level of practical knowledge does not decrease and that its development is ensured.[15]

By the UN INSARAG Guidelines, the HUNOR rescue organisation can be deployed for 10 days, self-sufficiently, 24 hours a day, at two intervention locations at the same time regarding the following tasks:

- flood defence works
- bracing and support operations
- rescue tasks by lifting heavy objects
- rescue from water and areas covered with water
- cutting and demolition of steel structures and reinforced concrete
- resuscitation, keeping alive and injury classification (Triage)
- detection, classification and separation of dangerous substances
- special operations with ropes
- search and rescue with technical search equipment and dogs[16]

The rescue organisation has 16 tons of equipment and tools that allow them to perform these tasks safely. These are the following:

1. Technical rescue tools
- tools for the rescue task of lifting a large object: pneumatic lifting cushion (up to approximately 60 tons), crane (up to 100 tons), mechanical chain hoist (up to approximately 5 tons), hydraulic oil lift (up to approximately 8–10 tons)
- demolition tools for reinforced concrete and steel structures: drill-chisel combi hammer, gasoline-powered concrete cutter, chain saw (35 cm thick reinforced concrete structures), demolition hammer, air hammer
- tools for special operations with ropes: uniform rope technology tools; personal protective equipment such as harness, breast harness, bridle, carabiner, abseil machine, climbing machine and rope cutter

2. Management and control tools (info-communication tools)
- TETRA radios (for communication in Hungary)
- VHF radios (for foreign communication)

3. Discovery and research tools

[15] Jackovics–Herbák 2017: 245–262.
[16] Muhoray–Teknős 2015: 14–23.

- devices for the detection of dangerous substances with special gas-measuring devices
- hazard detection tools: gas measuring instrument, a thermal camera, a laser distance meter, a radiation dose meter and an electricity measuring instrument
- tools for search with search dogs and technical search equipment: fibre-optic ruin search cameras or ultrasonic-acoustic vital sign detectors (in the search of persons trapped under ruins)

4. In the field of logistics tools
- 10 days of self-sufficiency tools

5. In the field of medical equipment
- professional resuscitation and life support equipment
- medical supplies

6. Other tools suitable for material handling and transport
- quad, bobcat, rescue boats
- heated-cooled, fully comfortable, stable inflatable tent with a floor grid[17]

Based on the list, it can be seen what complex activities the HUNOR rescue organisation performs during search and rescue activities. For the safe use of all these tools – as mentioned earlier – repeated practice is necessary since specific knowledge can only become professional if it is regularly performed both theoretically and practically. In addition to tools and equipment, the staff also needs protective clothing, as they work with dangerous machines, often in extreme weather.

The personal protective equipment used by the rescue organisation HUNOR may vary depending on the specific activity. The different activities are as follows:

- rope rescue
- rescue from a confined space
- ditch rescue
- structural collapse
- water rescue[18]

The personal protective equipment ensures the appropriate level of safety for the members of the staff – in addition to the skill-level professional knowledge – which is essential during such a dangerous activity. The type, design, weight of protective clothing and protective equipment greatly affect the ability to perform work, so the use of high-quality materials is essential. Personal protective equipment can be e.g. a protective helmet, protective gloves, eye protection devices, etc. A list of all these tools is included in the INSARAG Guideline.

In addition to all this, the psychological preparation of the research and rescue staff to process the experiences experienced during a disaster situation is a significant issue. The legal basis for this is provided by Act XCIII of 1993 on Labour Safety, which is provided in Section 54 (1) d) as follows:

[17] Muhoray–Teknős 2015: 14–23.
[18] OCHA 2020: 23–29.

- "(1) To ensure safe and healthy work, the employer must take into account the following general requirements:
- d) taking into account the human factor in the design of the workplace, in the choice of work tools and work processes, with particular regard to the reduction of the duration of monotonous, fixed-paced work and the reduction of its harmful effects, the scheduling of working hours, and the avoidance of strain caused by the psychosocial risks associated with work"[19]

Therefore, the risk assessment prepared by the employer also covers the psychological risks that occur in the case of the given job. In doing so, all preventive measures can be taken to reduce the chance of the expected danger occurring.

In case of rescue organisations, in addition to theoretical and practical preparations, it can be extremely useful if a psychologist is already present at the scene of the intervention, and is thus able to provide psychological assistance to the affected persons from the beginning. After all, not everyone reacts in the same way to the given situation, to the perceived sight. Some people become incapacitated and some people only develop psychological symptoms weeks later (e.g. PTSD).[20]

In addition to the previous points, it should be emphasised that the members of the staff must also be physically fit. The legal basis for this is Decree 45/2020 (XII.16.) of the Ministry of the Interior on fitness tests for professional and administrative law enforcement personnel employed by certain law enforcement agencies under the authority of the Minister of the Interior. In addition, each person must have the appropriate international vaccination, which ensures protection for the human body dependant on the intervened area.

HUNOR in Turkey

As previously mentioned, the 50-person team of HUNOR was deployed to the city of Antakya to search for the survivors of the building collapses caused by the earthquake on 6 February 2023. At 7:00 a.m. the next day, the team left for the province of Hatay with four trucks and two buses, where they received a briefing from the coordinating local bodies in the morning, and then designated the operational area for themselves. In addition, a five-hundred-square-meter campsite was prepared for the rescue team, in which nine tents were placed. The Hungarians worked 24 hours a day, with shifts every eight hours (Figure 3). Conditions were trying even at night as the temperature dropped below freezing. In the course of their activities, in addition to rescuing survivors, they also lifted dead people from the ruins, so they were not only physically but also psychologically stressed.[21]

[19] Act XCIII of 1993 on Labour Safety 54. § (1) d).
[20] PTSD: Posttraumatic Stress Disorder is an anxiety disorder caused by very stressful, frightening or distressing events.
[21] National Directorate General for Disaster Management 2023b.

Figure 3: HUNOR in Antakya
Source: ***Metropol 2023.***

After the return of the HUNOR, several interviews were conducted with individual members of the rescue team. One of these conversations can be listened on the podcast channel of TEOL, where one of the HUNOR rescue members – whose profession is a firefighter – speaks about the event in Turkey. In the process, we learn that the injured were constantly transported, even though the hospital in the city was destroyed. The rescue processes were also complicated by the fact that the relatives of the victims and survivors under the ruins were constantly present and tried to convince the members of the rescue organisations to rescue their relatives first, so the help of the local police was often needed. The search in the ruins was done by hand, so it was very stressful for the members, who were able to evacuate a survivor in up to 4–7 hours. During the rescue, they had many tools at their disposal, such as fibre optics, a sound detector, an angle grinder, a demolition hammer, a reciprocating saw, etc. In addition, the firefighter also reported that it was also possible to communicate with the person to be rescued continuously during the rescue. It was stressful from a psychological point of view because there were many aftershocks during the rescue tasks, and in the event of a larger earthquake, it would not have been possible to escape from the scene.[22]

During the rescue, many effects can be a source of stress for the members of the rescue units. We distinguish between immediate and delayed effects. The following sources of stress occur during task execution:

- responsibility
- physical load
- executor or hero role

[22] Szeri 2023.

- time pressure
- extreme traumatisation
- the risk of injury or death
- observed actor
- suprathreshold stimuli

A delayed stress source is what can appear hours, days, weeks, or even years after the task has been completed:

- flashbacks, nightmares
- accusation[23]

On 29 March 2023, Dr. Selman Salim Kesgin (research coordinator, Turkish Red Crescent Academy) gave a lecture on the earthquake at the Zrínyi Miklós University Campus of the University of Public Service in Budapest, during which the audience was able to gain a lot of useful information. In the presentation, he highlighted all the factors that can be used to increase resilience in such a case, e.g. the construction of special buildings that are more resistant to the effects of an earthquake. It was also discussed what other important activities are necessary in such a case in addition to the rescue activity. This includes feeding, sheltering, protecting, educating the survivors, and ensuring their health care. He emphasised that it is important to prepare the person involved in the rescue, as they can easily become victims (e.g. aftershocks).

Whether it is an immediate or delayed effect, the goal is for the person participating in the rescue to react to the given situation appropriately, without any hindering emotional reaction (e.g. panic), and for the full processing of what has been experienced to take as little time as possible. Psychologists who are already present at the scene provide help for this and use different techniques to try to ease the psychological burden of the intervening colleagues.

Solutions, results

The use of the correct personal protective equipment plays a major role in overcoming physical obstacles that arise during the rescue. Ergonomic features, such as breathability, weight, room for movement, view (breathing mask), and communication in clothing are playing an increasingly important role nowadays, since in addition to fulfilling the function, additional roles have also become important, which contribute to working more efficiently and for longer periods.[24] In addition to personal protective equipment and professional equipment, injuries can also occur during various events against which there is no technical protection (e.g. carelessness of the injured party or another person, etc.). In such cases, it must be expected that the team will be

[23] Ruzsa 2014: 31–40.
[24] Horváth 2022:49–70.

weakened since it has to perform the same task with fewer people than in the case of the original number of employees.[25]

In addition, when dealing with an unpredictable situation, the capabilities of the given organisation cannot be neglected. In case of a high level of organisational culture, all four organisational/individual skills (perception, learning, integration and coordination) are present and the opportunity to develop them is also given.[26] Therefore, proper health and psychological preparation for a disaster situation requires a well-functioning company management.

It is also worth reviewing the methods of mental preparation and aftercare at certain intervals. After the disasters that occurred in the world, using the experience of interviews, questionnaires, group training, etc., there is always an opportunity for a small change in the given psychological program. Regular use of stress-reduction training can help prepare the affected persons for the extreme stress load.[27]

Discussion

The rescue organisation HUNOR played a key role in the search and rescue work following the earthquake in Turkey on 6 February 2023. Testing the limits of their endurance, the members of the staff searched for the survivors of the disaster 24 hours a day. Even with the appropriate professional knowledge and equipment, there were stressful situations that required a suitable health and psychological state, as well as the support of comrades, i.e. good team cohesion.

This emergency also clearly highlighted the need for rescue organisations of this type, since their help can save lives in such an event. For this, the members of the rescue organisation need adequate health and physical endurance as well as regular theoretical and practical training, so that they can withstand as many types of events as possible.

References

Act XCIII of 1993 on Labour Safety

Antal, Örs – Révai, Róbert (2014): Az egészségügy szerepe a katasztrófák megelőzésében [The Role of Healthcare in Disaster Prevention]. *Bolyai Szemle,* 23(1), 60–69.

Cimer, Zsolt – Vass, Gyula – Zsitnyányi, Attila – Kátai-Urbán, Lajos (2021): Application of Chemical Monitoring and Public Alarm Systems to Reduce Public Vulnerability to Major Accidents Involving Dangerous Substances. *Symmetry,* 13(8), 1–16. Online: https://doi.org/10.3390/sym13081528

[25] Pántya 2018: 109–144.
[26] Révai 2021: 165–168.
[27] Szabó–Horváth 2018: 224.

CNBC (2023): Death Toll Rises after Fresh Earthquake Hits Turkey–Syria Border. *CNBC,* 21 February 2023. Online: www.cnbc.com/2023/02/21/death-toll-rises-after-fresh-earthquake-hits-turkey-syria-border.html

Decree 45/2020 (XII.16.) of the Ministry of the Interior on fitness tests for professional and administrative law enforcement personnel employed by certain law enforcement agencies under the authority of the Minister of the Interior.

Hallam, Jonny – Gezer, Yusuf – Sariyuce, Isil – Kourdi, Eyad – Karadsheh, Jomana –Alkhaldi, Celine – Khadder, Kareem (2023b): Magnitude 6.3 Aftershock Strikes Southern Turkey, Killing 6 and Injuring Hundreds 2 Weeks after a Massive Quake Killed Thousands. *CNN,* 21 February 2023. Online: https://edition.cnn.com/2023/02/20/middleeast/turkey-quake-aftershock-intl/index.html

Giardini, Domenico – Grünthal, Gottfried – Shedlock, Kaye M. – Zhang, Peizhen (1999): The GSHAP Global Seismic Hazard Map. *Annali Di Geofisica,* 42(6), 1225–1230. Online: https://doi.org/10.4401/ag-3784

Hábermayer, Tamás – Muhoray, Árpád (2021): Földrengések következményeként várható sérültek és halottak számának becslése – 2. rész [The Estimated Number of the Injured and Dead after an Earthquake – Part 2]. *Hadtudomány,* 31(4), 94–110. Online: https://doi.org/10.17047/HADTUD.2021.31.4.94

HUNOR (s. a.): *Hungarian National Organisation for Rescue Services.* Online: www.katasztrofavedelem.hu/189/hunor

Hornyacsek, Júlia (2011): Földrengés! Fel vagyunk készülve? A lakosság földrengés során való védelmére való felkészülés hazánkban a kárterület és a mentési rendszer tükrében [Earthquake! Are We Ready? Preparing to Protect the Population during an Earthquake in Hungary in the Light of the Damage Area and the Rescue System]. *Hadmérnök,* 6(1), 276–295.

Horváth, Lilla (2022): Examination of the Application of Currently Used, New or Additional Firefighting Personal Protective Equipment. *AARMS,* 21(3), 49–70. Online: https://doi.org/10.32565/aarms.2022.3.3

Irwansyah, E. – Winarko, E. – Rasjid, Z. E. – Bekti, R. D. (2013): Earthquake Hazard Zonation Using Peak Ground Acceleration (PGA) Approach. *Journal of Physics: Conference Series,* 423. Online: https://doi.org/10.1088/1742-6596/423/1/012067

Jackovics, Péter – Herbák, Dóra (2017): Magyarország központi mentőszervezete: a HUNOR [Hungarian Central Rescue Organization: HUNOR]. *Védelem Tudomány,* 2(1), 245–262.

Kawoosa, Vijdan M. (2023): How Turkey Has Been Rattled by Aftershocks since the Feb. 6 Earthquake. *Reuters,* 01 March 2023. Online: www.reuters.com/graphics/TURKEY-QUAKE/AFTERSHOCKS/dwpkdzklevm/

Metropol (2023): Drámai részleteket árult el a HUNOR mentőcsapat parancsnoka a törökországi mentésekről [The Commander of the HUNOR Rescue Team Revealed Dramatic Details about the Rescues in Turkey]. *Metropol,* 23 February 2023. Online: https://metropol.hu/aktualis/2023/02/dramai-reszleteket-arult-el-a-hunor-mentocsapat-parancsnoka-a-torokorszagi-mentesekrol

Mogul, Rhea – Tuysuz, Gul – Sariyuce, Isil – El Damanhoury, Kareem – Picheta, Rob (2023a): More than 4,300 Dead in Turkey and Syria after Powerful Quake.

CNN, 06 February 2023. Online: https://edition.cnn.com/2023/02/05/europe/earthquake-hits-turkey-intl-hnk/index.html

Muhoray, Árpád – Teknős, László (2015): A HUNOR hivatásos nehéz kutató-mentő mentőszervezet alkalmazásának logisztikai feladatai [Logistic Tasks of the Operation of HUNOR Professional Heavy Urban Search and Rescue Team]. *Hadtudomány,* 25(E Issue), 14–23. Online: https://doi.org/10.17047/HADTUD.2015.25.E.11

National Directorate General for Disaster Management (2023a): A legnehezebb terepen fog dolgozni a HUNOR. További túlélőket talált a HUNOR [HUNOR Will Work in the Most Difficult Terrain. HUNOR Has Found More Survivors]. *Katasztrófavédelem,* 12 February 2023. Online: www.katasztrofavedelem.hu/29/hirek/273171/a-legnehezebb-terepen-fog-dolgozni-a-hunor

National Directorate General for Disaster Management(2023b): Hazaérkezett a HUNOR [HUNOR Has Arrived Home]. *Katasztrófavédelem,* 13 February 2023. Online: www.katasztrofavedelem.hu/29/hirek/273332/hazaerkezett-a-hunor

Németh, György (2015): Mit jelent a földrengés? [What Does an Earthquake Mean?] *Ókor,* 14(3), 19–22.

OCHA (2020): *INSARAG Guidelines 2020, Volume II. Preparedness and Response, Manual A: Capacity Building.* Online: www.katasztrofavedelem.hu/application/uploads/documents/2021-04/74739.pdf

OpenQuake Map Viewer (s. a.): *Global Seismic Hazard Map.* Online: https://maps.openquake.org/map/global-seismic-hazard-map/#5/47.828/31.773

PreventionWeb (s. a.): Türkiye: Izmit Earthquake 1999. *PreventionWeb,* s. a. Online: www.preventionweb.net/collections/turkiye-izmit-earthquake-1999

Pántya, Péter (2018): A Katasztrófavédelem beavatkozó hatékonyságának fejlesztése a tűzoltósági területen [Developing the Efficiency of the Intervention Part of the Disaster Management in the Field of Fire Service]. *Hadmérnök,* 13(Special Issue), 109–144.

Révai, Róbert (2021): A rendvédelmi hivatás egészségügyi aspektusai, 50 éves a rendészeti felsőoktatás [Health Aspects of Law Enforcement, 50 Years of Law Enforcement Higher Education]. Jubileumi kiadvány 1971–2021. Budapest: Ludovika University Press. 165–168.

Ruzsa, Dóra (2014): Stresszforrások, stressztünetek és stresszoldási mechanizmusok vizsgálata tűzoltók körében. [Research of Stressors, Symptoms of Stress and Coping Mechanisms among Firefighters]. PhD thesis. Budapest: University of Public Service, Doctoral School of Military Engineering. Online: https://doi.org/10.17625/NKE.2015.011

Szabó, József – Horváth, Péter (2018): A Zala Különleges Mentők mentális felkészítése krízishelyzetekben történő beavatkozásokhoz [Mental Preparation of the Zala Special Rescue Team for Interventions in Crisis Situations]. *Lege Artis Medicinae,* 28(4–5), 221–226.

Szeri, Árpád (2023): Élve eltemetett embereket mentett meg a haláltól a szekszárdi tűzoltó [Firefighter from Szekszárd Saved People Buried Alive from Death]. *TEOL,* 20 March 2023. Online: www.teol.hu/helyi-eletstilus/2023/02/elve-elasott-embereket-mentett-meg-a-halaltol-a-szekszardi-tuzolto

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
18. évfolyam (2023) 3. szám 57–67.
DOI: 10.32567/hm.2023.3.5

Benjámin Hózer,[1] László Teknős,[2] Ferenc Varga,[3] Lajos Kátai-Urbán[4]

Examination of the Practice for Protection against Landfill Fires

The scientific examination of residential waste management has become an increasingly important scientific problem nowadays. Waste disposal and incineration are the most important elements of the modern waste management system. The handling, disposal and burning of residential wastes have significant fire safety risks. In this article, the authors examine the fire protection characteristics of landfills, the legal background of their operation, the causes and circumstances of the individual fires that have occurred, the measures to increase the efficiency, as well as the technical and technological possibilities of fire safety operations.

Keywords: waste, waste management, landfill, fires, fire prevention, safety

Introduction

Waste management as a global environmental problem is a consequence of humanity's survival process.[5] It can be said as a general rule that in nature waste does not exist. It is also well known that matter is not lost, only transformed.[6] Waste is material that is formed in the built environment by the economic activity of society, which can no longer be used at the place of origin.[7] An example for the advantage of waste generation is that many archaeological findings have become important historical values thanks to the preservation of "waste".

1 PhD student, University of Public Service, Doctoral School of Military Engineering, e-mail: hozer.benjamin@uni-nke.hu
2 Assistant Professor, University of Public Service, Faculty of Law Enforcement, Institute of Disaster Management, e-mail: teknos.laszlo@uni-nke.hu
3 Assistant Professor, Head of Department, University of Public Service, Faculty of Law Enforcement, Institute of Disaster Management, e-mail: Varga.Ferenc2@uni-nke.hu
4 Associate Professor, University of Public Service, Faculty of Law Enforcement, Institute of Disaster Management, e-mail: katai.lajos@uni-nke.hu
5 Wilson–Velis 2015: 1049–1051.
6 Darvay et al. 2016: 88–104.
7 Solymosi 2016: 171.

The composition and quantity of modern waste is significantly different from what was customary in earlier centuries. Waste generation and related treatment methods – as a result of human production that became more intense – became a social issue after the industrial revolution and then became a global environmental problem after the boom in machine manufacturing and the plastics industry.[8]

Currently, it is necessary to move in the direction of zero waste from the point of view of the disposable world.[9] However, as a result of the currently experienced population growth, the related dynamic urbanisation process, and changes in consumer social habits, society and modern civilisation can no longer coordinate the increasing waste production at the place of origin.[10] Therefore, there is a need for solutions such as the application of waste-free or low-waste technologies, the separate collection, utilisation, recycling of the generated waste, the disposal of waste not used as secondary raw materials, the temporary storage, disposal of non-reusable waste.

Among the domestic legislation Act. CLXXXV of 2012 on waste management (Act on Waste Management) is the primary applicable legislation source in Hungary. The Act on Waste Management defines that during the prevention activities of waste generation and waste management, the following activities must be applied in order of priority:

- prevention of waste generation
- preparation of waste for recycling
- waste recycling
- utilisation of waste in other ways, especially energetic utilisation, as well as disposal of waste at waste landfill sites

In this article, the aim of the authors is to assess the legal regulation and law enforcement practice of waste disposal activities in accordance with fire protection. In the course of this evaluation process, in addition to the analysis of the effective international and domestic legal regulatory environment and the technical guidance materials we will analyse the causes and circumstances of the occurrence of major fires, the measures to increase the efficiency of fire safety operations, and technical and technological possibilities for intervention procedures and methods.

The role of landfills in waste management

Based on the examination of the so-called waste hierarchy,[11] it can be concluded that final landfill disposal of waste as a waste management procedure is used to a significant extent in Hungary. Based on data received upon our request from the Ministry of Energy, the rates of waste processing procedures in our country at the end of the year 2021 were as follows:

[8] Faragó 2013: 43–76; Supka 2020.
[9] Directive (EU) 2018/849 of the European Parliament and of the Council.
[10] UNEP 2015.
[11] Directive 2008/98/EC of the European Parliament and of the Council; National Waste Management Plan (2021–2027).

- proportion of waste used in its own material: 36.6%
- proportion of energetically utilised waste: 12.4%
- proportion of landfilled waste: 51%

Waste disposal (landfilling, incineration without energy recovery, illegal dumping) is a common and relatively cheap solution for waste management.[12] When choosing waste management methods, it is important to apply the higher levels of the elements of the waste hierarchy. In addition, a technical solution suitable for the given conditions must be selected as well. The last procedure – and at the same time the least favourable way according to the hierarchy – is the dumping of waste.

The elements of the regulations related to landfills – based on European Union legislation – are the followings:

- Act CLXXXV of 2012 on Waste
- Decree 20/2006 (IV.5.) of the Ministry of Environment and Water on certain rules and conditions relating to the landfill of waste and the landfilling of waste

Additional useful legal and technical information can be obtained from the National Waste Management Plan prepared by the Environment Authority.

In line with the relevant regulation, landfills can be categorised in the following ways:

- Category A – inert waste landfills
- Subcategory B1b and B3 non-hazardous waste landfill sites
- Category C hazardous waste landfill sites[13]

Waste disposal methods include landfilling, thermal disposal and chemical, biological or physical processes. Waste disposal can be done by cumulate waste in a prismatic, frontal, circular system, or by mound construction accumulation. In relation to the latter treatment method, we can state that it requires a large area, increases the load and pollution of environmental elements and cannot provide a solution to the global waste problems of the society. Landfilling waste is actually a "superficial" treatment, as it does not reduce the growing amount of waste, nor does it have the motivating force to reduce waste in an institutional, legal, administrative or technical sense.

Hungary has not increased its waste incineration capacity in recent years. However, the modernisation process of the existing facilities is currently underway, with the aim of creating closed material cycles by increasing reuse and recycling, as well as reducing the amount of waste to be disposed of.

Waste should be considered a material flow in the cycle, which is part of the green transition processes according to the National Energy and Climate Plan, and a determining part of reducing greenhouse gas emissions strategies. This is also an environmental protection objective of the European Union, within the framework of which Hungary has made significant voluntary commitments.

[12] Act CLXXXV of 2012 on Waste.
[13] Decree 20/2006 (IV.5.) of the Ministry of Environment and Water on certain rules and conditions relating to the landfill of waste and the landfilling of waste.

Overall, the trend is towards reducing the role of landfills, and in the waste hierarchy, zero waste and waste generation at the point of origin come to the fore. Based on the current social processes, the secondary objective of waste management is the reintroduction of waste into production as a resource of civilisation activities.[14] It can be concluded that the operation of landfills has no return benefit, regardless of this, even today, the importance of landfills is still considered decisive. Among the types of waste accumulated in landfills, we can find many combustible materials, which pose a significant fire safety risk and have the potential to pollute the surrounding environment.

The analysis and evaluation of waste disposal activities from the point of view of fire protection and environmental safety aspects is the main objective of this article, the results of which will be presented in the following section.

Evaluation of legal regulations concerning the fire protection of landfills

Directive 1999/31/EC of the Council of the European Union on landfills[15] specified in its Annex I some fire protection requirements concerning the installation and operation of landfill facilities. Among the general measure requirements, the directive lists a fire incident among the events with a disturbing effect or danger to the landfill facility. Regrettably, it can be stated that the European Union regulations dealing with the safety situations of landfills leave some room for improvement as the regulation only defines the main standards of waste disposal and acceptance. However, disaster prevention or fire prevention aspects are not examined in this legislation. In addition, the cited legislation in its Article 5 paragraph (3) b) point classifies flammable and explosive substances as waste that cannot be accepted in landfills. However, it does not make recommendations or technical prescription regarding the implementation of this legislation. It also does not have recommendations for filtering out flammable or explosive substances from waste. Unfortunately, this burden ultimately falls only on the operator's discretion. As a result, the operator determines internal norms within his own competence, which can be supplemented with the professional recommendations of the fire prevention authority or the specialised fire protection service organisation. Of course, this significantly can reduce the security level of the facility.

It can be concluded that no process or technology is currently available to filter out flammable substances entering the territory of the landfill's site. Perhaps the only option is to draw the public's attention on the public awareness to collect waste selectively. In the capital city of Budapest, for example – within the framework of the annual garbage collection program – the collection of small-sized hazardous waste, such as paints and thinners, takes place at a separate collection point from municipal waste. In this way, the Capital City Public Area Maintenance Office, which organises

[14] Berek et al. 2021: 87–96.
[15] European Council Directive 1999/31/EC (26 April 1999) on landfills.

the garbage collection, strives to improve the level of recycling and to reduce the possibility of fires and work accidents during the collection process.

We can also cite a precedent for an accident related to flammable substances mixed with waste. In November 1996, a spark and then an explosion occurred in the cargo hold of a garbage truck in Rákospalota Budapest presumably from the mixing and shaking of the paint solvents and metal shavings. The explosion opened the rear wall of the garbage truck and the waste stored there caught fire. Fortunately, there were no personal injuries.[16]

It is also worth mentioning that the previously mentioned European Union regulation also prohibits the dumping of used transport vehicle tires. According to the main rule, it is not possible to deposit these materials in the landfill site. Filtering out tires is no longer an easy task, as residential waste collection machines do not transport them either. However, practical experience shows that tires still appear in several landfills, therefore, during their burning a significant amount of toxic combustion products are produced that can endanger the surrounding environment and the population.

Picture 1: Consequences of a large amount of accumulated car tire fire
Source: Facebook page of the Zalaháp Volunteer Fire Department.

In Hungary, the general regulation of waste management is contained in the Act on Waste Management. In addition, Decree 20/2006 (IV.5.) defines the exact rules for the establishment and operation of landfill facilities. The two mentioned legislations do not discuss the safety aspects of the facilities in a separate provisions. The establishment criteria for the fire protection of landfills are stipulated only by the National

[16] Hajdú-Bihari Napló 1996.

Fire Protection Regulations (NFPR) introduced by the decree of the Ministry of the Interior (hereafter: NFPR)[17] in its point 6 of paragraph 72. According to the regulations "the outdoor storage area of the municipal waste dump must be provided with an intensity of 1,800 litres/minute of extinguishing water for one and a half hours".

Practical experience shows that the nearest fire hydrant is usually at a significant distance of 1 to 3 kilometres from the facilities. It is therefore only possible to provide extinguishing water from specially installed axillary fire protection reservoirs.[18] According to domestic regulations, the requirement is to keep a minimum of 162 cubic meters of extinguishing water ready per facility. Pursuant to paragraph 274 of the NFPR, reservoirs must be reviewed on an annual basis. In addition, a pressure test is also performed every five years during the fully implemented review. Typically, the response forces of the regionally competent professional firefighting organisation take part in the pressure test.

It is worth noting that professional fire departments carry out relatively few local preparation visits or practical exercises in the area of landfill sites. However, it would be advisable to increase the number of visits, as the terrain conditions in the area of the landfills change frequently. There may be other variable factors including changes in ground conditions, access roads, also the quantity and location of other stored flammable substances, as well as the number and operational readiness of the operator's machines that can be involved in extinguishing activities.

The legislation in force has relatively few practical prevention regulations regarding the fire safety landfill sites. In case of most facilities, the fire protection policy is drawn up by the plant's owner or commissioned employee with fire protection qualification. However, these fire safety regulations mostly only provide guidance on the placement of fire extinguishers and their readiness to usage. In our opinion, the development of a general sample fire protection policy can be one of the solutions that the landfill operator can adapt to the conditions of the local facility. In accordance with our practical experience, operators often give general verbal instructions to their workers. Among them we can also find prevention and practical firefighting advice.

Operators may also have protective devices that are not specifically required by law to be kept in readiness. As an example of this, some operators utilise the so-called mobile, i.e. fire extinguishers with a large charge mass.

Evaluation of fire-hazardous activities of landfills

Risks posed by landfilled waste materials

We can determine from the heterogeneous composition of the deposited waste that many substances are capable of causing fire or other accident hazards stored in the landfill areas.

[17] Decree 54/2014 (XII.5.) of the Ministry of the Interior on the National Fire Protection Regulations.
[18] Érces–Vass 2019: 131–161.

Fires that occur in landfill facilities can be divided into two large groups according to their cause of occurrence. There are fires caused by human activity or natural decomposition of waste materials. Human activities include primarily the use of open flames, typically smoking. This also includes the ignition of combustible substances due to the hot surface of work machines in case of relatively hot weather conditions. Similar cases can lead to "flying fires" and then fires involving large territories.

Another large group is fires resulting from the decomposition of deposited materials. A significant part of the waste that ends up in landfills comes from biodegradable, typically household waste. Biologically degradable wastes significantly form flammable methane gas during the decomposition process. Methane trapped in waste can easily ignite from a spark or other heat source. The gases produced during decomposition are called landfill gas. Of course, methane can also be used in energetic solutions. We can understand that within the disposal body, different layers are formed from the deposited waste. The individual layers are mostly covered with geotextiles and then covered with earth, which minimises the amount of landfill gas reaching the surface level. Before covering with geotextiles and earth, drain pipes are installed horizontally to pump out the landfill gases. In some cases, the less efficient vertical piping is also used instead of horizontal piping. In this case, the pipelines pass through the waste layers, as a result of which regional extraction can be less effective. Vertical piping is typically recommended for landfills with small areas, as well as for disposal below the ground level.

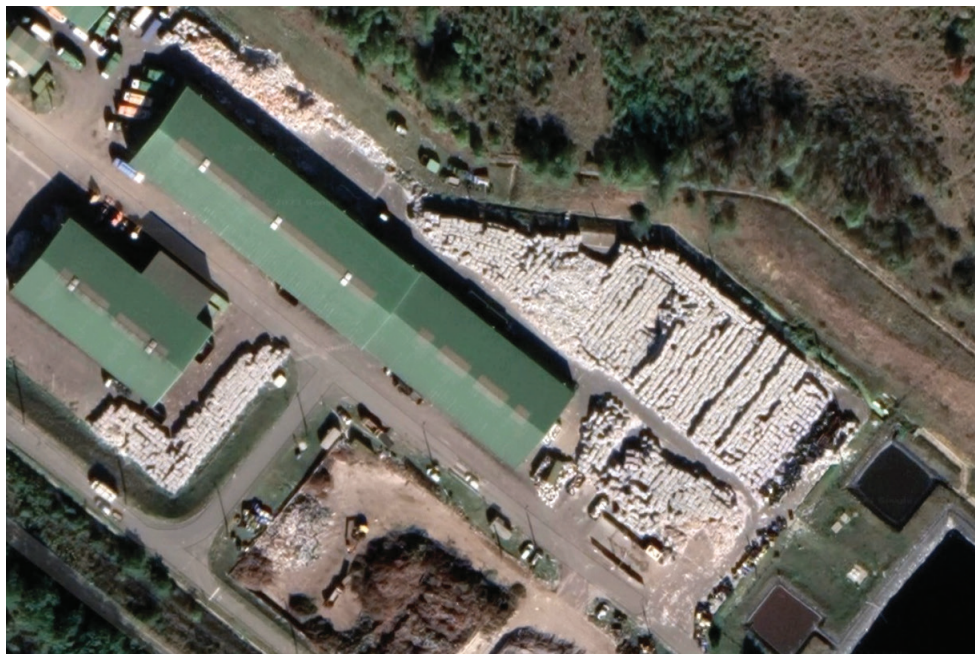
Fire hazard of waste selected for recycling

On the basis of official data from 2021, the Hungarian population produced nearly four million tons of waste. As we have already mentioned, about 51% of that amount was landfilled in storage facilities. Based on the so-called circular economy aspirations of the European Union, it intends to bring the rate of landfilling below 10% by the year 2035. In accordance with the data collected between 2017 and 2021, it can be seen that the landfill rate in Hungary is stagnating based on the data requested from the Ministry of Energy. The trend can therefore be clearly perceived that the operation of landfills will remain a particularly important task for decades to come.[19]

The majority of landfill sites operate manual sorters, where the waste is grouped according to its material. In this way, paper, glass, metal and plastic waste are sorted separately. Plastic waste is compacted and baled on site of the territory of the landfill facility. At the end of the process, the waste becomes a saleable commodity ready for recycling. However, the landfill operator cannot sell the goods until he receives permission from the authority to do so. In some cases, it can take weeks or months to grant permission. As a result, the amount of baled waste increases continuously, often until the end of the plant's storage capacity. All these can increase the risk of the occurrence of fire and the severity of the possible consequences to the environment.

[19] Kirovné Rácz 2021: 21–36.

The following photo clearly shows the significant amount of bales of plastic waste accumulated in the area of one of the landfill sites in Hungary.



Picture 2: Baled plastic waste is considered a significant source of danger
Source: Google Maps. Edited by Benjámin Hózer.

Similar waste accumulation activity significantly increases the risk of fire, as well as the speed of fire spread between bales in the event of a fire situation.

Recently, a fire broke out on the territory of a waste disposal and processing company, which took three days to completely extinguish. The fire affected a nearly 5,000 square metres territory. Units from several local fire departments were sent to the scene of the major fire. After requesting data from the local waterworks, we found out that the responders used a significant amount of nearly 1,500 cubic metres of firewater during the three days of response work. In the area, as mentioned in the previous example, a large amount of sorted, baled waste ready for transportation was accumulated. The facility is located in a natural wind tunnel, so the fire spread quickly. The waste was surrounded by concrete retaining walls, so the fire did not significantly spread to the protective forest lane just beyond the fence.[20] The intensity of the heat effect is well characterised by the fact that the protective wall made of concrete elements was significantly damaged.

[20] Decree 20/2006 (IV.5.) of the Ministry of Environment and Water on certain rules and conditions relating to the landfill of waste and the landfilling of waste; Attachment 1, point 3.2.

Hazards of biowaste and compost processing

In addition to the problem of baled waste, damage often occurs from the treatment of biowaste. Biowaste is typically composted in the landfill area. Biowaste is usually brought to the plant in bags. To produce compost, the raw material gets removed from the bags, it gets grinded and then the bio-stabilisation process begins. The resulting mixture is sorted into so-called "prisms", after which the mixture is composted for several weeks. During the process, biochemical decomposition starts, which is accompanied by the intense heat development of decomposition bacteria. Despite regular rotation, self-ignition can often occur.

Picture 3: Compost caught fire in the landfill area
Source: Picture made by Benjámin Hózer.

The fire hazard potential of stored compost can be easily minimised in case of regular technological procedures. The deposited compost can be stored almost indefinitely by covering it with a layer of earth. There is no legal obstacle to the latter.[21] In addition, biochemical decomposition stops at the end of composting, so further gas production and heat generation are significantly reduced.

[21] Cimer–Varga 2015: 209–218.

Conclusion

In the Hungarian waste management system, the general goal – in addition to increasing the amount of recycled waste – is to reduce the amount of landfilled waste. The main reason for this is the transition to a circular economic model and the fulfilment of the European Union's related obligations. Landfill sites remain of a great importance. Depending on the types of waste treated, landfill facilities can have a significant fire safety risk.

Although fires at landfill sites occur frequently worldwide, there are still no commonly used prevention and firefighting protocols at the international or domestic level. As a result, most operators and intervening organisations follow the procedures applied within their own jurisdiction. Most of the operating rules applied in landfills are considered sufficient; however, unexpected fires do occur in large numbers, concerning which the necessary fire prevention and mitigation measures must be introduced widely.

References

Antal, Imre – Nagy, Rudolf (2021): A települési hulladékkezelés tűzbiztonságának munkavédelmi szempontú vizsgálata. *Védelem Tudomány,* 6(4), 42–72.

Berek, Tamás – Földi, László – Padányi, József (2021): Hungary's Energy and Water Security Countermeasures as Answers to the Challenges of Global Climate Change. *AARMS,* 20(2), 87–96. Online: https://doi.org/10.32565/aarms.2021.2.7

Cimer, Zsolt – Varga, Ferenc (2015): Application of Special Risk Reduction Protective Measures in Combiterminals for Dangerous Goods. *AARMS,* 14(2), 209–218. Online: https://doi.org/10.32565/aarms.2015.2.7

Darvay, Sarolta – Nemcsók, János – Ferenczy, Áron (2016): Fenntartható fejlődés. *Polgári Szemle,* 12(4–6), 88–104.

Érces, Gergő – Vass, Gyula (2019): Veszélyes ipari üzemek fenntartható tűzbiztonságának BIM alapú fejlesztési lehetőségei. *Védelem Tudomány,* 4(1), 131–161.

Faragó, Tibor (2013): A globálisan növekvő hulladékmennyiség és a kezelésére irányuló nemzetközi törekvések. *Ipari Ökológia,* 2(1), 43–76.

Kirovné Rácz, Réka Magdolna (2021): Climate Adaptation in Terms of Water Security in the Danube Countries. *AARMS,* 20(3), 21–36. Online: https://doi.org/10.32565/aarms.2021.3.2

Solymosi, János (2016): Hulladékok keletkezése és kezelése egy elektronikai termelő cégnél. *Hadmérnök,* 11(1), 170–182.

Supka, Zsófia (2020): *Szelektív hulladékgazdálkodás Magyarországon.* Thesis. Budapest: Eötvös Loránd Tudományegyetem, Informatikai Kar. Online: http://lazarus.elte.hu/hun/digkonyv/szakdolg/2020-msc/supka_zsofia.pdf

Szakál, Béla – Cimer, Zsolt (2014): Major Disaster Recovery Plans. *The Science for Population Protection,* 6(1), 1–7.

UNEP (2015): *Global Waste Management Outlook.* Online: https://eprints.whiterose.ac.uk/99773/1/GWMO_report.pdf

Wilson, David C. – Velis, Costas (2015): Waste Management – Still a Global Challenge in the 21st Century: An Evidence-Based Call for Action. *Waste Management and Research,* 33(12), 1049–1051. Online: https://doi.org/10.1177/0734242X15616055

Legal sources

Directive (EU) 2018/849 of the European Parliament and of the Council Directive 2000/53/EC on end-of-life vehicles, Directive 2006/66/EC on batteries and accumulators and waste batteries and accumulators, and on waste electrical and electronic equipment on the amendment of Directive 2012/19/EU

Directive 2008/98/EC of the European Parliament and of the Council on waste and repealing certain Directives

Directive 1999/31/EC of the European Parliament and Council on landfills

Act CLXXXV of 2012 on Waste

Decree 20/2006 (IV.5.) of the Ministry of Environment and Water on certain rules and conditions relating to the landfill of waste and the landfilling of waste

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

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

18. évfolyam (2023) 3. szám 69–81.
DOI: 10.32567/hm.2023.3.6

Jánosi Andrea,[1] Fekete Árpád,[2] Szám Dorottya[3]

Markov-láncok alkalmazása az aszályos napok valószínűségének megállapítására Budapest térségében

Application of Markov Chains to Estimate the Probability of Drought Days in the Budapest Area

Absztrakt

A klímaváltozás egyik hatása hazánkban az aszályos időszakba eső napok számának növekedése. Ennek következtében egyre nagyobb szükség van a hatékony csapadékvíz-gazdálkodásra, valamint a hőhullámok elleni védekezésre. Budapest térségének csapadékadatait felhasználva becslést adunk arra, hogy a jövőben mekkora eséllyel fog egy nap aszályos időszakba esni. Egy viszonylag új vizsgálati módszert, a Markov-láncok elméletét használtuk fel a budapesti csapadékadatsorok elemzéséhez. Hipotézisvizsgálattal azt is bizonyítottuk, hogy az aszályos időszakok között eltelt idő exponenciális eloszlást követ.

Kulcsszavak: aszály, Markov-lánc, átmenet-valószínűség, határeloszlás, csapadékvíz-gazdálkodás

Abstract

One of the effects of climate change in Hungary is the increase in the number of days falling into the drought period. As a result, there is an increasing need for efficient rainwater management and protection against heat waves. Applying precipitation data for the Budapest area, we estimate the probability of a day falling into a drought period in the

[1] BSc-hallgató, Nemzeti Közszolgálati Egyetem Víztudományi Kar, e-mail: janosi.andrea@stud.uni-nke.hu
[2] Adjunktus, Nemzeti Közszolgálati Egyetem Víztudományi Kar, e-mail: fekete.arpad@uni-nke.hu
[3] Kutató, Nemzeti Közszolgálati Egyetem Víztudományi Kar, e-mail: szam.dorottya@uni-nke.hu

future. The theory of Markov chains is a relatively new method of analysis, and it was applied to analyse the Budapest precipitation data series. We also tested the hypothesis that the time between drought periods follows an exponential distribution.

Keywords: drought, Markov chain, transition probability, limit distribution, rainwater management

Bevezetés

A globális éghajlatváltozás következtében Magyarországon a hőmérséklet átlagos emelkedése 1901 és 2009 között 1,36 °C-ra tehető.[4] Míg a hőmérséklet-változásra pontos számszerű adatokkal tudunk szolgálni, a csapadék hosszú távú mennyiségi eloszlására jóslatot adni közel sem ilyen egyszerű vállalkozás. Az erre vonatkozó kutatások egyik része vitatja az évi csapadékösszegek jelentős változását,[5] más része kimutatja a csökkenő trendet. A csapadék területi eloszlásának szignifikáns változását is kimutatták Magyarországon.[6]

Az elmúlt éveket vizsgálva kijelenthető, hogy egyre gyakoribbá váltak a szélsőséges időjárási formák, mint a rövid időn belül lehulló nagy intenzitású csapadéktevékenység vagy a hosszabb csapadékmentes időszakok és ezzel együtt az aszályok.[7] Gyakrabban észlelhetünk hevesebb záporokat és zivatarokat, mint több napig tartó enyhébb csapadékhullást. Ezzel együtt a lehulló csapadék relatíve nagyobb része folyik le, és kisebb hányada szivárog be a talajba vagy tározódik. Emiatt az árvízveszély is növekedhet.[8] Ezzel párhuzamosan az éghajlati előrejelzések és modellek az aszályos időszakok gyakoribbá válására hívják fel a figyelmet. Jó példa erre a 2022-es történelmi aszály, amely tükröződött a rendkívül alacsony mezőgazdasági terméshozamokban.[9]

A kutatás a Markov-láncok elméletét használja fel, amely viszonylag újszerűnek számít a csapadékviszonyok statisztikai elemzésében. Haan és társai már 1976-ban modellezték az átmenetvalószínűségi mátrix használatával a különböző időszakok csapadékos és csapadékmentes napjainak egymás után következő folyamatát.[10] Egy viszonylag friss kutatásban Freidooni és társai a Markov-láncokat annak kiszámítására alkalmazták, hogy egy nap mekkora valószínűséggel esik hőhullámos időszakba. A módszer jogosságát részletesen bizonyították.[11] Ezt az ötletet használta Fekete és Keve annak vizsgálatára bajai mintaterületen, hogy egy nap mekkora valószínűséggel esik aszályos időszakba.[12]

Ez a tanulmány Budapest aszályos időszakait vizsgálja a növények vegetációs időszakában (április 1. és október 31. között) egy rövid, 10 éves idősoron (2011–2020) keresztül a gyors ellenőrizhetőség végett. Számításokkal előrejelzést próbálunk adni

[4] Bartholy et al. 2011: 146–169.
[5] Kocsis 2018: 187.
[6] Országos Meteorológiai Szolgálat 2022.
[7] Lakatos et al. 2014: 158–163; Országos Meteorológiai Szolgálat 2022.
[8] Padányi–Halász 2012: 120–121.
[9] KSH 2022.
[10] Haan–Allen–Street 1976: 443–449.
[11] Freidooni–Ataei–Shahriar 2015: 26–45.
[12] Fekete–Keve 2020: 60–70.

arról, hogy a jövőben mekkora eséllyel fog egy nap aszályos időszakba esni. Így következtetni tudunk a budapesti éghajlat jellemzőinek jövőbeli változásaira.

Az aszály fogalma, mérőszámai

Az aszály az egyik legnagyobb természeti katasztrófaként is számon tartott állapot, amely világszerte a legtöbb embert érinti. Az aszály pontos megfogalmazása körül nagy a bizonytalanság, ami annak tudható be, hogy az aszály fogalmát több tudományágban is használják, figyelembe véve a csapadék, a csapadék és a párolgás vagy a talajnedvesség adatait.[13] Az agrometeorológiában a Palmer-féle definíció terjedt el, amely szerint *az aszály tartós és jelentős vízhiány,* amely negatív hatást gyakorol a mezőgazdaságra, a vízgazdálkodásra és a bioszférára.[14]

Ahogy az aszály definíciója, úgy a jellemzéséül szolgáló mérőszámok és azok kiszámítása sem egységes. A legtöbb ilyen jellemzés az előző évek időszakaiból származtatott átlagokat és az attól való eltérést írja le, míg más számítások figyelembe veszik a hőmérsékletet, illetve a kipárolgás mértékét, vagy a növények vízfelvételének mennyiségét is.

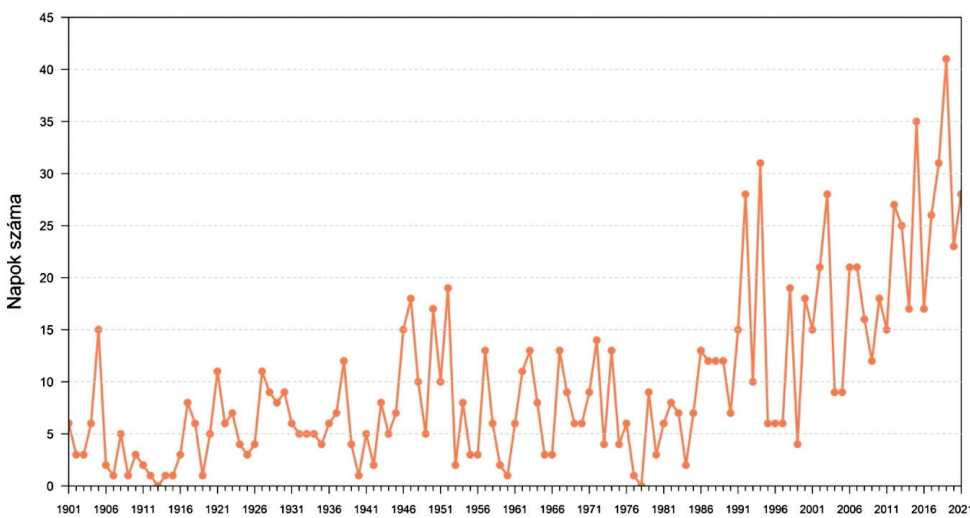
Az aszály mérőszámai két csoportra oszthatók: indikátorokra és indexekre. Az indikátorok mérik a hidrológiai és a meteorológiai paramétereket, mint például a csapadékok mennyiségét, intenzitását, időbeni eloszlását, a hőmérsékletet, a talaj nedvességszázalékát, a levegőmozgást. Az indexek e paramétereket felhasználva matematikai egyenleteket alkalmazva egyetlen számmal jellemzik az aszály mértékét (területi és időbeli kiterjedését). A jelenség komplexitását fokozza, hogy nincs egyetlen átfogó aszályindex, hiszen a Föld különböző pontjain más és más hatást gyakorol a csapadékhiány, illetve a különböző tudományágaknak is más paraméterek a meghatározók. A Magyarországon kifejlesztett aszályindexek közül első helyen kell említeni a Pálfai Imre által 1988-ban megalkotott PAI indexet.[15] Ezt az indexet elsősorban a mezőgazdaságra vonatkozóan, de kimondottan a magyarországi viszonyokhoz alkották meg. A havi csapadékösszeg és a havi középhőmérséklet felhasználásával, egyetlen számértékkel adja meg az indexértéket. Hat aszályossági zónát állapít meg az aszálymentestől (1) a nagyon erősen aszályosig (6). Budapest térsége e skála alapján az ötödik kategóriába, az erősen aszályos zónába tartozik. Megemlítendő a 2015–2016 folyamán kidolgozott Magyar Szárazság Index (Hungarian Drought Index, HDI) is, amely napi gyakorisággal számítható és alkalmas a napi vízhiány/aszály jellemzésére. Legfontosabb újdonsága, hogy aktuális, talajtípusonként differenciált talajnedvességet vesz figyelembe. Számos előnye közt szerepel, hogy a kiszámítása algoritmizálható, szubjektív emberi döntésektől mentes.[16]

A legtöbb tanulmány az aszály mezőgazdaságra, biológiai sokféleségre és erdőtűzveszélyekre gyakorolt hatását emeli ki, kevésbé foglalkozik a városok helyzetével. Az aszályokat kísérő hőhullámok orvosmeteorológiai, humánegészségügyi hatásai

[13] Urbán 1993: 113–135; Pálfai 2004: 255–264.
[14] Palmer 1965: 2.
[15] Pálfai 2004: 258–263.
[16] Fiala 2018: 1–5.

is számottevők. A hőhullámok a nagyvárosokban fokozott gondot jelenthetnek. Budapest az 1 674 014 lakosával (2023. január 1-jei KSH-adat) hazánk egyetlen világvárosa. A második legnépesebb városunk Debrecen, lakossága már jóval kisebb, csupán 191 428 fő (2023. január 1-jei KSH-adat). Ha ehhez hozzávesszük, hogy hazánk népességének 71%-a városban él, az urbanizáció trendszerű folyamat Magyarországon, a városokban pedig a lélekszám növekedésével fokozódik az aszályos és meleg időszakokban a hőszigethatás, akkor indokolt a főváros vizsgálata, a hőszigethatás megértése és az ellene való védekezés lehetőségeinek feltárása.

1901 és 2021 között lineáris trenddel becsülve több mint 7 nappal nőtt a hőhullámos napok száma Magyarországon. (Hőhullámos napnak nevezzük a legalább 25 °C-os napi középhőmérsékletű napokat.) A legtöbb hőhullámos nap 2015-ben fordult elő, ekkor átlagosan 28 ilyen napot detektáltunk, kevéssel maradt el ettől 2012 és 2021, amely években sorra 24 és 21 hőhullámos nap fordult elő országos átlagban.[17] A napi középhőmérséklet mellett a minimumhőmérsékletek vizsgálata is elterjedt a legforróbb időszakok elemzésében, mivel a hőhullámos időszakok rendszerint meleg éjszakákkal járnak együtt. Azokat az éjszakákat, amikor a minimumhőmérséklet nem csökken 20 °C alá, trópusi éjszakának nevezzük. Az 1901 és 1921 közötti OMSZ-adatokból (1. ábra) megállapítható, hogy Budapest belterületén az utóbbi évtizedekben meredeken nőtt a trópusi éjszakák száma, a legtöbb ilyen éjszaka (41) ezen időszakon belül 2019-ben fordult elő.

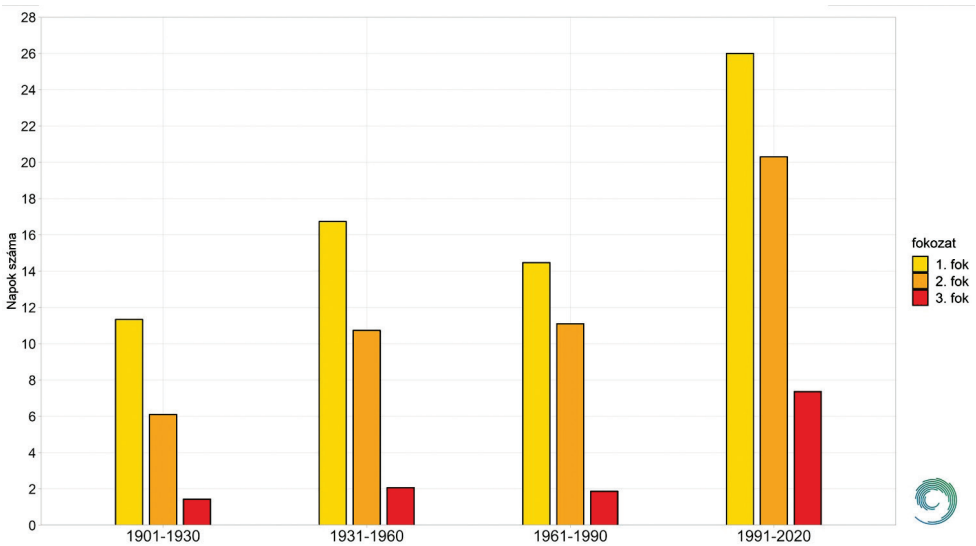


1. ábra: A trópusi éjszakák számának éves összegei Budapest-belterület állomáson az 1901–2021 időszakban

Forrás: Bokros–Lakatos 2022.

[17] Bokros–Lakatos 2022.

Egy további OMSZ-statisztika[18] is alátámasztja Budapest belterületének hőhullámokkal való veszélyeztetettségét. A Nemzeti Népegészségügyi Központ háromfokozatú hőségriasztást alkalmaz. Megvizsgálhatjuk az 1901 és 2020 közötti években a különböző hőségriasztási fokozatok bekövetkezési gyakoriságát (2. ábra). Ha ebben az időintervallumban összehasonlítjuk a négy egymást követő harmincéves időszakot, akkor azt tapasztaljuk, hogy mind az első (legalább 25 °C-os napi középhőmérséklet), mind a második és harmadik fokú hőségriasztással (legalább 3 napig 25 °C, illetve 27 °C vagy annál magasabb a napi középhőmérséklettel érintett napok száma) növekvő trendet követ.



2. ábra: A hőségriadó különböző fokozatainak megfelelő napok átlagos száma évente Budapest-belterület állomáson

Forrás: Bokros–Lakatos 2022.

Az aszályok és a hőhullámok a civil védelmi, népegészségügyi feladatok mellett a katonai erőkre is hatással vannak. A hőhullámok és az aszályok, valamint a szélsőségessé váló csapadékviszonyok jelentős és tartós nem harci jellegű fenyegetést jelentenek a katonák egészségére, kiképzésére és műveleti tevékenységük hatékony elvégzésére.[19] Ez fokozottan igaz bizonyos tevékenységekre, mint amilyen például a katonai vegyvédelem. Például a vegyvédelmi felszerelés viselése kétszeresére növeli a szükséges pihenések időtartamát, mivel ebben a felszerelésben nagymértékben csökken a szervezet hőleadási képessége.[20] Hőség hatására a szervezet hőleadási képessége

[18] Bokros–Lakatos 2022.
[19] Moran et al. 2023: 60.
[20] Kohut 2008.

romolhat, a hőleadás zavart szenvedhet, aminek következménye a testhőmérséklet kóros tartományba emelkedése.[21]

Az aszályok és a hőhullámok a katonák személyes teljesítőképességen túl a katonai kihívások természetében is változást hozhatnak.[22] Hazánkban a menekültek ellenőrzése, az illegális migráció elleni védelem (kezdve a hírszerzéstől és az államhatár védelmétől a menekült tranzitforgalom szervezéséig) az a terület, amelyben kiemelt szerepe van a meleg (nyári) periódusoknak.[23] A menekült tranzitforgalom szempontjából fontos szerepet kap fővárosunk, ezen belül is a három nagy vasúti személypályaudvar és a Liszt Ferenc Nemzetközi Repülőtér.

A Markov-láncok rövid elméleti összefoglalója

A matematikában a Markov-lánc olyan diszkrét sztochasztikus folyamatot jelent, amely Markov-tulajdonságú. Ez azt a tulajdonságot jellemzi, hogy a jövőbeni állapotok lehetséges alakulásainak valószínűsége csupán a jelenbeli állapottól függ. Másképpen fogalmazva, adott jelen mellett a jövő feltételesen független a múlttól. Tehát a múlt nem ad előrejelzést a jövőre nézve, csupán a jelenlegi helyzetből kiindulva tudhatjuk, hogy milyen kimenetelek a lehetségesek.

Jelöljék valamely rendszer állapotait a $t_0, t_1, t_2, \ldots, t_n, \ldots$ időpontokban az $X_0, X_1, X_2, \ldots, X_n, \ldots$ valószínűségi változók felvett értékei. Legyen a t_0 időpontban $X_0 = x_0$, és a t_n időpontban i, a t_{n+1} időpontban j állapotban a rendszer, azaz $X_n = i$ és $X_{n+1} = j$. Egylépéses átmenetvalószínűségnek nevezzük azt a valószínűséget, hogy X_{n+1} a j állapotban van, feltéve, hogy X_n az i állapotban van. Képlettel: $P_{ij}^{n,n+1} \coloneqq P(X_{n+1} = j \mid X_n = i)$.

Ha az egylépéses átmenetvalószínűségek függetlenek n-től, azaz az időtől, akkor azt mondjuk, hogy a Markov-folyamatnak *stacionáriusak az átmenetvalószínűségei*.[24] A Markov-láncok döntő többsége rendelkezik ezzel a tulajdonsággal, ezeket *homogén Markov-láncoknak* nevezzük. Ebben az esetben $P_{ij}^{n,n+1} \coloneqq P_{ij}$. A P_{ij} számokat mátrixformába rendezve kapjuk, hogy

$$\mathbf{P} = \begin{bmatrix} P_{00} & P_{01} \ldots & P_{0n} \\ P_{10} & P_{11} \ldots & P_{1n} \\ \vdots & & \vdots \\ P_{n0} & P_{n1} \ldots & P_{nn} \end{bmatrix} \tag{1}$$

A $\mathbf{P} = (P_{ij})$ mátrixot a folyamat *átmenetvalószínűség-mátrixának* nevezzük. A P minden egyes P_{ij} eleme annak a valószínűségét jelenti, hogy az állapotok értéke az i-ből j-be megy át egy lépésben. Egy lépés egy időegységnek tekinthető. A P_{ij} mennyiségek nemnegatív számok, sorösszegük egységnyi, mert valamely esemény soronként biztosan bekövetkezik. A főátlóban szereplő értékek a helyben maradás valószínűségét adják meg, és a mátrix egy sora eloszlást fejez ki. Az átmenetvalószínűségeken kívül az úgynevezett φ_0 kezdeti eloszlás határozza meg a Markov-láncot. Ez egy n

[21] Radics 2016: 39–44.
[22] Földi–Padányi 2022: 37–48.
[23] Tárik–Párducz 2023.
[24] Karlin–Taylor 1985: 54–56.

hosszúságú vektor, amely az egyes állapotokban való tartózkodás valószínűségeit adja meg. Adott φ_0 esetén *k* lépés múlva az eloszlás: $\varphi_k = \varphi_0 \mathbf{P}^k$. Jelölje $P_{ij}^{(n)}$ azt az átmenetvalószínűséget, hogy a rendszer *n lépésben* megy át az i állapotból a j állapotba. A Markov-láncot *ergodikusnak* nevezzük, ha léteznek a

$$\lim_{n\to\infty} P_{ij}^{(n)} = P_j \tag{2}$$

határértékek (*határvalószínűségek*), amelyek i-től függetlenek, és

$$\sum_{j=0}^{n} P_j = 1 \tag{3}$$

tehát a j-edik oszlop elemei egyenlők, és a mátrix sorösszege egységnyi.[25] A határvalószínűségekből alkotott *határmátrix* ($\mathbf{P}^*$) az ergodikus Markov-láncok határeloszlására vonatkozó *Markov-tétel* alapján:

$$\mathbf{P}^* = \lim_{n\to\infty} \mathbf{P}^n = \begin{bmatrix} P_0 & P_1 \dots & P_n \\ P_0 & P_1 \dots & P_n \\ \vdots & & \vdots \\ P_0 & P_1 \dots & P_n \end{bmatrix} \tag{4}$$

A határmátrix minden sora egyforma. A határvalószínűségek által alkotott valószínűségeloszlást *stacionárius* vagy *határ-* vagy *invariáns* eloszlásnak is nevezzük. (A $\mathbf{P}^*$ mátrix további hatványozásra nem változik.) A $P_0, P_1, \dots, P_n$ valószínűségek azt fejezik ki, hogy mekkora valószínűséggel találjuk a rendszert hosszú állapotváltozások sorozata után az egyes $0, 1, \dots, n$ állapotokban. Az invariáns eloszlás számításánál a lényeg tehát az, hogy az egylépéses átmenetvalószínűségi mátrixot addig hatványozzuk, amíg az oszlopainak elemei állandósulnak.[26]

Aszályos időszakok Budapest térségében

Az aszályos időszakok kutatásakor a hazai mezőgazdaság számára kiemelkedően fontos vegetációs időszakot vizsgáltuk. Mivel a tényleges vegetációs időszak növényfajonként változik,[27] és sok más tényező, köztük az éghajlatváltozás is befolyásolja,[28] így egy önkényesen kijelölt hosszabb időszakot (április 1-jétől október 31-ig, összesen 214 nap) elemeztünk.

Tíz év aszályos időszakaiból (2011–2020) számítottuk ki hosszú távra a Markov-modellel az aszályos időszakba eső napok valószínűségeit. A bevezetésben már említettük, hogy a módszer jogosságát Freidooni és társai megmutatták, de más kutatók is alátámasztották ugyanezt.[29]

[25] Kontur et al. 1993: 507–508.
[26] Markov 1906: 135–156; Seneta 1996: 255–263.
[27] Mesterházy et al. 2015: 40–41.
[28] Lakatos 2019: 14–16.
[29] Alizadeh 2013.

A modell alkalmazásakor minden egyes évhez kiszámítottuk az aszályos időszakba eső napok határvalószínűségeit. Fontos azonban tisztázni, hogy az aszály melyik megfogalmazása lenne a leghasznosabb számunkra. Egy adott vizsgálat során maga a kutató határozhatja meg a jelentős vízhiányt jelentő küszöbértéket, s azt is, hogy ezt milyen hosszú időszakra vonatkozóan elemzi.

Az állami kárenyhítési szabályok szerint aszálynak minősül az a

„kedvezőtlen időjárási jelenség, amelynek során a kockázatviselés helyén az adott növény vegetációs időszakában harminc egymást követő napon belül a lehullott csapadék összes mennyisége a 10 millimétert nem éri el, vagy a lehullott csapadék összes mennyisége a 25 millimétert nem éri el, de ennél a feltételnél a napi maximum hőmérsékletnek a harminc napból legalább tizenöt napon meg kell haladnia a 31°C-ot".[30]

Kutatásunkban ez utóbbi definíciót vettük alapul annyi módosítással, hogy a harminc egymást követő napot huszonötre csökkentettük. Az alábbi, 1. táblázat tartalmazza az aszályos időszakokat 2011-től 2020-ig a budapesti mérések alapján.

1. táblázat: A vegetációs periódusra vonatkozó aszályos időszakok Budapest térségében (2011–2020)

Év	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
Időszakok száma	3	3	3	3	3	3	3	4	4	2
Időszakba eső napok száma	147	113	112	92	94	78	90	129	147	90
Időszakok kezdete és vége	04.01. 05.07.	04.08. 05.11.	04.03. 05.01.	04.01. 04.25.	04.01. 05.12.	04.01. 04.26.	05.24. 06.27.	04.01. 04.25.	04.10. 05.03.	04. 01. 05. 23
	06.15. 07.18.	06.26. 07.23.	06.29. 08.25.	05.25. 06.28.	06.12. 07.07.	06.16. 07.12.	07.12. 08.05.	06.30. 07.20.	06.23. 07.26.	09.01. 09.25.
	08.05. 10.19.	07.29. 09.18.	09.17. 10.11.	09.15. 10.16.	07.10. 08.04.	08.23. 09.16.	09.22. 10.21.	07.24. 08.22.	07.29. 09.06.	
								09.05. 10.27.	09.10. 10.28.	

Forrás: a szerzők szerkesztése

[30] 2011. évi CLXVIII. törvény 2. § (1) bekezdés.

A határeloszlások számítása

Először kiszámítjuk a 2011-es évet alapul véve az aszályos időszakba eső napok valószínűségeit hosszú távra a Markov-láncok segítségével. A 0 állapot legyen a nem aszályos időszakba tartozó nap, míg az 1 állapot az aszályos időszak napja. Az átmenetgyakorisági mátrix ekkor:

$$\begin{pmatrix} g_{00} & g_{01} \\ g_{10} & g_{11} \end{pmatrix} = \begin{pmatrix} 64 & 2 \\ 3 & 144 \end{pmatrix} \tag{5}$$

Az értelmezéshez vegyük például a g_{01} elemet. Ez az érték 2, mivel kétszer fordult elő, hogy nem aszályos periódusú napból tértünk át aszályos időszakba eső napra. A g_{11} elemet nézve megállapíthatjuk, hogy összesen 147 aszályos időszakba eső napunk volt, így 144 átmenet volt az ebbe az állapotba tartozó napok között (az időszakok első napjaitól indulnak az átmenetek, tehát mivel 3 aszályos időszak volt, így 147 – 3 = 144 átmenet van). A g_{00} elemet vizsgálva láthatjuk, hogy 214 – 147 = 67 nem aszályos időszakba tartozó nap volt 3 periódusban (az időszakok első napjaitól indulnak az átmenetek, tehát mivel 3 nem aszályos időszak volt, így 67 – 3 = 64 átmenet van). Az átmenetgyakorisági mátrixból megkapjuk az átmenetvalószínűségi mátrixot:

$$\mathrm{P} = \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} = \begin{pmatrix} \frac{g_{00}}{g_{00}+g_{01}} & \frac{g_{01}}{g_{00}+g_{01}} \\ \frac{g_{10}}{g_{10}+g_{11}} & \frac{g_{11}}{g_{10}+g_{11}} \end{pmatrix} = \begin{pmatrix} \frac{64}{66} & \frac{2}{66} \\ \frac{3}{147} & \frac{144}{147} \end{pmatrix} \tag{6}$$

A Markov-láncokkal kapcsolatban célunk mindig a hosszú távú viselkedésük vizsgálata. Ez tulajdonképpen a $\boldsymbol{P}^n$ vizsgálatát jelenti nagy n-ek esetén. Ahogy a Markov-láncokról szóló fejezetben írtuk, az egylépéses átmenetvalószínűségi mátrixot addig hatványozzuk, amíg az oszlopainak elemei állandósulnak. Az átmenetmátrixok segítségével becsléseket adhatunk arra vonatkozóan, hogy a jövőben egy nap aszályos vagy csapadékos időszakba fog-e esni. A számításokat Excelben végeztük el, a 256. hatványnál az oszlopokra teljes azonosságot kaptunk. A számításokból adódott, hogy $\boldsymbol{P}_0$ = 0,392 és $\boldsymbol{P}_1$ = 0,608. Tehát hosszú távon 60,8% az esélye egy aszályos időszakba tartozó napnak a vegetációs időszakban. (Érdemes összevetni az eredményeket a klasszikus valószínűségi számítással kapott eredményekkel. A „kis" különbség is az ismertetett módszer jogosultságát mutatja. Például 2012-ben az aszályos nap határvalószínűsége 0,536 lett. Ebben az évben a vizsgált 214 napból 113 nap esett aszályos időszakba. Tehát a valószínűség 113/214=0,528, ami „igen közel" van a 0,536-hoz.)

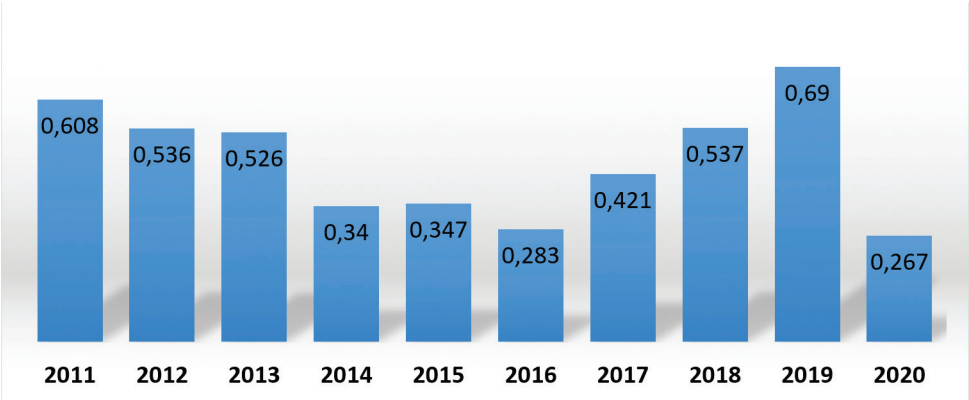
Hasonló módon számítható ki az invariáns eloszlása a többi évnél is, ezeket nem részletezzük, de az átmenetvalószínűségi mátrixokat és a határeloszlásokat a 2. táblázatba foglaljuk.

2. táblázat: Az átmenet-valószínűségi mátrixok és határeloszlások (2011–2020)

Év	**P**	**(P0, P1)**
2011	$\begin{pmatrix} 0{,}969 & 0{,}031 \\ 0{,}02 & 0{,}98 \end{pmatrix}$	(0,392 ; 0,608)
2012	$\begin{pmatrix} 0{,}97 & 0{,}03 \\ 0{,}026 & 0{,}974 \end{pmatrix}$	(0,464 ; 0,536)
2013	$\begin{pmatrix} 0{,}97 & 0{,}03 \\ 0{,}027 & 0{,}973 \end{pmatrix}$	(0,474 ; 0,526)
2014	$\begin{pmatrix} 0{,}983 & 0{,}017 \\ 0{,}033 & 0{,}967 \end{pmatrix}$	(0,66 ; 0,34)
2015	$\begin{pmatrix} 0{,}983 & 0{,}017 \\ 0{,}032 & 0{,}968 \end{pmatrix}$	(0,653 ; 0,347)
2016	$\begin{pmatrix} 0{,}985 & 0{,}015 \\ 0{,}038 & 0{,}962 \end{pmatrix}$	(0,717 ; 0,283)
2017	$\begin{pmatrix} 0{,}976 & 0{,}024 \\ 0{,}033 & 0{,}967 \end{pmatrix}$	(0,579 ; 0,421)
2018	$\begin{pmatrix} 0{,}964 & 0{,}036 \\ 0{,}031 & 0{,}969 \end{pmatrix}$	(0,463 ; 0,537)
2019	$\begin{pmatrix} 0{,}94 & 0{,}06 \\ 0{,}027 & 0{,}973 \end{pmatrix}$	(0,31 ; 0,69)
2020	$\begin{pmatrix} 0{,}992 & 0{,}008 \\ 0{,}022 & 0{,}978 \end{pmatrix}$	(0,733 ; 0,267)

Forrás: a szerzők szerkesztése

A 3. ábrán szereplő határvalószínűségek átlagát véve 0,4555 adódik, tehát mondhatjuk, hogy a jövőben átlagosan ekkora valószínűséggel lesz a vegetációs időszak egy napja az aszályos periódusban, ami már igen figyelemre méltónak számít.



3. ábra: Az aszályos időszakba eső napok határvalószínűségei Budapest térségében (2011–2020)
Forrás: a szerzők szerkesztése

A 10 éves idősor alapján megvizsgáltuk az aszályos időszakok között eltelt időt is. A vegetációs időszakon belül ennek átlaga 30,6 nap, szórása 24,7 nap. X^2 próbával igazoltuk 95%-os valószínűségi szinten, hogy az eloszlás közelítőleg exponenciális. Ehhez a 10 éves adatsor alapján az aszályos időszakok között eltelt napok számát kategorizáltuk. Ezt mutatja a 3. táblázat.

3. táblázat: Az aszályos időszakok között eltelt napok számának kategorizálása a X^2 próbához

Aszályos időszakok között eltelt napok száma	**0–15**	**16–30**	**31–45**	**46–60**	**61–**
Észlelt	10	3	4	6	2
Exponenciális eloszlás szerint feltételezett	10	6	3	3	3

Forrás: a szerzők szerkesztése

A X^2 számított értéke a próba alapján (a szabadsági fokok száma 4):

$$\sum_{i=1}^{5} \frac{(észlelt_i - feltételezett_i)^2}{feltételezett_i} = 5{,}17 \qquad (7)$$

A X^2 eloszlás táblázatában a megfelelő érték 9,49, ami lényegesen magasabb, mint a számított érték, ezért az exponenciális eloszlás bizonyított. Az exponenciális eloszlás alapján becsülhetjük tehát annak valószínűségét is, hogy két aszályos időszak között mennyi idő telik el.

Összefoglalás

Kutatásunkban Budapest térségének 2011–2020 közötti csapadékadataiból kiindulva rámutattunk arra, hogy számottevő a valószínűsége (45,55%) annak, hogy a növények vegetációs időszakának egy napja az aszályos periódusba esik.

A kutatásban használt matematikai modell a Markov-láncok elméletét használja fel, amely viszonylag újszerűnek számít a csapadékviszonyok statisztikai elemzésében. Meghatároztuk az egyes évekhez tartozó átmeneti valószínűségi mátrixokat, és ezek hatványozásával megkaptuk a határvalószínűségeket. Adatsorunkból hipotézisvizsgálattal (X^2 próba) bizonyítottuk, hogy az aszályos időszakok között eltelt idő exponenciális eloszlást követ. Vizsgálati eredményeink további kutatások alapjait képezhetik: segíthetnek a hatékonyabb településrendezési és -fejlesztési feladatok kijelölésénél, de felhasználhatók a katonai haderőfejlesztésben és a humánegészségügyi igazgatásban is.

Irodalomjegyzék

Alizadeh, A. (2013): *The Principles of Applied Hydrology.* 36th Edition. Mashhad: Imam Reza University, Mashhad.

Bartholy Judit et al. (2011): Hazai éghajlati tendenciák. In Bartholy Judit – Bozó László – Haszpra László (szerk.): *Klímaváltozás – 2011, Klímaszcenáriók a Kárpát-medence térségére.* Budapest: Magyar Tudományos Akadémia és az Eötvös Loránd Tudományegyetem Meteorológiai Tanszéke, 146–169.

Bokros Kinga – Lakatos Mónika (2022): *Hőhullámok Magyarországon.* Országos Meteorológiai Szolgálat. Online: www.met.hu/ismeret-tar/erdekessegek_tanulmanyok/index.php?id=3196&hir=Hohullamok_Magyarorszagon

Fekete Árpád – Keve Gábor (2020): A csapadékösszegek és az aszályos időszakok vizsgálata Markov-láncokkal. *Hidrológiai Közlöny,* 100(4), 60–70.

Fiala Károly et al. (2018): *Development of an Operational Drought and Water Scarcity Monitoring System in Hungary*. Global Water Partnership.

Földi, László – Padányi, József (2022): Climate Change as a Challenge to the Armed Forces. *Sodobni Vojaski Izzivi/Contemporary Military Challenges,* 24(4), 37–48. Online: https://doi.org/10.33179/bsv.99.svi.11.cmc.24.4.2

Freidooni, Farnood – Ataei, Hooshmand – Shahriar, Fatemeh (2015): Estimating the Occurence Probability of Heat Wave Periods Using the Markov Chain Model. *Journal of Sustainable Development,* 8(2), 26–45. Online: https://doi.org/10.5539/jsd.v8n2p26

Haan, C.T. – Allen, D. M. – Street, J. O. (1976): A Markov Chain Model for Daily Rainfall. *Water Resources Research,* 12(3), 443–449. Online: https://doi.org/10.1029/WR012i003p00443

Karlin, Samuel – Taylor, Howard M. (1985): *Sztochasztikus folyamatok*. Budapest: Gondolat.

Kocsis Károly szerk. (2018): *Magyarország Nemzeti Atlasza – Természeti környezet.* Budapest: MTA CSFK Földrajztudományi Intézet.

Kohut László (2008): *Extrém fizikai terhelésnek kitett katonai állomány keringési és élettani vizsgálata.* PhD-disszertáció. Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Katonai Műszaki Doktori Iskola.
Kontur István et al. (1993): *Hidrológiai számítások.* Budapest: Akadémiai.
KSH (2022): *Főbb növénykultúrák terméseredményei.* Online: www.ksh.hu/s/kiadvanyok/fobb-novenykulturak-termeseredmenyei-2022/index.html
Lakatos Mónika et al. (2014): A klímaváltozás magyarországi jelei. *Légkör,* 59(4), 158–163.
Lakatos Mónika (2019): Korábban kezdődő vegetációs időszak – Előny vagy hátrány? *Agrofórum,* 30(2), 14–16.
Markov, A. A. (1906): Rasprostranenie zakona bol'shih chisel na velichiny, zavisyaschie drug ot druga. *Izvestiya Fiziko-matematicheskogo obschestva pri Kazanskom universitete, 2-ya seriya,* 15(94), 135–156.
Mesterházy Ildikó et al. (2015): A vegetációs időszak számításának módszerei. *Agrofórum Extra,* 61. 40–41.
Moran, Daniel S. et al. (2023): Beating the Heat: Military Training and Operations in the Era of Global Warming. *Journal of Applied Physiology,* 135(1), 60–67. Online: https://doi.org/10.1152/japplphysiol.00229.2023
Országos Meteorológiai Szolgálat (2022). Online: www.met.hu/eghajlat/eghajlatvaltozas/megfigyelt_hazai_valtozasok/homerseklet_es_csapadektrendek/csapadek_szelsosegek
Padányi József – Halász László (2012): *A klímaváltozás hatásai.* Budapest: Nemzeti Közszolgálati Egyetem.
Palmer, Wayne C. (1965): *Meteorological Drought*. Research Paper No. 45. Washington: Office of Climatology.
Pálfai Imre (2004): *Belvizek és aszályok Magyarországon. Hidrológiai tanulmányok.* [h. n.]: Közlekedési Dokumentációs Kft.
Rácz Tibor – Waltner István – Gelybó Györgyi (2022): Városi csapadékvízgyűjtő tározó méretének vizsgálata az 1901–2020 időszak napi meteorológiai adatai alapján. *Journal of Central European Green Innovation,* 10(2), 38–58. Online: https://doi.org/10.33038/jcegi.3553
Radics Judit (2016): A klímaváltozás – elsősorban a hőség – lehetséges hatásai az emberi szervezet működésére, különös tekintettel a pszichiátriai gyógyszereket szedő páciensekre. *Neuropsychopharmacologia Hungarica,* 18(1), 39–44.
Seneta, Eugene (1996): Markov and the Birth of Chain Dependence Theory. *International Statistical Review,* 3(64), 255–263. Online: https://doi.org/10.2307/1403785
Tárik Meszár – Párducz Árpád (2023): *Migrációs helyzet a csúcstalálkozók után – A déli határszakasz aktualitásai.* Migrációkutató Intézet Gyorselemzések 2023/6.
Urbán L. (1993): Az aszály fogalma és jelentősége. In *Beszámolók 1989.* Budapest: OMSZ, 113–135.

Jogi forrás

2011. évi CLXVIII. törvény a mezőgazdasági termelést érintő időjárási és más természeti kockázatok kezeléséről

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

18. évfolyam (2023) 3. szám 83–102.
DOI: 10.32567/hm.2023.3.7

Mihály István[1]

Túlnyomásos füstmentes lépcsőházak tervezése

Design of Pressurized Staircases

Absztrakt

A túlnyomásos füstmentes lépcsőházak hatékony működésének egyik legfontosabb feltétele, hogy megfelelően legyen meghatározva a légellátó rendszer kapacitása. Az ehhez szükséges bevezetendő levegőmennyiség számításához hazánkban a hő és füst elleni védelemről szóló Tűzvédelmi Műszaki Irányelv javasol műszaki megoldást. Az Országos Tűzvédelmi Szabályzatban meghatározott biztonsági szint elérhető a tűzvédelmet érintő nemzeti szabvány betartásával is, amely az MSZ EN 12101-13:2022 szabvány, illetve az abban szereplő számítási módszerek. Jelen publikációban egy meglévő túlnyomásos füstmentes lépcsőházba bevezetendő levegőmennyiség meghatározását mutatom be, figyelembe véve annak adottságait. A hazai, valamint a harmonizált szabvány számítási módszereinek alkalmazásával kapott értékeket összevetem a meglévő lépcsőház légtechnikai mérésének eredményeivel.

Kulcsszavak: füstmentes lépcsőházak, differenciálnyomás-mérés, PDS, légtechnikai rendszerek

Abstract

One of the most important conditions for the efficient operation of pressurized stairwells is to properly determine the capacity of the air supply system. In order to determine the required amount of air to be introduced for this purpose, the Fire Protection Technical Guideline on Protection against Heat and Smoke spread recommends a technical solution. The safety level defined in the National Fire Protection Regulation can also be achieved by complying

[1] Tűzvédelmi tervező, igazságügyi szakértő, ügyvezető, BRANDPLAN Kft.; doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: m.istvan@brandplan.hu

with the national fire protection standard, which is the MSZ EN 12101-13:2022 standard, and the calculation methods included in it. In this publication, the determination of the amount of air to be introduced into an existing pressurized stairwell is presented, taking into account its characteristics. The values obtained by applying the calculation methods of the domestic as well as the harmonized standard are compared with the results of the ventilation measurement of the staircase.

Keywords: pressurized staircases, differential pressure measurements, PDS, ventilation systems

Bevezetés

A füst és a mérgező égésgázok füstmentesített térbe való bejutásának megakadályozása két alapelv mentén valósul meg. Egyrészt a bevezetett levegő által létrehozott túlnyomás megakadályozza a füstmentesítendő térbe irányuló áramlásokat úgy, hogy az a lépcsőházba való bejutást nem gátolja. Ez főként a kis keresztmetszetű hézagokon, réseken értelmezhető.[2] Másrészt a levegő áramlása bizonyos mértékben képes irányítani a füst áramlását, ha az átlagos légsebesség megfelelő nagyságú.[3]

Egyes vizsgálatok azt mutatták, hogy a füst bejutásának megakadályozásához szükséges átlagos légsebesség 0,7 m/s.[4] A bevezetendő levegőmennyiség meghatározásának szempontjából fontos a számításba vett nyitott nyílászárók mennyisége és azok mérete.[5]

A réseken keresztüli füstbejutás megakadályozása nemzetközi előírásokban a lépcsőház egyéb jellemzőitől is függ; 2,7 m átlagos belmagasság mellett sprinklerezetlen épületben 20–30 Pa közötti érték jellemző.[6] A füstmentesítéssel kapcsolatos követelményeket újonnan tervezendő túlnyomásos füstmentes lépcsőházak esetén az Országos Tűzvédelmi Szabályzat (OTSZ) határozza meg.[7] Ezen előírások kielégítésére alkalmazható megoldási javaslatokat tartalmazó műszaki irányelv a hő és füst elleni védelemről szóló Tűzvédelmi Műszaki Irányelv (TvMI).[8]

Külföldi megfigyelések azt mutatják, hogy a tervezők egy része sok esetben saját tapasztalatai alapján végzi a füstmentesítő rendszerek méretezését, ami a követelmények keretrendszerének betartása mellett bizonyos (kisebb léptékű) épületek esetén megfelelő lehet.[9] A tűzvédelmi hatóság a tűzvédelmi műszaki irányelvektől vagy a nemzeti szabványtól részben vagy teljesen eltérő megoldást kérelemre jóváhagyhatja, ha a legalább azonos biztonsági szintet a kérelmező igazolja.[10]

A levegő épületen belüli áramlását irányító alapvető erők a hőmérséklet-különbségből adódó áramlás, az égési gázok térfogatának növekedése, az égési gázok

[2] Hurley et al. 2016: 1785; Lougheed–Ko 2016.
[3] Klote–Milke 1992: 37.
[4] Lee–Lau 2023: 132–153.
[5] International Code Council and Society of Fire Protection Engineers 2022: 210.
[6] NFPA 92 2021: 92-8; International Code Council 2021: 909; MSZ EN 12101-13 2022: 10; AS 1668.1 2015: 8.3.
[7] 54/2014. (XII. 5.) BM rendelet.
[8] Bérczi–Badonszki 2021: 66–96.
[9] Klote el al. 2012: 227.
[10] 489/2017. (XII. 29.) Korm. rendelet.

és a környezet hőmérséklet-különbségéből adódó felhajtóerő, szél, valamint gépi szellőzőberendezések.[11]

A lépcsőházi túlnyomásos szellőztetőrendszerek csoportosíthatók aszerint is, hogy a levegő bevezetése egy vagy több ponton történik, azonban a lépcsőház füstmentesítését jellemzően egyetlen ventilátor biztosítja.[12]

A túlnyomásos füstmentes lépcsőházak méretezésének alapjait csaknem 24 éven keresztül az ME-04–132–84 építésügyi ágazati műszaki előírás tartalmazta, amelyet a későbbiekben lényegében elhanyagolható módosításokkal a 9/2008. (II. 22.) ÖTM rendeletbe emeltek át.[13]

A tervezési szabványok útmutatást adnak például a létrehozandó túlnyomásra, minimális légsebességekre, ajtónyitáshoz szükséges erőre.[14] Egyes létesítményekben a füstmentesítő rendszerek szerepe alárendelt lehet egyéb céloknak (például radioaktív anyagok kikerülésének megakadályozása), amely esetekben azok különleges feltételekkel tervezendők.[15]

Túlnyomásos füstmentes lépcsőházak méretezési és tervezési módszereit is tartalmazó harmonizált európai szabvány az MSZ EN 12101-13. A szabvány táblázatos értékeket is tartalmaz egyes épületszerkezetek (falak, födémek), ajtók és egyéb elemek résméreteire.[16]

A hatékony füstmentesítés elérésének két fontos eleme a megfelelő túlnyomás és légmennyiség biztosítása csukott, illetve nyitott nyílászárók esetén. Nem csupán az épület kiürítésében, hanem a tűzoltói beavatkozás hatékonyságában is fontos szerepe van, továbbá lehetőséget ad a beavatkozást végző tűzoltók számára a helyszín biztosítására is.[17]

Fenti célok elérésének egyik eleme a légellátó rendszerek körültekintő méretezése. Jelen publikációm célja megvizsgálni a hazai és a harmonizált európai előírások szerinti méretezési módszereket annak érdekében, hogy javaslatot tudjak tenni ezek fejlesztésére az általam végzett gyakorlati mérések eredményeivel támogatva.

A vizsgálat tárgyának bemutatása

A vizsgált lépcsőházat tartalmazó épület főbb paraméterei a helyszíni felmérés alapján

A vizsgálat tárgyát képező, előtér nélkül kialakított túlnyomásos füstmentes lépcsőház egy budapesti középmagas oktatási intézmény épületében található. Az építmény két pinceszint, földszint és négy emelet felépítésű, legfelső használati szintjének szintmagassága +14,75 m, legalsó használati szintjének szintmagassága –7,64 m

[11] Klote–Milke 2002: 66.
[12] Klote 1991: 155.
[13] Ambrus et al. 2006: 11–12.
[14] NFPA 92 2021: 92-8; International Code Council and Society of Fire Protection Engineers 2022: 210.
[15] Antal–Vass–Kátai-Urbán 2017: 17–30.
[16] Recknagel–Sprenger–Albers 2022: 1842.
[17] Varga 2018.

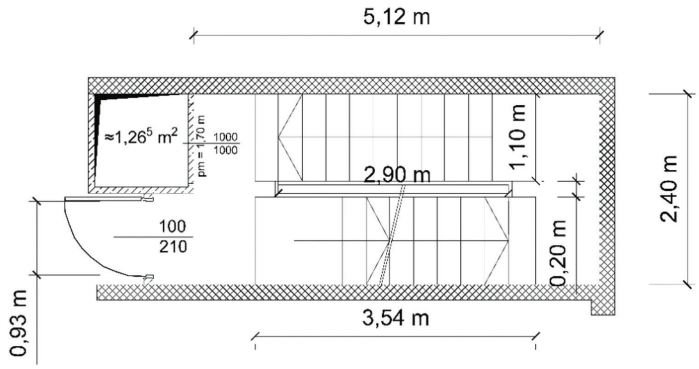
a kijárati szinthez (földszinthez) viszonyítva. A talajszint feletti szinteken oktatási tevékenységet végeznek (oktatótermek, irodák), a talajszint alatti szintek alapterületének döntő hányada személygépjárművek tárolására szolgál. A földszinten helyezkedik el egy előadóterem, amelynek befogadóképessége meghaladja a 300 főt, továbbá a helyiségen belül a fajlagos létszámsűrűség meghaladja az 1,0 fő/m^2-t. Az oktatási épületben jellemzően önállóan menekülésre képes személyek tartózkodnak, azonban a rendeltetéséből adódóan segítséggel menekülő személyek jelenlétére is kell számítani.

Az épület engedélyezése során a 2/2002. (I. 23.) BM rendelettel kiadott Országos Tűzvédelmi Szabályzat előírásai voltak irányadók. Ez alapján az épület „C" tűzveszélyességi osztályba tartozott, épületszerkezeteit legalább a II. tűzállósági fokozat követelményeinek megfelelően alakították ki. Az épület kiürítésének fő irányait jelentő füstmentes lépcsőházakba vezető nyílászárók általános helyeken 30 perc tűzállósági határértékkel rendelkeznek, tűzszakaszhatáron ez az érték 60 perc. A füstmentes lépcsőházak tervezésekor figyelembe kellett venni az ME-04–132–84 építésügyi ágazati műszaki előírást is.

A jelenleg hatályos, többszörösen módosított, 54/2014. (XII. 5.) BM rendelettel kiadott Országos Tűzvédelmi Szabályzat alapján az épület mértékadó kockázati osztálya KK (közepes kockázat). A 14 m-t meghaladó szintkülönbség miatt az épület kiürítésre figyelembe vett lépcsőházait jelenleg is füstmentes lépcsőházként kellene kialakítani. A füstmentes lépcsőházból a biztonságos térbe jutás napjainkban előírt követelményét a lépcsőházak nem tudják teljesíteni, azonban a létesítéskor még nem volt ilyen jellegű kötelezettség.

A füstmentesítő rendszer főbb paraméterei a helyszíni felmérés alapján

A lépcsőház füstmentesítő ventilátora a tetőn helyezkedik el, visszacsapó közbeiktatásával csatlakozik az előírt tűzállósági teljesítménnyel rendelkező, szerelt gipszkarton szerkezetből készült, hozzávetőleg 1,3 m^2 keresztmetszetű befúvó aknába. A lépcsőház három oldalról 20 cm vastagságú monolit vasbeton fallal határolt, negyedik oldalán a szerelt gipszkarton befúvó akna és a lépcsőházba vezető ajtók találhatók, szintén szerelt szerkezetbe építve. Az aknából a lépcsőházba a levegő bevezetése szintenként történik az akna falába épített 1000/1000 mm méretű, fix zsalukon keresztül. A lépcsőházba egyéb nyílászáró nem nyílik.



1. ábra: A mérés tárgyát képező lépcsőház alaprajzi elrendezése a kijárati szinten
Forrás: a szerző szerkesztése

A lépcsőházban kialakuló relatív túlnyomást két darab differenciálnyomás-érzékelő (nyomástávadó) érzékeli, amelyek a pinceszinten és a harmadik emeleten találhatók. Viszonyítási pontjuk a lépcsőház légtere és az adott szint közlekedőjének légtere. A lépcsőházba nyíló egyszárnyú tűzgátló ajtók éghetősége építőipari műszaki engedélyük szerint „nem éghető", vizsgálattal igazolt tűzállósági határértékük „TH = 0,5 óra", légzárási fokozatuk L4. A talajszint alatti szinteken, illetve tűzszakaszhatáron elhelyezkedő ajtók tűzállósági határértéke „TH = 1,0 óra". Túlnyomáslevezetésre szolgáló felület a lépcsőházban nem létesült.

2. ábra: A lépcsőház füstmentesítő ventilátora a zárófödémen
Forrás: a szerző felvétele

A lépcsőházi nyomásszabályozás PI szabályozással történik 0,5 arányossági tényezővel és 20 s integrálási idővel, amelyen a mérések során nem változtattunk. A beállított alapjel 40 Pa, a minimális frekvencia 20 Hz, amely megegyezett a startfrekvenciával. A ventilátor tervezett légszállítása 36 000 m^3/h, össznyomása 336 Pa. A lépcsőház légtechnikai mérése során az engedélyezéskor érvényes követelmények teljesülését ellenőriztem.

Bevezetendő levegőmennyiség meghatározása

A hazai és a harmonizált szabvány szerinti méretezés összehasonlítása végett meghatároztam a meglévő lépcsőházba bevezetendő levegőmennyiséget a hatályos TvMI, valamint az MSZ EN 12101-13 szabvány alapján is. Az alábbiakban a TvMI és a szabvány ajánlása szerinti méretezést mutatom be.[18]

Bevezetendő levegőmennyiség meghatározása hazai ajánlások szerint[19]

A túlnyomásos füstmentes lépcsőházba bevezetendő levegőmennyiség meghatározásához a TvMI ad méretezési javaslatot. Ez alapján csukott ajtók esetén az (1) egyenlet szerint számított levegőmennyiséget szükséges a lépcsőházba betáplálni, továbbá középmagas épületben a füstmentes lépcsőházi nyitott ajtók légveszteségi értéke a szabad nyílás m^2-enkénti felületére számítva 1,0 m^3/s.[20] A nyitott ajtók légveszteségi értékét a (2) képlettel határoztam meg.

$$\dot{V} = c \cdot \Delta p^n \cdot l \tag{1}$$

$$\dot{V_{ny}} = N \cdot (\zeta) \cdot A \cdot 1 \cdot 3600 \tag{2}$$

Fentiek alapján a méretezendő lépcsőházba csukott, illetve a TvMI szerint meghatározott 3 db nyitott lépcsőházi ajtó esetén a bevezetendő levegőmennyiség, egyszerűsítés végett $\zeta = 1{,}0$ feltételezésével, az (1)–(2) képletekkel számítva:

$$\dot{V} = 1{,}11 \cdot 50^{0{,}67} \cdot 6 \cdot (2 \cdot 2{,}27 + 2 \cdot 1{,}00) \cong 599\ m^3/h \tag{3}$$

$$\dot{V_{ny}} = 3 \cdot 1 \cdot (2{,}27 \cdot 1{,}00) \cdot 1 \cdot 3600 = 23\,121\ m^3/h \tag{4}$$

A lépcsőházi ajtók nem teljesítik az S200 füstgátlási követelményt, azonban a rendelkezésemre álló vizsgálati jegyzőkönyv szerint az ajtó légáteresztése 50 Pa nyomáskülönbségen vizsgálva 26,1 m^3/h volt, így a TvMI szerinti képlet alkalmazását elfogadhatónak tartottam. A (3) és (4) képletek alapján nyitott ajtók mellett körülbelül negyvenszeresre növekedett az igényelt légmennyiség.

[18] Hő és füst elleni védelemről szóló Tűzvédelmi Műszaki Irányelv 2022; MSZ EN 12101-13 2022: 10.
[19] Hő és füst elleni védelemről szóló Tűzvédelmi Műszaki Irányelv 2022.
[20] Hő és füst elleni védelemről szóló Tűzvédelmi Műszaki Irányelv 2022.

Bevezetendő levegőmennyiség meghatározása az MSZ EN 12101-13:2022 szerint

Az MSZ EN 12101-13:2022 szabvány szerinti méretezéskor három állapotot vizsgáltam, amelyek közül az első kettő kizárólag a szabvány ajánlásain alapul, míg a harmadik esetben a TvMI által javasolt paramétereket alkalmaztam.

1. táblázat: Az MSZ EN 12101-13 szabvány szerinti méretezéskor meghatározott állapotok

Eset	Lépcsőházi ajtók állapota			Tervezési nyomás	Tervezett légsebesség
	Kijárati szint	Tűzzel érintett szint	Egyéb szinteken		
A)	csukva	csukva	csukva	30 Pa	–
	csukva	nyitva	csukva	–	1 m/s
B)	nyitva	csukva	csukva	30 Pa	–
	nyitva	nyitva	csukva	–	1 m/s
C)	csukva	csukva	csukva	50 Pa	–
	nyitva	nyitva	további egy nyitott	–	1 m/s

Forrás: a szerző szerkesztése

Valamennyi állapotra meghatároztam a bevezetendő levegőmennyiséget a szabvány szerinti számítási módszer alkalmazásával. A méretezéskor a lépcsőházat 1. osztályba soroltam, így a tervezett légsebesség nyitott nyílászáró esetén a tűzzel érintett szinten 1 m/s volt. Az A) és B) állapotok a szabvány szerinti elrendezéseket mutatják, amelyben megkülönböztetünk csukott kijárati szinttel és nyitott kijárati szinttel tervezett rendszereket. A C) állapotban az ajánlások közötti összehasonlítás végett a hazai követelményekkel végeztem el a számításokat a szabvány szerinti számítási módszerrel.

A méretezési képletekben nem tüntettem fel azon összetevőket, amelyek értéke a vizsgált lépcsőház kialakításából adódóan zérus. Ilyen például az ablakok résein áramló levegő, levegőelvezető aknák. A méretezés során figyelembe vett és a számítások során releváns paramétereket, továbbá a szabvány által ajánlott és alkalmazott állandókat a 2. és 3. táblázatban foglaltam össze.

2. táblázat: Az MSZ EN 12101-13:2022 szabvány által javasolt és a méretezés során alkalmazott értékek

Jellemző	Jelölés	Érték
Lépcsőházba nyíló ajtó résfelülete	A_D	0,01 m^2
Lépcsőházból nyíló ajtó résfelülete		0,02 m^2
Falak réshányada (átlagos tömörség)	A_{LW}/A_{WALL}	$1{,}1 \times 10^{-4}$
Födémek réshányada	A_{FL}/A_{FLOOR}	$5{,}2 \times 10^{-5}$
Légsebesség a homlokzati nyíló szerkezeten	v_{vent}	2,5 m/s

Forrás: a szerző szerkesztése

3. táblázat: Az MSZ EN 12101-13:2022 szabvány szerinti számítások során a lépcsőház kialakítására vonatkozó releváns paraméterek összefoglalása

Jellemző	Érték	Jellemző	Érték
Szintek	–1/0/1/2/3/4	Ajtó szabad szélessége	1,00 m
Alapterület	13,56 m²	Ajtó szabad magassága	2,27 m
Kerület	16,10 m	A_{LW}	$3{,}66 \times 10^{-2}$
Átlagos belmagasság	3,40 m	A_{LF}	$1{,}41 \times 10^{-3}$
Teljes magasság	20,69 m	Méretezési osztály	1

Forrás: a szerző szerkesztése

A) Méretezés a szabvány szerint, a kijárati szinten csukott nyílászárót feltételezve

A vizsgált lépcsőház esetén – figyelembe véve annak adottságait és sajátosságait – a tervezési nyomáskülönbség fenntartásához szükséges levegőmennyiséget a kijárati szinten csukott nyílászárót feltételezve a szabvány szerinti képlettel számítottam (5).

$$Q_{TDC}^{\square} = 1{,}5 \cdot Q_{SDC}^{\square} = 1{,}5 \cdot (Q_{DC}^{\square} + Q_{WALL}^{\square} + Q_{FLOOR}^{\square}) \tag{5}$$

$$Q_{DC}^{\square} = 0{,}83 \cdot A_D \cdot 30^{0{,}5} \tag{6}$$

$$Q_{WALL}^{\square} = 0{,}83 \cdot A_{WALL} \cdot \left(\frac{A_{LW}}{A_{WALL}}\right) \cdot 30^{0{,}625} \tag{7}$$

$$Q_{FLOOR}^{\square} = 0{,}83 \cdot A_{FLOOR} \cdot \left(\frac{A_{LF}}{A_{FLOOR}}\right) \cdot 30^{0{,}625} \tag{8}$$

A tűzzel érintett szinten nyitott ajtó esetén a szabad keresztmetszetben 1 m/s légsebesség biztosításához szükséges térfogatáramot a (9) képlettel határoztam meg (szabvány szerinti 1. osztályba sorolt lépcsőház). Továbbá a közlekedőre jutó levegőmennyiség elvezetéséről is gondoskodni kell, amelyhez a szükséges hatásos elvezető/szellőző felületet a (10) képlettel számítottam, és a kialakuló térfogatáram jelen esetben megegyezik a tűzzel érintett szinten lévő nyitott ajtón átáramló levegőmennyiséggel. A tényleges felület méretezése természetesen az adott elemek ellenállásának figyelembevételével kell történjen. A szabvány ajánlása alapján az áramlási veszteségeket figyelembe véve a (11) képlettel meghatároztam a nyitott nyílászáró mellett a lépcsőházban fennmaradó túlnyomást. [A (11) képletben Q_{DO} a szabvány A.5.4. pontjában Q_{VA}-ként szerepel, amit jelen publikációban javítottam.] Ezzel a nyomással számítva, behelyettesítve azt a (12) képletbe számítottam ki a nyitott ajtó esetén bevezetendő összes levegőmennyiséget.

$$Q_{DO}^{\square} = v \cdot A_{DOOR}^{\square} (= Q_{VA}) \tag{9}$$

$$A_{VA}^{\square} = \frac{Q_{VA}^{\square}}{v_{vent}} \tag{10}$$

$$P_{SC}^{\square} = \left(\frac{Q_{VA}}{0{,}83 \cdot A_{VA}}\right)^2 + \left(\frac{Q_{DO}}{0{,}83 \cdot A_{DOOR}}\right)^2 \tag{11}$$

$$Q_{TDO}^{\square} = \left[0{,}83 \cdot (A_{LW} + A_{LF}) \cdot P_{SC}^{0{,}625}\right] + 0{,}83 \cdot A_D \cdot P_{SC}^{0{,}5} + Q_{DO} \tag{12}$$

Az A) esetben valamennyi csukott lépcsőházi ajtó esetén 30 Pa relatív túlnyomást, a tűzzel érintett szinten nyitott ajtót feltételezve annak keresztmetszetében 1 m/s légsebességet kell biztosítani.

A bevezetendő levegőmennyiség a (6)–(8) képletekkel, szabvány szerinti számítással:

$$Q_{DC}^{\square} = 0{,}83 \cdot 0{,}07 \cdot 30^{0{,}5} = 0{,}318\ m^3/s \tag{13}$$

$$Q_{WALL}^{\square} = 0{,}83 \cdot 333{,}11 \cdot 1{,}1 \cdot 10^{-4} \cdot 30^{0{,}625} = 0{,}255\ m^3/s \tag{14}$$

$$Q_{FLOOR}^{\square} = 0{,}83 \cdot 27{,}12 \cdot 5{,}2 \cdot 10^{-5} \cdot 30^{0{,}625} = 0{,}010\ m^3/s \tag{15}$$

Fentiek alapján az (5) képletbe behelyettesítve az összes bevezetendő levegőmennyiség csukott lépcsőházi ajtók mellett 0,875 m³/s (3 150 m³/h).

A tűzzel érintett szinten nyitott ajtót feltételezve, a nyitott ajtó szabad keresztmetszetében 1 m/s légáramlás biztosításához szükséges levegőmennyiség, a kiáramló levegő elvezetéséhez szükséges felület, valamint a lépcsőház becsült túlnyomása a (9)–(12) képletekkel, szabvány szerinti számítással:

$$Q_{DO}^{\square} = 1 \cdot 2{,}27 = 2{,}27\ m^3/s \tag{16}$$

$$A_{VA}^{\square} = \frac{2{,}27}{2{,}5} = 0{,}91 m^2 \tag{17}$$

$$P_{SC}^{\square} = \left(\frac{2{,}27}{0{,}83 \cdot 0{,}91}\right)^2 + \left(\frac{2{,}27}{0{,}83 \cdot 2{,}27}\right)^2 = 10{,}48\ Pa \tag{18}$$

Fentiek alapján a (12) képletbe behelyettesítve az összes bevezetendő levegőmennyiség a tűzzel érintett szinten nyitott lépcsőházi ajtó esetén 2,57 m³/s (9 252 m³/h).

A tervezés alapján bevezetendő levegőmennyiség a vizsgált lépcsőházba Q_{TDC} és Q_{TDO} közül a nagyobb érték 15% további biztonsági tartalékkal növelve, azaz jelen esetben 2,96 m³/s (10 656 m³/h). Nyitott ajtók mellett körülbelül háromszorosára növekedett az igényelt légmennyiség.

B) Méretezés a szabvány szerint, a kijárati szinten nyitott nyílászárót feltételezve

Ez a tervezési koncepció azon alapul, hogy a kijárati szinten lévő nyílászáró mindvégig nyitott állapotban van, azaz a kívánt túlnyomáshoz szükséges térfogatáram meghatározásakor a nyitott ajtón távozó levegőmennyiséget is kompenzálni szükséges.

Vagyis Q_{TDC} értéke kiegészül a nyitott kijárati ajtón keresztül tervezési nyomáson (30 Pa) kiáramló levegőmennyiséggel (20), illetve Q_{DC} értéke egy ajtónyi résen kiáramló levegő mennyiségével csökken, hiszen a kijárati ajtó ez esetben nyitva van.

$$Q_{TDC}^{\square} = 1{,}5 \cdot Q_{SDC}^{\square} + Q_{ED} = 1{,}5 \cdot (Q_{DC}^{\square} + Q_{WALL}^{\square} + Q_{FLOOR}^{\square}) + Q_{ED} \tag{19}$$

$$Q_{ED}^{\square} = 0{,}83 \cdot A_{ED} \cdot 30^{0{,}5} \tag{20}$$

A tűzzel érintett szinten nyitott ajtót feltételezve, annak szabad keresztmetszetében megkövetelt légsebesség jelen esetben is 1 m/s. A lépcsőházban fennmaradó túlnyomás egy része a határolószerkezetek, csukott ajtók résein keresztül hoz létre áramlásokat,

míg jelentős része a kijárati ajtón keresztül távozik a lépcsőházból. Q_{TDO} értéke ennek megfelelően kiegészül egy Q_{EDO} taggal, vagyis a nyitott ajtók mellett becsült lépcsőházi túlnyomás hatására a kijárati ajtón kiáramló levegő mennyiségével.

$$Q_{TDO}^{\square} = \left[0{,}83 \cdot (A_{LW} + A_{LF}) \cdot P_{SC}^{0{,}625}\right] + 0{,}83 \cdot A_D \cdot P_{SC}^{0{,}5} + Q_{DO} + Q_{EDO} \tag{21}$$

$$Q_{EDO}^{\square} = 0{,}83 \cdot A_{ED} \cdot P_{SC}^{0{,}5} \tag{22}$$

Vagyis a B) esetben a kijárati szinten nyitott állapotban lévő lépcsőházi ajtó esetén 30 Pa relatív túlnyomást kell biztosítani a lépcsőházban a kapcsolódó terekhez képest, továbbá a tűzzel érintett szinten is nyitott ajtót feltételezve annak keresztmetszetében 1 m/s légsebességet kell biztosítani, minimális túlnyomáskövetelmény nélkül.

Jelen szcenárió esetén bevezetendő levegőmennyiség a (6)–(8) és (20) képletekkel, szabvány szerinti számítással:

$$Q_{DC}^{\square} = 0{,}83 \cdot 0{,}05 \cdot 30^{0{,}5} = 0{,}227\ m^3/s \tag{23}$$

$$Q_{WALL}^{\square} = 0{,}83 \cdot 333{,}11 \cdot 1{,}1 \cdot 10^{-4} \cdot 30^{0{,}625} = 0{,}255\ m^3/s \tag{24}$$

$$Q_{FLOOR}^{\square} = 0{,}83 \cdot 27{,}12 \cdot 5{,}2 \cdot 10^{-5} \cdot 30^{0{,}625} = 0{,}010\ m^3/s \tag{25}$$

$$Q_{ED}^{\square} = 0{,}83 \cdot 2{,}27 \cdot 30^{0{,}5} = 10{,}32\ m^3/s \tag{26}$$

Fentiek alapján a (21) képletbe behelyettesítve az összes bevezetendő levegőmennyiség csukott lépcsőházi ajtók mellett 11,06 m³/s (39 816 m³/h).

A tűzszinten nyitott ajtót feltételezve, a lépcsőház becsült túlnyomása, valamint a tűzzel érintett szinten a nyitott ajtó szabad keresztmetszetében 1 m/s légáramlás biztosításához szükséges levegőmennyiség a (16)–(18) és (22) képletekkel, szabvány szerinti számítással:

$$Q_{DO}^{\square} = 1 \cdot 2{,}27 = 2{,}27\ m^3/s \tag{27}$$

$$A_{VA}^{\square} = \frac{2{,}27}{2{,}5} = 0{,}91\ m^2 \tag{28}$$

$$P_{SC}^{\square} = \left(\frac{2{,}27}{0{,}83 \cdot 0{,}91}\right)^2 + \left(\frac{2{,}27}{0{,}83 \cdot 2{,}27}\right)^2 = 10{,}48\ Pa \tag{29}$$

$$Q_{EDO}^{\square} = 0{,}83 \cdot 2{,}27 \cdot 10{,}48^{0{,}5} = 6{,}10\ m^3/s \tag{30}$$

Fentiek alapján a (21) képletbe behelyettesítve az összes bevezetendő levegőmennyiség a tűzzel érintett szinten nyitott lépcsőházi ajtó esetén 8,62 m³/s (31 032 m³/h).

A tervezés alapján bevezetendő levegőmennyiség a vizsgált lépcsőházba Q_{TDC} és Q_{TDO} közül a nagyobb érték 15% további biztonsági tartalékkal növelve, azaz jelen esetben 12,72 m³/s (45 792 m³/h). Nyitott ajtók mellett ebben az esetben körülbelül ötödével csökkent az igényelt légmennyiség.

C) Méretezés a szabvány ajánlásai alapján, a TvMI által javasolt értékekkel

A C) esetben megvizsgáltam, hogy valamennyi lépcsőházi ajtó csukott állapotában, a TvMI által javasolt 50 Pa relatív túlnyomás biztosításához a szabvány szerint mekkora levegőmennyiség bevezetése szükséges.

A bevezetendő levegőmennyiség a szabvány szerinti számítással a (6)–(8) képletekben szereplő értékek 50 Pa-ra való módosításával:

$$Q_{DC}^{\square} = 0{,}83 \cdot 0{,}07 \cdot 50^{0{,}5} = 0{,}411\ m^3/s \tag{31}$$

$$Q_{WALL}^{\square} = 0{,}83 \cdot 333{,}11 \cdot 1{,}1 \cdot 10^{-4} \cdot 50^{0{,}625} = 0{,}351\ m^3/s \tag{32}$$

$$Q_{FLOOR}^{\square} = 0{,}83 \cdot 27{,}12 \cdot 5{,}2 \cdot 10^{-5} \cdot 50^{0{,}625} = 0{,}014\ m^3/s \tag{33}$$

Fentiek alapján az (5) képletbe behelyettesítve az összes bevezetendő levegőmennyiség csukott lépcsőházi ajtók mellett 1,16 m³/s (4 176 m³/h).

A vizsgált lépcsőházban a TvMI alapján feltételezett nyitott lépcsőházi nyílászárók mennyisége 3 db (kijárati szinten és két további szinten), ami egyebekben megegyezik a létesítéskor megkövetelt értékkel. Ez alapján a szükséges bevezetendő levegőmennyiség a (16)–(18) és (22) képletekkel szabvány szerinti közelítéssel:

$$Q_{DO}^{\square} = 2 \cdot 1 \cdot 2{,}27 = 4{,}54\ m^3/s \tag{34}$$

$$A_{VA}^{\square} = \frac{2 \cdot 2{,}27}{2{,}5} = 1{,}82\ m^2 \tag{35}$$

$$P_{SC}^{\square} = \left(\frac{4{,}54}{0{,}83 \cdot 1{,}82}\right)^2 + \left(\frac{2{,}27}{0{,}83 \cdot 2{,}27}\right)^2 = 10{,}48\ Pa \tag{36}$$

$$Q_{EDO}^{\square} = 0{,}83 \cdot 2{,}27 \cdot 10{,}48^{0{,}5} = 6{,}10\ m^3/s \tag{37}$$

Fentiek alapján a (21) képletbe behelyettesítve az összes bevezetendő levegőmennyiség a földszint és két további szinti nyitott lépcsőházi ajtó esetén 10,86 m³/s (39 096 m³/h).

A tervezés alapján bevezetendő levegőmennyiség a vizsgált lépcsőházba Q_{TDC} és Q_{TDO} közül a nagyobb érték 15% további biztonsági tartalékkal növelve, azaz jelen esetben 12,49 m³/s (44 964 m³/h). Nyitott ajtók mellett ebben az esetben körülbelül kilencszeresére növekedett az igényelt légmennyiség.

Légtechnikai mérések eredményei

A lépcsőházban kialakuló légállapotokat több szempontból és több elrendezésben is vizsgáltam.

- Valamennyi nyílászáró csukott állapotában kialakul-e a létesítéskor előírt relatív túlnyomás, továbbá a földszinti és a két további szinti nyitott ajtó szabad keresztmetszetén kialakul-e a létesítéskor előírt légsebesség?

- A földszinti nyitott ajtó esetén különböző ventilátor-fordulatszámok mellett vizsgáltam a lépcsőházban kialakuló tényleges túlnyomást és a nyitott ajtón mért légsebességértékeket, amelyeket összehasonlítottam a szabvány ajánlásaival.

Az eredmények kiértékelésekor rendelkezésemre állt a létesítmény átadása előtt végzett légtechnikai mérési jegyzőkönyv, amely szerint a vizsgált lépcsőházban kialakuló relatív túlnyomás a frekvenciaváltók 19 Hz-es automatikus üzeme mellett 38 Pa volt. A lépcsőház légtechnikai méretezésével kapcsolatban nem állt rendelkezésre adat. A földszinti és a két szinti nyitott ajtó esetén a nyitott ajtók szabad keresztmetszetében mért légsebesség 1,1–1,4 m/s között változott. A mérések során alkalmazott eszközök pontos adatait korábbi publikációm részletezi.[21] A környezeti körülményeket a 4. táblázat mutatja be.

4. táblázat: Környezeti körülmények a mérés során

A mérés időpontja	**2022. 08. 24. 8:00**	**Légnyomás**	**1005 hPa**
Uralkodó szélirány	É	Szél erőssége	0,5 km/h
Külső hőmérséklet	21,7 °C	Lépcsőház hőmérséklete	25,6 °C
Külső rel. páratartalom	81%	Belső rel. páratartalom	61%

Forrás: a szerző szerkesztése

Létesítéskor érvényben lévő differenciálnyomás- és légsebesség-követelmények mérésekkel való vizsgálatának eredményei

A lépcsőház és a közlekedő között kialakuló differenciálnyomásokat valamennyi kapcsolódó térhez viszonyítva ellenőriztem. A létesítéskor irányadó előírás alapján a csukott nyílászárók mellett a közlekedőhöz viszonyított túlnyomás értéke 25–75 Pa között kell legyen.[22] Az adatrögzítés frekvenciája 1 Hz volt és valamennyi mérési sorozat időtartama legalább 60 s. Az 5. táblázat a műszerből kiolvasott adatok feldolgozásának eredményeit tartalmazza.

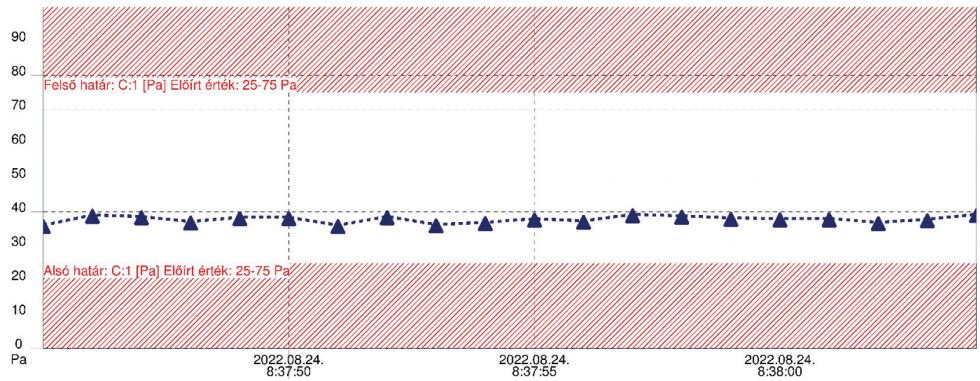
5. táblázat: A lépcsőház és a közlekedő között kialakuló nyomásviszonyok valamennyi ajtó csukott állapota esetén

Mérési pont	**Pmin [Pa]**	**Pmax [Pa]**	**Pátlag [Pa]**	**korr. tap. szórás**	**Előírt érték [Pa]**	**Megfelelés**	**Megjegyzés**
4. emelet	37,51	40,91	**39,46**	0,907	25-75	**Megfelel**	
3. emelet	38,62	40,94	**39,90**	0,506	25-75	**Megfelel**	
2. emelet	38,62	41,61	**40,31**	0,732	25-75	**Megfelel**	
1. emelet	37,98	42,45	**39,74**	0,927	25-75	**Megfelel**	
Földszint	37,84	40,79	**39,16**	0,743	25-75	**Megfelel**	
–1. szint	37,78	40,54	**39,24**	0,699	25-75	**Megfelel**	

Forrás: a szerző szerkesztése

[21] Mihály 2022: 69–93.
[22] ME-04–132–84 1984.

Valamennyi ajtó csukott állapota esetén a frekvenciaváltó 20 Hz-re szabályozott, ami megegyezett a minimális frekvenciával. Ajtó nyitásakor a frekvencia megfelelően emelkedett, ajtó csukásakor a frekvenciaváltó visszaszabályozása automatikusan megtörtént.

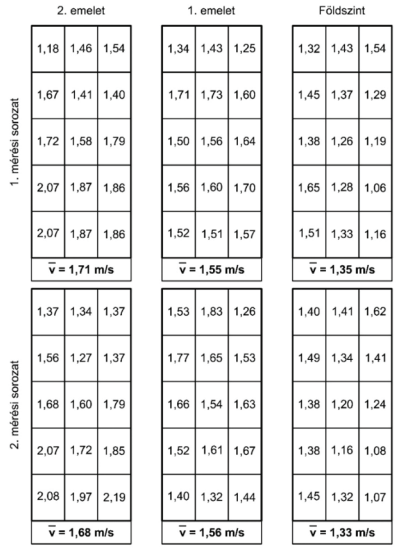


3. ábra: A lépcsőházban kialakuló relatív túlnyomás a kapcsolódó terekhez képest a nyomástávadó szintjén

Forrás: a szerző szerkesztése (Testo Comfort – Software X35 programmal)

A differenciálnyomás-méréseim alapján megállapítottam, hogy a lépcsőházban kialakuló túlnyomás a létesítéskori követelményeknek megfelelt. A jelenleg megkövetelt 50 Pa ±10% értéket a kialakuló túlnyomás nem éri el, azonban az alapjel növelésével vélhetően ebben a nyomástartományban is megvalósítható a működés. A szabvány szerinti 30 Pa az alapjel és a minimális frekvencia további csökkentésével vélhetően megvalósítható lenne, azonban szabályozási túllendülésekre lehet számítani.

A létesítéskori légsebesség-követelmények ellenőrzése céljából a földszinti és az 1–2. emeleti ajtók nyitott állapotát feltételeztem. Valamennyi mérés esetén ellenőriztem, hogy a mért légsebességértékek mennyire reprodukálhatók. Ennek érdekében egy nyílásnál egymás után két mérési sorozatot is végeztem. Az értékeket akkor tekintettem elfogadhatónak, ha a két mérési sorozat átlagértékei közötti eltérés nem haladta meg a ±10%-ot, ami összhangban van az MSZ EN 12101-13:2022 ajánlásával is. A mért értékeket a 3. ábra mutatja, amelyen jól látható, hogy az egyes mérési sorozatok közötti eltérés elhanyagolható mértékű.



4. ábra: A nyitott ajtók szabad keresztmetszetében rögzített légsebességértékek m/s-ban az első és a második mérési sorozat során

Forrás: a szerző szerkesztése

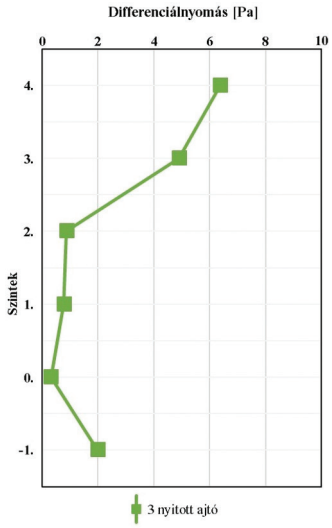
6. táblázat: A légsebességmérés eredményeinek összefoglaló táblázata

Mérési hely	**Szélesség [m]**	**Magasság [m]**	**Felület [m²]**	**Mért átlagos légsebesség [m/s]**	**Előírt érték [m/s]**	**Számított átlagos térfogatáram [m³/h]**	**Megfelelés**
4. emelet							
3. emelet							
2. emelet	1,00	2,27	2,27	1,70	1	≈ 13 892	Megfelel
1. emelet	1,00	2,27	2,27	1,56	1	≈ 12 748	Megfelel
Földszint	1,00	2,27	2,27	1,34	1	≈ 10 951	Megfelel
–1. szint							

Forrás: a szerző szerkesztése

A végeredményt táblázatba foglalva megállapítottam (6. táblázat), hogy a mért légsebességértékek a létesítéskor érvényben lévő előírásoknak megfelelőek, és biztosítják a füst lépcsőházba jutásának megakadályozását. Megjegyzendő, hogy a kialakuló légsebességek egyebekben a jelenlegi TvMI- és szabványkövetelményeknek is megfeleltethetők.

További méréseket végeztem a három nyitott ajtó mellett kialakuló relatív túlnyomás vizsgálatára. A mérési eredményeket a 4. ábra szemlélteti.

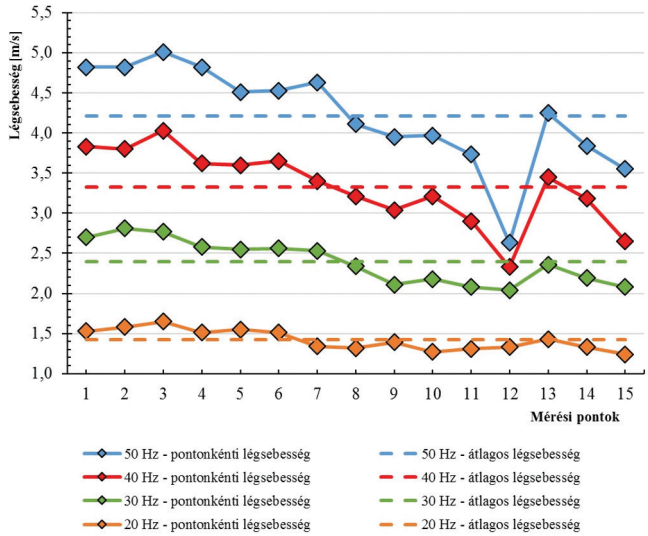


5. ábra: Szintenként mért differenciálnyomás a földszinti, 1. és 2. emeleti ajtók nyitott állapotában
Forrás: a szerző szerkesztése

A mérési eredmények jól szemléltetik, hogy három nyitott ajtó mellett a lépcsőház túlnyomása drasztikusan csökken.

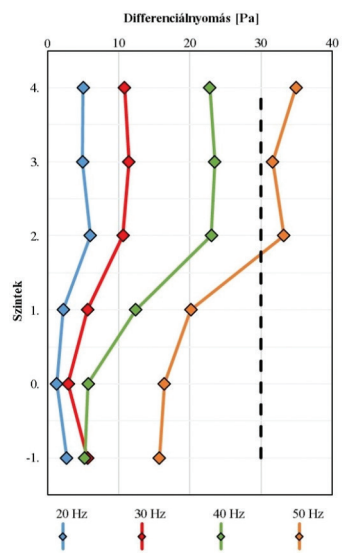
Földszinti nyitott ajtó mellett, különböző ventilátor-fordulatszámokon végzett mérések eredményei

A mérések elvégzése során a földszinti lépcsőházajtó teljesen nyitott állapotban volt. A frekvenciaváltón manuálisan beállított 20-30-40-50 Hz értékeken végeztem el valamennyi szinten a lépcsőház és a közlekedő között kialakuló nyomáskülönbség mérését, továbbá a földszinti ajtón kialakuló átlagos légsebesség mérését, ami több mint 1000 érték regisztrálását és feldolgozását jelentette. A légsebesség- és differenciálnyomás-mérések eredményeit az 5. és a 6. ábra szemlélteti.



6. ábra: A földszinti nyitott ajtón kialakuló mérési pontonkénti légsebességek és átlagos légsebességek különböző ventilátor-fordulatszám esetén

Forrás: a szerző szerkesztése



7. ábra: A földszinti nyitott ajtó esetén kialakuló relatív túlnyomás szintenként különböző ventilátor-fordulatszám esetén

Forrás: a szerző szerkesztése

Megállapítható, hogy a földszinti ajtó nyitott állapotában a lépcsőház légellátó rendszere a 2–4. emeleteken a szabvány kijárati szinten nyitott ajtót feltételező metódusában leírt 30 Pa értéket is elérte, ettől lefelé a túlnyomás jelentősen esett, azonban még a pinceszinten sem csökkent 10 Pa alá. Ekkor az átlagos légsebesség 4,21 m/s volt, azaz a földszinti ajtón körülbelül 34 404 m^3/h levegő áramlott ki. A kísérőakna szintenkénti befúvásának köszönhetően a magasabb szinteken közel állandó túlnyomás alakult ki.

Összegzés

Vizsgálatom tárgya egy meglévő előtér nélkül kialakított füstmentes lépcsőház volt. A lépcsőház felmérését követően számításokat végeztem a lépcsőházba bevezetendő levegőmennyiség meghatározására a hazai TvMI és az európai szabvány ajánlásai alapján.

Csukott lépcsőházi nyílászárók esetén a bevezetendő levegőmennyiség a szabvány szerinti módszerrel számítva több mint ötszöröse a TvMI szerinti számításnak az alacsonyabb tervezési nyomás ellenére is. Az ajtók számított résveszteségе a szabvány szerinti számítással körülbelül 2–4-szerese annak, mint amit a TvMI által ajánlott képlet meghatároz.

Nyitott ajtókra való méretezéskor a hazai előírás szigorúbbnak bizonyult, több nyitott ajtó feltételezését követelte meg a szabványban foglaltaknál, azonban a megkívánt légsebességérték a választott osztály esetén megegyező volt. A szabványtól eltérő, de annak számítási módszerével támogatott három nyitott ajtóra méretezés esetén körülbelül 1,8-szoros légmennyiség adódott.

Mérési eredményeim alapján a vizsgált lépcsőház a létesítéskori nyomás- és légsebesség-követelményeknek megfelelt, részben a jelenleg hatályos követelménynek is megfeleltethető.

Mérési eredményeim alapján a földszinti nyitott ajtó esetén a 2–4. emeleteken elérhető volt a szabvány szerint kijárati szinten nyitott ajtót feltételező méretezés nyomáskövetelménye.

A túlnyomásos füstmentes lépcsőházak légtechnikai mérésekor, illetve az eredmények kiértékelésekor tapasztalataim szerint a lépcsőházi légellátó rendszer méretezésére vonatkozó információk (például figyelembe vett nyitott ajtók száma, mérete, tervezett légmennyiségek) nem, vagy hiányosan állnak rendelkezésre.

Következtetések és javaslatok

Mind a harmonizált európai szabvány, mind a nemzetközi ajánlások 50 Pa-nál alacsonyabb relatív túlnyomást javasolnak fenntartani csukott lépcsőházi ajtók mellett. Mivel az ajtónyitáshoz szükséges erő kisebb nyomáson kedvezőbb, megfontolandó csukott ajtók esetén kisebb differenciálnyomás javaslata a műszaki irányelvben.

A szabályozások közötti eltérések miatt további vizsgálatok elvégzését javaslom az ajtók résveszteségértékének új mérésekkel történő meghatározásával.

Figyelembe véve a számítási módszerek összetettségét, a füstmentes lépcsőházak megfelelőségének értékeléséhez szükséges a tervezett állapot ismerete. Ennek

érdekében javaslom, hogy a füstmentes lépcsőházak méretezésében szerepet játszó alapvető adatok a tervdokumentációban részletezésre kerüljenek. Erre vonatkozó iránymutatások közzétehetők lennének akár a Magyar Mérnöki Kamara tervdokumentációk tartalmi és formai követelményeit tartalmazó szabályzatában is.

A füst lépcsőházba való bejutásának egyik kritikus pontja, hogy a nyitott ajtó szabad keresztmetszetén kellő légáramlás alakuljon ki. Az alkalmazott kiürítési stratégia miatt előfordulhat, hogy a hő és füst elleni védelemről szóló TvMI alapján meghatározotthoz képest több ajtó egyidejű nyitva tartása válhat szükségessé (pl. egyidejű teljes kiürítés, teljes szakaszos kiürítés). Ebben az esetben a tervezés során javaslom figyelembe venni, hogy a kiürítési stratégiának megfelelően kerüljön méretezésre a füstmentesítő rendszer.

Amennyiben a füstmentes lépcsőházat átmeneti védett térként alakítják ki, javasolható figyelembe venni, hogy rövid idejű vagy tartósan fennálló kedvezőtlen nyomásviszonyok miatt a réseken füst áramolhat a lépcsőházba, ami a mentendő személy(ek) számára pánikhoz vezethet. Az esetlegesen beszivárgó füst eltávolítására alkalmas lehet öblítőlevegő alkalmazása.

Jelmagyarázat

V – lépcsőházba bevezetendő levegőmennyiség csukott nyílászáró szerkezetekre vonatkoztatva (m^3/h)
c – TvMI szerinti állandó (Sa és S200) minősítésű nyílászárókra vonatkoztatva ($m^3h^{-1}Pa^{-0,67}m^{-1}$)
Δp – a nyílászáró két oldala közötti nyomáskülönbség (Pa)
n – TvMI szerinti állandó (Sa és S200) minősítésű nyílászárókra vonatkoztatva (-)
l – a nyílászáró kerülete, a névleges méretre vonatkoztatva (m)
V_{ny} – nyitott ajtók légveszteségi értéke (m^3/h)
N – feltételezett nyitott lépcsőházi ajtók darabszáma (-)
ζ – ellenállás-tényező (-)
A – nyitott lépcsőházi ajtó szabad nyílásmérete (m^2)
Q_{TDC} – csukott ajtók mellett bevezetendő teljes légmennyiség (m^3/s)
Q_{SDC} – résveszteségek pótlásához szükséges légmennyiség csukott ajtók mellett (m^3/s)
A_D – csukott ajtó résfelülete (m^2)
Q_{DC} – csukott ajtók résvesztesége (m^3/s)
A_{WALL} – lépcsőházat határoló falak felülete (m^2)
A_{LW} – lépcsőházat határoló falak résfelülete (m^2)
Q_{WALL} – határoló falak résvesztesége (m^3/s)
A_{FLOOR} – lépcsőházat határoló födémek felülete (m^2)
A_{LF} – lépcsőházat határoló födémek résfelülete (m^2)
Q_{FLOOR} – födémek résvesztesége (m^3/s)
Q_{DO} – nyitott ajtón kiáramló levegő térfogatárama (m^3/s)
v – tervezési sebesség (m/s)
A_{DOOR} – nyitott ajtó szabad felülete (m^2)
A_{VA} – elvezetőfelület hatásos felülete (m^2)

Q_{VA} – elvezetőfelületen kiáramló levegő térfogatárama (m^3/s)
v_{vent} – áramlási sebesség tervezett átlagos értéke az elvezető felületen (m/s)
P_{SC} – a lépcsőházban kialakuló túlnyomás nyitott nyílászáró(k) esetén (Pa)
Q_{TDO} – nyitott ajtó(k) mellett bevezetendő teljes légmennyiség (m^3/s)
Q_{ED} – nyitott kijárati ajtón kiáramló levegő térfogatárama tervezési nyomáson (m^3/s)
A_{ED} – kijárati szint nyitott ajtajának felülete (m^2)
Q_{EDO} – nyitott kijárati ajtón kiáramló levegő térfogatárama PSC nyomáson (m^3/s)

Irodalomjegyzék

Antal Zoltán – Vass Gyula – Kátai-Urbán Lajos (2017): Atomerőmű létesítés tűzvédelmi követelményeinek vizsgálata. *Védelem Tudomány,* 2(1), 17–30.

Ambrus István et al. (2006): Módosulások a hő- és füstelvezetésben. *Védelem Katasztrófa- és Tűzvédelmi Szemle,* 13(2), 11–12.

AS 1668.1:2015 (2015): *The use of ventilation and air conditioning in buildings, Part 1: Fire and smoke control in buildings.* Standards Australia Limited.

Bérczi László – Badonszki Csaba (2021): A tűzvédelmi tervezés fő tartópillérei a tűzvédelmi műszaki irányelvek. *Védelem Tudomány,* 6(2), 66–96.

Hurley, Morgan J. et al. szerk. (2016): *SFPE Handbook of Fire Protection Engineering*. New York, NY: Springer. Online: https://doi.org/10.1007/978-1-4939-2565-0

International Code Council (2020): *International Building Code.* Falls Church, VA: International Code Council.

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

Klote, John H. (1991): *Design Manual for Smoke Control Systems*. NISTIR ; 4551. U.S. Dept. of Commerce, National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.IR.4551

Klote, John H. – Milke, James A. (1992): *Design of Smoke Management Systems.* Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Society of Fire Protection Engineers.

Klote, John H. – Milke, James A. (2002): *Principles of Smoke Management*. Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers.

Klote, John H. et al. (2012): *Handbook of Smoke Control Engineering*. Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers.

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

Lougheed, Gary – Ko, Yoon J. (2016): *RP-1447 Performance of Stairwell Pressurization System with Open Doors.* Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

ME-04–132–84 (1984): Füstmentes lépcsőházak követelményei. Építésügyi Szabványosítási Központ.

Mihály István (2022): Túlnyomásos füstmentes lépcsőházak légtechnikai méréseinek tapasztalatai I. rész. *Védelem Tudomány, 7*(4), 69–93.
MSZ EN 12101-13 Füst- és hőszabályozó rendszerek. 13. rész: Nyomáskülönbség elvén működő rendszerek (PDS). Tervezési és számítási módszerek, átvételi vizsgálat, rutinvizsgálat és karbantartás. Magyar Szabványügyi Testület, 2022.
NFPA 92: Standard for Smoke Control Systems. National Fire Protection Association, 2021.
Recknagel, Hermann – Eberhard Sprenger – Albers, Karl-Josef (2022): *Taschenbuch für Heizung und Klimatechnik: einschließlich Brauchwassererwärmung und Kältetechnik 2023/2024,1, Band 1 : einschließlich Trinkwasser- und Kältetechnik sowie Energiekonzepte*, 81. Auflage. München: ITM InnoTech Medien GmbH: Oldenbourg DIV, Dt. Industrie-Verl. Kleinaitingen.
TvMI 3.4:2022.06.13. Hő és füst elleni védelem Tűzvédelmi Műszaki Irányelv. 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.

Jogi források

54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról
489/2017. (XII. 29.) Korm. rendelet a tűzvédelmi hatósági eljárások általános és különös szabályairól

HADMÉRNÖK
VÉDELEMGAZDASÁG

18. évfolyam (2023) 3. szám 103–119.
DOI: 10.32567/hm.2023.3.8

Mészáros Alexandra Ágnes[1]

A kontingenciaelmélet alkalmazása az innovatív kis- és középvállalkozások vizsgálata során az európai védelmi iparban

The Analysis of Small- and Medium-sized Enterprises in the European Defence Industry from a Contingency Theory Perspective

Absztrakt

A kontingenciaelmélet alapján a szervezet teljesítménye függ a környezet alakulásától, ennélfogva nincs egy előre meghatározott stratégia, amelyet minden vállalkozás alkalmazhat, hanem folyamatosan alkalmazkodni szükséges a dinamikusan változó környezeti tényezőkhöz. A helyi védelmi ipar fenntartása stratégiai jelentőségű minden európai országban, amelyben az innovatív technológiák fejlesztése területén úttörő kis- és középvállalkozások törekednek az igények minél magasabb színvonalú kiszolgálására. A kutatás célja azonosítani, hogy jelen geopolitikai környezetben mely külső és belső kontingenciaváltozóknak van releváns hatása az innovatív védelmi kis- és középvállalkozások működésére. A kvalitatív kutatás során az adatgyűjtés mélyinterjúk alkalmazásával, az adatelemzés tartalomelemzés módszertannal történt. Jelen környezetben a geopolitikai konfliktusok, az intenzív piaci kereslet, az ellátási problémák az alapanyag és a védelmi eszközök területén, a dinamikus technológiai fejlődés és az állami törekvések a védelmi ipar fejlesztésére néhány fontos változó a vállalkozásra ható kontingenciatényezők közül. Az eredmények keretrendszert biztosíthatnak a menedzsment számára a hatékony szervezeti stratégia megfogalmazásában.

[1] Doktorjelölt, Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: meszaros.alexandra@uni-obuda.hu

Kulcsszavak: kontingenciaelmélet; védelmi ipar; haditechnika; kis- és középvállalkozás; kutatás-fejlesztés-innováció

Abstract

According to contingency theory, an organization's performance depends on the changes in the environment, therefore there is no pre-determined strategy that every business can apply, but it is necessary to continuously adapt to dynamically changing environmental factors. Maintaining the local defence industry is of strategic importance for every European country where small and medium-sized enterprises play a prominent role in the development of innovative technologies. The research aims to identify which external and internal contingency variables have a relevant impact on the operation of innovative small and medium-sized enterprises in the current geopolitical environment. Data were collected through semi-structured in-depth interviews and analysed with qualitative content analysis. In the current environment, geopolitical conflicts, intense market demand, supply problems in the field of raw materials and defence equipment, dynamic technological development, and national efforts to develop the defence industry are some of the contingency factors that affect businesses. The results provide a framework for management to formulate an effective strategy.

Keywords: contingency theory; defence industry; military technology; small and medium-sized enterprises; research-development-innovation

Bevezetés

A kontingenciaelmélet alapján a szervezet teljesítménye függ a környezet alakulásától, ezáltal nincs egy előre meghatározott szervezeti stratégia, amelyet minden vállalkozás alkalmaz, hanem folyamatosan illeszkedni szükséges az őket körülvevő dinamikusan változó környezethez. Az elmélet szerint azon szervezeteknek van a legnagyobb esélyük a sikeres működésre, amelyek rugalmasan és gyorsan képesek reagálni a külső lehetőségekre és fenyegetésekre. Az európai védelmi ipar működését az elmúlt években feszült és kiszámíthatatlan környezet alakítja. A pandémia, a védelmi nagyhatalmak közötti geopolitikai feszültség, továbbá az Európai Unió és a NATO határán 2022 februárjában kirobbant fegyveres konfliktus olyan folyamatok sorozatát indította be, amelyek alapjaiban formálják át a teljes európai védelmi ágazatot. A pandémia okozta hirtelen leállások a teljes ellátási lánc mentén jelentős késedelmeket, alapanyaghiányt és dinamikus áremelkedést eredményeztek, majd az orosz–ukrán háború hatására bekövetkezett erőteljes keresletnövekedés és energiaválság tovább fokozta a védelmi iparban kialakult feszültségeket. Ezek az események olyan változó környezeti tényezők, amelyek nagymértékben befolyásolják a szervezet stabilitását, és értelmezésüktől függ a vállalat jövőbeni működése, így a kontingenciaelméleti megközelítésnek fontos szerepe van a hatékony szervezeti stratégia kidolgozásában.

Az innovatív helyi védelmi ipar fenntartása stratégiai jelentőségű minden európai ország számára, mivel olyan gazdasági, politikai és technológiai faktorokat foglal magában, amelyek kiemelten támogatják az egész ipar globális versenyképességét.[2] A védelmi ipar növeli a gazdaság válságállóságát, szerkezeti és ágazati diverzifikációját, ezáltal javítva versenyképességét, továbbá jelentős része innovációs tevékenységnek tekinthető, így az átlagosnál nagyobb hozzáadottérték- és jövedelemgeneráló képességgel rendelkezik.[3] A gazdasági előnyökön felül a védelmi ipar hozzájárul a nemzetbiztonság fenntartásához, továbbá részt vesz a kritikus infrastruktúra és az ellátási lánc zavartalanságának biztosításában.[4] Politikai szempontból elemezve a stratégiai függetlenség és a globális hatalmi pozíció kifejező eszköze,[5] ezenfelül a haditechnikai innovációk exportja a diplomáciai kapcsolatok kiemelkedő fontosságú területe.[6] A tudásintenzív ágazat támogatja az oktatást, az egészségügyet, továbbá csökkenti a munkanélküliséget, amellett munka- és kutatási lehetőséget teremt magasan képzett szakemberek számára.[7] A minőségi haditechnikai innovációk lokális fejlesztése jobban igazodik a helyi haderő igényeihez, hozzájárul az ellátásbiztonság fenntartásához, megvásárlása során az állam a hazai ipart támogatja, továbbá erősíti egy nemzet haderejének hadrafoghatóságát és műveleti képességét.[8] A rohamosan fejlődő technológia jelentős hatást gyakorol a védelmi iparra, következésképpen a katonai összeütközések módszerei és eljárásai is változnak,[9] ami megköveteli a helyi vállalkozásoktól az új technológiák fejlesztését. 2022-ben az Európai Unió területén több mint 2500 védelmi kis- és középvállalkozás működött,[10] amelyek közvetlenül 463 ezer főt foglalkoztattak.[11] Az európai védelmi iparnak célkitűzése, hogy a közeljövőben képes legyen teljes mértékben a kis- és középvállalkozásokból származó haditechnikai innovációkra támaszkodni.[12]

Mivel a kontingenciaelmélet 1960-as évekbeli elterjedése óta a szervezetek belső tényezői és külső környezete jelentős átalakuláson ment keresztül, a vezetéselmélet hatékony alkalmazása is új szemléletet igényel, ami teret enged az ágazatspecifikus, a vállalkozás működését befolyásoló, új változók azonosításának. Jelen kvalitatív kutatás a kontingenciaelmélet újszerű megközelítését alkalmazza, amelynek célja azonosítani, hogy jelen geopolitikai környezetben mely külső és belső kontingenciaváltozóknak van releváns hatása az innovatív védelmi kis- és középvállalkozások működésére, továbbá hogy milyen stratégiai eszközökkel lehet a vállalkozás működését hatékonyabbá tenni a feltárt környezeti változók figyelembevételével.

[2] Lásd: www.europarl.europa.eu/factsheets/en/sheet/65/defence-industry
[3] Taksás 2017: 167–174.
[4] Okun–Arun 2021: 190–215.
[5] Mănescu–Stan 2021: 204–209.
[6] Kurç–Neuman 2017: 2019–227.
[7] Durakovic–Trgo 2020: 26–33.
[8] Hegedűs –Gyarmati 2022: 17–32.
[9] Bodoróczki 2019.
[10] Lásd: https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-smes_en
[11] Lásd: www.europarl.europa.eu/factsheets/en/sheet/65/defence-industry
[12] Lásd: https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-smes_en

Kontingenciaelmélet

A klasszikus vezetéselméleti iskolák (Taylor, Fayol és Weber) a szervezetet egy zárt rendszernek tekintették, amelynek határai összetartották a vállalkozás elemeit és elválasztották a körülvevő környezeti tényezőktől. Az 1960-as évektől, a kontingenciaelmélet terjedésével a szervezet környezete egyre nagyobb figyelmet kapott a vezetéselméleti kutatások területén, mivel elfogadottá vált, hogy a vállalkozás teljesítménye attól függ, hogy mennyire képes megfelelni a külső környezetének és rugalmasan reagálni az onnan érkező fenyegetésekre, lehetőségekre és kihívásokra.[13] A kutatók felismerték, hogy a szervezet és az azt körülvevő környezet között állandó a kölcsönhatás, ezáltal a szervezethatároknak átjárhatónak kell lenniük minden irányból a sikeres működés érdekében.[14] Ennek a modern menedzsmentelméletnek nem célja definiálni egy univerzális, minden helyzetben és körülmények között jól működő szervezési módszert, inkább arra törekszik, hogy támogassa a döntéshozókat beazonosítani a különböző szituációk sajátosságait, majd megtalálni az ezekben a helyzetekben legmegfelelőbb reakciókat és válaszokat.[15] Azonban fontos megjegyezni, hogy az elmélet napjainkban működő vállalkozásokra való vetítése során nem szabad figyelmen kívül hagyni, hogy az 1960-as évek óta a kontingenciaelmélet hatóköre jelentősen kiszélesedett, azelőtt ismeretlen fenyegetések jelentek meg, a gazdaság globalizálódott, a szervezetek korábban hierarchikus szerkezete egyre laposabb, az ellátási láncok feldarabolódtak, és a szervezetek egy fókuszált területre specializálódnak, így az elmélet alkalmazása újszerű megközelítést igényel.[16]

A kontingenciaelmélet a vállalat viselkedését abból a szempontból vizsgálja, hogy a kontingenciatényezők hogyan befolyásolják a szervezet irányítását és a teljes működését,[17] továbbá két alapfelvetése, hogy nincs egyetlen legjobb alkalmazható stratégia, és a különböző módszerek nem egyformán hatékonyak.[18] A vállalkozás sikeres működése attól függ, hogy mennyire képes az általa befolyásolható belső tényezőket – az alkalmazott stratégiát, a szervezet struktúráját és a belső érintettek magatartását – a külső környezeti kontingenciaváltozókhoz illeszteni, amelyekre nincs vagy csak elenyésző a ráhatása.[19] A környezetébe hatékonyan illeszkedő szervezet nagyobb teljesítményt tud nyújtani és képes többletforrást generálni, ami terjeszkedéshez, továbbá több kutatás, fejlesztés és innováció megvalósításához vezethet.[20] A vezetési módszer, amelynek alkalmazásával az egyik szervezet versenyképesen tud teljesíteni, nem feltétlenül adaptálható egy másik vállalkozásra, mivel arra teljesen más tényezők hathatnak ugyanabban az időben.[21]

Bár a kontingenciaelmélet kutatói abban egyetértenek, hogy a klasszikus vezetéselméleti iskolák felfogása téves abból a szempontból, hogy létezik egyetlen legjobb

[13] Abdulwahab–Pandurics–Ugrai 1997.
[14] Llewellyn 1994: 4–23.
[15] Farkas–Balogh–Rideg 2015: 52–53.
[16] Otley 2016: 45–62.
[17] Islam–Hu 2012: 5159–5164.
[18] Galbraith 1973.
[19] Gresov 1989: 431–453; Donaldson 2001; Islam–Hu 2012: 5159–5164; Farkas–Balogh–Rideg 2015: 52–53.
[20] Hamilton–Shergill 1992: 95–113.
[21] Farkas–Balogh–Rideg 2015: 52–53.

módja egy szervezet hatékony működtetésének,[22] azonban hogy mely külső vagy belső kontingenciaváltozóknak van fontos szerepe a vállalkozás kialakításában, továbbá milyen szempontból szükséges ezeket kategorizálni, már számos eltérő eredmény olvasható a témát feldolgozó szakirodalomban.[23] Hayes (1977) a szervezeti belső tényezőket, a kölcsönösen függőségi változókat, továbbá a külső faktorokat nevezte meg a három fő kategóriának.[24] Mintzberg (1979) mélyebben elemezte a szervezeti kontingenciákat, és tizenegy változót azonosított, ezek a szervezet alkalmazott stratégiája, mérete és formalizáltsága; a döntéshozás központosításának foka; az alkalmazottak képzettségi szintje és a munka változékonysága; a szervezeti kultúra; a vállalkozás által kínált termékek és szolgáltatások szabványosítása és komplexitása; az alkalmazott technológia, továbbá a külső környezet,[25] amelyeket Child (1981) kiegészített a nemzeti kultúrával.[26] Donaldson (2001) szintén főbb kategóriákba sorolta a változókat, ezek a szervezet stratégiája, mérete és annak környezete.[27] Betts (2003) a szervezet környezetét, méretét, életkorát és az alkalmazott technológiát nevezte meg kontingenciaváltozónak.[28]

Az évek során a szerzők a kontingenciaelmélet újszerű megközelítését alkalmazva több új – a saját kutatási területükön releváns – kontingenciatényezőt definiáltak. Wong és szerzőtársai (2011) a piaci versenyt, a versenytársakat, az ellátási láncot és az információáramlást,[29] Alves és szerzőtársai (2017) a klímaváltozást, a fenntarthatóságot és a károsanyag-kibocsátást,[30] továbbá Engelseth és Kritchanchai (2018) a kórházi infrastruktúrát, az egészségügyi szolgáltatások színvonalát és a gyógyászati célú turizmust nevezték meg.[31] Az irodalmi áttekintés alapján arra lehet következtetni, hogy a kontingenciaelmélet modern megközelítése lehetőséget ad a kutatóknak arra, hogy a vizsgált ágazat szempontjából leginkább jelentős környezeti változókat definiálják. Jelen kutatás célja – a kontingenciaelmélet újszerű megközelítését alkalmazva – a védelmi iparban működő haditechnikai innovációk fejlesztése területén úttörő kis- és középvállalatokra ható külső és belső kontingenciaváltozók azonosítása.

Módszertan

A kvalitatív kutatás folyamán az adatgyűjtés félig strukturált, telefonon és személyesen zajló mélyinterjúk során történt 27 személlyel, akik az európai védelmi ipar területén folytatott munkásságuk során kiemelkedő tapasztalatra tettek szert. A kutatásban részt vevő megkérdezettek kiválasztása a védelmi iparban szerzett tapasztalataik alapján

[22] Tosi–Slocum 1984: 9–26; Donaldson 2001; Galbraith 1973; Gresov 1989: 431–453; Islam–Hu 2012: 5159–5164.
[23] Tosi–Slocum 1984: 9–26; Donaldson 2001.
[24] Hayes 1977: 22–39.
[25] Mintzberg 1979.
[26] Child 1981: 303–356.
[27] Donaldson 2001.
[28] Betts 2003: 123–130.
[29] Wong–Lai–Cheng 2011: 161–200.
[30] Alves et al. 2017: 223–236.
[31] Engelseth–Kritchanchai 2018.

történt, az interjúk által érintett vállalkozások profilját országok szerint felsorolva az 1. táblázat ismerteti. Az interjúk átlagosan 45–60 percesek voltak. Az adatfelvétel 2022 negyedik és 2023 első negyedévében zajlott.

1. táblázat: Az interjúkban érintett vállalkozások profilja országok szerint felsorolva

Ország	Profil	Ország	Profil
Anglia	• Repülőgépipar	Magyarország	• Befektetési alapkezelő, érdekelt a védelmi iparban • Fegyvergyártás • Fegyver- és műholdalkatrész-gyártás • Katonai járművek
Ausztria	• Fegyvergyártás • Páncélozott járművek		
Bulgária	• Nagykereskedés • Lőszergyártás		
Csehország	• Kézifegyvergyártás		
Franciaország	• Befektetési alapkezelő, érdekelt a védelmi iparban	Németország	• Katonai járművek • Fegyvergyártás • Optika
Horvátország	• Fémalkatrészgyártás	Szerbia	• Lőszergyártás • Fegyvergyártás • Optika
Lengyelország	• Fegyvergyártás • Fémalkatrészgyártás		

Forrás: a szerző szerkesztése a mélyinterjúk alapján

A kvalitatív, félig strukturált mélyinterjúk alkalmazásának előnye, hogy ez az adatgyűjtési módszer magas fokú szabadságot biztosít a megkérdezettek számára, hogy a beszélgetések során megosszák személyes véleményüket, tapasztalataikat és szakértelmüket az elmúlt évek alatt a védelmi iparban bekövetkezett változásokkal kapcsolatban, amelyek érintik az innovatív kis- és középvállalkozások működését. A kvalitatív mélyinterjús adatfelvétel egy olyan, személyes adatok gyűjtésére használt tudományos módszer, amely lehetővé teszi az alanyok számára, hogy a saját nézőpontjukból mutassák be a jelenséget, így segítve a kutatónak a téma kontextusának mélyebb megértését.[32] A technika támogatja a válaszadó véleményének, tapasztalatainak és meggyőződésének elemzését, mélyebb betekintést engedve a kutatott probléma természetébe, így válva az elmélet elsődleges forrásává.[33] A kvalitatív kutatás előnye, hogy személyes, nyitott, dinamikus és rugalmas metódus, amely hozzájárul az adatfelvétel közben felszínre kerülő információk alapján a beszélgetés irányításához, következményeképp mélyrehatóbb megértést tesz lehetővé, továbbá az alany személyisége, tudása és megnyilvánulásai kiindulási pontul szolgálhatnak a kutatás további folytatásához.[34] A félig strukturált interjúvázlat kérdései az európai védelmi iparban uralkodó körülmények megismerésére, az innovatív kis- és középvállalkozásokra ható külső környezeti tényezők feltárására, a releváns szervezeti belső faktorok

[32] Morris 2015.
[33] Scanlan 2020.
[34] Koronváry–Szegedi–Tóth 2015: 237–246.

feltérképezésére és a felsoroltak optimális összehangolásának lehetőségeire irányultak. Az alanyok szabadon oszthatták meg gondolataikat a vizsgált témával kapcsolatban.

Az interjúk során gyűjtött adatok elemzése tartalomelemzés módszertannal történt, amely egy olyan tudományos kvalitatív módszer, amely azon a hipotézisen alapszik, hogy az emberek között zajló kommunikáció rögzített formái értékes adatforrást biztosítanak egy vizsgált jelenség feltárásához.[35] A védelmi iparban a tartalomelemzés módszertan alkalmazása megszokott gyakorlat, mivel az egymással szemben álló felek ezzel a módszerrel próbálnak olyan információt kinyerni a másik fél kommunikációjából, amely feltárja a szöveg elsődleges jelentésén túli látens tartalmat.[36] A technika használata során az adatokat kódolással értelmezik, amelynek folyamán a rögzített kommunikációt kisebb részekre tördelik, a jelentéssel rendelkező kategóriákat képviselő fogalmakat elkülönítik, majd absztrakció használatával olyan módon kategorizálják, hogy az így nyert keretrendszer alapján leírható legyen a vizsgált probléma.[37] A kódok olyan rövid, leíró kifejezések, amelyek a kódolási folyamat során segítik a kutatókat szisztematikusan kategorizálni és értelmezni a nagy mennyiségű, a vizsgált jelenség leírását szolgáló gyűjtött adatot.[38]

Eredmények

A védelmi iparban uralkodó külső környezeti kontingenciák

A jelen geopolitikai környezetben az egyik legintenzívebb változó, amely hatást gyakorol az innovatív védelmi vállalkozásokra, a piacon kialakult magas kereslet. Az európai védelmi iparban a felszerelések iránti érdeklődés évek óta növekvő tendenciát mutatott, azonban az orosz–ukrán háború kitörése csak még intenzívebb keresletet eredményezett, ami kritikus ellátási problémákhoz vezetett. „Jelenleg a védelmi iparban jelentős ellátási problémák vannak, […] hatalmas az igény, de nem tudják kiszolgálni."[39] Azonban a hirtelen megnövekedett szükséglet csak egy környezeti változó, amely hozzájárult a védelmi iparban jelenleg tapasztalható ellátási problémákhoz. A pandémia miatt váratlanul részben vagy teljesen felfüggesztett nyersanyag-kitermelés és -gyártás, továbbá a több országot magában foglaló ellátási láncok világjárvány miatti lokális korlátozásai jelentős áremelkedéseket és késedelmeket okoztak a megrendelők kiszolgálásában. Az ipar még ki sem heverte a pandémia hatásait, amikor kirobbant a nyugati országokat váratlanul érő orosz–ukrán fegyveres konfliktus. A háború következményeként kialakult infláció és energiaválság, továbbá az alapanyagok árának jelentős növekedése és rendkívül hosszú beszerzési ideje még nehezebbé tették a magas kereslet kiszolgálását. A haditechnikai eszközök gyártásához a fémek és ötvözőanyagok jelentős részével Oroszország látta el az európai ipart,

[35] Kleinheksel et al. 2020: 127–137.
[36] Nagy 2018: 32–44.
[37] Kyngäs 2020: 13–21.
[38] Saldaña 2021.
[39] Interjúalany 22.

és bár ezek az anyagok most is elérhetők, de csak Európán kívüli közvetítő országon keresztül, ami többszörös beszerzési árat és jelentősen hosszabb beszerzési időt jelent.

A háború váratlanul érte az európai döntéshozókat, akik erre válaszul nyomást helyeztek a korábban elhanyagolt szektor szereplőire, gyors megoldásokat sürgetve a helyi védelmi ipar fejlesztésének kérdésében. Azonban ez az elmaradás nem hozható be pár hónap alatt, figyelembe véve a jelenlegi bizonytalan környezetet, a szűkös állami költségvetéseket, a több évre előre lefoglalt haditechnikai gyártási kapacitásokat és egy ilyen projekt technológiai igényét, amelynek piacát szintén készlethiányok, áremelkedések és bizonytalanság jellemzik. A fegyveres konfliktus hirtelen kirobbanása hamar jelentősen csökkentette Európa-szerte a védelmi készleteket, ami előtérbe helyezte a szektor korábbi elhanyagoltságát és a haditechnikai készletek hiányosságait. Mindazonáltal a hosszú távú megoldást szolgáló helyi védelmi ipar fejlesztése nem kivitelezhető pár hónapon belül, így a döntéshozók gyorsabb eredményeket sürgetve a megoldást sok esetben a védelmi eszközök Európán kívülről való importálásában látták. Ugyanakkor a fejlett védelmi iparral rendelkező nemzetek a csúcstechnológiák és komplex fegyverrendszerek fejlesztésére helyezik a hangsúlyt, a fegyveres erőknél régóta rendszeresített eszközök nagy mennyiségű gyártása helyett. Ezeket a haditechnikai felszereléseket a legtöbb állam nem képes magának előállítani, és csak import útján tudják beszerezni, magas árakon. Azonban a hadi eszközök tervezésénél, amelyeket akár több évtizedes időtartamra alakítanak ki, fontos szempont a tartósság. Abban az esetben, ha valamely európai országot kiszolgáló állam nem szállít többé, az újabb ellátási problémákhoz vezethet, és jelen biztonsági környezetben még pontos rövidtávú előrejelzéseket sem lehet készíteni. Az európai védelmi iparban kialakult helyzet kezeléséhez a helyi védelmi ágazat fejlesztése szükséges, de egy olyan ipar fejlesztése, amely teljeskörűen képes a funkcióit ellátására még egy váratlanul kialakuló krízishelyzet esetén is, csak több államot magában foglaló együttműködés keretén belül valósulhat meg. „Ha Európában védelmi ipart akarnak építeni, akkor azt közösen, összefogva kell csinálni […], és nem szabad kizárólag a rövidtávú válaszlépésekre összpontosítani."[40] A jelen környezetben a védelmi ágazaton belüli együttműködésekre és szövetségekre való igény egyre erősödik az alapanyag- és alkatrészbeszerzésben, a már rendszeresített termékek gyártásában és a technológiai innovációk fejlesztése területén egyaránt. Korábban egy vállalkozás egy technológiai innováció megvalósítására egymaga is képes volt, és bár a képességgel most is rendelkeznek, a megváltozott körülmények miatt a más vállalkozásokkal való együttműködés erősséget jelent.

Az orosz–ukrán háború előtt a haditechnikai innovációk fejlesztésével foglalkozó kis- és középvállalkozások nem tartoztak a befektetők által előnyben részesített szervezetek közé a magas kockázat miatt. Azonban mivel feltételezhető, hogy többek között a fegyveres konfliktus következményeként a gazdaság recesszió felé sodródik, és a védelmi ipar recesszióállónak számít, így egyre népszerűbb a befektetők körében, és jelentős tőke áramlik az iparban tevékenykedő kis- és középvállalkozásokba, továbbá startupcégekbe. Befektetési szempontból előnyben részesülnek azok a portfóliócégek, amelyek termékei duális felhasználású technológiaként alkalmazhatók. Az autonóm navigációt segítő, gépi tanulással támogatott ember nélküli járművek; a harcterek

[40] Interjúalany 17.

és csapatmozgások valós idejű megfigyelésére alkalmas műholdas felderítő rendszerek; a kiberbiztonsági rendszerek; a döntéshozatalt segítő, mesterséges intelligenciával és gépi tanulással támogatott rendszerek; a kvantumszámítógépek; a robotika, továbbá az irányított energiájú fegyverek csak néhány példa a mélyinterjúk során elhangzott haditechnikai innovációs területek közül, amelyekbe jelentős befektetés áramlik.

A katalizálófaktorok olyan külső környezeti impulzusok, amelyek hatására fogan meg az új technológia ötlete. Ez a külső kontingenciaváltozó jellemzően egy új megoldást igénylő stratégiai probléma vagy környezeti fenyegetés, azonban közrejátszanak a politikai célok, a nemzeti stratégia és a technológiák növekvő komplexitása. Jelen környezetben erőteljes katalizálófaktor az orosz–ukrán háború, amely az első nem aszimmetrikus fegyveres konfliktus a második világháború óta, amikor mindkét fél közel azonos technológiai színvonalú eszközöket vet be, amelyek közül sok fejlesztése a közel-keleti háborúk során gyűjtött tapasztalatok alapján valósult meg.

„Korábban a Közel-Keleten aszimmetrikus konfliktusok voltak, melyek hatására olyan magas szintű védelmet igénylő haditechnikai eszközöket fejlesztettek, amik célja a veszteségek minimalizálása volt. Ezekből az eszközökből kevés volt alkalmazva, nagyon magas költségeken. Az orosz–ukrán háborúban viszont más a helyzet, mindkét fél sok eszközzel rendelkezik, és a jelentős stratégiai és technológiai fölény elérése nem megoldható ezen a szinten."[41]

A háború során vált gyakorlattá, hogy a műholdas felderítő rendszer költséges fejlesztése helyett a jelentősen alacsonyabb költségeken megvalósítható, akár a civil piacon is beszerezhető drónokat alkalmaznak ugyanerre a célra. Ugyanakkor a drónok harctéri alkalmazásának elterjedése következményeként egyre nagyobb igény jelentkezik egy hatékony drónelhárító rendszer fejlesztésére.

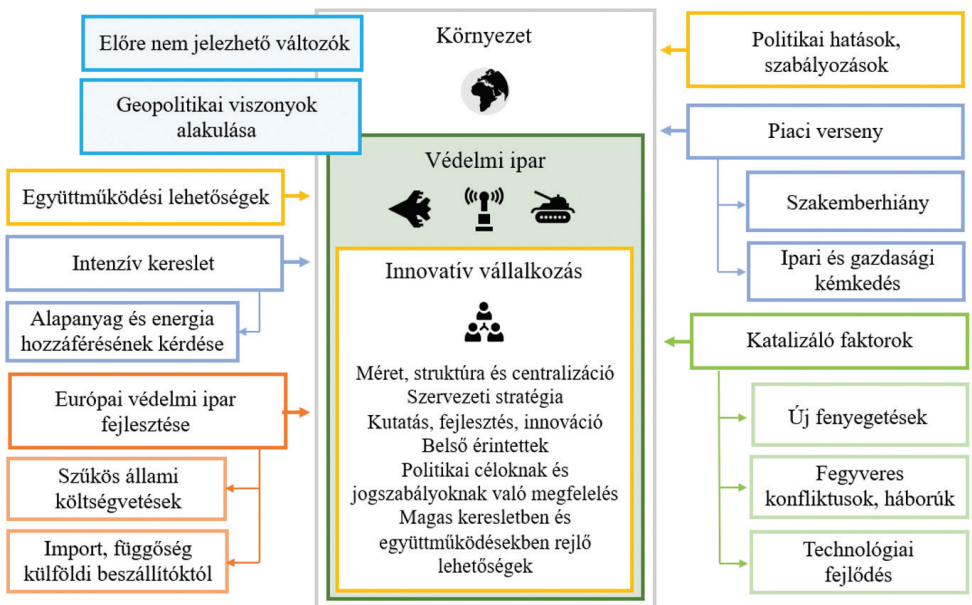
A védelmi ipar továbbra is kiemelkedő az innovatív új technológiák fejlesztésében, nap mint nap jelennek meg technológiai újdonságok, nagy nyomást helyezve a piac szereplőire. Azonban míg korábban feltételezhető volt, hogy a következő háborút ember nélküli eszközök fogják vívni, mesterséges intelligenciával támogatva, ezzel szemben az évtizedek óta rendszeresített eszközök gyártása teljes kapacitáson folyik, és a nagy keresletet így sem képes az ipar kiszolgálni. Technológiai szempontból érdekesek a diszruptív innovációk, mivel egy újfajta megközelítést kínálnak egy probléma megoldására, azonban jelenleg a védelmi piacon azokra az innovációkra van nagy igény, amelyek a régóta rendszeresített felszereléseket teszik precízebbé, hatékonyabbá és könnyen kezelhetővé.

„Minden innováció előnyös valamely tudományág szempontjából, mivel egy újfajta megoldást kínál. Azonban a védelmi iparban szem előtt kell tartani, hogy ha az innováció újdonságtartalma szignifikáns, és felhasználása jelentősen eltér a katonai doktrínákban jegyzett technológiáktól, akkor nehézséget okoz beilleszteni az alkalmazott fegyverrendszerek közé."[42]

[41] Interjúalany 23.
[42] Interjúalany 18.

A kis- és középvállalkozásoknak az innovációk piaci bevezetése és rendszeresítése során több akadályozó környezeti változóval is szembe kell nézniük, ilyenek a védelmi iparra jellemző szabályozottság, hierarchikus felépítés és bürokratikus szervezés, a magas belépési korlát, az innovációk jogi védelmének kérdése, a jövedelmező működéshez szükséges politikai kapcsolatok kiépítése, továbbá a nehéz hozzáférés a beszerzésekre kiírt pályázatokhoz és tenderekhez.

Bár a védelmi iparban tevékenységet folytató kis- és középvállalkozások stratégiai szerepet töltenek be, gyakran nem rendelkeznek elegendő pénzügyi vagy humán tőkével a megfelelő információvédelmi rendszer kialakításához, így sok esetben válnak ipari vagy gazdasági kémkedés áldozatává. A háború által generált szükséghelyzetben ez a probléma csak erősödött, mivel egy hirtelen jelentkező igényre sokszor csak lopott információval képesek rövid időn belül technológiát fejleszteni, amit csak fokoz a piacon jellemző intenzív verseny és a szektor bizonyos területein tapasztalható szakemberhiány. Az ipari vagy gazdasági kémkedés módszerei gyors és költséghatékony megoldást kínálnak az információlopást szervező fél számára a szükséges tudás megszerzésére. Az 1. ábra összefoglalja a kutatás során feltárt, védelmi iparban ható külső kontingenciatényezőket.



1. ábra: A védelmi iparban azonosított külső kontingenciatényezők
Forrás: a szerző szerkesztése a kutatás eredményei alapján

A védelmi kis- és középvállalkozások működésére ható belső kontingenciaváltozók

A kontingenciaelmélet megfogalmazása alapján az a szervezet alkalmas a versenyképes és jövedelmező tevékenység folytatására, amely mindenkor hatékonyan tudja a belső kialakítását, irányítását és teljes működését a környezeti változókhoz illeszteni, amihez a környezet folyamatos megfigyelése és értelmezése elengedhetetlen. A szervezet méretét vizsgálva a kis- és középvállalkozások agilisabb és rugalmasabb magatartást mutatnak, mint a nagy védelmi vállalatok, továbbá gyorsabban képesek alkalmazkodni a változó vevői igényekhez és piaci feltételekhez. Figyelembe véve kisebb méretüket és fókuszált szakterületi specializálódásukat, a kis- és középvállalkozások nagyobb hajlandóságot mutatnak olyan kutatás, fejlesztés és innovációs projektek megvalósítására, amelyek a nagyobb védelmi vállalatok számára túl kockázatosnak számítanak. Bár sok szektorban jellemző, hogy a vállalkozások struktúrája laposodik, ez nem minden ágazatban vezet a hatékonyság növekedéséhez. A védelmi ágazat hierarchikus felépítése miatt a vállalkozások magasabb teljesítményt tudnak elérni hierarchikusan kialakított rendszerrel, a menedzsment szintjén centralizált irányítással. A védelmi kis- és középvállalkozásoknál jellemzően a döntéshozás szintje magasan összpontosul, és a menedzsment közvetlenül felügyeli a folyamatokat és hozza az üzleti döntéseket, ennélfogva gyorsan és rugalmasan tud reagálni a környezeti változásokra. A hierarchikus struktúrában a belső érintettek felelősségei és feladatai világosan meg vannak határozva, és a szabályozott információáramlás biztosítja, hogy mindenki tisztában legyen a felülről jövő utasításokkal.

A védelmi ágazatra jellemző szigorú szabályozottság okán a vállalkozások szervezésének és működésének minden körülmények között meg kell felelnie az irányadó jogszabályoknak. Az ágazat stratégiai jelentősége miatt a menedzsmentnek szükséges szem előtt tartania a politikai célokat és a nemzeti stratégiát. Mivel a védelmi iparban jellemzően a kormányzati megrendelések dominálnak, a megfelelő politikai kapcsolatok kiépítése támogathatja a vállalkozást az ipar hierarchikus és bürokratikus jellegéből fakadó akadályok legyőzésében, a szükséges tőke és egyéb finanszírozási lehetőségek elérésében, továbbá új üzleti lehetőségek kialakításában. A vállalkozás vezetősége több csatornát használhat a szükséges kapcsolatok létesítéséhez, mint az üzleti partnerek vagy közvetítők kiépített kapcsolati hálózata, együttműködés olyan vállalkozásokkal, amelyek már kiépített kapcsolati rendszerrel rendelkeznek, rendezvényeken való részvétel, lobbizás vagy közvetlen kapcsolatfelvétel. A jelenlegi geopolitikai helyzetben az európai kormányok nagyobb hajlandóságot mutatnak az olyan versenyképes védelmi innovációkba való befektetésre, amelyek hozzájárulnak az ütőképes védelmi ipar megvalósításához. Ennek oka, hogy az orosz–ukrán háború megmutatta az európai védelmi készletek hiányosságait, továbbá hogy mely területeken szükséges fejleszteni, hogy előnyre tegyenek szert egy nem aszimmetrikus konfliktus során.

Az orosz–ukrán háború kitörése következményeként még intenzívebbé vált a védelmi piacon uralkodó, korábban is magas kereslet, amely lehetőséget kihasználhatják a vállalkozások bővítésre, terjeszkedésre, továbbá újabb piacok felkutatására és kiszolgálására. A védelmi iparban a magánkereslet növekedése ellenére az állami

szereplők jelentik a fő vásárlóerőt, így olyan országokra érdemes fókuszálni, ahol a védelmi kiadások növekedése észlelhető. Az új fejlesztési projektek indításánál célszerű figyelembe venni, hogy a célpiacon megfogalmazott nemzeti védelmi stratégiába milyen innovatív felszerelések illeszthetők be. A bizonytalan környezet, az alapanyag- és energiaárak dinamikus emelkedése, továbbá a védelmi iparban jelenleg jellemző több hónapos teljesítési idő olyan kritikus környezeti változók, amelyek mellett nehéz a vállalkozásoknak menedzselni a magas keresletet. E feltételek között kockázatos többéves keretszerződéseket kötni a megrendelésekre, és a probléma kezelésére még nem alakult ki a szükséges kultúra és a megfelelő jogi háttér. A helyzetet tovább élezi, hogy miután felszínre kerültek az európai védelmi készletek hiányosságai, hirtelen megnőtt a védelmi iparba való beruházási szándék az európai országok között, azonban a politikai nyomáshoz sok esetben szűkös állami költségvetések társulnak. A helyzet kezelését segítheti, hogy a korábbi gyakorlattal ellentétben nem kötnek a vállalkozások hosszú távú szerződéseket, továbbá a rövid és középtávú keretszerződésekbe is belefoglalják az árváltoztatás jogát a felhasznált alapanyag- és az energiaárak növekedésével arányosan, és a felelősséget a beszállítókra hárítják, amennyiben a megrendelést nem képesek a szerződésbe foglalt időn belül teljesíteni.

Jelen környezetben a szervezeti stratégia részét képezheti a más vállalkozásokkal való közös tevékenység folytatása, mivel a kis- és középvállalkozások együttműködések keretein belül versenyképesebben tudnak fellépni a dinamikus védelmi piacon. A közös munka többféle jogi formában valósulhat meg, és a jelenlegi kiszámíthatatlan környezetben stratégiailag erősebb pozíciót biztosít a részt vevő vállalkozásoknak, bizonyos fokú kockázatcsökkentő hatással rendelkezik, redukálja a projektekhez szükséges költségeket, és hozzáférést biztosíthat új piacokhoz. A kooperációk támogatják az ellátási problémák kezelését az alapanyag- és alkatrészbeszerzés során, növelik a hatékonyságot a gyártás és összeszerelés területén, továbbá serkentően hatnak a haditechnikai innovációk megvalósítására. A közös kutatási és fejlesztési projektek előnye, hogy elősegíti a vállalkozások közötti tudásmegosztást, ezáltal a magasabb szintű kompatibilitást a védelmi rendszerek között. Más vállalkozásokkal együttműködve a védelmi kis- és középvállalkozások versenyképesebb ajánlatokat tudnak benyújtani a beszerzési pályázatokra, így nagyobb projektekhez juthatnak hozzá.

A környezetben végbemenő gyors ütemű technológiai előrehaladással a szervezeteknek is együtt szükséges fejlődni, figyelemmel kísérve más vállalkozások fejlesztési projektjeit és a piacon uralkodó kereslet irányultságát. A környezeti változások megkövetelik az innovatív vállalkozásoktól, hogy az alkalmazott technológia és géppark megfeleljen a piacon uralkodó legújabb irányoknak. Az innovatív kis- és középvállalkozásoknak nem célja versenyezni a nagyvállalatokkal a régóta rendszeresített védelmi eszközök gyártásában. Specializálódhatnak a hosszú ideje alkalmazott védelmi eszközök korszerűsítésére, alkatrészek fejlesztésére és gyártására nagyobb vállalatok részére, új, akár diszruptív innovációk fejlesztésére vagy egyedi igények megvalósítására. „Technológiailag érdekesek a megszokottól elrugaszkodó innovációk, azonban az alkalmazásuk megkérdőjelezhető. Nagyon ritkán van lehetőség valós helyzetben

tesztelni egy innovációt. Jelen esetben a piac azokat az újításokat igényli, amelyek a jól bevált eszközöket teszik eredményesebbé."[43]

Az egyik legfontosabb tényező a vállalkozás szempontjából, amelyet a környezeti változókhoz szükséges alakítani, a rendelkezésére álló emberi erőforrás, akiknek a képzettsége a haditechnikai kis- és középvállalkozásoknál általában magasabb szintű, mint a hagyományos vállalkozásoknál. Bár a háború előtt jellemző volt, hogy a magasan képzett mérnökök a nyugat-európai országokban vállaltak munkát, a válság hatására csökken a nyugati szervezetek által kínált lehetőségek vonzereje, ami enyhítheti a szakemberhiányt a kelet-európai vállalkozásoknál. A haditechnikai innovációk fejlesztésénél fontos szempont, hogy jelen környezetben nemcsak az a cél, hogy a projektek során a mérnökök demonstrálják kimagasló szaktudásukat, hanem az is, hogy az új technológiák bevethetők legyenek a gyakorlati felhasználás során. Építő lehet egy harctéri tapasztalattal rendelkező személy bevonása a fejlesztési folyamatba, így összehangolva a mérnöki elképzelést a felhasználó igényével, ami csökkentheti az innováció alkalmazása során felszínre kerülő súlyos hibák lehetőségét. „Az ideális eset az lenne, hogy például egy volt katona, aki megjárt háborút, leszerel, elvégez egy egyetemet, és elkezd tervezni, de ez a valóságban nagyon ritkán valósul meg."[44]

Az ipari és gazdasági kémkedés elleni védekezési stratégia kidolgozása során a menedzsmentnek figyelembe kell vennie az információs és kommunikációs technológia fejlődésével járó információbiztonsági kockázatot, a munkavállalók által megtestesített belső, továbbá a külső szereplők jelentette fenyegetést is. A minden tevékenységre kiterjedő, átfogó információvédelmi rendszer megvalósítása a gyakorlatban a kis- és középvállalkozások számára kihívást jelent, és megléte önmagában nem garantálja annak hatékonyságát. Az ipari és gazdasági kémkedés elleni rendszernek magában kell foglalnia a jogosulatlan behatolások elleni és a belső érintettek megfigyelésére alkalmas fizikai infrastruktúrát, a kiberfenyegetések elhárítására alkalmas információtechnológiai biztonsági elemeket (szoftver és hardver), továbbá az információbiztonsági kultúra kialakításának támogatását, amely ösztönzi a szervezeti érintettek tudatos viselkedését, hogy az információ védelme a hétköznapi munkavégzés szerves részévé váljon. Érdemes megfontolni a technológiai fejlődéssel megjelenő új, magasabb szintű védelmet biztosító eszközök alkalmazását, mint a blokklánc-technológia mesterséges intelligenciával támogatva.

Konklúzió

A kontingenciaelmélet megfogalmazása alapján az a szervezet alkalmas a versenyképes és jövedelmező tevékenység folytatására, amely mindenkor hatékonyan tudja belső tényezőit a külső környezeti változókhoz illeszteni, ennélfogva nem lehet előre meghatározni egy stratégiát, amelyet minden szervezet alkalmazhat, hanem a dinamikusan változó, ágazatspecifikus külső tényezőkhöz kell alkalmazkodni. Mivel az elmélet megfogalmazása óta a vállalkozások környezete átalakult és azóta is gyors

[43] Interjúalany 7.
[44] Interjúalany 14.

ütemben változik, a környezeti kontingenciatényezőket folyamatosan figyelni, elemezni és értelmezni szükséges. Az eredmények gyakorlati alkalmazása támogatja a védelmi iparban működő kis- és középvállalkozások menedzsmentjét a külső környezetből érkező hatásokra való hatékony válaszreakció definiálásában.

A védelmi ipar még ki sem heverte a pandémia hatását, amikor elkezdődött az orosz–ukrán háború okozta válsághelyzet. A kialakult helyzetben – figyelembe véve többek között az ellátási problémákat és az energiaválságot – az intenzív kereslet kiszolgálása nehézséget okoz a vállalkozásoknak. Mivel ilyen helyzetre még nem volt példa, a probléma kezelésére nem alakult ki a szükséges kultúra és megfelelő jogi háttér. A vállalkozások a felelősségek alapos definiálása mellett is csak rövidtávú szerződésekkel biztosíthatják, hogy a megrendelések teljesítése ne legyen veszteséges. Az orosz–ukrán fegyveres konfliktus hamar felemésztette Európa védelmi készleteit, amire válaszul a döntéshozók elrendelték az ipar azonnali fejlesztését. Csakhogy ez nem kivitelezhető pár hónap alatt, így a hosszú távú megoldást szolgáló helyi védelmi ipar fejlesztése helyett a probléma enyhítését a védelmi eszközök Európán kívülről való importálásában látták. Ugyanakkor aki ma szövetséges és érdekében áll kiszolgálni, az a jelenlegi instabil geopolitikai környezetben lehet, hogy holnap már ellenség, és nem áll szándékában szállítani, ami súlyos problémákat okozhat. Jelen helyzetben az európai védelmi ipar fejlesztését nagyban támogatná a vállalkozások közötti együttműködések kialakítása, mivel a kis- és középvállalkozások összefogások keretein belül eredményesebben képesek innovációs tevékenységet folytatni. Ellenben a nemzetközi védelmi kooperációk előnyei és a megalakulásokat célzó kezdeményezések mellett is Európa-szerte jellemző, hogy a lokális védelmi iparok nagyrészt nemzeti alapon működnek, korlátozott számú, országhatárokon átnyúló együttműködéssel.[45]

Pár évvel ezelőtt a védelmi ágazat túl kockázatos volt a befektetők számára, ugyanakkor jelen helyzetben egyre több befektetés áramlik az iparba. A könnyebb hozzáférés a finanszírozási forrásokhoz támogathatja a vállalkozásokat, hogy a technológiai fejlődéssel lépést tartva alakítsák az alkalmazott műszaki megoldásokat és gépparkot. A kis- és középvállalkozások jövedelmezően működhetnek, ha tevékenységüket a régóta alkalmazott eszközök hatékonyabbá tételére, részegységek fejlesztésére és gyártására nagyobb vállalatok részére, új technológiák fejlesztésére, vagy egyedi igények megvalósítására fókuszálják. Mindazonáltal fontos, hogy az innovációs tevékenység során a mérnökök kimagasló képességeinek reprezentálásán felül a termék gyakorlati alkalmazhatósága is szempont legyen. A legfőbb innovációs irány a haditechnika területén a közvetlen emberi jelenlét nélkül bevethető eszközök, amelyek célja az emberi áldozatok csökkentése. Szintén kiemelt terület a számítástechnika és az autonóm rendszerek fejlesztése, amelyek a nagy mennyiségű adat feldolgozásával támogatják a döntési folyamatot, azonban a felelősségre vonható ember mindig is kritikus része marad a katonai döntéshozatalnak.

A védelmi kis- és középvállalkozásokat kiemelten fenyegeti az ipari vagy gazdasági kémkedés, mivel jellemzően nem rendelkeznek elegendő pénzügyi és humán tőkével a kritikus információk védelmét biztosító rendszerek megvalósításához. A védelmi

[45] Lásd: https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-smes_en

ipar az egyik legfenyegetettebb szektor az ipari és gazdasági kémkedés szempontjából.[46] A menedzsment kiemelt fontosságú feladatai között szükséges kezelni a minden tevékenységre kiterjedő, átfogó információbiztonsági rendszer megvalósítását és folyamatos frissítését, a fenyegetések fejlődésével párhuzamosan.

A kutatás limitációja, hogy egy folyamatosan változó globális helyzetnek egy pillanatát ragadja meg, és figyelembe véve a bizonytalan környezeti tényezőket, nem alkalmas hosszú távú következtetések levonására. Mivel az interjúk 2022 negyedik és 2023 első negyedévében készültek, az alanyok főként az orosz–ukrán háborúra asszociáltak a kérdések megválaszolása során. A vizsgált probléma komplexitása és interdiszciplináris természete okán bizonyos környezeti tényezők feltáratlanul maradhattak, azonban a szerző törekedett a téma minél szélesebb körű bemutatására. Az eredmények jó alapot biztosítanak a védelmi iparban érvényesülő hatások mélyebb megismerésére és további kutatások folytatására.

Irodalomjegyzék

Abdulwahab Ádám – Pandurics Anett – Ugrai Péter (1997): *Vállalati és vállalatközi integráció*. Budapest: Budapesti Közgazdaságtudományi Egyetem.

Alves, Marcelo Wilson Furlan Matos et al. (2017): Contingency Theory, Climate Change, and Low-carbon Operations Management. *Supply Chain Management: An International Journal,* 22(3), 223–236. Online: https://doi.org/10.1108/SCM-09-2016-0311

Betts, Stephen C. (2003): Contingency Theory: Science Or Technology? *Journal of Business & Economics Research,* 1(18), 123–130. Online: https://doi.org/10.19030/jber.v1i8.3044

Bodoróczki János (2019): A magyar különleges erők – 2035 (2. rész). Biztonságpolitikai, hadseregszervezeti és technológiai kutatások elemzése. *Hadmérnök,* 14(2), 56–73. Online: https://doi.org/10.32567/hm.2019.2.5

Child, John (1981): Culture, Contingency and Capitalism in the Cross-national Study of Organizations. *Research in Organizational Behavior: An Annual Series of Analytical Essays and Critical Reviews,* 3, Amsterdam: Elsevier, 303–356.

Donaldson, Lex (2001): *The Contingency Theory of Organizations.* New York: Sage Publications. Online: https://doi.org/10.4135/9781452229249

Durakovic, Benjamin – Trgo, Erwin (2020): Perspectives and the Role of Bosnian Defense Industry in National Innovation System. *Defense and Security Studies,* 1, 26–33. Online: https://doi.org/10.37868/dss.v1.id145

Engelseth, Per – Kritchanchai, Duangpun (2018): Innovation in Healthcare Services – Creating a Combined Contingency Theory and Ecosystems Approach. *International Conference on Industrial and System Engineering (IConISE)*, 337(012022), 1–8. Denpasar, Bali, Indonesia. Online: https://doi.org/10.1088/1757-899X/337/1/012022

[46] Pellegrino 2015; Kim–Kim 2021: 55–65.

Farkas Ferenc – Balogh Gábor – Rideg András (2015): *Menedzsment alapvetések és funkciók.* Pécs: Pécsi Tudományegyetem.

Galbraith, Jay (1973): *Designing Complex Organizations.* Boston: Addison-Wesley Pub. Co.

Gresov, Christopher (1989): Exploring Fit and Misfit with Multiple Contingencies. *Administrative Science Quarterly,* 34(3), 431–453. Online: https://doi.org/10.2307/2393152

Hamilton, R. T. – Shergill, G. S. (1992): The Relationship Between Strategy-Structure Fit and Financial Performance in New Zealand: Evidence of Generality and Validity with Enhanced Controls. *Journal of Management Studies,* 29(1), 95–113. Online: https://doi.org/10.1111/j.1467-6486.1992.tb00654.x

Hayes, David C. (1977): The Contingency Theory of Managerial Accounting. *The Accounting Review,* 52(1), 22–39.

Hegedűs Ernő – Gyarmati József (2022): A haditechnikai kutatás-fejlesztés helye, szerepe és sajátosságai. *Hadmérnök,* 17(2), 17–32. Online: https://doi.org/10.32567/hm.2022.2.2

Islam, Jesmin – Hu, Hui (2012): A Review of Literature on Contingency Theory in Managerial Accounting. *African Journal of Business Management,* 6(15), 5159–5164. Online: https://doi.org/10.5897/AJBM11.2764

Kim, Se Yong – Kim, Yeek Hyun (2021): A Study on the Understanding of the Analysis of the Future Operational Environment for Smart Defense Innovation and the Application of the ROK MND, 스마트 국방혁신을 위한 미래 작전환경 분석의 이해와 군 적용방안에 대한 고찰. *Journal of Information Technology Services* (한국IT서비스학회지), 20(1), 55–65. Online: https://doi.org/10.9716/KITS.2021.20.1.055

Kleinheksel, A. J. et al. (2020): Demystifying Content Analysis. *American Journal of Pharmaceutical Education,* 84(1), 127–137. Online: https://doi.org/10.5688/ajpe7113

Koronváry Péter – Szegedi Péter – Tóth József (2015): Kutatás és képzés – módszertani felvetések az elvárások és a képzési portfólió összehangolására a repülőműszaki képzésben. *Hadmérnök,* 10(4), 237–246.

Kurç, Çağlar – Neuman, Stephanie G. (2017): Defence Industries in the 21st Century: A Comparative Analysis. *Defence Studies,* 17(3), 219–227. Online: https://doi.org/10.1080/14702436.2017.1350105

Kyngäs, Helvi (2020): Inductive Content Analysis. In Kyngäs, H. – Mikkonen, K. – Kääriäinen, M. (szerk.): *The Application of Content Analysis in Nursing Science Research.* Cham: Springer, 13–21. Online: https://doi.org/10.1007/978-3-030-30199-6_2

Llewellyn, Sue (1994): Managing the Boundary: How Accounting is Implicated in Maintaining the Organization. *Accounting, Auditing & Accountability Journal,* 7(4), 4–23. Online: https://doi.org/10.1108/09513579410069821

Mănescu, Gabriel – Stan, Sebastian-Emanuel (2021): The Influence of Disruptive Technologies on the Preparation of the National Economy and of the Territory for Defense. *International Conference Knowledge-based Organization,* 27(1), 204–209. Online: https://doi.org/10.2478/kbo-2021-0031

Mintzberg, Henry (1979): *The Structuring of Organizations.* London: Pearson.

Morris, Allen (2015): *A Practical Introduction to In-depth Interviewing.* London: Sage Publications. Online: https://doi.org/10.4135/9781473921344

Nagy Andor (2018): Az automatizált tartalomelemzés megvalósíthatósága. *Könyvtári Figyelő,* 1(1), 32–44.

Okun, Olcay – Arun, Korhan (2021): Entrepreneurship and Intrapreneurship as Innovation Source in the Defense Industry and Military. In Ojo, Sanya (szerk.): *Global Perspectives on Military Entrepreneurship and Innovation.* Nigeria: Nigerian Defence Academy, 190–215. Online: https://doi.org/10.4018/978-1-7998-6655-8

Otley, David (2016): The Contingency Theory of Management Accounting and Control: 1980–2014. *Management Accounting Research,* 31, 45–62. Online: https://doi.org/10.1016/j.mar.2016.02.001

Pellegrino, Massimo (2015): *The Threat of State-sponsored Industrial Espionage.* European Union Institute for Security Studies, 1–2. Online: https://doi.org/10.2815/184955

Saldaña, Johnny (2021): *The Coding Manual for Qualitative Researchers.* London: Sage Publications.

Scanlan, Camilla L. (2020): *Preparing for the Unanticipated: Challenges in Conducting Semi-Structured, In-Depth Interviews.* London: Sage Publications. Online: https://doi.org/10.4135/9781529719208

Taksás Balázs (2017): Hadiipari kutatások jelentősége. *Hadmérnök,* 12(3), 167–174.

Tosi, Henry – Slocum, John (1984): Contingency Theory: Some Suggested Directions. *Journal of Management,* 10(1), 9–26. Online: https://doi.org/10.1177/014920638401000103

Wong, Christina W. Y – Lai, Kee-hung – Cheng, T. C. E. (2011): Value of Information Integration to Supply Chain Management: Roles of Internal and External Contingencies. *Journal of Management Information Systems,* 28(3), 161–200. Online: https://doi.org/10.2753/MIS0742-1222280305

HADMÉRNÖK
VÉDELEMINFORMATIKA

18. évfolyam (2023) 3. szám 121–144.
DOI: 10.32567/hm.2023.3.9

Debrecceniné Deák Veronika[1]

Prototípus-implementáció kibervédelmi technikák gyakorlati oktatására

Prototype Implementation of Cybersecurity Techniques for Practical Education

Absztrakt

A kiberbiztonsági gyakorlatok feladata felkészíteni a felhasználókat a kibervédelmi stratégiák aktív és hatékony végrehajtására. Azonban számos jelenleg rendelkezésre álló platform és oktatási anyag alkalmazása szükségessé teszi a mélyebb informatikai ismereteket, így leginkább az IT-biztonság területén végzett szakértők képesek eredményesen ellátni ezeket a feladatokat.
A cél egy olyan oktatási anyag kidolgozása, amelyet akár a közszolgálatban, így például a közigazgatásban, illetve a honvédelemben részt vevő különböző szervezetekben vagy akár a magánszférában is képesek lehetnek alkalmazni olyan foglalkoztatottak továbbképzésére, akik nem rendelkeznek mélyebb informatikai előképzettséggel.
Jelen tanulmány célja a közszolgálati kiberbiztonsági gyakorlati oktatás keretében megvalósított szimulációs keretrendszer működésének definiálása, amelyben a hallgatók kibertámadások segítségével sajátíthatják el a védekezési mechanizmusok végrehajtásához szükséges készségeket, képességeket és ismereteket.

Kulcsszavak: kiberbiztonság, gyakorlati oktatás, szimulációs környezet, kibertámadás

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: deak.veronika@uni-nke.hu

Abstract

The aim of cyber security practices is to prepare employees to execute cybersecurity strategies actively and effectively. However, the use of several currently available platforms and educational materials requires deeper IT knowledge, hence mostly IT security experts are capable of performing these tasks effectively.
The ultimate goal is to develop educational materials that can be used to train employees without deeper IT background, either in various organizations of the public service, such as public administration or defence, or even in the private sector.
The aim of the present paper is to define the operation of a simulation framework implemented in the framework of public service cybersecurity training, in which students can acquire the skills, abilities and knowledge necessary to execute defence mechanisms in case of cyberattacks.

Keywords: cybersecurity, practical education, simulation environment, cyberattack

Bevezetés

A kiberbiztonság szerepe egyre nagyobb teret nyer az infokommunikációs eszközök és technológiák folyamatos fejlődésének köszönhetően. A hackerek sok esetben a felhasználók előtt járnak egy lépéssel, így mindig újabb és újabb kihívásokkal kell megküzdeni, ha biztonságban szeretnénk tudni információinkat és eszközeinket.

Számos, kibertérből érkező támadás veszélyeztetheti a saját infokommunikációs eszközeinket így például hordozható számítógépünket, mobiltelefonunkat, televíziónkat, okosóránkat és egyéb okoseszközeinket. Azonban gyakran tapasztalható, hogy a felhasználók csak felületesen ismerik eszközeik biztonságának összetevőit, valamint a hatékony és eredményes védekezési módszereket. Ebből következik, hogy a kiberbiztonság legnagyobb rizikóját a gyakorlati képességek hiánya okozza, amit már számos tanulmányban rögzítettek. Conklin, Cline és Roosa[2] szerint a kiberbiztonsági oktatás egyik legnagyobb problémája a hallgatók gyakorlati tapasztalatainak hiánya, ami azt eredményezi, hogy az elsajátított készségek nem felelnek meg az ipar igényeinek.

Több kutatás is vizsgálta már a kiberbiztonság oktatásának lehetőségeit, aminek keretében olyan platformokat is kialakítottak, amelyekkel a kibertámadások a gyakorlatban is kipróbálhatók. A probléma azonban sajnos az, hogy a legtöbb felhasználó nem rendelkezik részletes informatikai szaktudással, ami miatt az így átadható tudást nehezen vagy egyáltalán nem képesek felszívni. A meglévő platformok lehetőséget adnak a védelmi stratégiák kipróbálására, azonban olyan jellegű megoldásokat nehéz találni, amelyek elsősorban a védekezésre fókuszálnak.

Emiatt fontos feladat egy olyan gyakorlati képzés kialakítása, ahol a részt vevő hallgatók valós helyzetekben élhetik át a kibertámadásokat, és a védekezésre fókuszálnak úgy, hogy a támadás részletes felépítését, kialakítását, technikai hátterét nem kell ismerni. Egy ilyen gyakorlati képzés kialakítása komplex támadások implementációját

[2] Conklin–Cline–Roosa 2014: 2006–2014.

igényli mind szervezeti szinten (szerverkomponensek, VPN, egyéb perifériák stb.), mind személyes szinten (hordozható laptopok, mobiltelefonok stb.). Ezek alapján a gyakorlati képzést két szinten kell megvalósítani: saját infokommunikációs eszközök védelme, illetve szervezeti szintű rendszerek üzemeltetése és védelme.[3]

Jelen publikációban a saját infokommunikációs eszközök védelmére vonatkozó gyakorlati oktatásra készítettem egy egyszerűsített szimulációs környezetet, amelynek célja mély informatikai tudással nem rendelkező hallgatók kibervédelmi képességeinek fejlesztése és ezek gyakorlása.

Hipotézisek

A fentiek igazolására az alábbi hipotéziseket állítottam fel:

- H1 Szükséges egy olyan szimulációs környezet kidolgozása, amelynek segítségével kibervédelmi technikák gyakorolhatók.
- H2 Szimulálható olyan kibertámadás, amelynek azonosításához és megoldásához nem szükséges mély informatikai tudás.

Kutatásmódszertan

A fentebb említett hipotézisek megválaszolására az alábbi módszereket használtam fel:

A H1 hipotézis igazolására megvizsgáltam a jelenleg publikusan elérhető, kiberbiztonsághoz kapcsolódó platformokat, amelyeken részletes összehasonlító elemzést végeztem, hogy képesek-e kibertámadások szimulálására és ezzel a kibervédelmi képességek fejlesztésére.

A H2 hipotézis esetén kibertámadási forgatókönyveket definiáltam és szimuláltam egy általam kialakított platformon, amelyet mély informatikai tudás nélküli hallgatói csoporton értékeltem ki.

Előzetes technikai és fogalmi áttekintés

Ahhoz, hogy a jelen tanulmányban definiált szimulációs keretrendszer-prototípus minden részletre kiterjedő bemutatása megvalósulhasson, elengedhetetlen a kapcsolódó főbb fogalmak meghatározása.

Kibertámadások

Az első ilyen fogalom a *kibertámadás,* amelynek meghatározására számos definíció létezik. Az Egyesült Államok Kiberparancsnoksága által kiadott lexikon szerint a kibertámadás: számítógép vagy kapcsolódó hálózatok vagy rendszerek segítségével

[3] Deák 2020a: 159–177.

végrehajtott ellenséges cselekedet, amelynek célja egy ellenfél kritikus kiberrendszereinek, eszközeinek vagy funkcióinak megzavarása és/vagy megsemmisítése.[4] Hathaway és szerzőtársai szerint a kibertámadás minden olyan intézkedést magában foglal, amelyet politikai vagy nemzetbiztonsági célok eléréséért, a számítógépes hálózat funkcióinak aláásása érdekében hajtanak végre.[5] Owens meghatározása alapján a kibertámadás olyan szándékos cselekedetek végrehajtása, amelyek célja az ellenfél számítógépes rendszereinek vagy hálózatainak, illetve az ezekben a rendszerekben vagy hálózatokban maradó vagy azokon átmenő információk és/vagy programok megváltoztatása, megzavarása, megtévesztése vagy megsemmisítése.[6] Uma és Padmavathi szerint a kibertámadás a kibertér kiaknázása bizalmas információk megszerzése érdekében, ami magában foglalja például a kémkedést, a hálózatok letiltását, valamint adatok és pénz illetéktelen eltulajdonítását.[7]

A kibertámadások az alkalmazott technikától függően rendkívül sokfélék lehetnek, a teljesség igénye nélkül többek között ide sorolhatók a DoS-, DDoS-támadások, adathalászat, kártékony programok, keylogger programok, jelszavakra irányuló támadások, SQL-injektálás, közbeékelődéses (man-in-the middle) támadások.

A jelen tanulmányban ismertetett prototípusban a szolgáltatásmegtagadásos támadás (DoS), az adathalászat *(phishing)* és a hátsóajtó programok *(backdoor)* alkalmazását mutatom be a gyakorlatban, így ezen fogalmak ismerete is elengedhetetlen.

A DoS (Denial of Service), más néven *szolgáltatásmegtagadással járó támadás* lényege, hogy olyan sok kéréssel támadják meg a hálózatot, vagy azon keresztül valamelyik alkalmazást, amennyit a fogadó oldal már nem tud feldolgozni. Ennek következtében nem lesz elérhető az adott szolgáltatás, mivel nem tud kiszolgálni egyszerre ennyi kérést a szerver.[8] A támadás irányulhat a célpont hálózati kapcsolatának vagy pedig a célpont rendszerében működő valamely – szolgáltatást nyújtó – alkalmazásának túlterhelésére, amelynek során a támadó célja a célpont erőforrásainak lefoglalása.[9]

Az *adathalászat,* más néven phishing lényege abban rejlik, hogy az adathalászok a felhasználókat valamilyen elektronikus csatornán keresztül – például e-mailben, azonnali üzenetben vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában azonban egy hamis weboldalra irányítják, ahol arra kérik őket, hogy adják meg bizalmas adataikat. Az adathalászatnak számos válfaja van, aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra.[10]

A hátsóajtó-alkalmazás *(backdoor)* a felhasználók számára általában nem látható elem, amely a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti

[4] Cartwright 2011.
[5] Hathaway et al. 2012: 817–885.
[6] Owens–Dam–Lin 2009.
[7] Uma–Padmavathi 2013: 390–396.
[8] Fehér 2016.
[9] Gyányi 2007.
[10] Muha–Krasznay 2018.

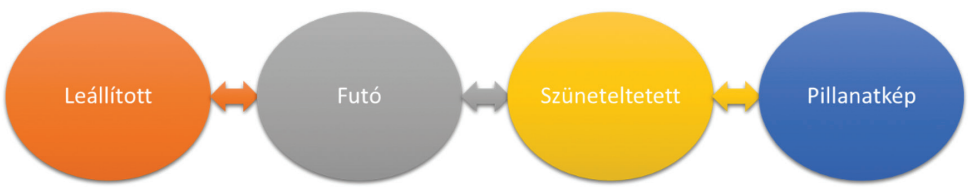
a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nemcsak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti.[11]

Virtualizáció

A *virtualizáció* több számítógép szimulációja egy hardverkonfiguráción, vagyis hardverek emulációja szoftveres környezetben. Ez lehetővé teszi egy eszköz erőforrásainak felosztását több környezet között. A virtualizáció céljai közé tartozik a meglévő erőforrások kihasználtságának maximalizálása, az IT-szolgáltatások rugalmasságának fejlesztése, a rendszerek biztonságának növelése és a leállások szükséges idejének csökkentése, valamint a meglévő rendszerek kezelésének egyszerűsítése, költségeinek csökkentése.[12]

A virtualizációt csoportosíthatjuk például aszerint, hogy a fizikai eszközöktől milyen szinten választják el a rendszert. Jelen tanulmányban a prototípus elkészítése szempontjából releváns virtualizációtípus az operációs rendszer virtualizációja. Amikor operációs rendszert virtualizálunk, általában egy gazda *(host)* operációs rendszeren futtatunk egy vagy több vendég *(guest)* operációs rendszert.[13]

Egy virtuális gép állapotait, általános struktúráját szemlélteti az 1. ábra, illetve látható, hogy mely állapotokból mely állapotokba lehet jutni. A virtuális gépeket először is leállított formában hozzuk létre. A leállított virtuális gépet el lehet indítani, aminek hatására futó állapotba kerül. A futó állapotban természetesen a virtuális gép leállítható, illetve szüneteltethető. A szüneteltethető állapotban a virtuális gép nem áll le, csak felfüggesztjük a működését, és elmentjük a memória tartalmát. A szüneteltetésből azonnal folytatható a működés, ekkor futó állapotba kerül, illetve a szüneteltetett állapotban pillanatkép készíthető. A pillanatképből a virtuális gép automatikusan elindítható úgy, hogy a szüneteltetett állapotba kerül.



1. ábra: Virtuális gépek állapotai
Forrás: a szerző szerkesztése

[11] Deák 2019: 256–271.
[12] Varga 2010.
[13] Varga 2010.

Kibergyakorlatok csoportosítása

A gyakorlati kiberbiztonsági ismeretek átadására már számos technológia áll rendelkezésünkre. Fő szempont, amely megkülönbözteti őket egymástól, hogy a támadók és a védekezők aktív vagy passzív szerepet vállalnak a kibergyakorlatokban. Ezek alapján az alábbi típusokat különböztethetjük meg:

- *aktív-aktív:* a támadó és a védekező oldalt is valós személy képviseli, avagy valós személy irányítja a támadást, illetve a védekezést (Elsősorban csapatjátékok, ahol az egyik csapat megpróbálja feltörni a másik csapat rendszerét, miközben a másik csapat védekezik. Ilyen például a Capture the Flag, Red-Blue Team gyakorlatok.);
- *aktív-passzív:* az áldozat egy passzív rendszer, míg a gyakorlat során a hallgatóknak kell a támadó szerepét megszemélyesíteni annak érdekében, hogy az áldozat infrastruktúra gyenge pontjait felderítve adatokat szerezzen meg;
- *passzív-aktív:* a támadó egy passzív rendszer, amely előre beállított támadási szekvenciát játszik le automatizáltan, külső felügyelet nélkül, míg a hallgatóknak az áldozat szerepét kell megvalósítaniuk, amelynek során fel kell ismerniük az aktuális támadásokat, és azokat meg kell akadályozniuk, helyre kell állítaniuk és reagálniuk kell a már bekövetkezett eseményekre;
- *passzív-passzív:* elsősorban tesztelési célból, illetve kibertámadások szemléltetésére alkalmazzák, valamint többek között olyan automatizált kibervédelmi rendszerek tesztelésére, amelyeknek célja helyettesíteni, kiváltani az áldozatot, ezáltal külső felügyelet nélkül megakadályozni a kibertámadásokat;
- *általános:* olyan kiberbiztonsági gyakorlatok végrehajtására alkalmas platformok, amelyeken az előbb felsorolt típusok bármelyike megvalósítható. Legtöbb esetben hálózatok és számítógépek emulálását végzik, amelyen keresztül tetszőleges kibergyakorlat szimulálható;
- *egyéb:* olyan kiberbiztonsági gyakorlatok, amelyek az előző kategóriákba nem sorolhatók, de szorosan kapcsolódnak a kibergyakorlatokhoz és a kiberbiztonsági ismeretek gyakorlati oktatásához, így különösen társasjátékok, számítógépes játékok.

Publikusan elérhető kiberbiztonsági platformok összehasonlítása

A H1 hipotézis vizsgálatához szükséges áttekinteni az aktuálisan publikusan elérhető kiberbiztonsági gyakorlatokhoz használható platformokat, amelyeket a korábban bevezetett csoportosítás alapján mutatok be. Az 1. táblázat szemlélteti kategóriánként a rendelkezésre álló releváns technológiákat, platformokat és azok jellemzőit.

1. táblázat: Kiberbiztonsági platformok összehasonlítása

Technológia	Kategória	Elérhetőség	Célközönség	Telepítés
KYPO	aktív-aktív	online	akadémia/kutatás	×
CDX	aktív-aktív	offline	hallgatók/szakértők	×
Emulab	általános	offline	akadémia/kutatás	komplex
Cytrone	általános	offline	akadémia/kutatás	komplex
Leaf	általános	offline	hallgatók/szakértők	komplex
Cyber-Physical Security Testbed	általános	offline	hallgatók/szakértők	komplex
VulnHub	aktív-passzív	offline	hallgatók/szakértők	szabadkéz
TryHackMe	aktív-passzív	online	hallgatók/szakértők	×
WebGoat	passzív-aktív	online	hallgatók/szakértők	×
Metasploitable	aktív-passzív	offline	hallgatók/szakértők	szabadkéz
Blackjack	passzív-passzív	offline	hallgatók/szakértők	komplex
ACD	passzív-passzív	offline	hallgatók/szakértők	komplex
Cyber Defence Tower Game	egyéb	offline	gyerekek	egyszerű
Riskio	egyéb	offline	gyerekek	×

Forrás: a szerző szerkesztése

Kategória

A feldolgozott technológiákat, eszközöket több csoportba lehet sorolni aszerint, hogy a kibergyakorlatok korábban nevesített osztályozása alapján melyik csoportba oszthatók.

Az Emulab, a Cytrone, a Leaf és a Cyber Security Testbed általános platformokat definiálnak. Az Emulab[14] egy olyan rugalmas felépítésű gyakorlati kurzus, amely során valódi hackertámadások végrehajtásával mutatják be a kibertámadások egyes módszereit, ami irányítható környezetet biztosít a támadó és védekező kiberbiztonsági kísérletek előkészítésére és mérésére. A Cytrone[15] nevű integrált kiberbiztonsági képzési keretrendszer magában foglalja a támadásorientált, az elemzésorientált, valamint a védelemorientált képzést. Ennek keretében speciálisan erre a célra létrehozott képzési környezetben végrehajtható gyakorlati feladatokat biztosítanak a hallgatók számára. A keretrendszer elemei közé sorolhatók a következők: a felhasználói felület, a képzési adatbázis, a menedzsmentmodul, lehetséges további hozzáadható modulok, valamint a szerverek és hálózati eszközök infrastruktúrája. A Leaf[16] kiberinfrastruktúrák szimulálására, valósághű IoT-forgatókönyvek reprodukálására és versenyképes kiberbiztonsági tréningek végrehajtására szolgáló nyílt forráskódú platform. A Cyber

[14] Kuo et al. 2018: 2245–2258.
[15] Beuran et al. 2017: 157–166.
[16] Ficco–Palmieri 2019: 107–129.

Security Testbed[17] egy kiberfizikai biztonsági platform, amely alkalmas kibertámadások szimulálására és kiértékelésére, valamint a segítségével végrehajtott behatolástesztek által feltárhatók az elektromos hálózatokra irányuló kibertámadások következményei és hatásai.

A KYPO és a CDX elsősorban olyan környezetet határoznak meg, ahol Capture The Flag jellegű feladatok hajthatók végre, vagyis mind a támadó, mind a védekező félnek aktívnak kell lennie. A KYPO[18] egy kibergyakorlati és kutatási platform, amely komplex számítógépes rendszerek és hálózatok modellezésére és szimulálására összpontosít. A platform virtualizált környezetet biztosít előre meghatározott forgatókönyv szerinti, komplex kibernetikai támadások végrehajtásához egy szimulált kritikus infrastruktúra ellen. A CDX[19] gyakorlat sajátossága, hogy a részt vevő csapatoknak saját magunknak kell kialakítani hálózatukat, azon elvégezni a biztonsági beállításokat, amit a támadás külső fél általi végrehajtása követ. A biztonsági kihívások megértése és az incidensekre való reagálás, valamint a csapatmunkával kapcsolatos készségek fejlesztése egyaránt célja a gyakorlatnak.[20]

A Vulnhub,[21] a TryHackMe[22] és a Metasploitable[23] elsősorban a támadó felek számára biztosítanak lehetőséget a fejlődésre (aktív-passzív), míg a WebGoat[24] alkalmazás elsősorban védekezésorientált (passzív-aktív).

Automatizált kibervédelemmel kapcsolatos technológiák a Blackjack,[25] illetve az ACD,[26] amelyek célja, hogy emberi beavatkozás nélkül képesek legyenek a támadások elhárítására, emiatt ők a passzív-passzív kategóriába sorolhatók.

Végül a Cyber Defence Tower Game[27] egy egyszerű számítógépes Tower Defense játék, míg a Riskio[28] egy társas táblajáték, amelyek inkább kedvcsináló és ösztönző eszközök lehetnek az oktatásban, mintsem konkrét tudásátadásra használható technológiák.

Elérhetőség

A technológiák kiválasztásánál fontos szempont lehet az is, hogy a felhasználó képes-e internetelérés nélkül is használni a technológiát. Ez alapján a kapcsolódó munkák lehetnek

- *online elérhetők,* vagyis internethálózatra van szükség ahhoz, hogy a feladatokat megoldják,

[17] Hong et al. 2015.
[18] Čeleda et al. 2015.
[19] Schepens–James 2003: 4300–4305.
[20] Szabó 2018: 286–301.
[21] Lásd: www.vulnhub.com
[22] Lásd: https://tryhackme.com
[23] Kennedy et al. 2011.
[24] Lásd: https://owasp.org/www-project-webgoat
[25] Heckman et al. 2013: 72–77.
[26] Herring–Willett 2014: 46–55.
[27] Jin et al. 2018: 68–73.
[28] Hart et al. 2020.

- *offline elérhetők,* vagyis nem szükséges az internethálózat, a felhasználó a saját lokális számítógépén is előállíthatja a környezetet.

Míg a KYPO, a TryHackMe és a WebGoat esetében szükséges az internetelérés, addig a többi esetben offline elérhető technológiákról beszélhetünk.

Célközönség

A különböző technológiák különböző célközönséget szólítanak meg. Ez alapján az alábbiak lehetnek:

- *akadémia/kutatás:* elsősorban az akadémiai életben használják a technológiát, leginkább prototípus szinten, mintsem termékként. Az elért eredményeket pedig kutatási célokra is felhasználják.
- *hallgatók/szakértők:* olyan kiforrott maga a technológia, hogy arra már termékként is tekinthetünk, amelyeken szervezett oktatás zajlik kiberbiztonsági szakértők számára, akik már jártasak az informatikai ismeretekben is.
- *gyerekek:* azok a technológiák, amelyek elsősorban figyelemfelhívásra, a tudatosság növelésére, esetleg kedvcsinálásra és motiválásra alkalmasak.

A KYPO, a Cytrone és az Emulab rendszer elsősorban akadémiai célból készült, míg a Riskio, valamint a Cyber Defence Tower Game a biztonságtudatosság növelését célozza minden korosztály számára. A többi technológia a célcsoportot tekintve a szakértők kategóriába sorolható, vagyis mély informatikai tudással rendelkező, önmagukat képezni kívánó szakembereket szólít meg.

Telepítés

A vizsgált technológiák kategorizálhatók aszerint, hogy a kibergyakorlatok során alkalmazott technológiák telepítése hogyan történik:

- *komplex*: amely során komplex rendszereket, többféle alkalmazást, programot szükséges telepíteni, továbbá számos beállítás, virtualizáció indokolt;
- *szabadkéz*: nincs meghatározva, hogy mit kell telepítenie a felhasználónak, egy virtuális gépet kap, amelyet szabadon felhasználhat;
- *egyszerű*: a telepítéshez nem szükséges mélyebb informatikai tudás.

A Vulnhub és a Metasploit nem definiál részletes környezetet a gyakorlatok elvégzéséhez, mindössze egy-egy virtuális gépet kell letöltenie a felhasználónak, amelyet oly módon használ, ahogyan csak szeretne. Az Emulab, a Cytrone, a Leaf és a Cyber-Physical Security Testbed esetén egy teljes architektúrát kell előállítani különböző programok segítségével, amelyhez bár részletes leírás tartozik, mégis komplex műveletnek tekinthető. Végül a Cyber Tower Defence Game esetében egy egyszerű programról van szó, amelyet a számítógépünkre kell telepíteni. A többi technológiához kapcsolódóan nincs szükség telepítés elvégzésére.

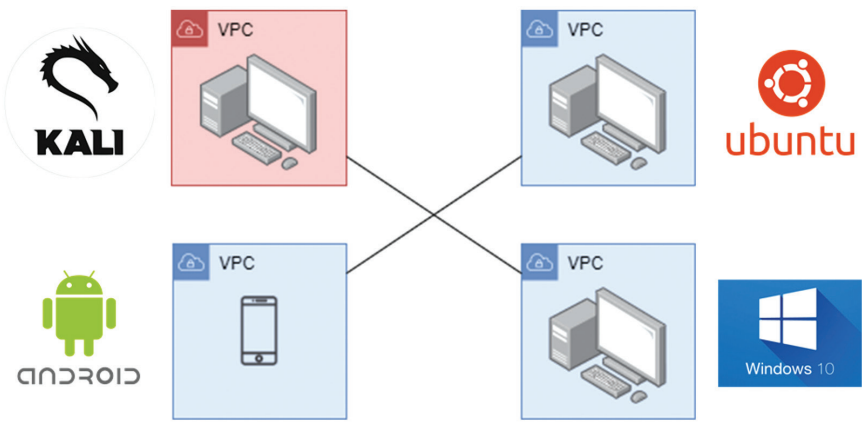
Következtetések

A bemutatott összehasonlítás alapján a H1 hipotézist érdemes tovább pontosítani a fejezetben meghatározott kategóriák mentén. Ezek alapján a H1 hipotézist az alábbiak szerint módosítom: Szükséges egy olyan *passzív-aktív, offline, hallgatók számára elérhető* szimulációs környezet kidolgozása, amelynek segítségével kibervédelmi technikák gyakorolhatók.

A részletes összehasonlítás alapján megállapítható, hogy jelenleg nem elérhető olyan kibervédelmi platform, amely támogatja a H1 módosított hipotézisben megfogalmazott tulajdonságokat. Ezek alapján a *H1 hipotézist bizonyítottnak* tekintem.

Egyszerűsített szimulációs környezet

A H2 hipotézis vizsgálatához létrehoztam egy egyszerűsített szimulációs környezetet, amely megfelel a H1 hipotézisben meghatározottaknak, vagyis képes a passzív-aktív végrehajtásra, elérhető offline módon, és a hallgatók számára is könnyen biztosítható. Az egyszerűsített környezet architektúráját a 2. ábra szemlélteti.



2. ábra: Szimulációs hálózat
Forrás: a szerző szerkesztése

Infrastruktúra

Az infrastruktúra összesen négy komponensből épül fel, amelynek célja egy támadó komponens, illetve több infokommunikációs eszköz szimulálása, amit a közszolgálatban dolgozó emberek is használhatnak a mindennapjaik során. Minden komponens egy-egy virtuális gép, amelyekre különböző operációs rendszereket telepítettem.

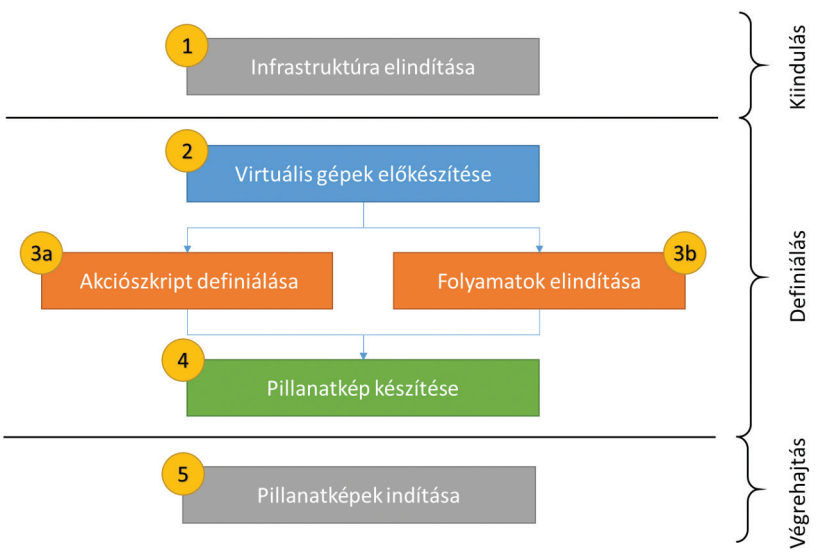
- Kali Linux: Sérülékenységvizsgálatra és behatolástesztelésre kialakított Linux-disztribúció. Olyan alkalmazásokat és eszközöket tartalmaz előre telepített

formában, amelyek segítségével etikus támadások indíthatók a hálózatban található eszközök ellen.
- Ubuntu: Az egyik legszélesebb körben használt Linux-alapú operációs rendszer. Fő erőssége, hogy a mindennapokban szükséges feladatok elvégzéséhez is található rajta megfelelő alkalmazás. A kiválasztás oka, hogy sok szervezeten belül gyakran találkozhatunk Linux-/Unix-alapú operációs rendszerekkel.
- Windows: A legelterjedtebb operációs rendszer személyi számítógépekre, amelyet egyetemek, vállalatok és (közszolgálati) szervezetek is előszeretettel használnak.
- Android: Az egyik legelterjedtebb mobil operációs rendszer, amely megtalálható mobiltelefonokon, tableteken és egyéb infokommunikációs eszközökön egyaránt.

Az összes virtuális komponenst egyetlen hálózatra csatlakoztattam, amelyen keresztül képesek egymással kommunikálni. Minden komponensnek fix hálózati címet állítottam be (IP-cím), ezáltal minden egyes újraindítás során ugyanazon a címen érhetők el.

Támadás meghatározása és végrehajtása

A definiált infrastruktúrán felvehetők, rögzíthetők és végrehajthatók kibertámadások a komponensek között. A támadó fél minden esetben a Kali Linuxszal rendelkező virtuális gép volt. A támadás meghatározásához a 3. ábra szerinti feladatokat kell elvégezni. A meghatározás során elsődleges cél, hogy a támadás elmenthető és automatizáltan újra végrehajtható legyen.



3. ábra: Támadás szimulációjának előkészítése
Forrás: a szerző szerkesztése

A támadás szimulációjának előkészítése három szakaszból áll. A kiindulás szakaszában kerül sor első lépésként az *infrastruktúra elindítására,* ami mindössze annyit jelent, hogy azokat a virtuális gépeket, amelyeknek szerepük lesz a szimuláció során, elindítjuk.

A definiálás folyamat során a virtuális gépeket úgy módosítjuk, hogy a kibertámadás végrehajtható legyen. Ezek a módosítások magukban foglalják a virtuális gépek előkészítését, az akciószkript definiálását és a támadáshoz kapcsolódó folyamatok elindítását.

A *virtuális gépek előkészítése* során az egyes virtuális gépeken elvégezzük a szükséges támadásspecifikus módosításokat, beállításokat. Ha szükséges, ezek érvényre juttatásához újraindítjuk őket.

A következő lépést jelentősen meghatározza, hogy a támadás komplex, több lépésből álló szekvenciális folyamat (3a), vagy folyamatos támadás lesz (3b), amelyekhez olyan szolgáltatásokat kell elindítani, amelyek megállás nélkül futhatnak.

A szekvenciális folyamat során *akciószkript deifinálása* indokolt, ilyenkor lépések sorozatát írjuk le. Az egyik lépés felhasználhatja az előző lépés kimenetét, de minden esetben, minden lépés befejeződik a támadás végrehajtása során. A támadás lépései shell szkript[29] segítségével definiálhatók a Kali Linuxot kiszolgáló virtuális gépen, amit az asztalon található *start.sh* fájlban kell eltárolni. Ennek a fájlnak sajátossága, hogy hozzáadtam a *crontable* konfigurációhoz, emiatt minden újraindításkor automatikusan végrehajtódik a fájl tartalma. Ha a szkript írása befejeződött, és elmentettük, akkor a gépet állítsuk le, továbbá a többi komponenst is leállíthatjuk.

Folyamatos támadás esetén kerül sor a *folyamatok elindítására,* amely során a támadáshoz kapcsolódó szolgáltatásokat kell elindítani, amelyek folyamatosan futni fognak a támadás során. Ebben az esetben a virtuális gépeket nem állítjuk le, csak szüneteltetjük. (Természetesen ez a fajta folyamat is megoldható lenne a 3a lépéssel, azonban ebben az esetben nincs szükség a szkript megírására, ezáltal sokkal gyorsabb és a könnyebb a támadás definiálása.)

Az eddig bemutatott lépésekkel sikeresen elindíthatók a támadások, azonban a cél, hogy ezek a támadások könnyen hordozhatók és újra végrehajthatók legyenek. Emiatt szükséges a folyamat utolsó lépése. Mivel a virtuális gépeken módosításokat hajtottunk végre, pillanatképeket kell készíteni róluk. A pillanatkép készítésének célja, hogy a számítógépet abba az állapotba töltsük vissza, amikor a kibertámadás éppen zajlott. Minden elindított komponens esetén azonos nevet adtam a pillanatképeknek, hogy könnyen azonosítható legyen, mely támadáshoz mely pillanatkép tartozik.

Utolsó lépésként a támadások szimulálásához az előzőekben ismertetett módon elkészített *pillanatképeket* kell *elindítani.* Ez a jelenlegi implementációban manuálisan történt meg, de a virtuális gépek automatikusan is indíthatók.

Kibertámadások szimulációja

A szimulációs környezetbe három korábban ismertetett kibertámadási típust implementáltam a szolgáltatásmegtagadásos támadás *(DoS),* az adathalászat *(phishing)*

[29] Garrels 2004.

és a hátsóajtó programok *(backdoor)*. Ezeket úgy alakítottam ki, hogy különböző infokommunikációs eszközökön, operációs rendszereken lehessen szimulálni.

Minden egyes támadás leírása során a következő felosztást alkalmazom:

1. Támadó gép beállítása: bemutatja, hogy melyek azok a fontosabb lépések, amelyeket a támadó gépen elvégeztem a támadás szimulációjához.
2. Áldozat gép beállítása: bemutatja, hogy melyek azok a fontosabb beállítások, amelyeket az áldozat eszközén végrehajtottam annak érdekében, hogy a támadás sikeres legyen.
3. Támadás érzékelése: bemutatja, hogy az áldozat/támadó mit tapasztal a támadás során.
4. Megszerezhető tudás: bemutatja, hogy mi az a tudáshalmaz, amelyet a szimuláció során az áldozat megismerhet.

Szolgáltatásmegtagadásos támadás (DoS)

Támadó gép beállítása

A DoS-támadáshoz a Kali Linuxon előretelepített *hping3*[30] alkalmazást használtam az alábbi paraméterezéssel:

```
hping3 10.0.2.5 –icmp –flood
```

A kiadott parancs hatására a támadó gép a hálózaton található 10.0.2.5 IP-címmel rendelkező eszközt szólítja meg az úgynevezett Internet Control Message Protocol[31] (ICMP) protokollban meghatározott kérésekkel. A támadógép pillanatképét akkor készítettem el, amikor a parancsot kiadtam. Ezáltal újraindítás után a kiadott parancs fog futni.

Áldozat gép beállítása

A DoS-támadáshoz kapcsolódóan a Windows operációs rendszerrel rendelkező virtuális gépet választottam. A Windows alapértelmezetten nem reagál az ICMP-kérésekre, ezért módosítottam a tűzfalat úgy, hogy egy olyan bemenő szabályt vettem fel, amely engedélyezi az ICMP-kérésekre való válaszadást (4. ábra). Az áldozat pillanatképét a szabály aktiválása után kikapcsolt állapotban készítettem el.

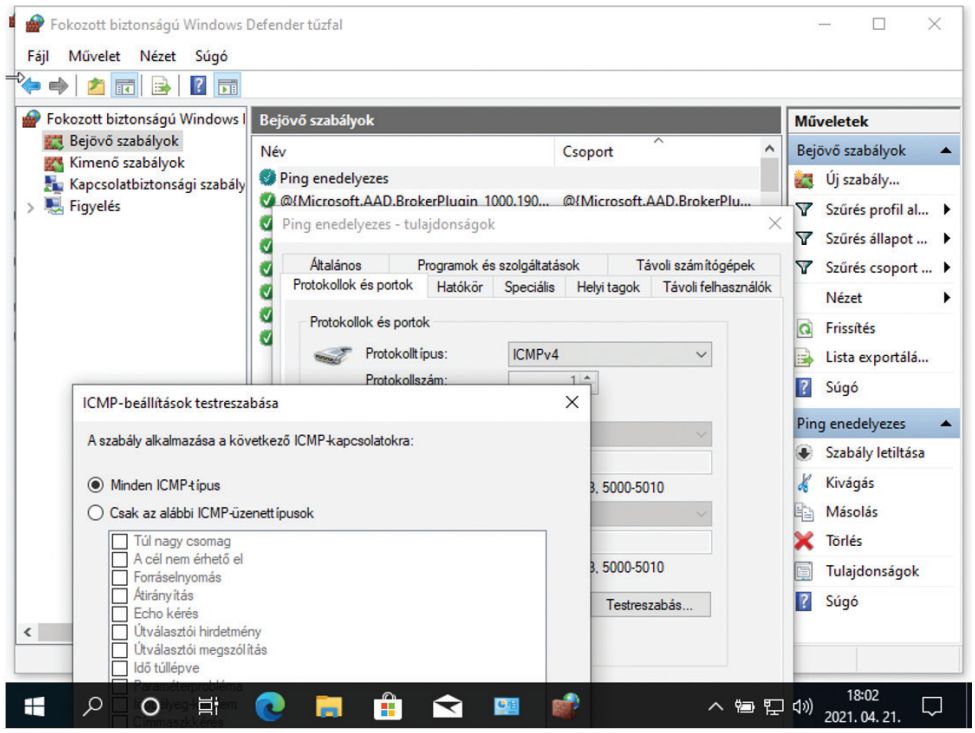
Támadás érzékelése

A szimulációs környezet elindítása után, amikor az áldozat gépe csatlakozik a hálózathoz, teljes mértékben használhatatlanná válik a rengeteg kérés kiszolgálása miatt. Elsősorban a processzor lesz túlterhelve, ami miatt az áldozat nem képes a rendszert használni.

[30] hping3, Kali Tools, https://tools.kali.org/information-gathering/hping3
[31] ICMP, IETF Standards, https://tools.ietf.org/html/rfc792

Megszerezhető tudás

Az áldozat ebben a szimulációban szembesül azzal, hogy fizikai beavatkozásra is szükség van ahhoz, hogy egy kibertámadást elhárítson, hiszen a hálózati kábelt ki kell húznia a gépből (esetleg a routert le kell állítani). Ezenkívül megismerkedik az áldozat a Windows tűzfal beállításaival és képes lesz értelmezni a bejövő és kimenő szabályokat.



4. ábra: Windows tűzfal szabályok beállítása
Forrás: a szerző szerkesztése

Adathalászat (phishing)

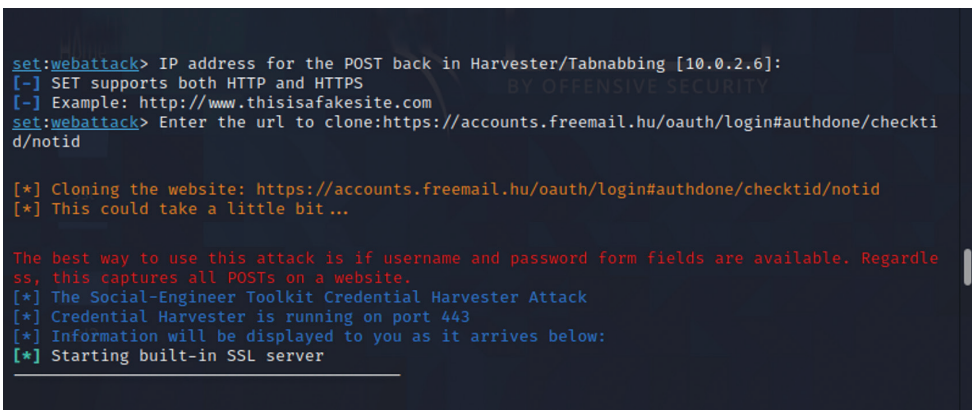
Támadó gép beállítása

Ehhez a támadáshoz a Kali Linuxon lévő *SEToolkit* csomagjában található *credential harvester* alkalmazást használtam, annak érdekében, hogy lemásoljam a https://freemail.hu levelező oldal bejelentkező felületét és megszerezzem az áldozat e-mail-címét és jelszavát. A beállítás során engedélyeztem a biztonságos *https*

kapcsolatot, amihez az *openssl* alkalmazás segítségével létrehoztam egy tanúsítványt is. Ennek célja, hogy a felhasználóval elhitessük, hogy egy biztonságos weboldalra látogat.

A pillanatkép elkészítéséhez két fontos alkalmazásnak kellett futnia:

- Egy egyszerű webszerver fut abban a mappában, amelyben megtalálható az a tanúsítvány, amelyet a kliensnek telepítenie kell a böngészőben.
- python2 -m SimpleHTTPServer 80
- A credential harvester fut, vagyis várja, hogy az áldozat meglátogassa a támadó által klónozott weboldalt (5. ábra).



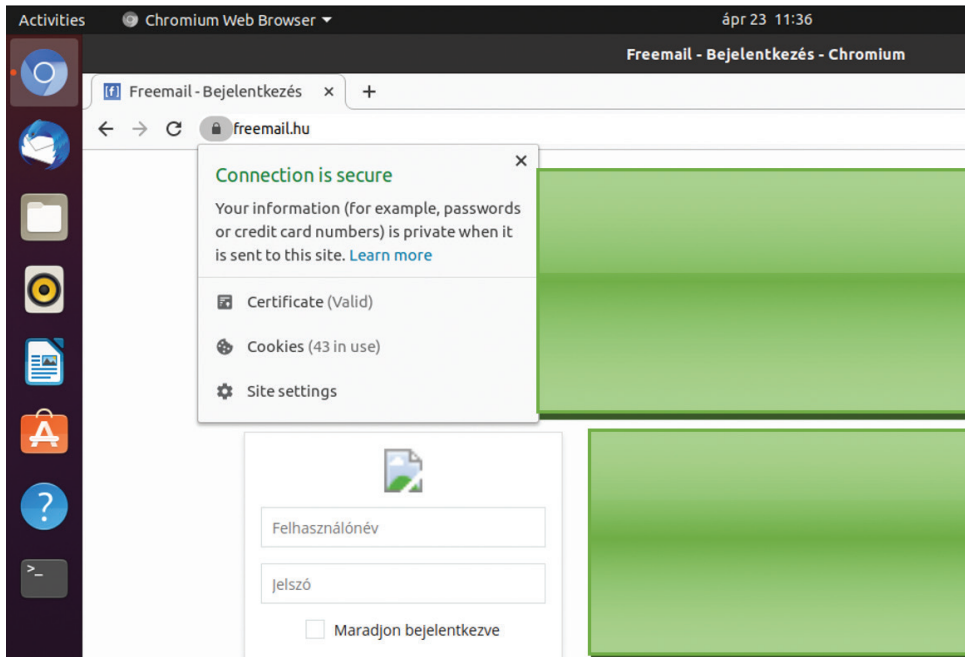
5. ábra: A támadó gép várakozik, hogy valaki meglátogassa az áloldalt
Forrás: a szerző szerkesztése

Áldozat gép beállítása

Az áldozat gépe jelen támadás során az Ubuntu operációs rendszerrel rendelkező virtuális gép, amelyen az előkészület során két fontos módosítást kellett végrehajtani. Először is az alapértelmezett böngészőn keresztül letöltöttem és telepítettem a megfelelő tanúsítványt úgy, hogy az engedélyezze a támadó gépen lévő oldallal való biztonságos kommunikációt. Majd az */etc/hosts* fájlhoz kellett felvennem az alábbi sort:

10.0.2.4 freemail.hu

Ennek segítségével a támadó által előállított weboldal az ismert domaincímen keresztül is elérhető, ahogy azt a 6. ábra is mutatja:



6. ábra: A kliensoldalon biztonságosnak tűnő megtévesztő oldal
Forrás: a szerző szerkesztése

Támadás érzékelése

A felhasználó megpróbál belépni az e-mail-fiókjába, beírja felhasználónevét és jelszavát, azonban az oldal elsőre újratöltődik, viszont másodjára sikeresen be lehet jelentkezni az e-mail-fiókba. A támadás észlelését korlátozza, hogy a kommunikáció biztonságos, mivel a megfelelő tanúsítványok rendelkezésre állnak. Azonban a weboldalhoz kapcsolódó domainnévhez tartozó IP-cím lekérdezésével láthatóvá válik, hogy a hálózaton belüli szerverhez kapcsolódik a felhasználó, amiből már sejthető, hogy támadás érte.

Fontos feladat az áldozat számára megmutatni a támadó felhasználói felületét és jelezni, hogy ténylegesen megkapja a támadó a beírt adatokat, hiszen ennek segítségével még valóságosabbá válik a támadás (7. ábra).

```
10.0.2.4 - - [22/Apr/2021 22:17:00] "GET / HTTP/1.1" 200 -
10.0.2.4 - - [22/Apr/2021 22:17:01] "GET /fng-static/images/cbn.svg HTTP/1.1" 404 -
10.0.2.4 - - [22/Apr/2021 22:17:01] "GET /fng-static/images/logo.svg HTTP/1.1" 404 -
10.0.2.4 - - [22/Apr/2021 22:20:49] "GET / HTTP/1.1" 200 -
10.0.2.4 - - [22/Apr/2021 22:20:51] "GET /fng-static/images/cbn.svg HTTP/1.1" 404 -
10.0.2.4 - - [22/Apr/2021 22:20:51] "GET /fng-static/images/logo.svg HTTP/1.1" 404 -
10.0.2.4 - - [22/Apr/2021 22:20:51] "GET /loader.gif HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=teszt.elek
POSSIBLE PASSWORD FIELD FOUND: password=AzÂnJelszavam11#
POSSIBLE USERNAME FIELD FOUND: loginBtn=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

7. ábra: A támadó sikeresen ellopta az adatokat
Forrás: a szerző szerkesztése

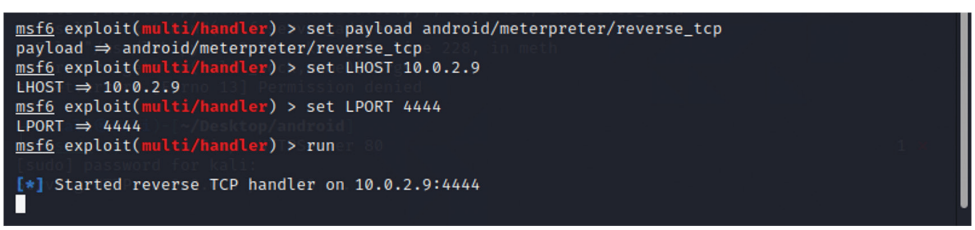
Megszerezhető tudás
Az áldozat megismerkedik a tanúsítványok *(certificate)* szerkezetével és jellemzőivel, a böngészők limitációival, illetve az SSL-kapcsolat jelentésével. Ezenkívül a DNS szerverek alapjaival, a domainnév feloldásával, illetve az operációs rendszerek *hosts* fájljával.

Hátsóajtó program (Backdoor)

Támadó gép beállítása
A Kali Linuxon található *metasploit* keretrendszer segítségével lehetőség van olyan androidos telepítő alkalmazás létrehozására, amely egy hátsó kaput nyit azon az androidos eszközön, amely telepíti az így létrehozott alkalmazást. Az alkalmazást az alábbi paranccsal lehet létrehozni, ahol azt az IP-címet és portot kell megadni, amelyen a támadó gép figyelni fog, és várni fogja, hogy az áldozat elindítsa az alkalmazást:

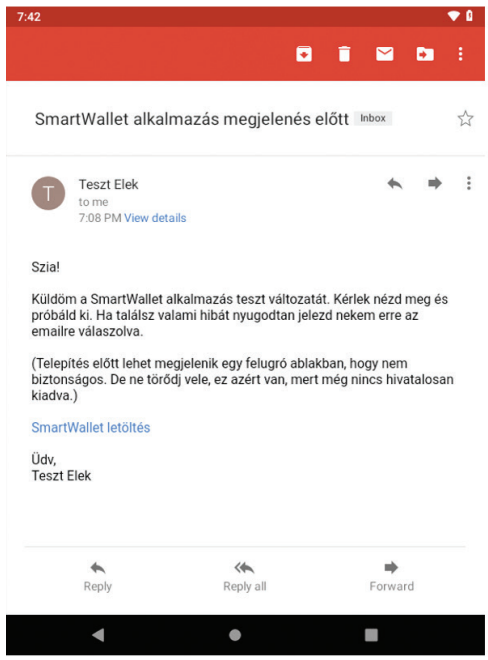
```
msfvenom -p android/meterpreter/reverse_tcp
        LHOST=10.0.2.4 LPORT=4444 R
```

Az alkalmazás elkészülte után el kell indítani a várakozást, amihez a *metasploit* keretrendszer *exploit/multi/handler* alkalmazását szükséges elindítani megfelelő paraméterezéssel (8. ábra). Végül ahhoz, hogy az áldozathoz is eljusson a kívánt telepítő, egy üzenetet küldtem az áldozat e-mail-címére a letöltő linkkel együtt (9. ábra).

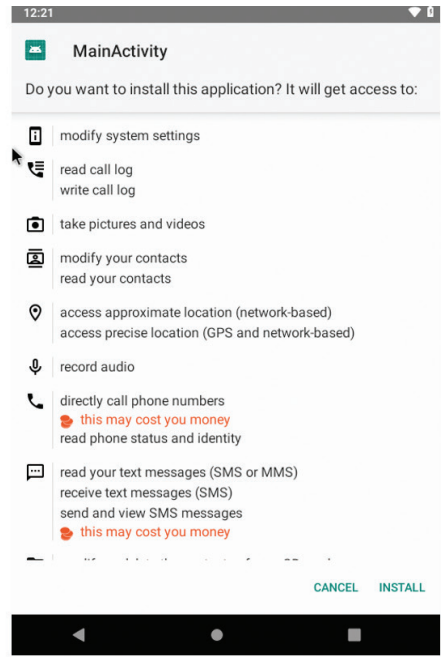


8. ábra: A támadó gép várakozik backdoor indítására
Forrás: a szerző szerkesztése

Áldozat gép beállítása
Az áldozat gépe az Android operációs rendszert futtató virtuális gép, amely megszemélyesíthet mobiltelefont, tabletet, tv-t vagy bármilyen egyéb okoseszközt. Az áldozat gépén engedélyezni kellett az ismeretlen alkalmazások telepítését a Google Chrome alkalmazásból, aminek hatására az áldozat képes telepíteni olyan alkalmazásokat, amelyeket nem a hitelesített Play Áruházból tölt le.



9. ábra: Megtévesztő e-mail
Forrás: a szerző szerkesztése

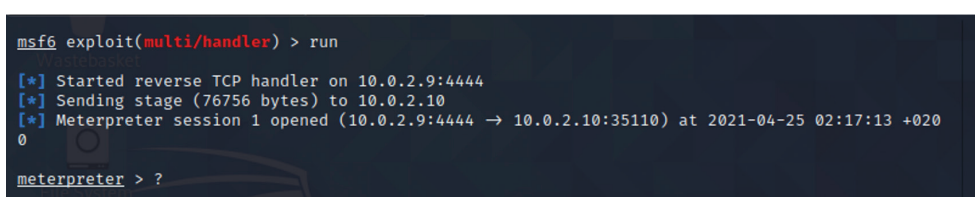


10. ábra: Alkalmazás telepítése
Forrás: a szerző szerkesztése

Támadás érzékelése

A támadás érzékeléséhez az áldozatnak telepítenie kell a létrehozott alkalmazást (10. ábra). Ahhoz, hogy az áldozat lássa, milyen hatása lehet annak, ha egy ilyen alkalmazást telepít, érdemes megmutatni neki a támadó terminálját (11. ábra), amelyen keresztül néhány parancs beírásával könnyedén szembesülhet azzal, hogy mi minden elérhető távolról. A teljesség igénye nélkül az alábbi parancsokat lehet érdemes megmutatni:

- *dump_sms*: az összes sms letöltése a támadó gépére;
- *dump_contacts*: az összes névjegy letöltése a támadó gépére;
- *webcam_stream*: a kamera képének továbbítása a támadó gépére;
- *geolocation*: a telefon helyzetének elküldése a támadó gépére.



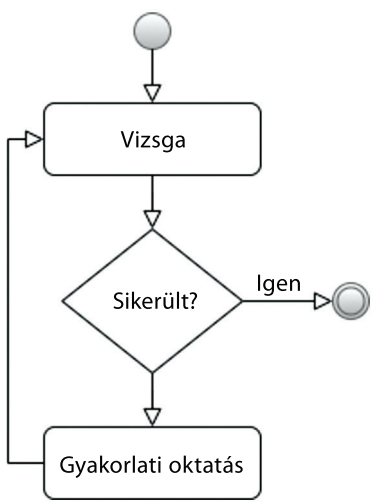
11. ábra: A backdoor aktivizálódott a támadó gépén
Forrás: a szerző szerkesztése

Megszerezhető tudás
Az áldozat szembesül a megtévesztő e-mailek céljával és legfőbb típusával, az Androidhoz kapcsolódó telepítőfájlokkal és beállításokkal, a Play Protect alkalmazás fontosságával.

Kiértékelés

A kiértékelést úgy folytattam le, hogy egy előre kiválasztott, mély informatikai tudással nem rendelkező felhasználói csoporton kísérletet hajtottam végre, amely során a szimuláció működését és a tudásátadás hatékonyságát vizsgáltam. A kiértékelés során a csoportnak vizsgán és gyakorlaton kellett részt vennie. Ezeken a korábban bemutatott kibertámadások szimulációja zajlott, minimális paraméterbeli eltérésekkel (például más weboldal álcázása, más IP-címek használata stb.), illetve a gyakorlati rész során egy oktatási segédanyag is rendelkezésre állt.

A kiértékelés igazolása lehet a H2 hipotézisnek, amely szerint szimulálható olyan kibertámadás, amelynek azonosításához és megoldásához nem szükséges mély informatikai tudás. Ehhez két feltételt kellett ellenőrizni. A résztvevők technikai segítségnyújtás nélkül képesek a gyakorlatot és a vizsgát végrehajtani, illetve a résztvevők mély informatikai tudás nélkül is képesek teljesíteni a vizsgát.



12. ábra: Kiértékelés folyamata
Forrás: a szerző szerkesztése

A kiértékelés menetét a 12. ábra mutatja be, miszerint a résztvevők először megpróbálkoztak a vizsga teljesítésével, amennyiben az rosszul sikerült, akkor a gyakorlati oktatás keretében sajátították el a vizsga teljesítéséhez szükséges ismereteket, ezután ismételten megpróbálkoztak a vizsga végrehajtásával. A gyakorlati oktatást addig

hajtották végre, amíg a vizsga sikeresen nem zárult. Annak az oka, hogy a résztvevőket rögtön a vizsgakérdésekkel szembesítjük, mindössze az volt, hogy ellenőrizzük, tényleg szükséges-e a gyakorlati oktatás megtartása és elvégzése, vagy esetleg rendelkeznek már a megfelelő informatikai tudással.

Résztvevők

Összesen 12 résztvevővel végeztem el a kísérletet, akik között vegyesen találhatók nők és férfiak is. A 24–56 éves korosztályból, megfelelően elosztott mértékben választottam személyeket, többségében a közszolgálatból, de egyéb szakmák is képviseltették magukat, ahol az informatikai tudás nem jelentkezett követelményként, előfeltételként.

Eredmények

A résztvevők által a környezet összeállítása és a vizsga végrehajtása teljesen önállóan zajlott, azonban a gyakorlati oktatás során személyesen is jelen voltam, aminek fő célja, hogy az oktatási anyag minőségét fejlesszem. Abban az esetben, ha valamilyen oktatási rész nehezen érthető volt, vagy a résztvevő érdeklődését felkeltette az adott téma, személyesen válaszoltam a felmerült kérdésekre.

A kiértékelés során a személyek azonos teljesítményt értek el, mindössze a teljesítés idejében voltak eltérések. Egyetlen résztvevő sem volt képes a vizsgát gyakorlati oktatás nélkül teljesíteni, viszont a gyakorlati oktatás után mindenki teljesítette azt.

A virtuális gépek előkészítése és elindítása a résztvevők többségének könnyedén ment, de néhány esetben indokolt volt a technikai segítségnyújtás arra vonatkozóan, hogy a virtuális gépeket és a pillanatképeket milyen módon lehet kiválasztani és elindítani.

Tapasztalatok

A résztvevők többsége korábban nem tapasztalt a gyakorlat során bemutatottakhoz hasonló kibertámadásokat, kizárólag e-mailben érkező adathalász-támadással találkoztak, amelyet a legtöbb esetben az üzenet helytelen magyarsággal íródott tartalma miatt ismertek fel. Éppen ezért a szimulációs oktatás előnyeként emelték ki a különféle támadási technikák bemutatását, azok felismerésének lehetőségeit, hiszen a támadás elhárítására irányuló intézkedések csak akkor alkalmazhatók eredményesen, ha a támadás észlelése megtörtént.

A támadások szimulálása során a résztvevők felismerték, hogy a kibertámadások típusai és céljai rendkívül sokrétűek. A szimulációs gyakorlati oktatást követően a résztvevők azt nyilatkozták, hogy a jövőre nézve sokkal elővigyázatosabbak lesznek, továbbá sokkal tudatosabban használják majd különféle infokommunikációs eszközeiket és az online platformokat, kiemelt figyelmet fordítva az általános védelmi intézkedésekre és az esetleges fenyegetések felismerésére.

Minden résztvevő kiemelte, hogy a támadó gép megmutatása a támadás után sokkal jobban motiválta és meglepte őket, mintha csak az áldozat gépén kellett volna végrehajtaniuk a védelmi intézkedéseket a gyakorlat során, hiszen így azt is megtapasztalhatták, hogy milyen információkhoz férhet hozzá a támadó, így még valósághűbbnek tűnt a gyakorlat. Több résztvevő is jelezte, hogy a támadások valóságos átélése ráébresztette őket a biztonságtudatosság fontosságára, a szükséges védelmi intézkedések megismerésének, betartásának és kivitelezésének szerepére, a kibertérből érkező fenyegetések káros következményeinek mérséklése érdekében. A gyakorlat előnyeként fogalmazták meg azt a véleményt, hogy segítségével nemcsak elméletben tanulják meg, hogyan reagáljanak a különféle támadásokra, hanem a „saját bőrükön" tapasztalják, milyen szembesülni egy valódi kibertámadással, így sokkal hatékonyabban képesek megjegyezni a védekezés során alkalmazandó intézkedéseket, hiszen így a gyakorlatban ki is próbálhatják az egyes lépéseket.

Összegezve, a tapasztalatok alapján megállapítható, hogy a szimulációs gyakorlat során olyan tudást sikerült átadni, amelynek segítségével elérhető, hogy a résztvevőket ne érje váratlanul egy valós támadás, illetve a már megszerzett tudást éles helyzetekbe is képesek legyenek átültetni.

Következtetés

Az eredmények alapján összegezhető, hogy a résztvevők közül senki sem volt képes gyakorlat nélkül teljesíteni a vizsgát, ami alátámasztja, hogy nem rendelkeztek mély informatikai tudással. Képesek voltak azonban a gyakorlati oktatás után önállóan és eredményesen végrehajtani a vizsgát. Ezek alapján teljesült az a két feltétel, amely szükséges ahhoz, hogy a H2 hipotézist bizonyítottnak tekintsük, vagyis *a résztvevők technikai segítségnyújtás nélkül képesek a gyakorlatot és a vizsgát végrehajtani, illetve a résztvevők mély informatikai tudás nélkül is képesek teljesíteni a vizsgát.* Ezek alapján a *H2 hipotézist bizonyítottnak* tekintem.

Összefoglalás és jövőbeni tervek

Ebben a publikációban megvizsgáltam a nyilvánosan elérhető kiberbiztonsági keretrendszereket, amelyek felhasználhatók a kiberbiztonsági ismeretek gyakorlati oktatására. Ezeket több szempontból is értékeltem, amely alapján kijelenthető, hogy szükség van egy olyan passzív-aktív offline szimulációs platformra, amely képes a kibervédelmi technikák gyakorlati kipróbálására.

Ehhez kapcsolódóan bemutattam egy egyszerűsített architektúrát a kibertámadások automatikus szimulációjára. A kibertámadások során virtuális gépeket lehet használni, amelyeket akár a saját számítógépünkön is elindíthatunk. A szimulációk definiálására pillanatképeket lehet használni, illetve szükség szerint szkripteket is lehet írni, amelyek a virtuális gépek indításakor automatikusan lefutnak.

Az így kialakított architektúrán megvalósítottam egy DoS-, egy backdoor és egy phishing támadást is különböző platformokon, amelyek más és más infokommunikációs

eszközt szimbolizáltak (asztali számítógép, mobiltelefon, tablet stb.). A szimulációhoz kapcsolódóan a feladatokat csak az áldozat gépen kellett végrehajtani, de szemléltetésképpen a támadó gépen található konzolt is meg lehetett tekinteni.

Az így kialakított rendszert különböző, mély informatikai tudással nem rendelkező személyekkel teszteltem le. Mindenki az előre elkészített szimulációs környezetében próbálta ki a vizsgafeladatokat és a gyakorlati oktatást. Ezek alapján kijelenthető, hogy szimulálható olyan kibertámadás, amelynek azonosításához és megoldásához nem szükséges mély informatikai tudás.

A kutatás folytatásaként szeretném kibővíteni a meglévő támadásokat további példákkal, mivel a hosszú távú cél, hogy az így kialakított gyakorlat a közszolgálati kiberbiztonsági képzés keretében a saját infokommunikációs eszközök védelme című tantárgy teljes gyakorlati anyagát lefedhesse.[32] Ezután a kiértékelés körét érdemes kibővíteni nagyobb létszámra és a képzéshez kapcsolódóan részletesebb méréseket végrehajtani. Végül az architektúrát szeretném úgy kibővíteni, hogy ne csak saját infokommunikációs eszközökön történő támadásokat lehessen szimulálni, hanem szervezeti szintű kiberfenyegetéseket is.

Irodalomjegyzék

Beuran, Razvan et al. (2017): CyTrONE: An Integrated Cybersecurity Training Framework. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy, Porto, Portugal,* 157–166. Online https://doi.org/10.5220/0006206401570166

Cartwright, General James (2011): *Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5.* Washington, D.C.: Department of Defense.

Čeleda, Pavel et al. (2015): *KYPO – A Platform for Cyber Defence Exercises. M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence.* NATO Science and Technology Organization. Online: http://dx.doi.org/10.14339/STO-MP-MSG-133-08-doc

Conklin, Arthur – Cline, Raymond – Roosa, Tiffany (2014): Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. In *47th Hawaii International Conference on System Sciences,* 2006–2014. Online: https://doi.org/10.1109/HICSS.2014.254

Deák Veronika (2019): Kártékony programok terjedése social engineering technikákon keresztül. *Hadmérnök,* 14(2), 256–271. Online: https://doi.org/10.32567/hm.2019.2.21

Deák Veronika (2020a): A közszolgálati kiberbiztonsági képzés helye nemzetközi viszonylatban. *Hadmérnök,* 15(4), 159–177. Online: hhttps://doi.org/10.32567/hm.2020.4.11

[32] Deák 2020b: 157–178.

Deák Veronika. (2020b): A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon. *Hadmérnök,* 15(3), 157–178. Online: hhttps://doi.org/10.32567/hm.2020.3.9
Fehér Krisztián (2016): *Kezdő hackerek kézikönyve.* Budapest: BBS-INFO Könyvkiadó és Informatikai Kft.
Ficco, Massimo – Palmieri, Francesco (2019): Leaf: An Open-source Cybersecurity Training Platform for Realistic Edge-IoT Scenarios. *Journal of Systems Architecture,* 97, 107–129. Online: https://doi.org/10.1016/j.sysarc.2019.04.004
Garrels, Machtelt (2004): *Bash Guide for Beginners.* United Kingdom: Fultus Corporation.
Gyányi Sándor (2007): DDOS támadások veszélyei és az ellenük való védekezés. *Hadmérnök,* Különszám. Online: http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html
Hart, Stephen et al. (2020): Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security,* 95. Online: https://doi.org/10.1016/j.cose.2020.101827
Hathaway, Oona et al. (2012): The Law of Cyber-attack. *California Law Review,* 100(4), 817–885. Online: https://doi.org/10.15779/Z38CR6N
Heckman, Kristin et al. (2013): Active Cyber Defense with Denial and Deception: A Cyber-Wargame Experiment. *Computers & Security,* 37, 72–77. Online: https://doi.org/10.1016/j.cose.2013.03.015
Herring, Michael – Willett, Keith (2014): Active Cyber Defense: A Vision for Real-time Cyber Defense. *Journal of Information Warfare,* 13(2), 46–55. Online: www.jstor.org/stable/26487121
Hong, Junho et al. (2015): *Cyber-physical Security Test Bed: A Platform for Enabling Collaborative Cyber Defense Methods.* PACWorld Americas Conference.
Jin, Ge et al. (2018) Game Based Cybersecurity Training for High School Students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education, Baltimore,* 68–73. Online: https://doi.org/10.1145/3159450.3159591
Kennedy, David et al. (2011): *Metasploit: The Penetration Tester's Guide.* San Francisco: No Starch Press.
Kuo, Cheng-Chung et al. (2018): Cyber Attack and Defense Training: Using EMULAB as a Platform. *International Journal of Innovative Computing, Information and Control,* 14, 2245–2258. Online: https://doi.org/10.24507/ijicic.14.06.2245
Muha Lajos – Krasznay Csaba (2018): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem. Online: http://hdl.handle.net/11410/11173
Owens, William – Dam, Kenneth E. – Lin, Herbert S. (2009): *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities.* Washington, D.C.: The National Academies Press. Online: https://doi.org/10.17226/12651
Schepens, Wayne – James, John (2003): Architecture of a Cyber Defense Competition. In *2003 IEEE International Conference on Systems, Man and Cybernetics, Washington,* 4300–4305. Online: https://doi.org/10.1109/ICSMC.2003.1245660
Szabó András (2018): Technikai kiberbiztonsági gyakorlatok – Nemzetközi kitekintés. *Hadmérnök,* 13(1), 286–301.

Uma, M. – Padmavathi, Ganapathi (2013): A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security,* 15(5), 390–396. Online: https://doi.org/10.6633/IJNS.201309.15(5).09

Varga Máté (2010): *Számítógépes virtualizáció.* Online: https://docplayer.hu/2946347-Szamitogepes-virtualizacio.html

HADMÉRNÖK
VÉDELEMINFORMATIKA
18. évfolyam (2023) 3. szám 145–160.
DOI: 10.32567/hm.2023.3.10

Hankó Viktória[1]

SCADA-rendszerek kiberbiztonsága a létfontosságú rendszerelemek tekintetében 1.[2]

Cybersecurity of SCADA Systems from Critical Infrastructure Aspect 1

Absztrakt

Napjainkban a technológiai fejlődéssel a kiberbiztonság szerepe is egyre meghatározóbb, hiszen mind a magánszemélyeknek, mind a vállalatoknak lépést kell tartani a kibertámadások alakulásával – legyen szó azok számosságáról vagy módozatairól. Ezeknek a támadásoknak kiemelt célpontjai az ipari létesítmények, létfontosságú rendszerelemek, amelyeknek meghatározó elemei a SCADA-rendszerek. Ezzel összefüggésben elmondható, hogy ezekben a létesítményekben az átlagosnál jóval magasabb szintű védelemre van szükség szerepükből fakadóan. A tanulmány első részében a szerző ismerteti a SCADA-rendszer alapfogalmait, valamint azokat az előírásokat, jó gyakorlatokat, amelyek a létesítéshez, illetve működtetéshez szükségesek. Továbbá bemutatja a korábbi, illetve az aktuális kiberbiztonsági kihívásokat mind általános, mind pedig SCADA-rendszerre fókuszálva – a támadási metódus, a támadás éve, valamint az érintett szektor besorolása alapján.

Kulcsszavak: SCADA, kiberbiztonság, létfontosságú rendszerelem

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: viktoria.hanko@protonmail.com

[2] A cikk a Kulturális és Innovációs Minisztérium ÚNKP-22-I-NKE-36 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Abstract

Today, as technological advances continue, the role of cybersecurity is becoming increasingly important, as both individuals and companies need to keep up with the evolution of cyberattacks – in terms of both, their number and their methods. Industrial facilities and critical systems, of which SCADA systems are a key component, are prime targets for these attacks. In this context, these installations require a much higher level of protection than the average due to their role. In the first part of the article, the author describes the basic concepts of SCADA systems, as well as the specifications and good practices required for their installation and operation. It also describes past and current cybersecurity challenges, both general and SCADA system-focused, based on attack method, year of attack, and classification of the sector involved.

Keywords: SCADA, cybersecurity critical infrastructure

Bevezetés

Az Industrial Control Systems, azaz ipari vezérlőrendszerek (ICS) és a Supervisory control and data acquisition, azaz a felügyeleti ellenőrző és adatgyűjtő rendszerek (SCADA) az ipari létesítmények és a létfontosságú rendszerelemek, vagy a köznyelvben ismert kritikus infrastruktúrák működésének kritikus elemei. A világ számos ipari területén exponenciálisan növekszik a SCADA-rendszerek használata. Az információs és kommunikációs technológia fokozott és jelentős növekedése arra kényszeríti a szervezeteket, hogy SCADA-rendszereiket a szabadalmaztatott technológiáról és a protokollalapú rendszerekről az internetalapúakra állítsák át. Ez a paradigmaváltás megnövelte a SCADA-rendszereket célzó kockázatokat is.[3] A kritikus infrastruktúrában számos szervezet telepített SCADA-/ICS-rendszert a folyamatok vezérlésének és az adatgyűjtésnek az automatizálására. Ezek a rendszerek nagy értékű célpontokká váltak az üzleti műveletek megzavarására törekvő támadók számára.[4] Ennek kitűnő példája, hogy 2022 augusztusában[5] az Egyesült Királyságban egy zsarolóvírus-csoport legalább egy vízszolgáltatót megtámadott, de némi zavar van abban, hogy valójában kinek a rendszereit törték fel. A Cl0p csoport weboldalán megjelent, hogy betörtek a Thames Water rendszereibe, amely az Egyesült Királyság legnagyobb víz- és szennyvízszolgáltatójaként hirdeti magát, és 15 millió embert szolgál ki. Kiberbiztonsági szakértők azonban rámutattak, hogy bár a Cl0p a Thames Watert nevezi meg a weboldalán, a betörés bizonyítékaként kiszivárgott fájlok valójában egy másik, a South Staffordshire nevű vízszolgáltatóhoz tartoznak, amelynek leányvállalatai, a South Staffs Water és a Cambridge Water 1,6 millió embert és több tízezer vállalkozást szolgálnak ki az Egyesült Királyságban. Pár nappal később a South Staffordshire megerősítette, hogy kiberbűnözők célpontja lett.

[3] Krasznay 2019: 25–29.
[4] Tóth 2022: 123–132.
[5] Kovacs 2022.

Ebből fakadóan jelen kutatás célja a releváns hazai és nemzetközi szakirodalmak vizsgálatával meghatározni azokat a kiberbiztonsági kihívásokat, amelyek a SCADA-rendszereket érintik. Első lépésként szükséges felmérni, hogy milyen elemekből épül fel egy ilyen rendszer, illetve mely folyamatok során alkalmazzák ezeket a különböző létfontosságú rendszerelemek létesítményeiben. Ezáltal összegyűjtöm és rendszerezem a lehetséges kiberbiztonsági fenyegetéseket, mind általánosan, mind pedig rendszerspecifikusan.

Kutatási módszertan

Elsődlegesen a hazai és nemzetközi releváns szakirodalmak feldolgozásával a SCADA-rendszerek felépítését, használatát, valamint működésének szabályait határozom meg, a létfontosságú rendszerelemek definiálása mellett. A jogszabályok, szabványok esetében összehasonlító elemzést végzek a hazai és nemzetközi szabályozások tekintetében. Ezt követően rendszerezem a kiberbiztonsági fenyegetéseket – annak bekövetkezési éve, a támadás típusa, illetve az érintett szektor szempontjai alapján.

SCADA-rendszerek és a létfontosságú rendszerelemek

Az ICS egy általános kifejezés, amely többféle vezérlőrendszer-típust foglal magában, beleértve a felügyeleti vezérlő és adatgyűjtő (SCADA-) rendszereket, a Distributed Control Systems, azaz elosztott vezérlőrendszereket (DCS) és más vezérlőrendszer-konfigurációkat, például az ipari ágazatokban és a kritikus infrastruktúrákban – vagy a magyar szabályozói megnevezés szerint létfontosságú rendszerelemekben – megtalálható Programmable Logic Controllers, vagyis programozható logikai vezérlőket (PLC). Az ipari vezérlőrendszer olyan vezérlőelemek (például elektromos, mechanikus, hidraulikus, pneumatikus) kombinációiból áll, amelyek együttesen működnek egy ipari cél (például gyártás, anyag- vagy energiaszállítás) elérése érdekében.[6]

A DCS-ek olyan számítógépes szoftvercsomagok, amelyek kommunikálnak a vezérlő hardverrel, és Human Machine Interface-t, azaz központosított ember-gép interfészt (HMI) biztosítanak a vezérelt berendezések számára.[7] A PLC olyan szilárdtestes vezérlőrendszer, amely felhasználó által programozható memóriával rendelkezik utasítások tárolására, illetve olyan speciális funkciók megvalósítása céljából, mint a bemenetek/kimenetek vezérlése, logika, időzítés, számlálás, három üzemmódú vezérlés, kommunikáció, aritmetika, valamint adat- és fájlfeldolgozás.[8]

A SCADA-rendszerek több komponensből tevődnek össze – hardverkomponensekből és szoftverprogramokból, ahol a hardver magában foglalja a Remote Terminal Units, azaz a távoli terminálegységeket (RTU), a Master Terminal Unitot, vagyis a főterminálegységet (MTU), a működtetőket és az érzékelőket. A szoftverprogramok a HMI-ből,

[6] National Institute of Standards and Technology 2020.
[7] Dunn 2015: 103–110.
[8] Stouffer 2020.

a Historian, tehát a központi adatbázisból és más felhasználói szoftverekből állnak. Ezek a szoftverek biztosítják a hardver és a szoftver közötti kommunikációs interfészt. A fizikai környezet kapcsolódik a működtető eszközökhöz és érzékelőkhöz, amelyek tovább kapcsolódnak az RTU-khoz. Az RTU-k összegyűjtik az érzékelők információit és adatait, és a telemetriai adatokat továbbítják az MTU-nak a SCADA-rendszer megfigyelésére és vezérlésére.[9] A mélyebb betekintés érdekében az egyes komponensek működésének, feladatainak ismertetése is szükséges, amelyek a következők:

- Az RTU felelős a valós idejű adatok és információk gyűjtéséért a fizikai környezethez LAN-/WAN-kapcsolaton keresztül csatlakoztatott érzékelőkből. Az RTU-k továbbítják az információkat az MTU-nak. Ezek felelősek továbbá a rendszerhez kapcsolódó fizikai eszközök aktuális állapotadatainak továbbításáért.
- Az MTU a központi felügyeleti állomás. Feladata a vezérlés, az RTU-gépek kommunikációs kapcsolatokon keresztüli vezérléséért és irányításáért felelős. Válaszol az RTU-tól érkező üzenetekre is, valamint feldolgozza és tárolja az adatokat.
- A HMI kommunikációs interfészt biztosít a SCADA hardver- és szoftverkomponensek között. Felelős a SCADA működési információinak vezérléséért, például az RTU és MTU közötti vezérlésért, felügyeletért és kommunikációért, szöveg, statisztika vagy más érthető tartalom formájában.
- A Historian a kétirányú kommunikációs adatok, események és riasztások felhalmozására szolgál. Leírható központi adatbázisként vagy távoli helyen található szerverként. A Historiant a HMI-n megjelenő grafikus trendek feltöltéséhez kérdezik le.
- A kommunikációs hálózat kommunikációs szolgáltatásokat nyújt a SCADA-rendszer különböző összetevői között. A használt közeg lehet vezeték nélküli vagy vezetékes.[10]

A SCADA-rendszer fő célja az ipari folyamatok berendezéseinek felügyelete és vezérlése. Így több területen is alkalmazzák ezeket: gyártás, vízgazdálkodás, olaj- és gázellátás, szállítás, megújuló energiaforrások, valamint az áramelosztás és -szabályozás területén is. Ezekben az iparágakban a SCADA-rendszerek értékes információkat szolgáltatnak a kulcsfontosságú érdekelt feleknek. A rendszer segítségével javíthatják az ipari üzemek teljesítményét, nyomon követhetik az üzemek hatékonyságát, és a rendszertől kapott üzeneteken keresztül mérsékelhetik a hibákat és a leállásokat. Napjaink fejlett ipari világában a SCADA-rendszerek kulcsfontosságúak az ipari üzemek hatékonyabb működéséhez, mivel sokkal könnyebben és gyorsabban gyűjtik össze a lényeges adatokat. Ez sok vállalkozásnál lehetővé teszi az erőforrások jobb elosztását. A SCADA-rendszer számos különböző típusú berendezéshez csatlakozik: az időjárás-érzékelőktől és szivattyúktól az energiatermelésig és a motorokig mindent felügyel és vezérel, attól függően, hogy milyen adatokra van szükség.[11]

[9] Yadav–Paul 2021.
[10] Pathak–Patel 2014: 1639–1699.
[11] Lásd: https://scada-international.com/what-is-scada/

A rendszer felépítése és alkalmazási területei mellett érdemes kitérni arra, hogy általánosságban milyen előnyei lehetnek a használatának. Ennek részleteit az 1. táblázat foglalja össze.

1. táblázat: A SCADA-rendszer előnyei

Tulajdonság	Leírás
Sokoldalúság	A SCADA-t heterogén eszközök összekapcsolására fejlesztették ki. A számos rendelkezésre álló meghajtó lehetővé teszi a csatlakozást bármilyen típusú és összetettségű eszközhöz, így lehetséges a PLC, valamint a speciális célú eszközök vagy kommunikációs multiplexer vezérlése minden átviteli módszerrel és médiával.
Sebesség	Az eseményvezérelt architektúra rendkívül gyors válaszidőt tesz lehetővé, ezért a rendszer teljesítményét nem befolyásolja a csatlakoztatott bemenetek/kimenetek száma.
Hatékonyság	A SCADA korlátozott memória- és feldolgozási teljesítményt igényel, ami lehetővé teszi a költséghatékony konfigurációkat, amelyek még mindig képesek használni a rendszer összes funkcióját.
Könnyű használat	A kezdeményezést fejlesztő környezet és a természetes használat: az interfész, valamint a projekt helyességének bármikori ellenőrzése lehetővé teszi a komplett alkalmazások órák alatti fejlesztését, napok vagy hónapok helyett.
Megbízhatóság	A SCADA moduláris és védett felépítése az egyik olyan elem, amely növeli a rendszer stabilitását és megbízhatóságát, lehetővé téve az üzemeltető számára, hogy csak kiválasztott modulokat kapcsoljon ki és frissítsen anélkül, hogy az egész rendszer leállna.
Kompakt jelleg	A SCADA-t kifejezetten a rendszer erőforrásainak hatékony felhasználására tervezték, amit a nagymértékben optimalizált kódok és algoritmusok révén érnek el.
Biztonság	Az összes végrehajtott művelet szigorúan ellenőrzött és auditált. Az üzemeltetők a rendszernek csak az általuk engedélyezett részét használhatják.
Funkciók	A SCADA leegyszerűsíti az adatbázis létrehozását és a konfigurációs eljárást az űrlapok kitöltésére, így csak a projekt valóban szükséges paramétereit határozza meg. Ezek a módszerek nemcsak a tervező feladatát könnyítik meg, hanem ténylegesen meg is mutatják a megfelelő módszert a világos és teljes dokumentáció automatikus létrehozására.
Szelektív riasztáskezelés	A riasztások logikai csoportokba rendezhetők és prioritással láthatók el, így lehetővé téve az adott üzem különböző részeihez kapcsolódó értesítések áttekintését, valamint a kevésbé jelentős riasztások elrejtését egy adott állapotban.
Online konfiguráció	Minden SCADA-projekt-paraméter – akár adatbázis-objektum, akár grafikus szimbólum – online hozzáadható, módosítható vagy törölhető, miközben az összes valós idejű felügyeleti és vezérlési tevékenység aktív marad. Ez a funkció növelheti a projektek összehangolásának sebességét, amelyet általában az ügyfél telephelyén végeznek el az összes eszköz rendszeres működése mellett.

Forrás: a szerző szerkesztése G. L. 2016 alapján

Az előző rész alapján kijelenthető, hogy ezek a rendszerek kiemelt jelentőségűek egy ország és annak állampolgárai szempontjából egyaránt. Ebből következik, hogy a biztonság is kiemelt szerepet kap a rendszer kialakításánál és működtetésénél.[12] Különböző

[12] Paráda–Farkas 2020: 159–182.

előírásoknak kell megfelelni a biztonságos működés érdekében, amelyek egyik pillérét általánosságban SCADA biztonsági keretrendszernek nevezik. Ez különféle biztonsági intézkedéseket foglal magában, amelyek képesek kezelni a különböző problémákat:

- adminisztratív intézkedések: szervezet vezetése és biztonsága, szabványok, irányelvek és kivételek, kockázatértékelés, oktatás és képzés, megfelelőségi keretrendszer;
- SCADA-intézkedések: sérülékenységmenedzsment, fizikai biztonság, hálózati biztonsági ellenőrzések, identitás- és hozzáférés-kezelés, adatvagyon-menedzsment;
- alkalmazás és adatbiztonság: adatbiztonság, alkalmazásbiztonság, rosszindulatú kódok megelőzése és észlelése, változáskezelés;
- rendszer biztosítása: biztonságos konfiguráció, rendszer ellenálló képessége, üzletmenet-folytonosság és katasztrófa-helyreállítás tervezése;
- ellenőrző intézkedések: forensics, fenyegetés monitorozása, incidenskezelés;
- külső intézkedések: partnerbiztonsági menedzsment, szállítói biztonsági menedzsment.

Az előbbi intézkedések összefoglalva egy biztonságpolitikát alkotnak. Ezek a politikák, stratégiák létfontosságúak a fenntartható biztonsági rendszer kiépítéséhez.[13] Emellett a megfelelő adminisztráció is elengedhetetlen, ugyanis az előbb említett elemek nélkül lehetetlenné válik a rendszer megfelelő működése, hiszen kiszolgáltatott lesz a különböző sebezhetőségeknek.[14] Azonban nemcsak politikát, stratégiát, hanem más konkrét biztonsági dokumentumot, például biztonsági tervet és végrehajtási iránymutatást is lehet és kell készíteni a SCADA-rendszerben alkalmazandó konkrét gyakorlatok meghatározása érdekében.[15]

Emellett az ISA112 SCADA-rendszerek szabványügyi bizottsága aktívan dolgozik egy sorozat ISA-szabvány és műszaki jelentés kidolgozásán. A 2016-ban létrehozott bizottság munkájában jelenleg több mint 200 SCADA-szakértő vesz részt a világ minden tájáról, akik az iparágak széles körét képviselik. A két önkéntes társelnök által vezetett bizottság arra törekszik, hogy a következő felek között egyenletes egyensúly legyen: végfelhasználók, gyártók, forgalmazók, tanácsadók, mérnöki irodák, vállalkozók, rendszerintegrátorok, kormányzati szabályozók és más érdekelt felek. A szabvány- és jelentéssorozat a csővezetékek, a víz- és szennyvíz-, az energia-, az olaj- és gázipar, valamint más iparágak SCADA-rendszereinek rendszertervezésével, megvalósításával, üzemeltetésével és karbantartásával foglalkozik, így támogatva e rendszerek általános integritását és megbízhatóságát. A szabványok és a műszaki jelentések célja, hogy útmutatást nyújtsanak a SCADA-rendszerek tervezéséhez, megvalósításához, üzemeltetéséhez és karbantartásához azáltal, hogy számos iparágban dokumentálják a legjobb gyakorlatokat. A tervek szerint egy vagy több szabványt dolgoznak ki, amelyeket a megvalósítás részleteit és az iparágspecifikus iránymutatásokat kibővítő műszaki jelentések egészítenek ki. Jelenleg a belső bizottsági véleményezési és szerkesztési feladatok zajlanak, az első ISA112 szabványdokumentum közzétételét 2023 őszére tervezik.[16]

[13] Lásd: www.logsign.com/blog/scada-cybersecurity-framework
[14] Megyeri–Farkas 2017: 198–209.
[15] Lásd: www.logsign.com/blog/scada-cybersecurity-framework
[16] Lásd: www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa112

Továbbá vannak bizonyos jogszabályi kötelezettségek is, amelyek vonatkoznak a SCADA-t használó üzemekre, vállalkozásokra, ilyen például az Európai Unió (EU) tagállamaiban érvényes 2016/1148 (EU) európai parlamenti és tanácsi irányelv (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, röviden a NIS-irányelv.[17] Ennek hatálya alá tartozik az elektromosság, víz (beleértve a kezelést és a hulladékot), olaj-gáz, egészségügy, szállítás, digitális infrastruktúra (beleértve a felhőalapú tárolást, az online piactereket és a keresőmotorokat) iparágak. Az irányelv nemcsak e szolgáltatások és infrastruktúrák szolgáltatóit és üzemeltetőit érinti, hanem az egész európai társadalmat is. 2018 májusában lépett hatályba az összes EU-tagországban, és különleges követelményeket határoz meg a biztonsági kockázat kezelése, a kibertámadások elleni védelem, a kiberbiztonsági események észlelése és a kiberincidensek hatásának minimalizálása terén. Ez magában foglalja a kritikusinfrastruktúra-szolgáltatók és az alapvető szolgáltatások üzemeltetőinek információtechnológiai rendszereire, valamint az üzemeltetési technológiai rendszerekre vonatkozó irányelvi követelményeket, beleértve az ipari vezérlőrendszereket, például a SCADA-t is.[18] Kiemelendő, hogy a folyamatos fejlődés miatt a jogszabályok előírják, hogy a jogalanyok a védendő üzleti értékek alapján meghatározott kockázatalapú megközelítést alkalmazzanak, valamint megelőző és reagáló biztonsági kontrollokat alakítsanak ki. Ez a megközelítés optimális költségeket biztosíthat az informatikai, információs vagy kiberbiztonsági irányítási rendszer számára.[19]

Mindemellett az Európai Kiberbiztonsági Ügynökség (ENISA) jelentése tartalmazza a különböző szabványokat az ipari irányítórendszerekre vonatkozóan, amelyben megjelennek kifejezetten a SCADA-rendszerekre vonatkozó szabványok, iránymutatások. Ennek összefoglalását a 2. táblázat tartalmazza.[20]

2. táblázat: Szabványok és iránymutatások

Hatókör	Típus	Név	Bevezetés dátuma	Rövid leírás
Nemzetközi	Szabvány	IEEE 1711. Próbahasználati szabvány az alállomási soros vonal kiberbiztonságára szolgáló kriptográfiai protokollhoz	2011. február	Az IEEE 1711 egy speciális soros biztonsági protokollt határoz meg kétféle kriptográfiai modul számára: SCADA kriptográfiai modulok (SCM) a soros SCADA-csatorna védelmére és karbantartási kriptográfiai modulok (MCM) a karbantartási csatorna védelmére, amely általában egy betárcsázós kapcsolat.

[17] A cikk készítésének ideje alatt megjelenés alatt volt a NIS2-irányelv, azonban még nem lépett hatályba, így a szerző a korábbi irányelvet veszi alapul.
[18] Lásd: www.awencollective.com/nis-directive
[19] Bederna–Rajnai–Szádeczky 2021: 139–148.
[20] ENISA 2011.

Hatókör	Típus	Név	Bevezetés dátuma	Rövid leírás
Multi-laterális kezdemé-nyezések	Iránymu-tatás (jó gyakorlat)	Ipari vezér-lőrendszerek kiberbiztonsági értékelése. A jó gyakorlat útmutatója	2011. április	A dokumentum célja, hogy megismertesse az objektum tulajdonosait a kiberbiztonsági tesztelés általános folyamatával, és bete-kintést nyújtson a konkrét tesztelési mód-szerekbe, hogy a tulajdonosok megtanulják előírni az egyéni értékelést, amely maximali-zálja a tesztelési költségvetésük kimenetelét.
Nagy-Britannia	Iránymu-tatás (jó gyakorlat)	Jó gyakorlatok útmutató-ja – Folya-matirányítás és SCADA-biz-tonság	2008. június	Az iránymutatás hét elemből álló keretrend-szert javasol a következőkre a folyamatirá-nyítás biztonságának kezeléséhez. Általános útmutatás • Üzleti kockázat • Biztonságos architektúra bevezetése • Reagálási képességek kialakítása • Tudatosság és készségek fejlesztése • Harmadik fél kockázatának kezelése • Projektek bevonása • Folyamatos irányítás kialakítása
Nagy-Britannia	Iránymu-tatás (jó gyakorlat)	Tűzfal telepítése SCADA- és fo-lyamatirányító hálózatokhoz. A jó gyakorlat útmutató	2008. június	Ez a dokumentum a SCADA-tűzfal-telepítés jelenlegi gyakorlata vizsgálatának és össze-állításának eredménye. A cél az volt, hogy megvizsgálja a tűzfal-architektúrák, a tele-pítés és az ipari vezérlőkörnyezet védelmére használt menedzsment „korszerűségét”.
Svédország	Iránymu-tatás (jó gyakorlat)	Útmutató az ipari ve-zérlőrendszer fokozott biztон-ságához	2010. május	Ez az útmutató alapvető ajánlásokat tartal-maz az ipari vezérlőrendszerek biztonságára vonatkozóan. A dokumentum tippeket is ad arra vonatkozóan, hogy hol találhat további információkat. Az általunk nyújtott ajánlá-sok nemzetközileg elismert ajánlásokhoz, gyakorlatokhoz és szabványos munkamód-szerekhez kapcsolódnak.
Amerikai Egyesült Államok	Útmutató (műszaki jelentés és jó gya-korlat)	NIST SP 800-82. Út-mutató az ipari vezérlőrendsze-rek (ICS) biztон-ságához	2011. június	A dokumentum célja, hogy útmutatást adjon az ICS rendszerek biztonságossá téte-léhez, beleértve a SCADA-, a DCS és más, vezérlési funkciókat ellátó rendszereket. A dokumentum áttekintést ad az ICS-ről és a tipikus rendszertopológiákról, azonosít-ja e rendszerek tipikus fenyegetéseit és se-bezhetőségeit, és javasolt biztonsági ellenin-tézkedéseket kínál a kapcsolódó kockázatok mérséklésére.

Hatókör	Típus	Név	Bevezetés dátuma	Rövid leírás
Amerikai Egyesült Államok	Útmutató	Terepi eszköz-védelmi profil SCADA-rendszerekhez közepes robusztusságú környezetekben	2006. június	Ez a védelmi profil meghatározza az Egyesült Államok kormánya vagy kereskedelmi szervezete által közepes robusztusságú környezetben használt SCADA terepi eszközök minimális biztonsági követelményeit. A SCADA-eszköztulajdonosok számára ez a védelmi profil hasznos a vásárlási specifikációk során figyelembe vehető követelmények azonosításában. Alternatív megoldásként az eszköztulajdonosok megkövetelhetik a termékektől, hogy igazolják a jelen védelmi profilnak való megfelelést.
Amerikai Egyesült Államok	Iránymutatás (jó gyakorlat)	API 1164, Pipeline SCADA-biztonság	2009. június	Ez az iránymutatás kifejezetten arra szolgál, hogy az üzemeltetők rendelkezésére bocsássa a SCADA biztonságával kapcsolatos iparági gyakorlatok leírását, és hogy biztosítsa a megfelelő biztonsági gyakorlatok kialakításához szükséges keretet az üzemeltető egyes vállalatain belül.
Amerikai Egyesült Államok	Szabvány	12. számú AGA jelentés. A SCADA-kommunikáció kriptográfiai védelme	2006. március	Az AGA 12 sorozat célja, hogy időt és energiát takarítson meg a SCADA-rendszerek tulajdonosainak azáltal, hogy egy olyan átfogó rendszert javasol, amelyet kifejezetten a SCADA-kommunikáció védelmére terveztek. A végfelhasználók az AGA 12 sorozatot használhatják a SCADA kiberbiztonsági megoldás beszerzése általános követelményeinek meghatározására, ha ezt az előírást beépítik a beszerzési követelményeikbe. A rendszerintegrátorok az AGA 12 sorozatot használhatják annak biztosítására, hogy a SCADA-kiberbiztonságot megfelelően specifikálják, és hogy a rendszer tesztelési terve megfeleljen a biztonsági megoldás üzembe helyezéséhez szükséges valamennyi követelménynek. Végül a SCADA hardver-, szoftver- és firmware-gyártói használhatják az AGA 12 sorozatot annak biztosítására, hogy termékkínálatuk megfeleljen a végfelhasználó SCADA-kiberbiztonsággal kapcsolatos igényeinek.

Forrás: a szerző szerkesztése ENISA alapján

A táblázat alapján látható, hogy az Amerikai Egyesült Államokban már korábban, 2006-tól kezdődően nagy hangsúlyt fektetnek a SCADA-rendszerek biztonságos kialakítására és működtetésére, aminek oka a vállalatok üzleti kockázatainak csökkentése is. Az iránymutatások, útmutatók mellett megtalálható egy szabvány is, azonban ez európai viszonylatban nem mondható el – a kontinensen útmutatások, jó gyakorlatok vannak érvényben. Továbbá megállapítható az is, hogy időben viszonylag szorosan követi az amerikai tevékenységeket az európai gyakorlat. Elmondható azonban az is, hogy nemzetközi szinten, illetve multilaterális kezdeményezések útján implementálható szabvány, valamint további jó gyakorlat egyaránt megtalálható mindkét kontinensen.

Létfontosságú rendszerelemek megjelenési formái

Magyarországon a létfontosságú rendszerelem kifejezés van érvényben a törvényi szabályozás szerint, azonban a gyakorlatban rendszerint használják a kritikus infrastruktúra kifejezést is – nemzetközi viszonylatban utóbbi megnevezést használják kizárólagosan.[21]

A hazai szabályozás értelmében a létfontosságú rendszerelem a törvény 1. számú mellékletében meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, illetve azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, továbbá amelynek kiesése a meghatározott feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.

Az 1. számú mellékletben nevesített ágazatok és a hozzájuk tartozó alágazatok a következők:

- *Energia* – villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek), kőolajipar, földgázipar és távhő;
- *Közlekedés* – közúti, vasúti, légi, vízi közlekedés és logisztikai központok;
- *Agrárgazdaság* – mezőgazdaság, élelmiszeripar és elosztó hálózatok;
- *Egészségügy* – aktív fekvőbeteg-ellátás, és a működtetéséhez szükséges szolgáltatások, mentésirányítás, egészségügyi tartalékok és vérkészletek, magas biztonsági szintű biológiai laboratóriumok és gyógyszer-nagykereskedelem;
- *Társadalombiztosítás* – társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és nyilvántartások;
- *Pénzügy* – pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei, bank- és hitelintézeti biztonság és készpénzellátás;
- *Infokommunikációs technológiák* – internethozzáférési szolgáltatás és internetinfrastruktúra, elektronikus hírközlési szolgáltatások, elektronikus hírközlő hálózatok, műsorszórás, postai szolgáltatások és kormányzati elektronikus információs rendszerek;
- *Víz* – ivóvíz-szolgáltatás, felszíni és felszín alatti vizek minőségének ellenőrzése, szennyvízelvezetés és -tisztítás, vízbázisok védelme és árvízi védművek, gátak;

[21] 2012. évi CLXVI. törvény.

- *Honvédelem* – honvédelmi rendszerek és létesítmények;
- *Közbiztonság-védelem* – rendvédelmi szervek infrastruktúrái.

Emellett a jogszabály nevesíti a nemzeti létfontosságú rendszerelemet is, amelyet szintén a törvény alapján jelölnek ki, és annak kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt, elsősorban Magyarországon lenne jelentős hatással. Továbbá megjelenik az alapvető szolgáltatás fogalma is, amely úgy definiálható, hogy a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához szükséges, elektronikus információs rendszertől függő, az alapvető szolgáltatások jegyzékében feltüntetett szolgáltatás.[22] Az egyes ágazatonkénti, valamint ágazatonként lebontott alapvető szolgáltatások jegyzéke a 65/2013. (III. 8.) Korm. rendelet 3. mellékletében található meg.

A magyar szabályozáshoz hasonlóan a korábbi alfejezetben említett NIS-irányelv is alkalmazza az alapvető szolgáltatások kifejezést, kifejezetten szereplőként hivatkozva azon – a II. mellékletben – említett közjogi vagy magánjogi szervezetre, amely a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt, az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ, és az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában. Az irányelv ágazatok és alágazatok tekintetében bizonyos eltérést mutat a hazai szabályozáshoz képest – ennek oka, hogy az iránymutatást az országspecifikus tényezők határozzák meg a saját jogszabály kialakítása folyamán.[23] Elmondható, hogy a magyar szabályozás bővebb, több ágazatot nevesít, illetve az alágazatok is részletesebbek, specifikusabbak.

A hazai és EU-s viszonylathoz képest az amerikai A kritikus infrastruktúrák biztonsága és ellenálló képessége elnöki politikai irányelv 21 (PPD-21) nemzeti politikát dolgoz ki a biztonságos, működőképes és ellenálló infrastruktúrák megerősítésére és fenntartására. Ez 16 olyan infrastrukturális ágazatot nevesít, amelynek fizikai vagy virtuális eszközei, rendszerei és hálózatai létfontosságúak az Egyesült Államok számára. Ezek működésképtelensége vagy megsemmisülése gyengítő hatással lenne a biztonságra, a nemzetgazdaság biztonságára, a nemzeti közegészségügyre vagy közbiztonságra, vagy ezek bármely kombinációjára. Az irányelv a következő ágazatokat nevezi meg:

- vegyipari ágazat;
- kereskedelmi létesítmények ágazata;
- kommunikációs ágazat;
- kritikus termelési ágazat;
- gátágazat;
- védelmi ipari bázis ágazat;
- sürgősségi szolgáltatási ágazata;
- energiaágazat;
- pénzügyi szolgáltatások ágazata;
- élelmiszeripari és mezőgazdasági ágazat;
- kormányzati létesítmények ágazata;

[22] 2012. évi CLXVI. törvény.
[23] 2016/1148 (EU) irányelv.

- egészségügyi és közegészségügyi ágazat;
- informatikai ágazat;
- nukleáris reaktorok, anyagok és hulladékok ágazat;
- közlekedési rendszerek ágazata;
- víz- és szennyvízrendszerek ágazata.[24]

Megfigyelhetők hasonlóságok a korábban ismertetett szabályozásokkal, azonban az amerikai jogszabály nem nevesít alágazatokat. Mindazonáltal szükséges nagyobb figyelmet szentelni az informatika ágazatának. Ez a szektor központi szerepet játszik a nemzet biztonsága, gazdasága, valamint közegészségügye és közbiztonsága szempontjából, mivel a vállalkozások, kormányok, felsőoktatási intézmények és magánszemélyek egyre inkább függnek az informatikai ágazat funkcióitól. Ezek a virtuális és elosztott funkciók hardvert, szoftvert, informatikai rendszereket és szolgáltatásokat foglalnak magukban, valamint – a kommunikációs ágazattal együttműködve – kialakítják és biztosítják az internetet. Az ágazat összetett és dinamikus környezete megnehezíti a fenyegetések azonosítását és a sebezhetőségek értékelését, illetve megköveteli, hogy ezeket a feladatokat együttműködő és kreatív módon oldják meg a szervezetek. Az informatikai ágazat funkcióit olyan szervezetek – gyakran tulajdonosok és üzemeltetők, valamint a hozzájuk tartozó egyesületek – kombinációja működteti, amelyek fenntartják és újjáépítik a hálózatot, beleértve az internetet is. Bár az informatika infrastruktúra bizonyos fokú ellenálló képességgel rendelkezik, az egymástól függő és összekapcsolt kialakítás kihívásokat és lehetőségeket is jelent a köz- és magánszektor felkészültségi és védelmi tevékenységeinek összehangolása szempontjából. A létfontosságú rendszereknek – legyenek azok orvosi eszközök, internetre csatlakozó autók, SCADA, ICS vagy más rendszerek – döntő szerepük van a mai világban. Egyre több ilyen rendszer kapcsolódik össze a dolgok internetével (Internet of Things/IoT), azaz egyre nyilvánvalóbbá válik, hogy ezeket a rendszereket megfelelően kell védeni a hackerektől és a kibertámadásoktól.[25]

Kiberbiztonsági fenyegetések

Kifejezetten kritikus infrastruktúrát, annak is a SCADA-rendszerét érintő első kibertámadást 1982-ben jegyezték. Szibériai csővezeték-robbanás néven ismert az incidens, amely során a támadók trójai vírust telepítettek a SCADA-rendszerbe, amely a szibériai csővezetéket irányítja. Ez egy 3 kilotonna TNT-vel egyenértékű robbanást okozott. Ezt követően 1992-ben történt a Chevron vészjelző rendszer incidense. A Chevron vészhelyzeti riasztóhálózatának egy elbocsátott alkalmazottja úgy tette tönkre a cég riasztórendszerét, hogy feltörte a New York-i és a kaliforniai San José-i számítógépeket, és úgy konfigurálta át őket, hogy összeomoljanak. A vandalizmusra csak akkor derült fény, amikor a kaliforniai Richmondban található Chevron finomítóban vészhelyzet alakult ki, és a rendszer nem tudta értesíteni a szomszédos közösséget egy mérgező anyag felszabadulásáról. Amikor a rendszer tíz órán át nem működött, 22 államban

[24] Lásd: www.cisa.gov/critical-infrastructure-sectors
[25] Lásd: www.cisa.gov/information-technology-sector

és Kanada hat, meg nem határozott területén emberek ezrei kerültek veszélybe. Két évvel később, 1994. július 8. és augusztus 31. között egy támadó jogosulatlan hozzáférést szerzett a Salt River Project számítógépes hálózatához egy betárcsázós modemen keresztül, hogy hozzáférjen a számlázási programhoz és számlázási információkhoz. Egy backdoor[26]-t telepített a rendszerbe, amely későbbi időpontban való hozzáférést biztosított számára. Abban az időben a Salt River Project víztisztító SCADA-rendszer egy 131 mérföld hosszú csatornarendszert működtetett, amely a Phoenix nagyvárosi körzetében lévő fogyasztóknak szállított vizet. A támadók legalább 5 órán keresztül fértek hozzá a rendszerhez, amely a csatornákat irányította. Kompromittálódtak a víz- és áramfigyelés adatai, valamint a szállításra vonatkozó, pénzügyi, ügyfél- és személyes adatok. Ezek közé tartoztak a bejelentkezési és jelszófájlok, a számítógépes rendszer naplófájljai, valamint a root jogosultságok.[27] Jól látható, hogy már a 2000-es évek előtt megjelentek a SCADA-rendszerek elleni kibertámadások. Az ezredfordulót követően világszinten példaként szolgáló a Stuxnet incidens, amelyben a támadás célpontja az iráni nukleáris létesítmény volt Natanzban. A Stuxnet négy darab 0. napi sebezhetőséget (korábban ismeretlen sebezhetőségeket, így nem volt idő a javítások kifejlesztésére és terjesztésére) használt ki. A féreg a Siemens alapértelmezett jelszavait használta a Windows WinCC és PCS7 programokat futtató operációs rendszerekhez. Ezt kihasználva megváltoztatta az elektromos áram frekvenciáját a hajtóművekben, így magas és alacsony fordulatszámok váltakoztak, ebből következően a centrifugák a normálisnál nagyobb arányban hibásodtak meg.[28]

Az elmúlt években is több létfontosságú rendszerelemet érintő támadásról számoltak be, ezek közül a legjelentősebbeket – amelyekben a SCADA-rendszer is érintett volt – a 3. táblázat tartalmazza.

3. táblázat: A legjelentősebb SCADA-rendszereket célzó kibertámadások 2012–2022 között

Elnevezés	**Év**	**Támadás formája**	**Érintett szektor(ok)**
Shamoon	2012	malware	energia (villamos energia és földgáz)
New York Dam	2013	rendszer feltörése	víz (árvízi védművek, gátak)
German Steel Mill	2014	rendszer feltörése	energia (földgázipar)
Ukrajna villamosenergia-hálózata	2015	malware	energia (villamos energia)
„Kemuri"	2016	rendszer feltörése	víz (ivóvíz-szolgáltatás)
Ukrajna villamosenergia-hálózata II.	2016	malware	energia (villamos energia)
SamSam	2018	ransomware	infokommunikációs technológiák (kormányzati elektronikus információs rendszerek)

(Megjegyzés: a táblázat készítése során a támadások célpontjait figyelembe véve rendeltem hozzá a magyar szabályozásban megnevezett szektorokat.)

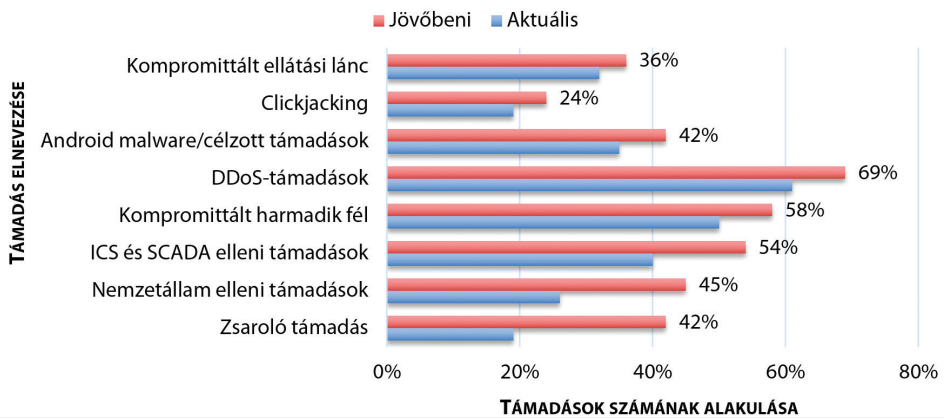
Forrás: a szerző szerkesztése DPS Telecom 2021. alapján

[26] Szoftverbe (vagy ritkább esetben hardverbe) épített olyan funkció, amelynek segítségével illetéktelen személyek hozzáférnek a programhoz, a géphez vagy annak bizonyos részeihez. Lásd: https://lexiq.hu/backdoor

[27] A root jog a legalapvetőbb, mindenre kiterjedő jogosultságot jelenti. Lásd: https://lexiq.hu/root

[28] Miller–Rowe 2012: 51–56.

A Raytheon és a Ponemon Institute 2017-ben készített egy tanulmányt, amelyben több mint 1100 vezető IT-szakembert kérdezett meg az Egyesült Államokban, Európában és a Közel-Keleten/Észak-Afrikában. Arra kérték őket, hogy értékeljék, mely kiberfenyegetések a leggyakoribbak ma, és várhatóan melyek fognak növekedni a következő három évben. A tanulmányban részt vevő szakemberek szerint a SCADA-rendszereket, valamint a nemzetállamokat érintő fenyegetések és a zsaroló támadások gyakorisága a jelenlegi szintekhez képest várhatóan emelkedni fog. Míg jelenleg a szakemberek 40%-a a SCADA-t jelöli meg gyakori problémaként, addig ez a szám 54%-ra ugrik fel a jövőben várható gyakoriság tekintetében.[29] Az elkészített elemzéshez tartozó statisztikai adatokat összefoglaló diagram a következő (1. ábra).



1. ábra: Kibefenyegetések alakulása szakemberek szerint 2017-ben
Forrás: a szerző szerkesztése Petrosyan 2023. alapján

Általánosságban elmondható, hogy újabb és újabb fenyegetéstípusok jelentek meg az idő előrehaladtával – például cryptojacking –, amellyel a szakembereknek korábban nem kellett szembenézniük. Az ipar 4.0 technológiák bevezetésével pedig a rendszerek hálózati támadásoknak való kitettsége fog várhatóan növekedni.[30]

Összegzés

Összegezve a leírtakat elmondható, hogy a SCADA-rendszerek szorosan kapcsolódnak a létfontosságú rendszerelemekhez, hiszen azon létesítményekben alkalmazzák a leginkább ezeket. A szakirodalmi szintetizálás alapján megállapítható, hogy a SCADA az ICS rendszerek egyik ága, valamint további komponenseseket tartalmaz: TRU, MTU, HMI, Historian, illetve egy kommunikációs hálózat. Emellett a rendszereknek számos előnye van, mint például a hatékonyság, a megbízhatóság és az online konfiguráció. A SCADA megfelelő kialakítása és működése, működtetése előírásokhoz

[29] Feldman 2019.
[30] Szádeczky 2021: 111–117.

van kötve, ennek egyik formája a biztonsági keretrendszer, amelyben intézkedések megfogalmazásával segítik elő az említett folyamatot. A keretrendszer mellett különböző szabványok, útmutatások és jó gyakorlatok segítik a szervezeteket, ezek között találhatunk európai, amerikai területi hatályút, de nemzetközi és multilaterális egyezményen alapuló dokumentum is alkalmazható. Ezek az intézkedések 2006 és 2011 között keletkeztek, és bár van olyan részük, amely a mai napig alkalmazandó, bizonyos részük elavult. Ennek okán indult el az ISA112 szabványügyi bizottságának kezdeményezése egy új SCADA-rendszerspecifikus szabvány kialakítására, amely várhatóan 2023 őszén válik elérhetővé. Mindemellett megjelenik még a NIS-irányelv is, amely szintén szabályozza a SCADA-t használó üzemeket, vállalkozásokat. Ezek a szervezetek különböző szektorokba, ágazatokba sorolhatók be. A magyar, az EU-s, illetve az amerikai szabályozások részben átfedéseket tartalmazó ágazatokat nevesítenek. Kiberfenyegetések tekintetében elmondható, hogy kifejezetten a SCADA-rendszerek esetében már 1982-ben detektáltak egy támadást, amelyet trójai vírus telepítésével valósítottak meg. Emellett beszámoltak számos egyéb jellegű incidensről is, legyen szó akár elbocsátott alkalmazott általi vandalizmusról, jogosulatlan hozzáférésről, vagy 0. napi sérülékenység kihasználásáról – ahogy az a leginkább ismert Stuxnet esetében történt. Az utóbbi időben 2013-ban, 2014-ben és 2016-ban számoltak be a legtöbb eseményről, ezek leginkább malware-es támadások voltak, vagy a rendszer feltörését hajtották végre a támadók. A szektorok tekintetében – a magyar szabályozás kategóriáit alkalmazva – elmondható, hogy leginkább az energiaágazat volt a célpont, azonban a vízágazat, valamint az infokommunikációs technológiák ágazati szereplői is beszámoltak őket ért atrocitásról. A SCADA-rendszereket ért támadások formái között megkülönböztethetünk a szoftvereket, illetve a kommunikációt érintő típusokat. A korábban leírtakat figyelembe véve kijelenthető, hogy szükség van a SCADA-rendszerek kiberbiztonsági kockázatainak hatékony kezelésére.

Irodalomjegyzék

Bederna Zsolt – Rajnai Zoltán – Szádeczky Tamás (2021): Business Strategy Analysis of Cybersecurity Incidents. *Land Forces Academy Review,* 26(2), 139–148. Online: https://doi.org/10.2478/raft-2021-0020

Dunn, Thomas (2015): 10 – Basics of Control Systems. In *Flexible Packaging.* Oxford: William Andrew, 103–110. Online: https://doi.org/10.1016/B978-0-323-26436-5.00010-2

ENISA (2011): *Annex III. ICS Security Related Standards, Guidelines and Policy Documents*. Online: www.enisa.europa.eu/publications/annex-iii

Feldman, Sarah (2019): Infographic: IT Says SCADA Will Continue to Be a Frequent Threat. *Statista Infographics,* 2019. március 6. Online: www.statista.com/chart/17267/cyber-security-threats/

G. L., Francis (2016): *SCADA: Beginner's Guide.* [H. n.]: [k. n.].

Kovacs, Eduard (2022): Ransomware Group Claims Access to SCADA in Confusing UK Water Company Hack. *Security Week,* 2022. augusztus 16. Online: www.securityweek.com/ransomware-group-claims-access-scada-confusing-uk-water-company-hack

Krasznay Csaba (2019): Kiberbiztonság a negyedik ipari forradalom korában. *Hiradástechnika: Hírközlés-Informatika,* 74, 25–29.
Megyeri Lajos – Farkas Tibor (2017): Kockázatkezelés, tudomány vagy kuruzslás? *Hadmérnök,* 12(3), 198–209.
Miller, Bill – Rowe, Dale Rowe (2012): A Survey SCADA of and Critical Infrastructure Incidents. *Proceedings of the 1st Annual Conference on Research in Information Technology*, RIIT '12, 51–56. Online: https://doi.org/10.1145/2380790.2380805
National Institute of Standards and Technology (2020): *NIST Special Publication 800-53 Revision 5*. Online: https://doi.org/10.6028/NIST.SP.800-53r5
Paráda István – Farkas Tibor (2020): Felderítés és Analízis a Penetrációs Tesztben – 1. Információgyűjtési Technikák. *Hadmérnök,* 15(1), 159–182. Online: https://doi.org/10.32567/hm.2020.1.11 ; DOI: https://doi.org/10.32567/hm.2020.1.11
Pathak, Neel H. – Patel, Hashmukh (2014): A Review on Modern SCADA Systems and Security Consideration of Individual SCADA System's Components. *International Journal of Engineering Development and Research,* 2(2), 1639–1699.
Petrosyan, Ani (2023): Frequency of Cyber Threats Worldwide by Type 2017 l Statistic. *Statista,* 2023. augusztus 25. Online: www.statista.com/statistics/883591/frequency-cyber-threats-expected-by-senior-it-practitioners-threat-type/
Stouffer, Keith et al. (2020): *NISTIR 8183 Revision 1.* National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.IR.8183r1
Szádeczky Tamás (2021): Víz 4.0? A digitális víziközmű-infrastruktúra kiberbiztonsági kitettsége. *Hadtudomány,* 31(4), 111–117. Online: https://doi.org/10.17047/HADTUD.2021.31.4.111
DPS Telecom (2021): *14 Major SCADA Hacks*. 2021. december 23. Online: www.dpstele.com/blog/major-scada-hacks.php
Tóth András (2022): Information Security Challenges and Solutions in Smart Nations. In Kovács, Anna et al. (szerk.): *Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach.* Heidelberg: Springer Netherlands, 123–132. Online: https://doi.org/10.1007/978-94-024-2174-3_10
Yadav, Geeta – Paul, Kolin (2021): Architecture and Security of SCADA Systems: A Review. *International Journal of Critical Infrastructure Protection,* 34, 100433. Online: https://doi.org/10.1016/j.ijcip.2021.100433

Jogi források

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Online: https://net.jogtar.hu/jogszabaly?docid=a1200166.tv
Az Európai Parlament és a Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148

HADMÉRNÖK
VÉDELEMINFORMATIKA

18. évfolyam (2023) 3. szám 161–176.
DOI: 10.32567/hm.2023.3.11

Katona Gergő[1]

Az autonóm közúti gépjárművek kiberbiztonsági aspektusa és társadalmi megítélése 1. rész

Cybersecurity Aspects and Public Perception of Autonomous Road Vehicles Part 1

Absztrakt

A beépített technológiai megoldások és a vezeték nélküli képességek elterjedésével a mai járművek már nem elszigetelt mechanikus gépek. Egy összekapcsolt rendszer részévé válnak, amelyben folyamatosan kommunikálnak a járművek egyes rendszerelemei egy belső hálózatban, továbbá a járművek egymással és a forgalomirányítási központtal egyaránt. Ezen összekapcsolt adatok halmazát nevezzük önvezető közlekedési eszközök irányítási rendszerének. Ez a rendszer képes támogatni az autonóm közlekedés jövőbeli bevezetését, és a mesterséges intelligencia használatával jelentősen javítani lehet a közlekedés biztonságát, hatékonyságát és fenntarthatóságát. Az autonóm közlekedési eszközök megjelenése azonban új biztonsági kérdéseket vet fel, amelyek az egész rendszert potenciális célponttá teszik a kiberbiztonsági támadásoknak, ezek pedig mind a közlekedés biztonságát, mind pedig az emberi életet veszélyeztethetik.

Kulcsszavak: autonómia, közlekedés, kiberbiztonság

Abstract

With the rise of embedded technologies and wireless capabilities, today's vehicles are no longer isolated mechanical machines. They are becoming part of an interconnected system

[1] Puskás Tivadar Műszaki Szakkollégium, e-mail: katona.gergo@uni-nke.hu

in which vehicles are constantly communicating with their individual system components in an internal network, as well as with each other and with the traffic control centre. This set of interconnected data is called a self-driving traffic management system. This system has the potential to support the future deployment of autonomous transport and to use artificial intelligence to significantly improve the safety, efficiency and sustainability of transport. However, the emergence of autonomous means of transport raises new security issues that make the whole system a potential target for cyber security attacks, which could endanger both transport safety and human life.

Keywords: autonomy, transport, cybersecurity

Problémafelvetés

A globális autonóm járművek piacát 2021-ben 94,43 milliárd USD-ra becsülték, és az előrejelzések szerint 2030-ra eléri a 1808,44 milliárd USD-t, ami 2021 és 2030 között 38,8%-os összetett éves növekedési ütemet mutat. Ezt a fejlődést támogatják a kormányzati finanszírozások, a szabályozási keretek és a digitális infrastruktúrába való befektetések. Emellett fokozott önálló mozgást biztosít a fogyatékossággal élők és a nem járművezetők számára is. Nagy fokú rugalmasságot és kényelmet kínálnak a pihenéshez, az olvasáshoz vagy akár a munkavégzéshez utazás közben, ami javítja a személyek hatékonyságát.[2]

Azonban ezt a fokú növekedést le kell követnie a biztonsági fejlesztéseknek és szabályozásoknak is. A technológiák műszaki-technikai és emberi oldala közötti[3][4] megfelelő összhang csak így biztosítható. Egy önvezető közúti jármű számos olyan technológiából áll, amelyek képesek kommunikálni egymással egy belső hálózaton, illetve képesek egy külső hálózatba adatokat továbbítani és onnan adatokat fogadni. Ezenfelül a járművek különböző megoldásokkal térképezik fel a környezetet, és más-más döntési mechanizmust alkalmaznak. Mind a kommunikáció, mind az egyes rendszerelemek rendelkeznek gyengeségekkel, sérülékenységekkel, amelyek kihasználása súlyos következményekkel jár.[5] Továbbá vizsgálandó terület e technológiáknak a társadalmi elfogadottsága is, illetve fontos felmérni azokat a félelmeket, amelyek megjelennek a társadalomban az önvezető járművek témakörében.

Jelen téma egy kétrészes cikksorozatban jelenik meg, amelynek ez a része bemutatja az autonóm közúti járművek felépítését, valamint a téma előfordulását a különböző közösségimédia-felületeken, illetve hírportálokon.

A második cikk az egyes autonóm rendszerelemeket fenyegető kockázatokat tárja fel, illetve azokat a megoldásokat, amelyek e kihívásokat hivatottak megszüntetni.

[2] Lásd: www.precedenceresearch.com/autonomous-vehicle-market
[3] Deutsch et al. 2019.
[4] Deutsch–Berényi 2023: 10–15.
[5] Megyeri–Farkas 2017: 205–206; Paráda–Farkas 2020: 159–182.

Ezenfelül bemutatom kérdőíves felmérésem eredményét, amelynek középpontjában az autonóm közúti járművek társadalmi megítélésének vizsgálata állt.

Kutatási módszertan

A cikkben megjelenő eredménytermékekhez megvizsgáltam egy state-of-art analízissel, hogy milyen technológiai megoldásokra van szükség az önvezető közúti járművek kialakításához. Szentimentanalízist végeztem, amelyben megvizsgáltam, hogy a világhálón, globális szinten az önvezető járművekkel kapcsolatos tartalmak hol és milyen formában jelennek meg.

Eredmények

Az autonóm vezetés műszaki aspektusai

Autonóm vezetés definiálása

Ahhoz, hogy megvizsgáljuk az autonóm közlekedési eszközök egyes aspektusait, fontos tisztázni, hogy mit is értünk autonóm jármű alatt. Ki kell hangsúlyozni, hogy az önvezetés fogalmát jelen kutatásban műszaki kontextusban használom fel.

Ehhez számos definíciót találunk a legáltalánosabbtól kezdve a komplexebb terminológiai rendszerig ebben a témában. Kichun Jo és szerzőtársai például a következő meghatározással éltek: Az autonóm jármű olyan közlekedési eszköz, amely emberi beavatkozás nélkül képes vezetni magát.[6] Tehát az autonóm rendszer olyan műszaki egység, amely bizonyos feladatokat ellát anélkül, hogy bármilyen emberi parancsoktól függene. Azonban, hogy műszaki értelemben részletesen tudjuk vizsgálni az önvezető járműveket, pontosabb definícióra lesz szükség. Ehhez szükséges egy olyan definíciós rendszer, amely kategorikus különbségeket tesz az automatizálás különböző módjai (szintjei) között. Erre az autóipari mérnökök globális szövetsége, a SAE International jelentését használtam fel, amelynek címe *A közúti gépjárművek vezetési automatizálási rendszereivel kapcsolatos kifejezések taxonómiája és meghatározása* (J3016™ szabványként is ismert).

A jelentés a vezetési automatizálás hat szintjét határozza meg az automatizálás nélkülitől a teljes automatizálásig. A kulcsfontosságú különbség a 2. és a 3. szint között van, hogy míg a 2. szinten a vezető végzi a dinamikus vezetési feladat egy részét, addig 3. szinten az automatizált vezetési rendszer látja el a dinamikus vezetési feladatok többségét. A 3. szint felett szintenként egyre nagyobb részt végez el a jármű e vezetési feladatokból. Azonban fontos definiálnunk a „dinamikus vezetési feladat" fogalmát, amely magában foglalja a vezetési feladat operatív részét (például

[6] Jo–Kim–Sunwoo 2018.

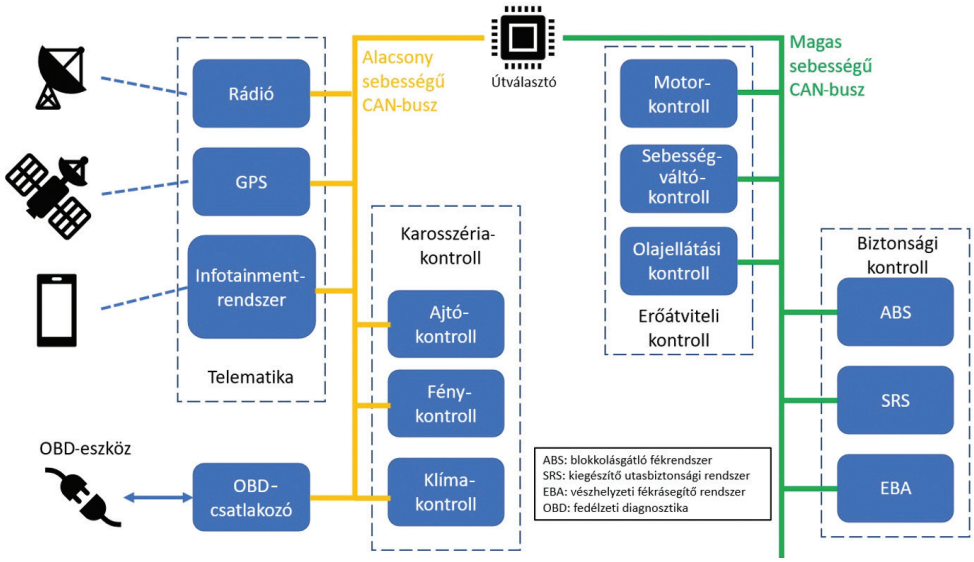
kormányzás, fékezés, gyorsítás, jármű és úttest figyelése) és taktikai részét (például eseményekre való reagálás, sávváltás, kanyarodás, jelzések használata stb.), de nem tartozik bele a vezetési feladat stratégiai aspektusa (például utazástervezés).[7]

Jelen cikkben az önvezető közúti járművek három fő rendszerelemét azonosítjuk és elemezzük kiberbiztonsági szempontból. E rendszerelemek megvizsgálásakor törekedtem a teljesen automatizált járműkategória feltérképezésére. A három rendszerelem csoportosításánál fontos azt kiemelni, hogy ezek a rendszerek nem szeparálhatók el egymástól teljesen, hiszen például egy GNSS- (Global Navigation Satellite System) technológia elősegíti az önvezetést mint képességet, illetve a kommunikációt is, hiszen képes a helyzetét kommunikálni a környezetével.

Gépjárművezérlő rendszerek

Az egyik legfontosabb egység ebben a kategóriában az elektronikus vezérlőegység (*electronic control units,* ECU). Az ECU vezérli például a jármű motorjának elektronikáját, a sebességváltót, az elektromos zár, a légzsák, a légkondicionáló rendszer és a fényvezérlés moduljait.[8] Jellemzően a kis és közepes méretű járművek körülbelül 50 ECU-t tartalmaznak, és legalább 70-et foglalnak magukban a luxusautók. Egyes csúcskategóriás járművek akár 80 ECU-val is rendelkeznek. A járműben lévő hálózat összeköti az ECU-kat és továbbítja az adatokat közöttük. Ez a hálózat magában foglalja többek között a vezérlőterületi hálózatot (*controller area network,* CAN), a helyi összekötő hálózatot (*local interconnect network,* LIN), ethernetet. A LIN egy alacsony sebességű hálózat, amelyet általában ajtózárakhoz, klímaberendezésekhez, biztonsági övekhez, napfénytetőhöz és tükörvezérlőhöz használnak. A FlexRay egy új generációs busztechnológia, amely nagy sebességű és hibatűrő kommunikációt biztosít.[9] Jelen vizsgálat a CAN-hálózat felépítésére és sebezhetőségeire fókuszál, mivel ez a hálózat a legelterjedtebb az autóiparban. Az 1. ábra mutatja be egy közúti gépjármű belső hálózatát, amely CAN-buszhálózatot használ. Jól látható, hogy ennek a buszrendszernek két típusa van. Az alacsony sebességű CAN-hálózat főleg a telematika és a karosszéria kontrollegységeiért felel, míg a magas sebességű rendszer főleg a jármű konkrét vezérléséért. Itt találhatók meg az erőátvitelért felelős ECU-k, mint például a sebességváltó kontrollja vagy a motor kontrollja.[10]

[7] SAE International 2021.
[8] Tóth 2017: 195–206.
[9] Kim et al. 2021: 102–150.
[10] Liu et al. 2017: 50–58.



1. ábra: A CAN-hálózat felépítése
Forrás: a szerző szerkesztése LIU *et al. 2017: 50–58. alapján*

Az ebbe a CAN-hálózatba kapcsolt ECU-k az üzeneteket CAN-keretbe küldik meg egymásnak. A CAN-keret felépítése az 1. táblázatban látható.

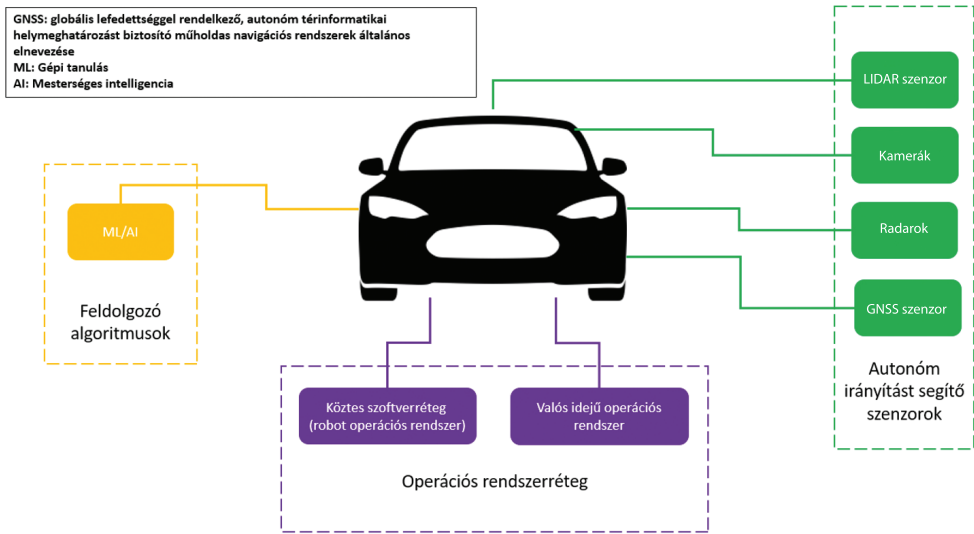
1. táblázat: A CAN-keret felépítése

CAN-keret részének megnevezése	**Funkciója**
Start of Frame	A keret kezdetét jelzi.
Identifier Field	Azonosító mező, többnyire az adatmező tartalmát azonosítja. Az RTR bittel együtt meghatározza a keret prioritását is.
RTR (Remote Transmit Request)	Távoli átviteli kérelem.
Control Field	Az adatmező hosszát adja meg.
Data Field	A tartalma tetszőleges.
CRC (cyclic redundancy check) Field	A ciklikus redundancia-ellenőrzés az üzenet hibamentes célba juttatását segíti.
ACK (acknowledge)	Az elfogadó bit a CRC-mező végén van, és ezt a bitet a vevő felülírja, ezzel tudatja a küldővel, hogy a küldés sikeres.
End of Frame	Ez a szakasz jelenti az üzenet végét.

Forrás: a szerző szerkesztése www.kvaser.com/can-protocol-tutorial/##canMessages alapján

Autonóm vezetési rendszerelemek

A 2. ábrán láthatók azon rendszerelemcsoportok, amelyek az önvezetést mint funkciót biztosítják. E fejezetben az ábrán megjelölt rendszerelemek bemutatása következik.



2. ábra: Az önvezetést biztosító rendszerelemek
Forrás: a szerző szerkesztése

Autonóm irányítást segítő szenzorok

Az önvezető járművek különböző érzékelőkre támaszkodnak a valós idejű helymeghatározás és a környezet érzékelése érdekében. A LiDAR, a kamera, a radar és a GNSS a legfontosabb érzékelők, amelyeket a különböző autonóm vezetési rendszerek használnak. Az ezekből az érzékelőkből gyűjtött adatokat a rendszer átalakítja és feldolgozza, legtöbbször a gépi tanulás technológiáját alkalmazva. Ezen érzékelőknek különböző feladata van távolságérzékelés szerint:

- Közeli érzékelés (0–5 m): az ultrahangos érzékelők olyan közelségérzékelők, amelyek célja az akadályok érzékelése a karosszériától néhány méteren belül. Elsősorban alacsony sebességű forgatókönyvekhez, például parkolássegítéshez tervezték őket.
- Kis hatótávolságú érzékelés (5–30 m): az előre néző kamerákat a sávelhagyásra figyelmeztetésre, a jelzőtáblák felismerésére, a hátrafelé néző kamerákat pedig parkolássegítésre használják.
- Közepes hatótávolságú érzékelés (80–160 m): a LiDAR és a közepes hatótávolságú radarok (*medium range radars,* MRR) az ütközéselkerülést és a gyalogosok felismerését biztosítják.

- Nagy hatótávolságú érzékelő (160–250 m): A nagy hatótávolságú radarok (*long-range radars,* LRR) adaptív sebességtartó automatika számára biztosítanak információkat, főleg nagy sebességnél.[11]

Ezeket az autonóm vezetést elősegítő érzékelőket a következő módon definiálhatjuk:

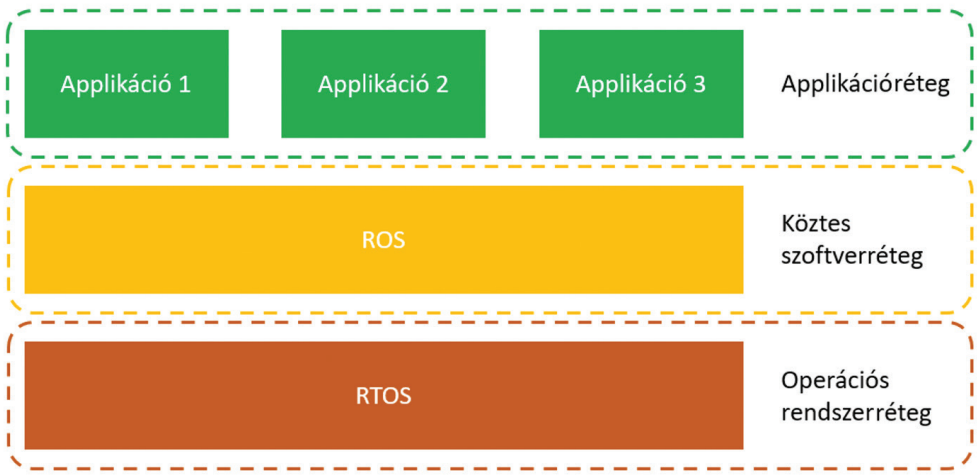
- A globális navigációs műholdrendszer egy műholdalapú helymeghatározó, navigációs és időmérő (Position, Navigation and Timing, PNT) rendszer. Jelenleg számos GNSS van a kiépítés és a működés különböző szakaszaiban. Az amerikaiak által használt globális helymeghatározó rendszer (Global Positioning System, GPS) vitathatatlanul a legismertebb. Mindazonáltal az európai vezetésű GALILEO, az orosz vezetésű GLONASS, a kínai BeiDou, az India által vezetett IRSS és a japán QZSS mellett áll.[12] Kollektív keretrendszerként a GNSS globálisan meghatározó és költséghatékony kültéri PNT-technológiává vált. Az egyes GNSS-technológiák alkalmazása elengedhetetlen egy önvezető jármű esetében, a pontos helymeghatározás érdekében. Továbbá az intelligens közlekedési rendszerben az egyes járművek és forgalmi helyzetek meghatározásához is szükséges e szenzorok alkalmazása.
- Több érzékelő, például a fényérzékelő és távolságmérő szenzor (Light Detection and Ranging, LiDAR), a kamerák, a radar és az ultrahang csatlakozik a döntéshozó mikrokontrollerhez különféle interfészeken, például Etherneten, CAN-hálózaton keresztül. A LiDAR-szenzor nyers bemenetét 3D pontfelhőnek nevezzük, amelynek dimenziója n×4, ahol n az adatpontok számát jelöli, és minden adatpont 4 dimenziós, amely áll egy 3D vektorból, wx, wy és wz koordinátákkal, valamint a pont intenzitásából. Ezeket az adatokat dolgozza fel a rendszer, és detektálja az akadályokat.[13]
- A kamerákat széles körben alkalmazzák az önvezető járművekben. Az autonóm és félautonóm járművek (SAE 2-es és magasabb szint) több pozícióban elhelyezett kamerákra támaszkodnak, hogy 360 fokos képet kapjanak a jármű környezetéről. A kamerák olyan fontos autonóm feladatokhoz nyújtanak információkat, mint például a közlekedési táblák felismerése és a sávfelismerés.[14] A kamerák a LiDAR helyettesítésére is használhatók tárgyészlelési feladatokhoz és alacsonyabb költségű távolságmérésekhez, de bizonyos helyzetekben, például esőben, ködben vagy hóban gyenge teljesítményt nyújtanak. A LiDAR-ral és a radarokkal együtt a kamerák bőséges és változatos adatokat szolgáltatnak az autonóm vezetéshez.
- A radar olyan érzékelő, amely elektromágneses hullámokat bocsát ki a rádió- vagy mikrohullámú tartományban, hogy észlelje a tárgyakat és mérje távolságukat és sebességüket a visszavert jelek érzékelésével. Az önvezető járművek esetében a radarok számos alkalmazásban hasznosak. Például a kis hatótávolságú

[11] Yan–Xu–Liu 2016.
[12] Santra et al. 2019: 2995–3008.
[13] Cao et al. 2019: 2267–2281.
[14] Bar Hillel et al. 2014: 727–745.

radarok lehetővé teszik a parkolás elősegítését. A nagy hatótávolságú radarok pedig segítik az automatikus távolságszabályozást és fékrásegítést.[15]

Operációs rendszerréteg

Itt két fő típusról beszélhetünk az autonóm járművek esetében. Az egyik, amely az önvezető funkciók összehangolásáért és működéséért felel, ebben megtalálható a valós idejű operációs rendszer (*real-time operating system,* RTOS), illetve a másik, amire szükségünk van az RTOS mellett, egy köztes szoftverréteg, amely összekapcsolja a különböző autonóm vezetési szolgáltatásokat. Ezt a legtöbb létező autonóm vezetési megoldás a robot operációs rendszer (*robot operating system,* ROS) segítségével éri el.



3. ábra: Az operációs rendszerréteg bemutatása
Forrás: a szerző szerkesztése Azumi–Maruyama–Kato 2020. alapján

Az RTOS operációs rendszerben van egy ütemező nevű modul, amely ütemezi a különböző feladatokat, és meghatározza, hogy egy folyamat mikor fusson le a processzoron, és így érhető el, hogy az egyes feladatok akár egyszerre is lefussanak. Két típusa van, a kemény és a puha RTOS. A kettő közötti különbség, hogy a kemény rendszer esetében határidőket határoznak meg, és a feladatokat az adott időkereten belül kell végrehajtani, különben a késlekedés katasztrofális következményekkel járhat, például légzsákrendszer esetében. A puha rendszernél annak válaszideje elsődleges, de nem kritikus a rendszer működése szempontjából, tehát a határidő fontos, de a rendszer elfogadja a határidők esetenkénti elmulasztását is.

A ROS egy kommunikációért felelős köztes szoftver, amely megkönnyíti az autonóm járműrendszer különböző részei közötti kommunikációt. Például a képrögzítő szolgáltatás üzeneteket tesz közzé a ROS-on keresztül, és mind a lokalizációs

[15] Yan–Xu–Liu 2016.

szolgáltatás, mind az akadályérzékelő szolgáltatás lekéri a közzétett képeket, hogy helyzet- és akadályfrissítéseket generáljon.[16]

Feldolgozó algoritmusok

Az automatizált vezetési rendszerek gyors fejlődésével a biztonságos vezetési környezethez elengedhetetlen a stabil és megbízható környezetelemzés. A feldolgozó algoritmusok olyan megoldások, amelyek az egyes autonóm közlekedést segítő szenzorok adatait dolgozzák fel, például a kameraalapú útszegmentálásnak mára már számos megoldása létezik. Ez a feldolgozás a 3. ábrán, az applikációrétegen megy végbe. E feldolgozást elősegíti a járművekbe implementált gépi tanulás is. A mélytanuláson alapuló képszemantikai szegmentálás az egyik legjobb megoldás, mivel kellően nagy kiterjedésű és bonyolult környezeteket képes kielemezni. A rögzített képet több régióra tagolja, és minden egyes pixel osztályát (objektumát) felismeri, így pixelszintű osztályozásnak tekinthető. A képosztályozástól eltérően a képszemantikai szegmentálás azonosítja a képeken található objektumosztályokat és megtalálja a képeken lévő objektumok helyét is. Ezenkívül pontos objektumhatár-információkat szolgáltat.[17] Az egyik ilyen technológiai megoldás a konvolúciós neurális hálózat (*convolutional neural networks,* CNN), amelyet már alkalmaznak számos járműmodellnél.

Külső kommunikációt támogató rendszerelemek

A külső kommunikációt részlegesen érintettem a szenzorok esetében, amikor például a GNSS-szenzort vizsgáltam, illetve a CAN-rendszernél a további műholdas kommunikáció is érintve volt. Azonban ezt a részt azért terveztem külön fejezetben tárgyalni, mert igen fontos annak a vizsgálata, hogy egy ilyen önvezető jármű pontosan mivel kapcsolódik még, és ezt milyen céllal teszi. Itt egy új rendszer fogalmát is tisztázni kell, amely nem más, mint az intelligens közlekedési rendszer (*intelligent transport system,* ITS), amely az összekapcsolt járművek rendszere. Ahol a járművekbe épített érzékelők és egy központi közlekedésirányítási rendszer adatai alapján a jármű képes az intelligens döntéshozatalra.[18]

Ez a rendszer azért is hangsúlyos, mert ezáltal a járműveknek nem csak a saját adataikra kell támaszkodniuk, például olyan esetekben, amikor a beépített szenzorok nem, vagy csökkent képességekkel rendelkeznek,[19] hanem egy központi rendszer tud adatot szolgáltatni olyan információkról, amelyeket a szenzorok a távolsági vagy akadályi korlátok miatt nem képesek érzékelni.

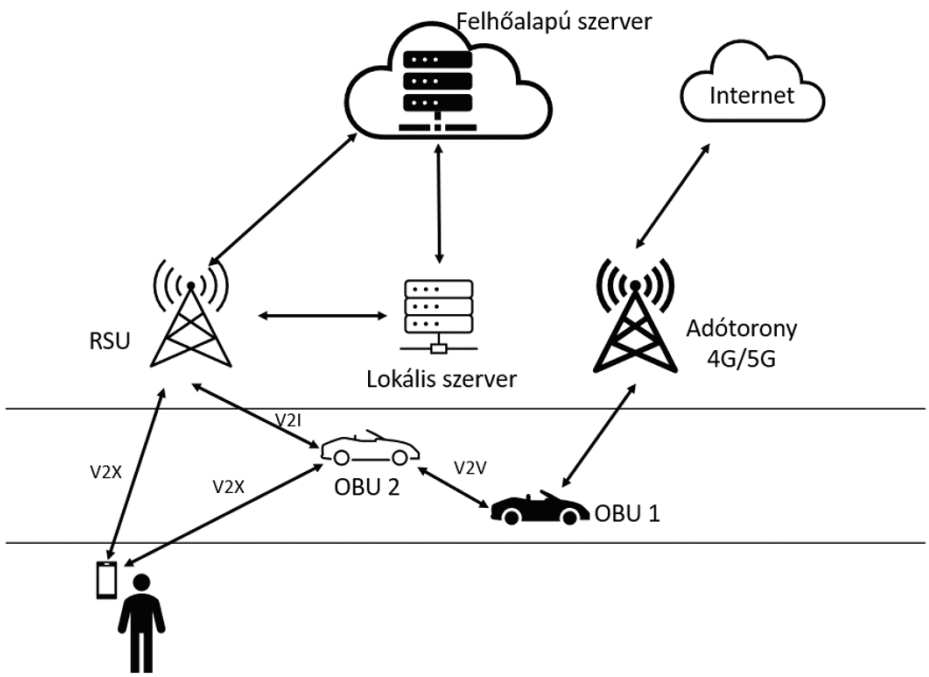
Az ITS keretében a kritikus vezetési információk megosztása a jármű ad hoc hálózatán (*vehicular ad hoc network,* VANET) megy végbe. Ez a VANET három fő kommunikációs típust különböztet meg:

[16] Azumi–Maruyama–Kato 2020.
[17] Chen et al. 2020.
[18] Zhao–Walker–Wang 2012: 107–115.
[19] Orbók 2015: 221–226.

- V2V (vehicle-to-vehicle) kommunikáció, amely a járművek egymással való kommunikációja;
- V2I (vehicle-to-infrastructure) kommunikáció, amely a járművek és a környező infrastruktúra kommunikációja;
- V2X (vehicle-to-everything) kommunikáció, amely a legtágabb csoport, magában foglalja az előző két területet, és tovább bővíti olyan eszközökkel, amelyek képesek a kommunikációra, illetve helyzetmeghatározásra, ilyen például a gyalogosok okostelefonja.[20]

Fontos az ITS-ben részt vevő elemeket is azonosítani, amelyek kommunikálnak egymással. Ezek a következők:

- fedélzeti egység (*on-board unit,* OBU), amely a járművekbe szerelt adóvevő;
- út menti egység (*road-side unit,* RSU), olyan adóvevő, amely az út mentén biztosítja a kommunikációt a közlekedési központ és a járművek között;
- digitális cellás távközlési állomások, amelyek biztosítják például a 4G és 5G kommunikációt;
- felhőalapú számítási réteg az, amely kezelheti a földi szervereken kívül az ITS-adatokat.[21]



4. ábra: Intelligens közlekedési rendszer lehetséges felépítése
Forrás: a szerző szerkesztése Al-kahtani 2012; Syfullah–Lim 2017. *alapján*

[20] Mostafa et al. 2011: 756–761.
[21] Al-kahtani 2012; Syfullah–Lim 2017.

A VANET három fő kommunikációs szabványt használ, amelyeket dedikáltan a járművek kommunikációjára alakítottak ki.

- Dedikált rövid távú kommunikáció (Dedicated Short Range Communications, DSRC) 75 MHz-es sávszélességű spektrumban található 5850–5925 GHz között. Ezt az amerikai Szövetségi Kommunikációs Bizottság (Federal Communication Commission, FCC) jelölte ki a jármű kommunikációja számára. A DSRC sáv 7 dedikált csatornára lett felosztva.
- A Villamos és Elektronikai Mérnöki Intézet (Institute of Electrical and Electronics Engineers, IEEE) által kiadott 1609 szabványcsalád a vezeték nélküli hálózati hozzáférésekkel foglalkozik a járműkörnyezetben (Wireless Access in Vehicular Environments, WAVE). E szabványok olyan architektúrát és szabványosított szolgáltatásokat, valamint interfészeket határoznak meg, amelyek lehetővé teszik a biztonságos VANET kommunikációt.[22]
- Az IEEE 802.11 eszközök olyan környezetben használhatók, ahol a fizikai réteg tulajdonságai gyorsan változnak, és ahol nagyon rövid ideig tartó kommunikációs adatcserére van szükség. A 802.11p meghatározza a VANET-ek fizikai és köztes hozzáférési rétegét.[23]

Az autonóm vezetés társadalmi megítélése

A cikkben vizsgálat alá vetettem az önvezető járművekkel kapcsolatos társadalmi megítélést. Ez az elemzés két fő részből áll, egy közösségimédia-elemzésből, ahol megvizsgálom, hogy miként jelenik meg a téma az egyes online felületeken, illetve egy kérdőíves kiértékelésből, amelyben többek között azt nézem meg, hogy mennyire tartanak a kitöltők az autonóm járművek használatától. Jelen cikkben a téma online platformokon való megjelenésének különböző aspektusait mutatom be. A cikksorozat második részében a társadalmi megítélés vizsgálatának kérdőívből származó eredménye jelenik majd meg.

Onlinetartalom-analízis

Ebben a fejezetben megvizsgáljuk, hogy az önvezető járművek témája miként jelenik meg az interneten. Ehhez a SentiOne[24] weboldalt használtam, amely teljes világot lefedő, 70 nyelvet feldolgozó és webes szöveganalitikán alapuló social listening szoftver. Ez kulcsszavas keresés alapján, valós időben vagy akár 3 évre visszamenőleg figyeli, indexálja és elemzi az internetes fórumokon, blogokon, weboldalakon és közösségimédia-csatornákon közzétett publikus szöveges tartalmak minden típusát, amelyek önmagukban vagy kontextusukban tartalmazzák a felhasználó által már előre definiált és a platformra felvitt kulcskifejezések bármelyikét. A SentiOne jelenlegi adattárházában

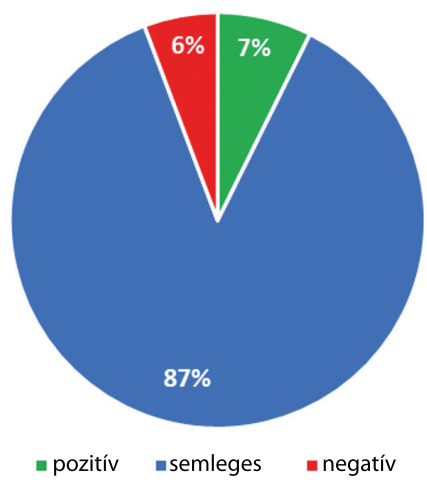
[22] Mejri – Ben-Othman – Hamdi 2014: 53–66.
[23] IEEE 2010.
[24] Lásd: https://sentione.com/hu

több mint 20 milliárd említés érhető el, és ez napról napra bővül. A nyelvfelismeréshez a SentiOne saját fejlesztésű algoritmust használ, amely a lingvisztikai tulajdonságokat és az elérhető metaadatokat is figyelembe veszi, így 99,93 százalékos pontossággal képes detektálni adott nyelvet. A rendszer működését több mint 200 dedikált offline adattároló szerver biztosítja, és nyílt forráskód alapján működik. A SentiOne a különböző socialmedia-oldalakról a hivatalos és nyilvános API-hozzáféréseken keresztül gyűjti be az adatokat. Például a legnépszerűbb Facebook-oldalak automatikusan bekerülnek a rendszerbe, az új oldalakat pedig a rendszerben már korábban is használt, felhasználói kulcsszóbázis alapján keresi és találja meg a technológia. A releváns tartalmakat kvantitatív kutatás céljából és ezt megkönnyítendő, különböző fókuszpontok és kutatási paraméterek mentén rendezi össze, amelyeket interaktív grafikonokon ábrázol. A kvalitatív mélyelemzéseket is támogató módszertani, technológiai felépítés pedig biztosítja a kutatáshoz kapcsolódó összes indexált tartalom, poszt, komment, cikk és említés egyenkénti elemzésének és kategorizálásának lehetőségét is.[25]

Az elemzés részletei

A vizsgált időtartam 2019. április 3-tól 2022. március 5-ig terjedt, ahol a következő kulcsszavakra kerestem rá: automated vehicle, intelligent vehicle, automated car, intelligent car, autonomus car, self-driving car, önvezető jármű, önvezető autó, autonóm jármű.

Az látható, hogy összesen ez alatt az idő alatt 221 146 találat született, amelynek a szentimentanalízis szerint 86,93%-a semleges megjegyzés volt, közel 5,73%-a negatív és 7,33%-a pozitív.

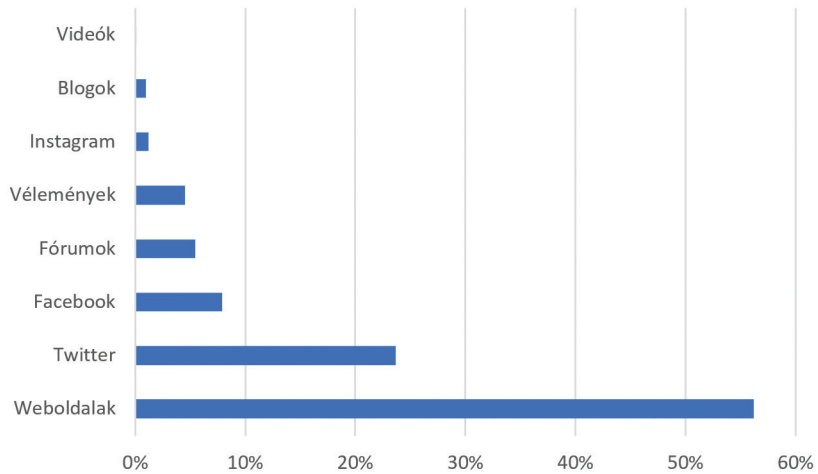


5. ábra: A posztok érzelmi töltete
Forrás: a szerző szerkesztése a SentiOne alapján

[25] Bányász–Tóth–László 2022: 99–125.

A SentiOne algoritmusa mind magyar, mind angol nyelven megvizsgálta a tartalmakat, hogy milyen szövegezéssel írták azt a bejegyzést, negatív, pozitív vagy semleges. Ez az eredmény azért jöhetett ki, mert van olyan megosztás, amelyben nem írnak semmit az adott tartalomról, amelyben a kulcsszavak szerepelnek, így az algoritmus nem tudja a megosztó látásmódját vizsgálni. Azonban ez a magas arány azzal is magyarázható, hogy a megosztások nagy része informatív jellegű volt, vagyis a megosztó személy vagy oldal információt akart megosztani a témában, nem pedig véleményét kifejteni.

Ezenfelül megvizsgáltam, hogy milyen platformokon fordultak elő a vizsgált kifejezések. Itt az látható, hogy a weboldalakon jelenik meg legnagyobb arányban az önvezető járművekről tartalom 56%-kal, ezt követi az X (amely a vizsgálat ideje alatt a Twitter nevet viselte) 24%-kal, majd a Facebook 8%-kal és a fórumok és vélemények 5-5%-kal, míg a blogok és az Instagram 1-1%-kal. Ez a megoszlás magyarázatot ad arra, hogy a szentimentanalízis során miért volt ilyen nagy arányú a semleges érzelmű tartalom, mivel a weboldalakon a szerzők nem a véleményüket írták le, hanem a témával kapcsolatban információt szándékoztak megosztani.



6. ábra: A posztok megjelenési platformjai
Forrás: a szerző szerkesztése a SentiOne alapján

Jelen esetben a weboldalak olyan szakmai és hírközlő oldalakat jelentenek, mint a VentureBeat,[26] a Green Car Reports[27] vagy a *Forbes*[28] magazin.

Így azt lehet megállapítani, hogy az önvezetés témája az online térben szakmai és híroldalakra korlátozódik, és nem épült be még szervesen a közösségimédia-platformokra. Ennek magyarázata az lehet, hogy jelenleg csak egyes autonóm funkciók

[26] VentureBeat: https://venturebeat.com/
[27] Green Car Reports: www.greencarreports.com/
[28] *Forbes:* www.forbes.com/

érhetők el a közúti járművekben, ami még nem alkalmas biztonságos önvezetés biztosítására.

Összegzés

A jelen cikkben megjelenő kutatási eredmény rámutatott arra, hogy az önvezető közúti járművek nem azonosíthatók különálló rendszerként, hanem inkább egy ökoszisztéma tagjaként. Ezen ökoszisztémának számos más szereplője is lehet, más-más technológiával és céllal. A technológiai vizsgálat azonban arra is rámutatott, hogy a jármű egyes rendszerelemtípusait sem tudjuk elszigetelten külön kezelni. A járművön belüli rendszerek is nagyban függenek az egymástól kapott információktól, ami felértékeli a kiberbiztonság három alapelvének (bizalmasság, sértetlenség, rendelkezésre állás) folyamatos meglétét. Az online térben az látható, hogy az önvezetés témaköre jelenleg a szakmai és híroldalakra korlátozódik.

Irodalomjegyzék

Al-kahtani, Mohammed Saeed (2012): Survey on Security Attacks in Vehicular ad hoc Networks (VANETs). *2012 6th International Conference on Signal Processing and Communication Systems*. IEEE, 1–9. Online: https://doi.org/10.1109/ICSPCS.2012.6507953

Azumi, Takuya – Maruyama, Yuya – Kato, Shinpei (2020): ROS-lite: ROS Framework for NoC-Based Embedded Many-Core Platform. In *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 4375–4382. Online: https://doi.org/10.1109/IROS45743.2020.9340977

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

Bar Hillel, A. et al. (2014): Recent Progress in Road and Lane Detection: A Survey. *Machine Vision and Applications,* 25, 727–745. Online: https://doi.org/10.1007/s00138-011-0404-2

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

Cao, Yulong et al. (2019): Adversarial Sensor Attack on Lidar-based Perception in Autonomous Driving. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2267–2281. Online: https://doi.org/10.1145/3319535.3339815

Chen, Ping-Rong et al. (2020): DSNet: An Efficient CNN for Road Scene Segmentation. *APSIPA Transactions on Signal and Information Processing,* 9(1), e27. Online: https://doi.org/10.1017/ATSIP.2020.25

Deutsch Nikolett et al. (2019): *A technológia szerepének stratégiai felértékelődése: Szemelvények a stratégiai technomenedzsment témaköréből.* Budapest: Budapesti Corvinus Egyetem.

Deutsch Nikolett – Berényi L. (2023): A technomenedzsment funkciói. *Magyar Minőség,* 32(6), 10–15.

IEEE (2010): IEEE Standard for Information technology – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments, 2010: IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009), 1–51. Online: https://doi.org/10.1109/IEEESTD.2010.5514475

Jo, Kichun – Kim, Chansoo – Sunwoo, Myoungho (2018): Simultaneous Localization and Map Change Update for the High Definition Map-Based Autonomous Driving Car. *Sensors,* 18, 3145. Online: https://doi.org/10.3390/s18093145

Kim, Kyounggon et al. (2021): Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense. *Computers & Security* 103, 102–150. Online: https://doi.org/10.1016/j.cose.2020.102150

Liu, Jiajia et al. (2017): In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions. *IEEE Network,* 31(5), 50–58. Online: https://doi.org/10.1109/MNET.2017.1600257

Megyeri Lajos – Farkas Tibor (2017): Kockázatkezelés, tudomány vagy kuruzslás? *Hadmérnök,* 12(3), 198–209.

Mejri, Mohamed Nidhal – Ben-Othman, Jalel – Hamdi, Mohamed (2014): Survey on VANET Security Challenges and Possible Cryptographic Solutions. *Vehicular Communications,* 2(1), 53–66. Online: https://doi.org/10.1016/j.vehcom.2014.05.001

Mostafa, Ahmad et al. (2011): A V2X-based Approach for Reduction of Delay Propagation in Vehicular Ad-Hoc Networks. In *2011 11th International Conference on ITS Telecommunications,* IEEE, 756–761. Online: https://doi.org/10.1109/ITST.2011.6060155

Orbók Ákos (2015): Az autonóm közlekedési technológia kihívásai. *Társadalom és Honvédelem,* 19(1), 221–226. Online: http://real.mtak.hu/50243

Paráda István – Farkas Tibor (2020): Felderítés és analízis a penetrációs tesztben – 1. Információgyűjtési technikák. *Hadmérnök,* 15(1), 159–182. Online: https://doi.org/10.32567/hm.2020.1.11

SAE International (2021): *J3016C: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.* Online: www.sae.org/standards/content/j3016_202104/

Santra, Atanu et al. (2019): Augmentation of GNSS utility by IRNSS/NavIC constellation over the Indian region. *Advances in Space Research*, 63(9), 2995–3008. Online: https://doi.org/10.1016/j.asr.2018.04.020

Syfullah, Mohammad – Lim, Joanne Mun-Yee (2017): Data Broadcasting on Cloud-VANET for IEEE 802.11p and LTE Hybrid VANET Architectures. *2017 3rd International*

Conference on Computational Intelligence Communication Technology (CICT), IEEE, 1–6. Online: https://doi.org/10.1109/CIACT.2017.7977321

TÓTH András (2017): Information Security for Electric Cars in Accordance with Nist Critical Infrastructure Cybersecurity Framework. *Hadmérnök,* 12(4), 195–206.

YAN, Chen – XU, Wenyuan – LIU, Jianhao (2016): *Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle.* Def Con.109.

ZHAO, Meiyuan – WALKER, Jesse – WANG, Chieh-Chih (2012): Security Challenges for the Intelligent Transportation System. In *Proceedings of the First International Conference on Security of Internet of Things,* ACM, 107–115. Online: https://doi.org/10.1145/2490428.2490444

HADMÉRNÖK
VÉDELEMINFORMATIKA
18. évfolyam (2023) 3. szám 177–187.
DOI: 10.32567/hm.2023.3.12

Szeleczki Szilveszter[1]

A metaverzum értelmezése és katonai célú meghatározása 1. rész – fogalmi szintű értelmezés[2]

Interpreting the Metaverse and Its Definition for Military Purposes Part 1 – Conceptual Interpretation

Absztrakt

Társadalmunkban intenzív fejlesztések tapasztalhatók számos területen, ami az emberek információs környezetének megváltozásával jár. Az információcserék és maga az információs környezet jelentősen befolyásolja a mindennapokat, aminek vonatkozásában a többdimenziós virtuális tér lehetőségeinek feltárása is aktuálissá vált. A jelenkorban egy már közismert szó, a metaverzum köré egy komplex képesség lett társítva, amely, mondhatni, még alakulóban lévő, formálódó szegmens a csúcstechnológiák innovatív folyamataiban. A metaverzummal kapcsolatos, már publikált szakmai dokumentációk vizsgálatával célom meghatározni a metaverzum civil és katonai fogalmát. Egy egységes, minden kapcsolódó szegmensre kiterjedő fogalmi vizsgálat a téma értelmezésének fontos kiindulópontja. A történeti előzmények, a főbb célok, az elvárható követelmények és technológiák vizsgálatával a metaverzum civil és katonai oldalról is értelmezhetővé válik.

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 ösztöndíjprogramjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Abstract

In our society, we are witnessing intense developments in many areas, which are changing the information environment in which people live. Information exchanges and the information environment itself have a significant impact on everyday life, in relation to which the exploration of the potential of a multidimensional virtual space has become topical. In the present day, a complex capability has been associated around a well-known word, metaverse, which is still a nascent and formative segment in the innovative processes of high technologies. My aim is to define the civilian and military concepts of metaverse by examining the already published technical documentation on metaverse. A coherent, conceptual analysis covering all related segments is an important starting point for the interpretation of the topic. By looking at the historical background, the main objectives, the requirements and the expected technologies, it will be possible to understand metaverse from both a civilian and a military perspective.

Keywords: metaverse, virtual, info communication, network, military

Bevezetés

A jelenleg folyamatban lévő kutatási területek közül kiemelkednek azok, amelyek kifejezetten az emberek mindennapos tevékenységeit támogató eszközök és rendszerek fejlesztési és üzemeltetési kérdéseivel foglalkoznak. A 21. században az embereket jelentős mértékben körülveszik infokommunikációs hálózatok. Minden bizonnyal kijelenthető, hogy a legtöbb ember egyfajta hibrid társadalmi életformát folytat, amelyben a valós, fizikai tér mellett a digitális, mesterségesen létrehozott virtuális tereket is felhasználja. Manapság az olyan digitális eszközök, mint a számítógépek vagy a telefonok, valamint azok hálózatai rendkívüli módon befolyásolják a mindennapi folyamatokat. Az internet hálózatán keresztül tömeges információs inger éri az embereket, aminek eredményeképpen társadalmunk megtanult az infokommunikációs technológiák folyamatos felhasználásával együtt élni. A virtuális terek realisztikus élményeket adnak a felhasználók részére, ami megfigyelhető többek között a számítógépes játékok esetén. Új technológiák bevezetésével párhuzamosan, sok esetben új fogalmakat, rendszerszintű struktúrákat, módszereket és eljárásokat is meghatároznak.

A tudományos életben a civil szféra mellett természetesen a katonai gondolkodásban is érdekeltek az új technológiák. A katonai fejlesztések körüli kutatások eredményeképpen a katonai vezetők gondolkodásában újszerű értelmezések és megfogalmazások születnek. Az infokommunikációs technológiák (IKT) fejlődése és azok sokrétű katonai alkalmazhatósága újabb és újabb elképzelésekkel bővíti a hadtudományi szakirodalmat. A NATO az elmúlt évtizedekben folyamatosan meghatározott újabb és újabb képességeket és követelményeket az IKT-k felé, figyelembe véve a technológiai fejlődést, a felhasználói képességeket[3] és a geopolitikai helyzetet.[4] Kifejezetten

[3] Farkas 2021: 9–15.
[4] Farkas 2020: 281–289.

aktuális témának tekinthető a katonai műveletek négydimenziós, virtuális térrel való támogatása. A katonai területeken is egyre inkább integrálnak olyan virtuális technológiai megoldásokat, amelyek a különböző műveleti szinteken (harcászati, hadműveleti és hadászati) egyaránt felhasználhatók. Mindez olyan technológiák fejlesztéséhez vezet, amelyekben a valós és virtuális terek egyformán részt vesznek egy komplex katonai infokommunikációs rendszerben. Idesorolhatók például a VR[5]- és AR[6]-technológiák, illetve ezek vegyes képességű MR[7]- és más technológiákkal fuzionált, egységes képessége, az XR[8]-technológia.

Mindez új fejlesztési igényeket, követelményeket von maga után. A kibővített valóságot leíró összetett rendszerben gondolkodva jön szóba a metaverzum, amelynek értelmezését a szakirodalomban már fel lehet ugyan lelni, mégsincs egységesen elfogadott értelmezés, különösen a hadtudományban. Jómagam mindezek figyelembevételével a következőkben az alábbi főbb kérdésekkel foglalkozom:

- Honnan ered a metaverzum kifejezés, milyen történeti előzményei vannak?
- Mit is jelent a civil megfogalmazásban, van-e már hivatalos definíciója?
- Milyen alkotóelemei, komponensei vannak, leírhatók-e egyáltalán?
- Miben különbözik a katonai értelmezés, van-e már kapcsolódó terminológia?

A fogalom rövid történeti áttekintése

A metaverzum fogalmának hallatán a legtöbb ember számára valamiféle új, kifejezetten a 21. századra jellemző technológia jut eszébe. Mindez nem áll messze a valóságtól, hiszen a metaverzum egy új technológiát, sőt annál is többet, igazából új irányzatot képvisel. Szükségszerű azonban megemlíteni, hogy a metaverzum fogalmának megjelenése már évtizedekre nyúlik vissza, még ha a szó sokaknak mindössze az utóbbi években kezdett ismertté válni, köszönhetően a szóbeszédnek és az elektronikus felületeknek. Érdekesnek és egyben lenyűgözőnek tartom, hogy a metaverzum kifejezés már több mint 30 éve megjelent egy regényben: „Neal Stephenson író alkotta meg a »metaverse« kifejezést 1992-ben megjelent »Snow Crash« című sci-fi regényében, amely az internet virtuális valóságon alapuló utódját vizionálja. A regényben az emberek saját maguk digitális avatárjait használják az online világ felfedezésére, gyakran azért, hogy elmeneküljenek a disztópikus valóság elől”[9] – olvasható egy kapcsolódó cikkben. A metaverzum tehát nem is az akkori technológiáknak megfelelően elgondolt, inkább valamelyest a jövőben elképzelt rendszer. Neal egyértelműen hangsúlyozta a társadalom számára a virtuális és a valós terek együttes felhasználásának sokrétű lehetőségét.

A következő fontosabb dátum 2003, az úgynevezett *Second Life* videójáték megjelenése, amelyet a Linden Research cég fejlesztett. A videójáték 2006-ban vált csak igazán népszerűvé és közismertté. A program igen egyszerű élményen alapul,

[5] Virtual reality (VR) – virtuális valóság.
[6] Augmented reality (AR) – kiterjesztett valóság.
[7] Mixed reality (MR) – kevert valóság.
[8] Extended reality (XR) – kibővített valóság.
[9] Huddleston 2021.

gyakorlatilag az ember egy saját avatárt hozhat létre, amelynek irányításával számos tevékenységet folytathat. „A több ezer virtuális élmény és közösség révén sosem fogysz ki a felfedezésre váró helyekből és a megismerhető emberekből. Zenei klubok, szerepjátékos közösségek, virtuális mozik és még sok más. A *Second Life* mindig csodálatos, néha furcsa, és 100%-ban lenyűgöző"[10] – olvasható a játék hivatalos oldalán. A játékban a felhasználók egyértelműen ízelítőt kaphatnak abból, hogy milyen is a fizikai valós világ mellett egy párhuzamos, virtuális világban létezni. Fontos hangsúlyozni, hogy akkoriban a számítási kapacitás, a hálózatok, a szoftveres és hardveres megoldások nem voltak olyan fejlett szinten, hogy a már akkoriban elképzelt világ teljes mértékben meg is valósulhasson.

Később, a közelmúltban már egyre többen foglalkoztak a metaverzum értelmezésével, és az immerzív technológiák fejlődése vonatkozásában számos új igény merült fel, amelyek által megvalósulhattak a korábban csak regényben olvasható virtuális terek. A virtuális és kiterjesztettvalóság-technológiák folyamatosan fejlődtek, párhuzamban a metaverzum elméleti elgondolásával.

Mára egyértelműen tapasztalható, hogy sok cég is foglalkozik (versenyben egymással) a technológiai lehetőségek kutatásával és fejlesztésével. Ezek közül kiemelkedik a Facebook, amely a metaverzum értelmezését, aktualitását és fejlesztési irányzatát saját magának tudatosította, és egyúttal megtette a kapcsolódó, szükséges kezdeti befektetési és tervezési lépéseket. Mindez azzal a fő változással járt, hogy a Facebook még a nevét is „Meta"-ra változtatta 2021 októberében.[11] Ugyan nagyon nehezen kivitelezhető fejlesztési gondolatokról van szó, manapság a metaverzum fokozatosan, egyre több embert érintve épül be a köztudatba. Mindemellett a kapcsolódó elképzelések, fogalmi és rendszerszintű értelmezések az aktuális és korszerű fejlesztési kérdéskörök közé kerültek be.

Egy új irányzat születőben

A 21. század rohanó technológiai változásait egyértelműen jellemzi, hogy egy adott új irányzat vagy eljárásmód vonatkozásában szükségszerű egyrészt fogalmi, másrészt rendszerszintű értelmezést végezni, meghatározni. Természetesen többféle aspektusból meg lehet vizsgálni a metaverzumokat, amihez jelen esetben két fontos megközelítést vettem alapul. Az első, mondhatni, legfőbb aspektus megítélésem szerint az információval összefüggő szemléletmód. A metaverzum egyértelműen egyfajta hibrid információs világként írható le, amely egyrészt mesterségesen előállított virtuális térből; másrészt természetes, valós fizikai térből származó információk együttes halmazát jelenti.

Ezek az információs igények feloszthatók annak függvényében, hogy egy adott szervezet vagy egy magánszemély számára például melyek a prioritások, szükségletek a mindennapi, lehetséges felhasználás során. A második aspektusnak mondható a technológiai megközelítés, azaz annak vizsgálata, hogy milyen technológiák

[10] Lásd: https://secondlife.com/
[11] Stöckert 2021.

kapcsolódnak a metaverzum elképzeléséhez.[12] Itt fontos megemlíteni, hogy a metaverzum, mondhatni, legfőbb élménye a hálózatalapú képességében rejlik. Több rövid, két-három szavas értelmezés született arra vonatkozóan, mi is a metaverzum. Ezekre példák a következők:

- az internet jövője vagy a következő internet;
- világunk digitális verziója;
- társadalmi evolúciós fejlődés.

Visszatérve a technológiai megközelítésre, azt lehet mondani, hogy olyan technológiák jöhetnek szóba, amelyek közel állnak a virtuális kutatási és fejlesztési területekhez, valamint segítik a célközönség információs igényeinek kiszolgálását. Itt kerülnek szóba többek között az immerzív technológiák, amelyek kifejezetten aktuális és korszerű fejlesztési lehetőségeket rejtenek, de célszerű megemlíteni az IoT[13]-t vagy az AI[14]-t is, hiszen a metaverzumban sokan az internet jövőjét látják. A virtuális valóság és a kiterjesztett valóság olyan mesterséges, hálózatba kapcsolt világot hozhat létre, amely egyrészt a civil szférában, másrészt a katonai alkalmazásban is érdekelt. Fontos leszögezni, hogy a már ismertetett immerzív technológiák közül a kibővített valóság felel meg a metaverzum elvi irányelvének. „Bármennyire is frusztrálóan homályos a metaverzum koncepciója, tudjuk, hogy a VR, az AR és az MR elemeit a hagyományos internethasználattal kombinálva a szocializáció, a játék és a munka platformjaként fogja használni. Ha ez nagyon úgy hangzik, mint az XR, az azért van, mert így is van."[15] A metaverzum megvalósíthatósága szempontjából tehát két főbb megközelítés létezik. Az egyik magát az információs igényt, míg a másik a technológiai lehetőségeket veszi kiindulópontnak. Egyik a másikkal természetesen összefügg, ami alapján egyedi és közös célok jelennek meg társadalmunkban. A különböző ágazatok a rájuk jellemző igényeket támasztják a technológiákkal szemben, amelyek a jövőt tekintve hosszú távú fejlesztési együttműködéseket jelenthetnek. Az irányzat célja tehát egyértelműen az emberek minden eddiginél magasabb szintű információs kiszolgálási lehetőségeinek megvalósítása, legyen szó munkahelyi találkozóról vagy egy otthonról végzett ételrendelésről.

Terminológiák nyomában

A metaverzum terminológiáját a kitűzött célok elérése érdekében kétféle megközelítésből vizsgálom. Egyrészt civil felhasználás tekintetében fogok definíciókat elemezni, másrészt előtérbe helyezem a metaverzum katonai célú alkalmazását. Mindezek alapján saját elgondolású fogalmakat szeretnék meghatározni, amelyekhez a fellelhető forrásokat, a metaverzumtól reálisan elvárható és kissé futurisztikus célokat egyaránt alapul veszem.

[12] Tóth 2022b: 128.
[13] Internet of Things (IoT) – dolgok internete.
[14] Artificial Intelligence (AI) – mesterséges intelligencia.
[15] Baker 2023.

Hétköznapi perspektíva

A metaverzum definíciójának meghatározására törekvő próbálkozásokról jelenleg legfőképpen a hétköznapi, polgári életben olvashatunk cikkekben, előadások anyagaiban vagy más szakmai dokumentumokban. A következőkben a célom több meghatározás összevetése és elemzése, amelyek alapján a lehetőségek szerint megfogalmazódhat bennem a metaverzum definíciója. Egy közismert hírportálon például a metaverzum „egy megosztott, virtuális világ, amit a felhasználók bármilyen platformról képesek elérni, és ahol a virtuális avatárjaikkal tudnak kapcsolatba lépni egymással".[16] Itt kiemelném a platformok sokrétűségét, valamint azok hálózatosítását. Fontos hangsúlyoznom, hogy a metaverzum definíciója nem szólhat csupán a virtuális világról, amelyhez legfőképpen a virtuálisvalóság-technológia köthető. A Meta cég például a következőket tartja a metaverzummal releváns, kapcsolódó technológiáknak:

- VR;
- AR;
- NFT;[17]
- blokklánc az NFT-k adminisztrálására és nyilvántartására;
- CC;[18]
- AI;
- IoT;
- 5G és 6G;
- Hologram;
- Web 3.0.[19]

Az élmény, a szolgáltatás tekintetében ténylegesen virtuális környezetről lehet beszélni, viszont a metaverzum a valós tér jelenléte nélkül nem megvalósítható, lásd például a kiterjesztett valóság vonatkozásában. A metaverzum fogalma tehát nem szólhat kizárólag a virtuális térről. Az immerzív technológiák fejlesztése egyértelműen az információs környezet virtuális térrel való bővítéséről szól. A kibővített valóság felel meg tehát gyakorlatilag a legmagasabb szintű immerzív technológiának és vele a metaverzum technikai megközelítésének, amelyben már például a mesterséges intelligencia és más modern kori technológiák is részt vesznek az információs szolgáltatásban. „Technikailag a Facebook (vagy Meta) által felvázolt metaverzum koncepciója az XR."[20]

A metaverzum definiálása azért is nehézkes, mert nem kizárólag egyetlen metaverzumról van szó (az más kérdés, hogy az irány egy globális, társadalmi elképzelésen alapul), hanem egyfajta infokommunikációs rendszerről. „A metaverzum nem egy dolog, több is létezik belőle. Van olyan, amit egy cég üzemeltet, mint a Meta, és vannak független, decentralizált metaverzumok."[21]

[16] Flachner 2022.
[17] Non-Fungible Token (NFT) – nem helyettesíthető token.
[18] Cloud Computing (CC) – felhőalapú számítástechnika.
[19] Lásd: www.telefonguru.hu/wiki/a_metaverzum_legfobb_technologiai
[20] Baker 2023.
[21] Papdi-Pécskői 2022.

A hangsúly tehát azon van, hogy ahogyan minden számítógépes hálózat, a metaverzum is csak úgy tud igazán hatékonyan működni, ha rendszerbe van foglalva. Lehetnek tehát kisebb-nagyobb kiterjedésű hálózatok, amelyek összekapcsolása által akár egy globális, kontinenseket érintő metaverzum infokommunikációs hálózata is létrejöhet.

A metaverzum jelentős digitális fejlődést jelenthet, amihez az emberek által felhasznált platformok minden eddiginél nagyobb együttműködést biztosítanak. Ez azt jelenti, hogy a különböző platformokon a digitális információink mozgathatóvá és egyúttal egymás között könnyedén megoszthatóvá válnak.[22] Matthew Ball, az Amazon világhírű cég korábbi vezérigazgatója is foglalkozott a metaverzum alapvető kérdéseivel. Egy kapcsolódó publikus írásában kifejtette sajátos véleményét arról, hogy melyek a metaverzummal szemben támasztott főbb követelmények, tulajdonságok. Ball szerint a metaverzum:

- legyen állandó, folyamatos, szünetek nélküli;
- legyen valós időben, élőben megtapasztalható;
- legyen képes befogadni bárkit egyedi entitásként;
- legyen teljes értékű gazdasági funkcionalitása az egyének és a vállalkozások számára egyaránt;
- legyen képes összefogni a digitális és fizikai világban tapasztalható élményeket;
- legyen képes az adatok átjárhatóságát megoldani a különböző eszközökön;
- legyen tartalmas és élménydús.[23]

A metaverzumokban általánosan érvényes, hogy a valós, fizikai téren túlmenően a virtuális terek, információk együttes felhasználása történik. Számítógépek és emberek közötti kapcsolatokon alapul, és tömeges információs lehetőségeket biztosít. Matthew Ball saját könyvében így ír a metaverzumról: „A metaverzum valós időben renderelt 3D-s virtuális világok és környezetek tömegesen skálázott és interoperábilis hálózata, amelyet szinkronban és tartósan, ténylegesen korlátlan számú felhasználó élhet át, egyéni jelenlétérzéssel és az adatok, például az identitás, az előzmények, a jogosultságok, a tárgyak, a kommunikáció és a fizetések folyamatosságával."[24]

Fontos megjegyezni, hogy mindezen kisebb és nagyobb hálózati elképzeléseket tekintve a metaverzum sajátos infokommunikációs berendezkedéseket von maga után, megreformálva az internet jelenlegi státuszát. Az eddigiek alapján úgy célszerű meghatározni a metaverzum fogalmát, hogy az független legyen a hálózat méretétől, de a különböző gazdasági és politikai céloktól is. Jómagam fontosnak tartom a kibővített, a valós, a virtuális, a digitális, az interakció, a hálózat és infokommunikáció szavak megjelenítését a metaverzum lehetséges fogalmában. Az elemzésekből kifolyólag nincsen hivatalos, kormányzat által elfogadott fogalmi meghatározás, bárki szabadon alkothat egy lehetséges definíciót a metaverzummal kapcsolatban.

Mindezen ismertetett összefüggést és az azokból kulcsfontosságúnak tartott szavakat felhasználva a metaverzum a saját elgondolásom szerint a következőként definiálható:

[22] Tóth 2022a: 164.
[23] Ball 2020.
[24] Ball 2021.

A metaverzum a valós tér virtuális elemekkel kibővített világa, amelyben 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.

Megjegyzem, hogy az általam ismertetett definíció a centralizált és decentralizált hálózattípusra egyaránt érvényes. A cél pontosan az, hogy akár magánszemélyek (otthoni), akár szervezet által létrehozott hálózatra egységesen érvényes legyen a fogalom. Az internet szó meglehetősen közel áll a metaverzumhoz, sokan az internet jövőjét látják ebben az irányzatban, tömeges digitális tartalommal, kibővített világban. Azt senki nem tudja, hogy a jövőben mi lesz az internettel. Azt sem tartom kizártnak, hogy az internetet fogják átnevezni idővel metaverzummá, éppen ezért nem használtam fel a szót a fogalom megalkotásában. Az infokommunikációs hálózatok felosztása a metaverzum szolgáltatási képessége vonatkozásában is fontos lépés lesz a jövőben.

Katonai megközelítés

A katonai műveleteket támogató technológiák rendkívül szerteágazók. Manapság a valós fizikai tér mellett újszerű felhasználásán dolgozva a virtuális megoldások a katonai fejlesztési területeken is előtérbe kerültek. A kapcsolódó immerzív technológiai lehetőségek feltárása a hadtudomány egy aktuális kutatási területének tekinthető. A virtuális térnek számos katonai aspektusa létezik, a szektoroktól (például logisztika) kiindulva a vezetési pontokon át (például harcászati szintű zászlóalj főharcálláspont) egészen az alegységek (például felderítő katonák) igényei vizsgálatának vonatkozásában. A NATO, még meglehetősen kezdetleges dokumentumában, a katonai metaverzum kapcsolódó technológiáit a következő főbb csoportokra osztotta fel: számítástechnika, szoftver, hálózat és biztonság, ember-gép interfészek, adatok és digitális iker, mesterséges intelligencia és adatelemzés, automatizálás és robotika, szenzorok.[25]

A katonai metaverzumban nemzeti és szövetségi szabályozók is érvényesek kell legyenek, amire nagyszerű példa bármely NATO-tagország kapcsolódó követelményrendszere. E képességek közé sorolható az interoperabilitás által támogatott hálózatalapú műveleti képesség, amely a katonai metaverzum követelményét alapjaiban képviseli. Úgy vélem, hogy a korábbi, Matthew Ball által alkotott általános követelmények teljes mértékben elvárhatók egy katonai metaverzum vonatkozásában. A NATO kutatói a katonai metaverzumot a következőként definiálták: „Tartós, biztonságos, hálózatba kapcsolt, interoperábilis, élő virtuális és konstruktív szimulációk, szinkronizálva a többdimenziós műveleti rendszerekkel és a szervezet egészére kiterjedő berendezések, platformok, infrastruktúra és személyzet digitális ikreivel, valamint a tágabb emberi és természeti világgal."[26] A fogalom kapcsán lényegesnek tartom kiemelni az interoperabilitást és a szervezet egészére kiterjedő hálózatban

[25] NATO 2022: 26-4.
[26] NATO 2022: 26-6.

való gondolkodást. Jómagam úgy gondolom, hogy a katonai metaverzumot két főbb, intézményi és műveleti információs környezetre lehet bontani, amivel meghatározható a katonai metaverzum fejlesztési lehetőségeinek a szervezet teljes egészére kiterjedő követelményrendszere.

A megközelítések és a szakmai vizsgálatok eredményeképpen a katonai metaverzumnak a következő definíciót határozom meg:

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.

Összefoglalás

A metaverzumban való gondolkodás nem egy, a közelmúltban elkezdődött folyamat, a kifejezés már jó ideje ismert a tudományos gondolkodók körében. Amilyen lassan kezdett el közismertté válni a múltban, annál intenzívebbek jelenleg a kapcsolódó kutatások és fejlesztések. A tudományos gondolkodók közül kiemelkedik Matthew Ball, aki mélyebben foglalkozik a témával. A metaverzum fogalmi megjelenése számos hosszabb-rövidebb definíciót teremtett azok által, akik foglalkoztak azzal az általános, mégis futurisztikus kérdéssel, mi is a metaverzum. Civil és katonai felhasználású elképzeléseket egyaránt vizsgáltunk a témában. A metaverzum strukturális elképzelése és a kapcsolódó technológiák meghatározása minden bizonnyal remek kiindulópont a civil vagy katonai célú metaverzum infokommunikációs hálózatainak megvalósításához. A szervezetek jelenleg, mondhatni, a megvalósíthatatlannak tűnő metaverzumos víziójukat próbálják egyetemes valóságként beállítani, amire remek példa a Meta cég, amelynek komplex elképzelései vannak a témában. A metaverzum fejlesztési megvalósításának alapját egyértelműen annak fogalmi és rendszerszintű értelmezése képezi.

Következtetések

Az eddigi tendenciák arra utalnak, hogy tömeges adatátvitelre lehet majd számítani a metaverzumban való gondolkodás vonatkozásában. Válaszolva a korábban feltett kérdéseimre, a következőket állapítottam meg. A kapcsolódó történeti előzmények fellelhetők, a metaverzum eredete, a *Snow Crash* című sci-fi regény is ismert. Az minden bizonnyal nyitott kérdés marad, hogy a civil megfogalmazásban mely publikus meghatározás fogadható el, ugyanis nincs hivatalos metaverzumdefiníció. A kapcsolódó publikus anyagokat és a számomra fontos kulcsszavakat felhasználva megalkottam definíciómat a metaverzum vonatkozásában. A metaverzum strukturális elképzelésére nem találtam konkrét leírást, a komponensek meghatározásához a kapcsolódó

technológiákat és az információs igényeket érdemes kiinduló vizsgálati pontnak venni. Egy következő publikáció alkalmával a katonai metaverzum megvalósításához szükséges főbb alkotóelemeket tervezem meghatározni. A fogalmi értelmezéshez fontos megjegyezni, hogy technikailag a metaverzum a kibővített valóságnak feleltethető meg. Katonai oldalról a NATO egyértelműen foglalkozik a katonai metaverzum fejlesztésével a Military Metaverse CONOPS 2035 koncepció vonatkozásában, amelynek információi nem publikusak. Katonai terminológiában nem találtam a katonai metaverzum fogalmát, de meglétét szükségesnek tartom. A fogalomhoz fűződő kulcsszavakat és a kapcsolódó kutatásokat felhasználva megalkottam saját definíciómat, a katonai metaverzum fogalmát. A katonai metaverzumok fejlesztése egyedi, speciális célokban, szolgáltatásokban és kapcsolódó infokommunikációs hálózatokban különbözik a civil szférától. A metaverzum civil és katonai szemléletmódban is egyfajta paradigmaváltásként értelmezhető.

Irodalomjegyzék

Baker, Luke (2023): What is XR and how will it underpin the metaverse? *Pocket-Lint,* 2023. június 9. Online: https://www.pocket-lint.com/ar-vr/news/160183-what-is-xr-and-how-will-it-underpin-the-metaverse/

Ball, Matthew (2020): The Metaverse: What It Is, Where to Find it, and Who Will Build It. *Matthew Ball,* 2020. január 13. Online: www.matthewball.vc/all/themetaverse

Ball, Matthew (2021): Framework for the Metaverse. *Matthew Ball,* 2021. június 29. Online: www.matthewball.vc/all/forwardtothemetaverseprimer

Ball, Matthew (2022): *The Metaverse: And How It Will Revolutionize Everything.* New York: WW Norton.

Farkas, Tibor (2020): Communication and Information Services – NATO Requirements, Part I. *Land Forces Academy Review,* 25(4), 281–289. Online: https://doi.org/10.2478/raft-2020-0034

Farkas, Tibor (2021): Communication and Information Services – NATO Requirements, Part II. *Land Forces Academy Review,* 26(1), 9–15. Online: https://doi.org/10.2478/raft-2021-0002

Flachner Balázs (2022): Mégis mi az a metaverzum, amibe hirtelen szerelmes lett az összes milliárdos tech-óriáscég? *Telex,* 2022. február 10. Online: https://telex.hu/komplex/2022/02/10/metaverzum-nft-blokklanc-kriptovaluta-microsoft-meta-videojatek-next-earth-1

Huddleston Jr, Tom (2021): This 29-year-old Book Predicted the 'Metaverse' — and Some of Facebook's Plans are Eerily Similar. *CNBC,* 2021. november 3. Online: www.cnbc.com/2021/11/03/how-the-1992-sci-fi-novel-snow-crash-predicted-facebooks-metaverse.html

NATO (2022): *Military Metaverse CONOPS.*

Papdi-Pécskői Viktor (2022): Mi az a metaverzum? *Index,* 2022. május 14. Online: https://index.hu/techtud/2022/05/14/metaverzum-virtualis-valosag-harver-jatek-jarvany-technika-paradigma/

STÖCKERT Gábor (2021): Mark Zuckerberg átnevezte a cégét, és megmutatta a Facebook jövőjét. *Telex,* 2021. október 28. Online: https://telex.hu/tech/2021/10/28/mark-zuckerberg-atnevezte-a-ceget-es-megmutatta-a-facebook-jovojet-meta

SZELECZKI, Szilveszter (2023): *Directions in the Development of Virtual Reality and Its Military Applicability.* Budapest: Ludovika.

TÓTH András (2022a): A digitális állam információbiztonsági kihívásai. Budapest: Ludovika.

TÓTH, András (2022b): Information Security Challenges and Solutions in Smart Nations. In *Security-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach.* Heidelberg: Springer, 123–132. Online: https://doi.org/10.1007/978-94-024-2174-3_10

HADMÉRNÖK
FÓRUM
18. évfolyam (2023) 3. szám 189–206.
DOI: 10.32567/hm.2023.3.13

Molnár Ákos Ádám[1]

A koronavírus idején a közösségi médiában megjelenő álhírek elemzése, az „infodémia" fontossága

Analysis of Fake News Appearing on Social Media During the Coronavirus, the Importance of the 'Infodemic'

Absztrakt

2019. decemberben Kína egyik tartományában, 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, napjainkban a legerőteljesebben az online térben. 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, mintsem valóságtartalmuk vagy forrásuk alapján, jelentősen befolyásolva a társadalom informáltságát. Kutatásom fő célja a koronavírussal kapcsolatos álhírek és érzelmek vizsgálata. Ezen belül az álhírek terjedését és a hallgatóságra tett hatásait vizsgáltam. Online felületeken végzett kulcsszóelemzést alkalmazva az álhírek terjedését, annak ütemét és miértjét kutattam.

Kulcsszavak: Covid–19, álhír, dezinformálás, megtévesztés

[1] Hallgató, Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar, e-mail: m.akos0911@gmial.com

Abstract

In December 2019, Covid–19, which is now well known and has since been declared a pandemic, emerged in Wuhan, a province in China. In spring 2020, the World Health Organization used the term 'infodemic' – when too much information, including a lot of misinformation, about an outbreak appears – to highlight 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 based on its emotional content rather than its veracity or source, significantly affecting the level of information in society. The main aim of my research is to investigate the pseudo-news and emotions associated with the Crown virus. Within this, I investigated the spread of fake news and its effects on the audience. Using keyword analysis of online platforms, I investigated the spread of fake news, its pace and why.

Keywords: Covid–19, fake news, disinformation, deception

Bevezető

A koronavírus-járvány 2019 decemberében vált világhírűvé, amikor Kína egyik tartományában, Vuhanban megjelent és azóta világjelenséggé vált. A járványt az álhírek és a dezinformációk növekedő terjedése kísérte, elsősorban az interneten, az online térben, és képes arra, hogy a világ bármely pontjáról különböző célcsoportokhoz bármilyen hírt eljuttasson, határok és korlátok nélkül, napok vagy órák alatt, emberek ezreit vagy akár millióit is elérve. A járvány idején a WHO az „infodémia" kifejezést használta arra, hogy ne csak a vírus, hanem a róla szóló dezinformáció és félretájékoztatás terjedésére is utaljon. Ma a „post-truth" korszakban élünk, ahol az emberek gyakran érzelmileg hajlamosak elhinni a híreket, függetlenül azok valóságtartalmától vagy forrásától, és ez jelentős hatással van az információs társadalomra. Az álhírek terjedése komoly károkat okozhat, közvetlenül, mint például a Pizzagate-botrány vagy az 5G rádiótornyok ledöntése, vagy közvetve, mint például amikor az emberek nem oltatják be magukat, és ennek következményeit elszenvedik. Ezek az esetek vagyoni károkat, személyi sérüléseket és akár halált is okozhatnak. Megfelelő szűréssel, tudatos megosztással és fogyasztással azonban ezek nagyrészt elkerülhetők lennének. A dezinformálás miatt az emberek egy része elhiszi, hogy körülötte minden hazugság, emiatt sokszor nem tesz eleget állampolgári kötelességeinek és buzdítja embertársait, sokszor olyan cselekményekre, amelyek a társadalmi rendet bomlasztják. Az álhírek megelőzése és terjedésének megállítása szintén jelentős humán, technikai és pénzügyi erőforrásba kerül. Az ilyen fajta álhírek és az ezzel kapcsolatos félrevezetések pedig a Covid–19-vírussal és az ellene kifejlesztett védőoltások megjelenésével még fontosabb problémává váltak.

A SentiOne programmal végzett kutatás során keresem a választ, hogy a vírus megjelenésekor legnépszerűbb álhírek a járvány többi szakaszában mennyire voltak elterjedve az interneten, továbbá hogy a vírus ellen kifejlesztett oltóanyagok

megjelenésével és tömeges használatával egyidejűleg megerősödtek-e a különböző álhírekre adott keresések és megosztások a korábbi időszakhoz képest.

Módszertan

A SentiOne a nyilvános online platformokon közzétett szöveges tartalmakat gyűjti és elemzi (cikkek, posztok, kommentek stb.), amelyek a rendszerben létrehozott projekt beállításai után azonnal elérhetővé válnak.[2] A SentiOne közösségimédia-adatokat és weboldalakról származó tartalmakat is gyűjt. Minden összegyűjtött adat egy adattárházba kerül, amelyben a megfelelő kulcssszavak megadásával lehet keresni, több mint 70 nyelven. A SentiOne jelenlegi adattárházában több mint 20 milliárd említés érhető el, és ez napról napra bővül. A nyelvfelismeréshez a SentiOne saját fejlesztésű algoritmust használ, amely a lingvisztikai tulajdonságokat és az elérhető metaadatokat is figyelembe veszi, így 99,93 százalékos pontossággal képes detektálni adott nyelvet. A rendszer működését több mint 200 dedikált offline adattároló szerver biztosítja, és nyílt forráskód alapján működik.[3]

A SentiOne nap mint nap új címeket ad hozzá a rendszerhez: automatizált folyamatok mentén, valamint kézi beállítások nyomán, online keresőmotor API-ok használatával. A domaincímeket azon jelszavak alapján szűri és bővíti, amelyekre a felhasználók már rákerestek a rendszerben. A rendszer azokat a domaineket figyeli, amelyeken felhasználói tartalom jelenik meg (blogok, fórumok, hírportálok, review oldalak). A SentiOne saját tulajdonú és fejlesztésű algoritmusokat használ a strukturálatlan HTML-tartalmak kinyeréséhez. Azokon a domaineken, ahol az automatikus algoritmusok nem működnek, vagy az oldal dinamikus tartalommal operál, az adatgyűjtés folyamata manuálisan írt XPath profilokon keresztül történik.[4]

A SentiOne a különböző közösségimédia-oldalakról a hivatalos és nyilvános API-hozzáféréseken keresztül gyűjti be az adatokat. A legnépszerűbb Facebook-oldalak automatikusan bekerülnek a rendszerbe. Az új Facebook-oldalakat pedig a rendszerben már korábban is használt, felhasználói kulcsszóbázis alapján keresi és találja meg a technológia. A Facebook esetében a SentiOne a nyilvános rajongói oldalakon közzétett tartalmakat figyeli. A privát Facebook-oldalakon publikált bejegyzéseket nem látja, még akkor sem, ha azok nyilvánosként lettek közzétéve (mert a Facebook API-szabályzatával ez nem összeegyeztethető).[5]

A Twitter nyilvános API-kódot használ, azaz lehetőség van a tweetek monitorozására, így azonnal láthatók a legfrissebb bejegyzések is. A nyilvános API-kódnak köszönhetően az Instagramon megosztott hashtagek is kereshetők a SentiOne-ban. Azonban a 2018. december 10-i új Instagram API bevezetése óta minden autorizált fiókból (admin által becsatornázott fiók a SentiOne-ba) maximum 30 hashtag-keresés indítható hetente. Az autorizált fiókokból az Instagram Storykat is megkapja a rendszer. A YouTube esetében is a nyilvános API-hozzáférést használja a rendszer.

[2] Bányász–Tóth–László 2022: 99–125.
[3] SentiOne (é. n. a).
[4] SentiOne (é. n. b).
[5] Kempa 2017.

Az API korlátozásai miatt a YouTube-ról származó adatok maximum 30 napig tárolhatók a SentiOne adatbázisában, és az adatvizualizációkban ezek az adatok nem jeleníthetők meg.[6]

A SentiOne teljesen és részben támogatott nyelvekkel operál, amelyek listája folyamatosan bővül. Jelenleg a következő nyelvek érhetők el teljesen támogatott formában: lengyel, német (+ svájci német, osztrák német), orosz, ukrán, angol (+ UK, US, Írország), holland (+ belga holland), francia (+ belga francia, svájci francia), szlovén, szlovák, magyar, román, bolgár, szerb, horvát, bosnyák, montenegrói, cseh, dán, finn, svéd, norvég, lett, litván, olasz, spanyol, portugál és görög.[7]

A bejegyzések érzelmi hátterének *(sentiment)* megállapításánál John R. Crawford és Julie D. Henry elemzését, a Positive and Negative Affect Schedule (PANAS) tézisét vették alapul a szoftverfejlesztők. Ezen algoritmus magyar nyelven körülbelül 87%-os pontossággal képes beazonosítani adott bejegyzés szerzőjének témához kötődő érzelmi viszonyát.[8] A rendszer továbbá automatikusan kategorizálja a szerzőket egy több mint 35 ezer nevet tartalmazó adatbázis, valamint a tartalmak lingvisztikai jellemzői alapján. A SentiOne különböző becsült elérést számító algoritmust használ a generikus weboldalak, a fórumok és a közösségimédia-felületek esetében.

Weboldalak esetén az adott weboldal forgalmának teljesítményét külső adatszolgáltató cég közreműködésével elemzi. Érdemes lehet a hálózati csomópontok közti kapcsolatokat is elemezni.[9] Figyelembe vesz olyan változókat, mint például a domain forgalma, a látogatószám, a tartalom kora, a website vitalitása (például milyen gyakran frissül), a tartalom típusa (komment, cikk) stb. Ahhoz, hogy egy egyedi említés elérése megbecsülhető legyen, a domain-statisztikákon kívül a SentiOne rendszerébe már mentett adatokat is figyelembe veszi. Ha nincsen a külső adatszolgáltató partnertől elérhető adat az adott website-ra nézve, akkor a domain Page Authority-értékét veszi figyelembe az algoritmus, amely minden domainnél elérhető és az oldal nézettségével *(page view)* arányos. A fórumok esetében a SentiOne neurális hálózati algoritmusokat alkalmaz, amely fórumonként és témánként különbözik.

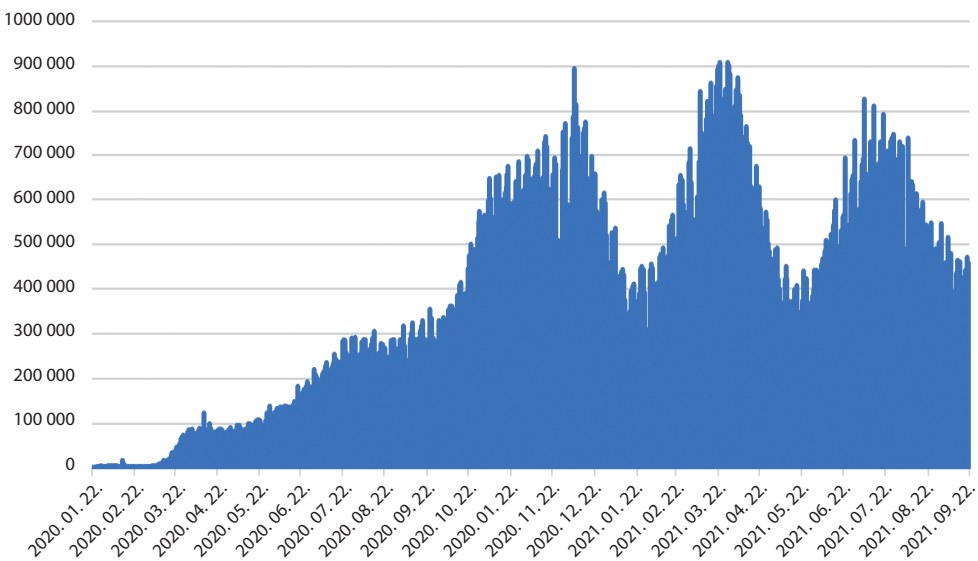
A közösségimédia-felületek esetében vagy az adott oldalra vonatkozó API-hozzáférésen keresztül megkapott értékeket veszi alapul a szoftver, vagy saját fejlesztésű algoritmusával a posztokra érkezett interakciókat (komment, lájk, megosztás) súlyozza a követőszám nagyságával.

A Covid–19-vírus megjelenése és az infodemic

2019 decemberében Kínában, azon belül is Vuhan tartományban megjelent a Covid–19 nevű vírus. Ez a vírus 2020 áprilisára elért 213 országot, és csaknem

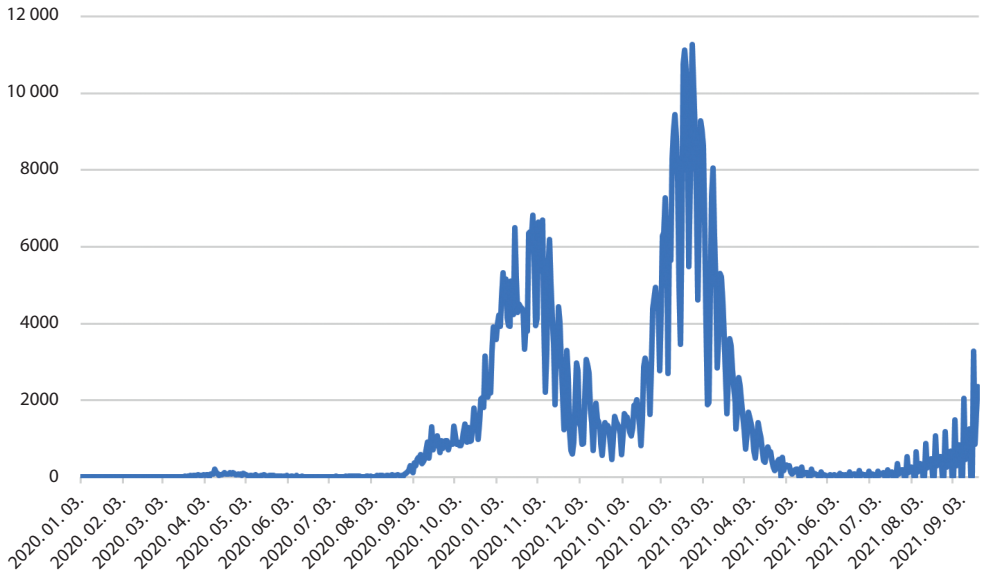
[6] SentiOne (é. n. b).
[7] SentiOne (é. n. b).
[8] Crawford–Henry 2004: 245–265.
[9] Bederna–Szádeczky 2021: 51–66.

150 ezer halálos áldozatot szedett.[10] Ez a szám 2021. szeptember 19-re 229 millió fertőzöttre, 4,7 millió halottra növekedett.[11] A vírust hivatalosan is világjárvánnyá nyilvánították 2020 márciusában, amit a WHO tett meg.[12] A koronavírus terjedése, a napi megbetegedéseket figyelve, azonban nem volt folyamatosan növekvő tendenciájú.[13] Országonként, régióként és világszinten is beszélhetünk úgynevezett hullámokról, minden ilyen hullámnak a csúcspontján a legmagasabb a napi fertőzöttek száma.[14] Egy hullámnak van egy kezdeti felszálló és egy végzeti leszálló ága, amikor, ellentétben a felszállóval, csökken a fertőzöttek száma. A WHO megfogalmazása szerint ahhoz, hogy egy hullám csökkenjen, ellenőrzés alá kell vonni az esetszámokat, egy hullám beindulásához pedig a fertőzöttek számának tartós növekedésére van szükség.[15] A 1. és 2. ábrán jól megmutatkoznak ezek a hullámok. A két ábra elkészítéséhez a WHO, illetve az ourworldindata.org adatszolgáltatásait használtam fel.[16] A két oldalról összesen megközelítőleg 200 ezres adatállományt töltöttem le, majd szeparáltam dátum szerint Excel-táblázatban, az adatokat ezután megtisztítottam és elemeztem, így megkapva az alábbi eredményeket, mind nemzetközileg, mind Magyarországot tekintve.



1. ábra: Napi új koronavírus-megbetegedések száma világszerte 2020. 01. 22. és 2021. 09. 22. között
Forrás: a szerző szerkesztése az ourworldindata.hu adatai alapján

[10] Naeem–Bhatti 2020: 233–239.
[11] Lásd: www.worldometers.info/coronavirus
[12] BBC News 2020.
[13] Lendvai–Krasznay 2021: 3–17.
[14] PRABHASH 2021.
[15] WHO 2021a.
[16] Bányász–Nagy–Molnár 2023: 20–36.



2. ábra: Napi új koronavírus-megbetegedések száma Magyarországon 2020. 01. 03. és 2021. 09. 22. között

Forrás: a szerző szerkesztése a Hungary Situation adatai alapján

A vírussal együtt megjelentek az új összeesküvés-elméletek, és az álhírek új tárháza indult meg a hallgatóság felé a különböző online felületeken, mint a Facebook, a Twitter, a TikTok vagy a WhatsApp.[17] Az álhírek sokasága elnyomva a híreket, sokszor pánikot keltett több országban, és tömeges árufelvásárlást okozott hazánkban is.[18] 2020. február 15-én a müncheni biztonsági konferencián a WHO akkori igazgatója, Tedrosz Adhanom Gebrejeszusz kijelentette: „We're not just fighting an epidemic; we're fighting an infodemic…" – azaz nemcsak a világjárvánnyal, de az „infodemic-kel" is küzdünk.[19] Ennek hatására a WHO létrehozta az úgynevezett Information Network for Epidemics (EPI-WIN) platformot, azzal a céllal, hogy releváns információkat közöljenek különböző csoportoknak. A koronavírus-járvány ugyanúgy hozza magával a hírek tömkelegét, mint bármely más nagyobb esemény, ami már a kezdetektől jellemző.[20] A probléma azonban, hogy ezt az információsokaságot szűrni kell, hogy az álhírek ne juthassanak el a közönséghez, továbbá a legnagyobb gond az online felületek miatt, hogy ezek az információk gyorsabban terjednek, mint valaha. Ez egy új kihívást jelent, hogy minél gyorsabban és hatékonyabban lépjenek fel ezek ellen a hírek ellen.[21]

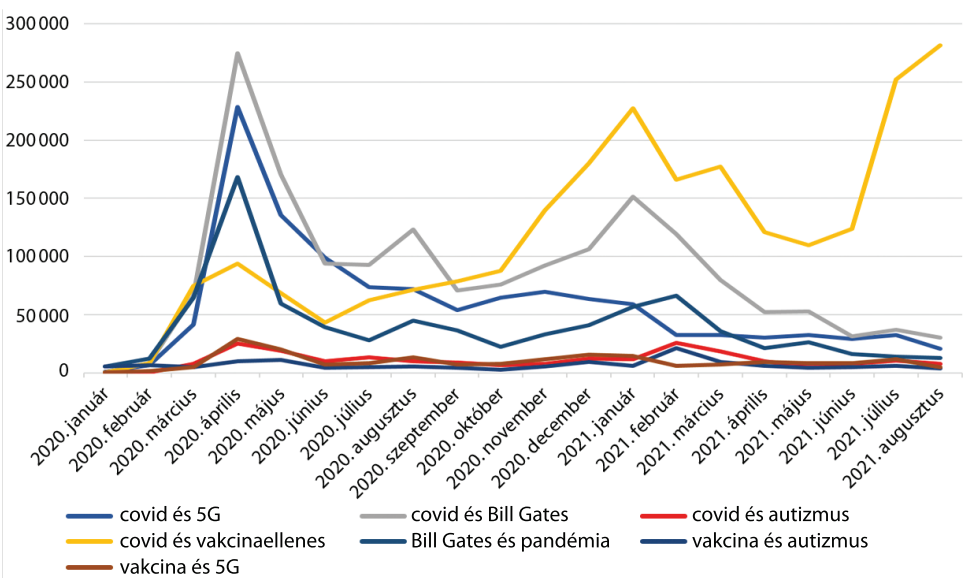
Ahogy fentebb is bemutattam, kutatások igazolják, hogy az álhírek gyorsabban terjednek, mint a valós társaik, és emiatt a kutatók félnek attól, hogy a közösségi média

[17] Bányász 2022: 601–609.
[18] Privátbankár 2020.
[19] WHO 2021c; Zarocostas 2020.
[20] Ináncsi–Farkas 2022: 42–53.
[21] Zarocostas 2020.

lesz a mozgatórugója az álhíreknek.[22] Ahogy azt Prachett is írja, „a hazugság körbefutja az egész világot, mire az igazság felhúzza a cipőjét".[23] Az úgynevezett „infodemic" következtében a Covid–19-vírussal megjelentek az álhírek új fajtái, amelyek a vírushoz és az azzal kapcsolatos intézkedésekhez fűződnek, kezdve azzal, hogy az 5G terjeszti, át azon, hogy az alkoholivás megöli a vírust, egészen addig, hogy a forró fürdő megelőzi a betegséget.[24]

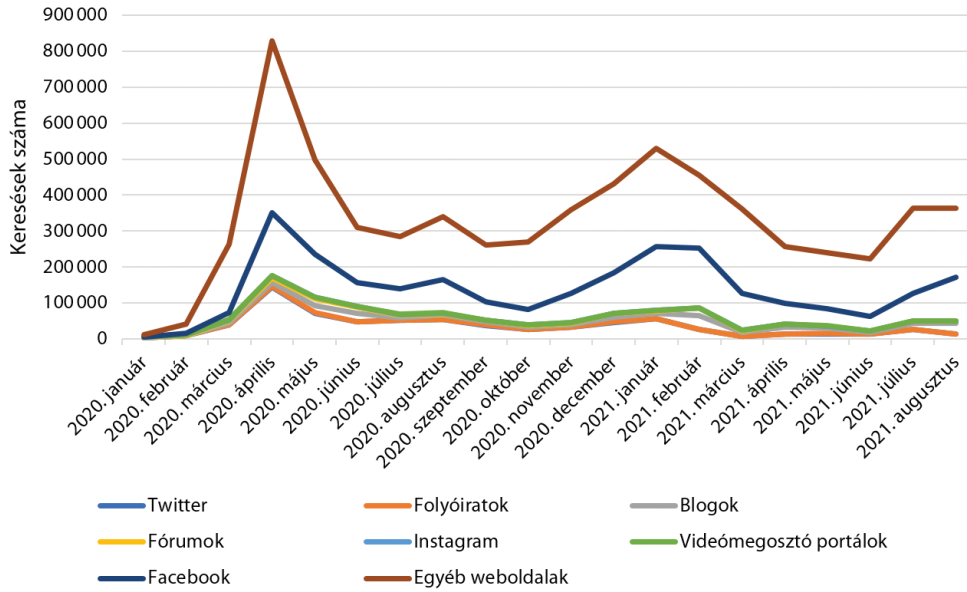
Koronavírussal kapcsolatos kifejezések az online térben

Az álhírek tömeges megjelenésével a keresések száma is jelentősen növekedett a Covid–19-cel kapcsolatban. Ahogy a 3. ábrán is jól látható, a „covid" és egyéb koronavírussal kapcsolatos kifejezésekhez köthető keresések száma jelentősen megnövekedett 2020 januárja és 2021 augusztusa között. Az elemzések és keresések alapján látható, hogy a „covid" és „Bill Gates", illetve „covid" és „anti vaccine" kifejezésekkel kapcsolatos álhírek keresése volt a legkiemelkedőbb. Tovább vizsgálva a 3. ábrán látható kereséseket megnéztem, hogy milyen online felületen van a legtöbb álhírrel kapcsolatos keresés. Az adatokat összesítve megfigyelhető a 4. ábrán, hogy az egyéb, kisebb weboldalakon a legnagyobb arányú a találat, és ezt követi a legnagyobb online közösségimédia-felület, a Facebook, majd utána a különböző videómegosztó portálok, idetartozik a YouTube vagy a Vimeo.



3. ábra: Koronavírussal kapcsolatos kifejezések keresései a SentiOne program segítségével
Forrás: a szerző szerkesztése a SentiOne adatai alapján

[22] Vosoughi–Roy–Aral 2018: 1146–1151; Farkas 2023: 11–30.
[23] Prachett (é. n.).
[24] Murphy 2007: 62–68.



4. ábra: Koronavírushoz és álhírekhez köthető kifejezések keresései a különböző online felületeken
Forrás: a szerző szerkesztése a SentiOne adatai alapján

Megvizsgálva a három legjobban kiugró egyenest a 3. ábrán azt láthatjuk, hogy ezek olyan keresések, amelyek a koronavírust vagy az ahhoz kapcsolódó védőoltásokat összekötik Bill Gatesszel vagy az 5G-vel.

A *New York Times* és a Zignal Labs tanulmányai szerint 2020 februárja és áprilisa között több mint 1,2 milliószor volt megemlítve Bill Gates a koronavírussal kapcsolatban különböző közösségimédia-felületeken. Legtöbbször nyilvános Facebook-csoportokban, ahonnan milliók osztották tovább.[25] A BBC dezinformáció ellen küzdő csapata különböző álhíreket talált Gatesszel kapcsolatban. Az általa és volt felesége által létrehozott alapítvány vakcinákat tesztel afrikai és indiai gyerekeken, aminek következtében meghalnak, vagy maradandó sérüléseket szenvednek. Ezenfelül volt olyan videó, amelynek a témája a masszív elnéptelenedés vakcinával és abortusszal, továbbá összekötötte a Kínai Kommunista Párttal, ez a videó több mint hatezerszer volt megosztva és 200 ezer megtekintés felett jár. Azonban nem mehetünk el amellett sem, hogy mikrochipeket fecskendeznek belénk a Covid–19 elleni védőoltással és így akarnak minket megfigyelni. Fontos kérdés azonban, hogyan is került Bill Gates a koronavírussal kapcsolatos álhírek középpontjába. Az amerikai összeesküvés-elméletekre szakosodott politológus, Joseph Uscinski szerint a válasz nagyon egyszerű, azért, mert híres és gazdag. Szerinte a teóriák mindig ugyanazok, csak a mögötte álló nevek mások. Ezek az összeesküvés-elméletek megpróbálnak megfélemlíteni minket, és így jön a képbe a mikrochip is, amelyet belénk fecskendeznek, és ki a legjobb személy egy

[25] Wakabayashi–Alba–Tracy 2020.

ilyen végrehajtására, ha nem a Microsoft alapítója.[26] A legnagyobb probléma azonban, hogy az amerikaiak több mint negyede el is hiszi, hogy ez az igazság.[27]

Az 5G az ötödik generációs vezeték nélküli hálózat rövidítése. A technológia elődje az 1G-ig vezethető vissza. Napjainkban egyre elterjedtebb, azonban kialakítása ma is tart, elsőként Dél-Korea kezdte kiépíteni az új hálózatot 2019 áprilisában.[28] Az első összeesküvés-elméletet a Covid–19-járvány és az 5G között John Gregory fogalmazta meg egy francia weboldalon. Elmélete szerint a vírust az új 5G-s tornyok terjesztik, ezt az elméletet egyszerűen azzal magyarázta, hogy Vuhanban, a vírus kitörése előtt építettek fel több ilyen tornyot is.[29] Fontos megjegyezni azonban, hogy az 5G-vel kapcsolatos álhírek már korábban is jelen voltak, továbbá, ahogy a WiFi- és 3G technológiánál is elterjedtek voltak a különböző álhírek, ezek csak „átterjedtek" az 5G-re.[30]

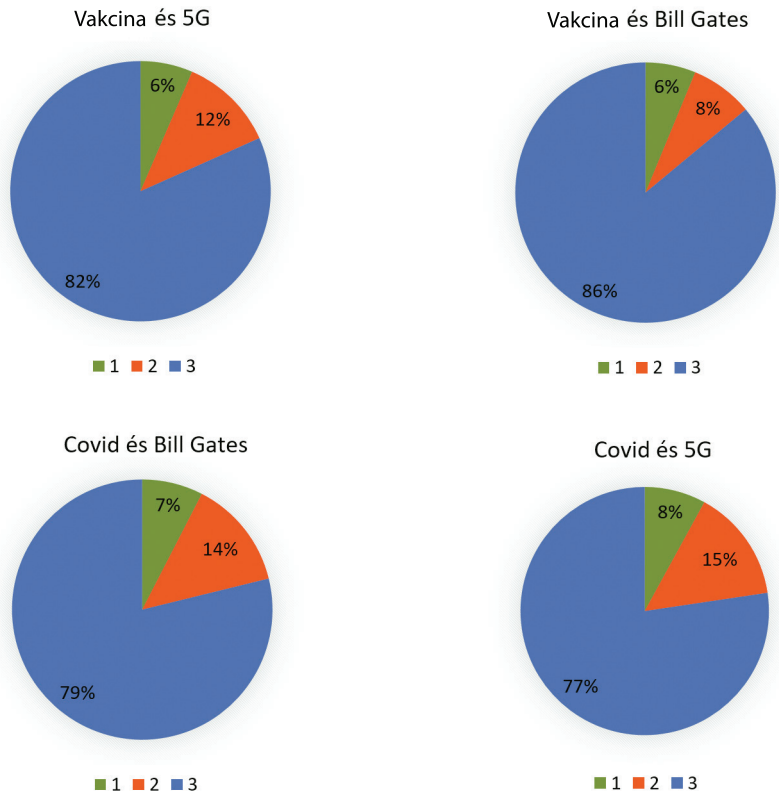
Évek óta több különböző álhír terjeng a vezeték nélküli technológiák körül, ami az új technológia elterjedésével ismét felerősödött. Ilyen összeesküvés-elmélet, hogy agyrákot okoz.[31] A kétezres évek elején felmerült, hogy a telekommunikációs eszközök, amelyek ilyen technológiát használnak, agykontrollra képesek.[32] Az 5G elődjeinél felmerült, hogy a vezeték nélküli hullámok rákot okoznak, megölik a madarakat vagy szimplán fejfájást okoznak, és gyengíti az immunrendszerünket a technológia által kibocsátott elektromágneses sugárzás.[33]

Az 5G-vel kapcsolatos álhírek 2020 tavaszán erősödtek meg ismét. A kapcsolat legfőbb indoka a vuhani új 5G-t sugárzó tornyok, amire több tweet (Twitter-poszt) kitért, mint például Ker Hilson énekesnő is: „Évek óta figyelmeztetnek minket az 5G miatt. Petíciók, szervezetek, tanulmányok. Amin keresztülmegyünk az mind a sugárzás hatása…" Ez az elmélet később több iránnyá alakult. Van, akik szerint a tornyok által sugárzott hullámok stimulálják a vírust, és így aki ilyen technológiát használ, el tudja kapni a fertőzést.[34] A másik tábor szerint a koronavírus csak egy álca, hogy fel tudják húzni az 5G-s tornyokat, amíg mindenki a vírussal van elfoglalva. Ezenfelül megjelent az elnéptelenedési tervben *(depopulate)* hívők csoportja is, akik szerint az 5G ugyanolyan része a népirtásnak, mint a koronavírus. Ennek a tervnek az egyik fő irányítója a korábban említett Bill Gates.

Ezek az álhírek és összeesküvés-elméletek végül odáig vezettek, hogy 2020 tavaszán Európa-szerte, Nagy Britanniában, Hollandiában és Belgiumban közel 20 tornyot rongáltak meg vagy gyújtottak fel olyan személyek, akik különböző álhírek olvasatán hittek a fentebb említett elméletekben.[35] Ezzel összefüggésben jól látható, hogy 2020 tavaszán jelentős mértékben megugrott a „covid" és „5g" kifejezésre adott keresések száma a SentiOne szoftver adatai alapján (3. ábra).

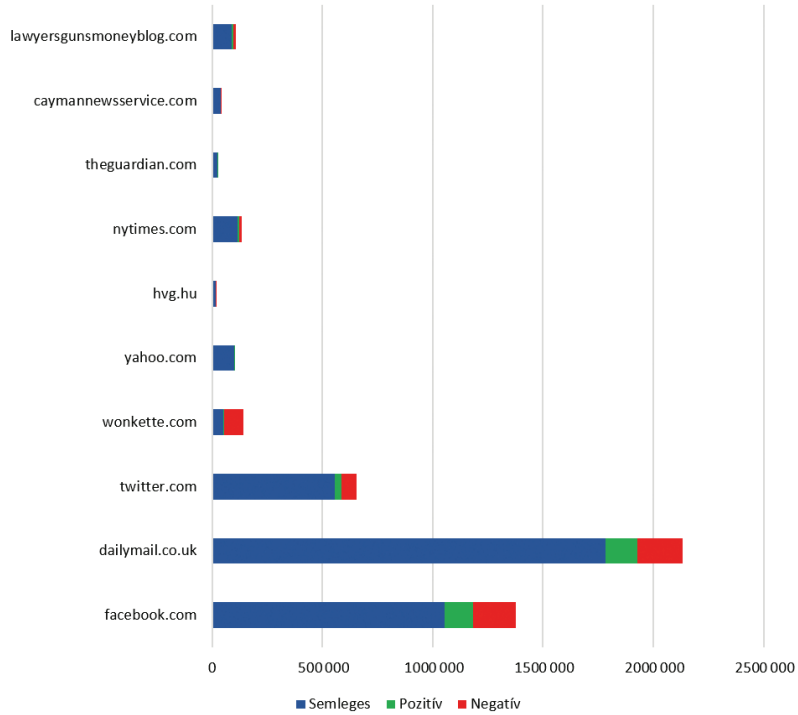
[26] BBC News 2020.
[27] Romano 2020.
[28] ITU 2021; Mobile World Live 2019.
[29] Heilweil 2020.
[30] Waterson–Hern 2020.
[31] Cancer.org.au (é. n.).
[32] Fields 2008.
[33] Dunne 2017; Kasprak 2018; Hern 2019.
[34] Lásd: https://twitter.com/JustOndieki/status/1230015534944673792
[35] Warren 2020; EUobserver 2020.

Hogy Bill Gates nevét és az 5G-t milyen vonatkozásban keresték, milyen szövegkörnyezetben, arra az alábbi vizsgálatot végeztem el. A kulcsszavas keresések alapján megnéztem 2020. január 1-jétől 2021. augusztus 31-ig az alábbi szópárokat (lásd 5. ábra). Ezeket az eredményeket vizsgálva látható, hogy negatív kontextusban minden esetben többen kerestek rá, mint pozitív szövegkörnyezetben. Ugyanakkor jól látható, hogy nemzetközileg még mindig a semleges keresések aránya a legmagasabb.



5. ábra: Álhírekkel kapcsolatos megemlítések minőségi aspektusai
Forrás: a szerző szerkesztése a SentiOne adatai alapján

Megvizsgálva az alábbi megemlítéseket platformok szerint, majd az eredményeket összeadva, illetve a keresések érzelmi töltetét külön jelölve, nemzetközileg a legjelentősebb hírszolgáltató a dailymail.co.uk, majd ezt követi a facebook.com és a twitter.com nemzetközi szinten. Ugyanakkor kitűnik, hogy a listán megjelenik egy magyar hírszolgáltató is, a hvg.hu. Az eredmények alapján a top 10 weboldalt megtekintve, a megosztások legjelentősebb része tájékoztató jellegű, míg minimális része érzelmi töltetű. Azonban ahol érzelmi töltetű, ott minden weboldal esetén magasabb a negatív érzelmű szövegkörnyezet (lásd 6. ábra).



6. ábra: Top 10 platform megoszlása és az érzelmi töltöttség aránya
Forrás: a szerző szerkesztése a SentiOne adatai alapján

Magyarországot tekintve is rengeteg, a vírussal kapcsolatos álhír terjeng az interneten. Ezeket azonban egyre nehezebb megtalálni az algoritmusok hátrébb sorolása miatt, vagy éppen azért, mert az online felületek már le is tiltják ezeket tartalmakat. Persze ezek az algoritmusok sem működnek tökéletesen, sokszor időbe telik a detektálás, és nem is mindig a legmegfelelőbb a működésük.[36] 2020 júniusában több Facebook-bejegyzés is megosztott egy olyan videót, amelyben az Amerikai Egyesült Államok Szenátusa bejelenti, hogy a koronavírus kitaláció, a média eltitkolja az igazságot, a WHO-t és a nagyobb gyógyszerészeti cégeket pedig felelősségre vonják majd. Ezt a hírt több mint 10 ezren osztották meg.[37] Azóta a hírt megcáfolták, és természetesen a különböző közösségimédia-felületek is letörölték a tartalmakat.

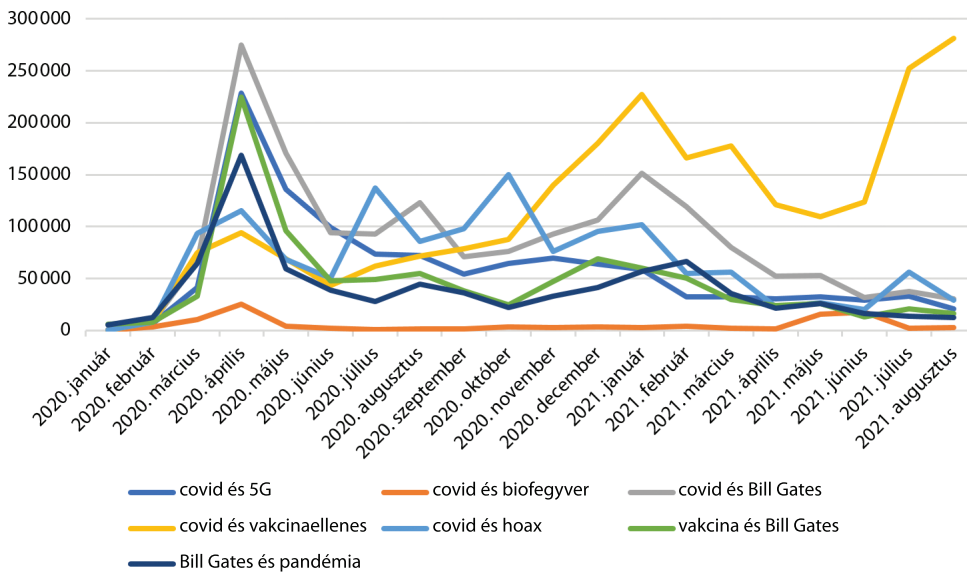
Hazánk egyik legismertebb dezinformáló szervezete az Orvosok és Egészségügyi Dolgozók a Tisztánlátásért. Ennek a társaságnak a vezetői doktorok és orvosok, azonban többüknek felfüggesztette a tagságát vagy etikai vizsgálatot indított ellenük a Magyar Orvosi Kamara.[38] Posztjaikat a saját weboldalukon osztják meg legfőképp (https://orvosokatisztanlatasert.hu), ennek egyik oka, hogy a különböző közösségi

[36] Magyar Hang 2020.
[37] AFP Ténykérdés 2021.
[38] T. O. 2021; Juhász 2020.

és videómegosztó portálok sorra törlik le a posztjaikat. Vannak azonban, akik így is hisznek ezekben az álhírekben. Például van, aki szerint a maszkviselés 85%-kal növeli a Covid–19-fertőzés esélyét, továbbá a saját levegőnk visszaszívása is roncsolja a tüdőt, ezzel pedig a kormány szándékosan gyilkolja a magyarokat, majd megosztott több forrást is, amelyekre hivatkozik, azonban ezek sem elérhetők már.[39]

Eredményeim vizsgálata

Kutatásom elején feltételeztem, hogy a koronavírus megjelenésekor legnépszerűbb álhírek az első hullám idején voltak leginkább elterjedve, szemben a többi hullámmal. A SentiOne szoftver használatával keresett kulcsszavak alapján azokra az álhírekre kerestek rá legtöbben a vírus terjedésének kezdetén, amelyek az 5G-hez, Bill Gates-hez, az oltásellenességhez és ahhoz kapcsolódnak, hogy a vírus kitaláció. Az ezekkel kapcsolatos kifejezések alapján a sentiment-keresésekre adott érzelmek eredményeit összesítve, majd diagramon ábrázolva a 7. ábrán látható eredményt kaptam.



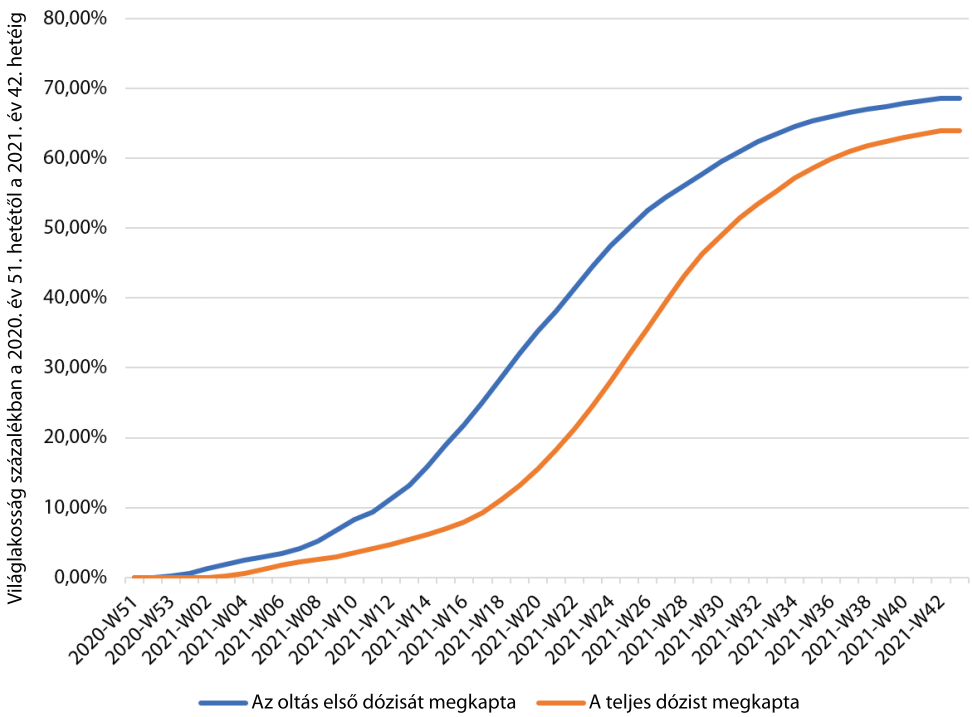
7. ábra: A különböző kifejezésekre adott keresések száma
Forrás: a szerző szerkesztése a SentiOne adatai alapján

Az ábra jól szemlélteti, hogy világszinten az első hullám idején, ami 2020 tavaszára datálható, a keresések száma a többszörösére ugrott mindegyik kulcsszó esetében. Ezt követően kisebb kiugrás figyelhető meg 2020 őszén és 2021 elején. Figyelve a nemzetközi trendeket és járványhullámokat megállapítható, hogy a vizsgált kifejezéseknek

[39] Lásd: https://vk.com/wall-1197685_1259

a jelentős részénél a keresések száma nem növekszik vagy csökken egyidejűleg a koronavírus-hullámokkal (lásd 1. és 7. ábra). Tovább elemezve a kapott adatokat, hipotézisem beigazolódott, miszerint ezen álhírek elterjedése az első hullám során volt a leginkább jellemző. A diagramról leolvasható, hogy egyedül a vakcinaellenes keresések egyenese haladja meg a kezdeti adatokat és növekszik később is. Ez a későbbi ellenanyag-előállítás, majd annak terjedése és használata miatt fordulhat elő. Eltekintve ettől, minden keresés száma csökkent.

Kutatásom során megvizsgáltam, hogy a Covid–19 elleni védőoltások megjelenésével és használatával a vírussal kapcsolatos álhírek ismét megerősödtek-e. A vírus elleni védőoltásokat elsőként 2020 decemberében engedélyezték, majd ezután terjedt el a világon a használatuk. Napjainkra már a világ lakosságának több mint a fele felvette a koronavírus elleni védőoltás valamelyik fajtáját.[40]



8. ábra: A világ lakosságának koronavírus ellen felvett oltási aránya százalékban
Forrás: a szerző szerkesztése a https://qap.ecdc.europa.eu/public/extensions/COVID-19/vaccine-tracker alapján

Megállapíthatjuk tehát, hogy az oltóanyagok megjelenése a 2020-as év végére tehető. Ezt a dátumot összevetve az eddig kapott eredményekkel egyértelmű, hogy az ellenanyagok megjelenésével ismét felerősödtek az álhírekre adott keresések az azt

[40] WHO 2021b.

megelőző időszakhoz képest. Továbbá fontos megjegyezni, hogy a „covid" és „anti vaccine" kifejezésekre adott keresések 2021 januárjában érik el a csúcspontot, ami egészen 2020 júniusától növekedett. Ezután csökkenő tendenciát mutat az egyenese (lásd 7. ábra). 2021 májusában kezd el ismét növekedni az ezzel kapcsolatos keresések száma, amit ha szintén összevetünk a világon beoltott emberek számával, jól látható, hogy időben egymáshoz közel kezdett el növekedni a keresések és a beoltott személyek száma is.

Összegzés

A kutatás során legfőképp a SentiOne nevű szoftvert használtam, amely az egész világot lefedő, 70 nyelven beszélő és webes szöveganalitikán alapuló social listening szoftver, amely kulcsszavas keresés alapján, valós időben vagy akár 3 évre visszamenően figyeli, indexálja és elemzi az internetes fórumokon, blogokon, weboldalakon és közösségimédia-csatornákon közzétett publikus szöveges tartalmak minden típusát, amelyek önmagukban vagy kontextusukban tartalmazzák a felhasználó által már előre definiált és a platformra felvitt kulcskifejezések bármelyikét. Továbbá különböző online felületekről gyűjtöttem adatokat a keresések és a különböző álhírek értelmezése érdekében.

A koronavírus 2019. decemberi megjelenése óta mára már világjárvánnyá vált, amely az egész globalizált világot érinti. A vírussal együtt azonban felütötte a fejét egy másik probléma, az álhírek és azok gyors terjedése, ami ellen több módszert is létrehoztak már. Megvizsgálva az álhírekkel kapcsolatos kulcsszavakra való kereséseket a SentiOne programmal megállapítottam, hogy a vírussal és az ahhoz köthető vakcinákkal kapcsolatos álhírek központi szereplői az 5G-s telekommunikációs eszközök, Bill Gates, és hogy az egész járvány és körülötte minden egy nagy átverés. Ezen álhírek már odáig jutottak, hogy több százezres vagy milliós megtekintések is láthatók rajtuk, vagy például odáig, hogy több európai országban is 5G-s tornyokat rongáltak meg, mondván, hogy Covid–19-vírust terjeszt.

A megosztások érzelmi töltöttségét tekintve a megtekintett kifejezések több mint 75%-ban semlegesek, tehát semmilyen érzelmi telítettség nem volt bennük. Ugyanakkor, a negatív kontextus minden esetben magasabb volt, mint a pozitív. A weboldalakat tekintve a kereséseket és ott figyelve az érzelmi töltöttséget a dailymail.co.uk hírportálon volt a legtöbb említés, majd ezt követték a facebook.com és a twitter.com közösségi felületek. Az érzelmeket vizsgálva weboldalanként is ugyanezek az arányok voltak megfigyelhetők.

Hazánkat tekintve az egyik legjelentősebb, vírussal kapcsolatos dezinformációs forrás az Orvosok és Egészségügyi Dolgozók a Tisztánlátásért nevű csoport, amelynek vezetői doktorok és orvosok, azonban a vírusról tett kijelentéseik miatt több személytől is megvonta a tagságot a Magyar Orvosi Kamara, és tevékenységük is sok tekintetben megkérdőjelezhető, posztjaikat, tartalmaikat sokszor letiltják a közösségi oldalak és videómegosztó portálok.

Megvizsgáltam, hogy a vírus megjelenésekor legnépszerűbb álhírek az első hullám idején voltak-e a legelterjedtebbek és legkeresettebbek. Elemezve a kapott számokat

és a diagramokat látszik, hogy az első hullámban nagyobb arányban kerestek rájuk, mint a többi hullám idején. Egyedül a „covid" és „anti vaccine" kifejezésekre adott keresések száma növekszik csak később, feltehetően a vírus ellen kifejlesztett ellenanyagok megjelenésével és azok tömeges használatának köszönhetően. Így a hipotézisem beigazolódott, hogy a vírus megjelenésekor legelterjedtebb álhírek keresései az első hullám idején voltak a legjelentősebbek, ez alól azonban kivétel a vakcinaellenes álhírek. A vírussal kapcsolatos álhírek 2020 végén ismét megerősödtek, majd a járvány elleni védőoltások tömeges beadásával 2021 tavaszán a vakcinaellenes keresések korábban nem látott módon kezdtek el megugrani, és az elemzett időszak végéig (2021. augusztus) ez a szám csak növekszik.

Irodalomjegyzék

5G Towers Set on Fire in UK, Netherlands, Belgium. *EUobserver,* 2020. április 20. Online: https://euobserver.com/tickers/148114

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 – 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

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

Cancer.org.au (é. n.): *I heard that the new 5G technology can cause cancer. Is this true?* Online: www.cancer.org.au/iheard/i-heard-that-the-new-5g-technology-can-cause-cancer-is-this-true

Coronavirus Confirmed as Pandemic by World Health Organization. *BBC News,* 2020. március 11. Online: www.bbc.com/news/world-51839944

Crawford, John R. – Henry, Julie D. (2004): The Positive and Negative Affect Schedule (PANAS): Construct Validity, Measurement Properties and Normative Data in a Large Non-Clinical Sample. *British Journal of Clinical Psychology,* 43(3), 245–265. Online: https://doi.org/10.1348/0144665031752934

Dunne, Carey (2017): My Month with Chemtrails Conspiracy Theorists. *The Guardian,* 2017. május 22. Online: www.theguardian.com/environment/2017/may/22/california-conspiracy-theorist-farmers-chemtrails

Dutta, Prabhash K. (2021): What Is a Covid-19 Wave? How Do We Identify It? *India Today,* 2021. május 10. Online: www.indiatoday.in/coronavirus-outbreak/story/what-is-a-covid19-wave-how-do-we-identify-it-1800810-2021-05-10

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.
Fields, Douglas R. (2008): Mind Control by Cell Phone. *Scientific American,* 2008. május 7. Online: www.scientificamerican.com/article/mind-control-by-cell
Heilweil, Rebecca (2020): How the 5G Coronavirus Conspiracy Theory Went from Fringe to Mainstream. *Vox,* 2020. április 24. Online: www.vox.com/recode/2020/4/24/21231085/coronavirus-5g-conspiracy-theory-covid-facebook-youtube
Hern, Alex (2019): How Baseless Fears over 5G Rollout Created a Health Scare. *The Guardian,* 2019. július 26. Online: www.theguardian.com/technology/2019/jul/26/how-baseless-fears-over-5g-rollout-created-a-health-scare
Ináncsi Mátyás – Farkas Tibor (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
ITU (2021): *ITU towards "IMT for 2020 and Beyond".* Online: www.itu.int:443/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx
Juhász Edina (2020): Etikai vizsgálat indul az álhíreket terjesztő orvos ellen. Index, 2020. április 16. Online: https://index.hu/techtud/2020/04/16/etikai_vizsgalatot_kezdemenyeztek_az_alhireket_terjeszto_orvos_ellen
Kasprak, Alex (2018): Did a 5G Cellular Network Test Cause Hundreds of Birds to Die? *Snopes,* 2018. november 13. Online: www.snopes.com/fact-check/5g-cellular-test-birds
Kempa, Katarzyna (2017): Natural Language Processing – What's New and How to Use It in Business? *SentiOne Blog,* 2017. május 30. Online: https://sentione.com/blog/natural-language-processing-in-business
Krasznay Csaba – Koczka Ferenc (2021): A távolléti oktatás jelentette kiberbiztonsági és adatvédelmi kihívások. In Koltay András – Török Bernát (szerk.): *Járvány sújtotta társadalom.* Budapest: Ludovika, 213–230.
Lendvai Tünde – Krasznay Csaba (2021): A SARS-CoV-2-vírus okozta fertőzés terjedését nyomon követő és karanténellenőrző applikációk. *Nemzetbiztonsági Szemle,* 9(3), 3–17. Online: https://doi.org/10.32561/nsz.2021.3.1
Cellphones and Cancer: What's the Risk? *Mayoclinic,* Online: www.mayoclinic.org/healthy-lifestyle/adult-health/expert-answers/cell-phones-and-cancer/faq-20057798
Mezei Kitti – Krasznay Csaba (2022): Cybersecurity and Cybercrime in Hungary During the COVID-19 Pandemic. In Chałubińska-Jentkiewicz, Katarzyna – Hoffman, István (szerk.): *The Role of Cybersecurity in the Public Sphere – The European Dimension.* Maribor, Lex Localis, 191–207. https://m2.mtmt.hu/api/publication/33118087
Mobile World Live (2019): *Samsung Dominates Korea 5G Deployments.* Online: www.mobileworldlive.com/asia/asia-news/samsung-dominates-korea-5g-deployments
Murphy, Jeannette (2007): International Perspectives and Initiatives. *Health Information & Libraries Journal,* 24(1), 62–68. Online: https://doi.org/10.1111/j.1471-1842.2007.00704.x

Naeem, Salman Bin – Bhatti, Rubina (2020): The Covid–19 'infodemic': A New Front for Information Professionals. *Health Information & Libraries Journal,* 37(3), 233–239. Online: https://doi.org/10.1111/hir.12311

Prachett (é. n.): "A lie can run round the world before the truth has got its boots on." *goodreads.com.* Online: www.goodreads.com/quotes/219878-a-lie-can-run-round-the-world-before-the-truth

Privátbankár (2020): Koronavírus-roham a boltokban – most akkor van vagy nincs? *Privátbankár,* 2020. február 27. Online: https://privatbankar.hu/cikkek/makro/koronavirus-roham-a-boltokban-most-akkor-van-vagy-nincs-331149.html

Romano, Andrew (2020): YouGov Poll Shows Coronavirus Conspiracy Theories Spreading on the Right May Hamper Vaccine Efforts. *Yahoo News,* 2020. június 9. Online: https://news.yahoo.com/new-yahoo-news-you-gov-poll-shows-coronavirus-conspiracy-theories-spreading-on-the-right-may-hamper-vaccine-efforts-152843610.html

SentiOne (é. n. a): *A social listening alapjai*. Online: https://sentione.com/hu/eroforrasok/social-listening

SentiOne (é. n. b): *Figyelj úgy, ahogy még soha*. Online: https://sentione.com/hu/tudasbazis/amit-a-projektekrol-tudni-erdemes

T. O. (2021): Felfüggesztették: fél évig nem dolgozhat a vírusszkeptikus orvos. *Medical Online,* 2021. július 19. Online: http://medicalonline.hu/eu_gazdasag/cikk/felfuggesztettek__fel_evig_nem_dolgozhat_a_virusszkeptikus_orvos

Több vírustagadó oldalt és csoportot is letiltott a Facebook. *Magyar Hang,* 2020. szeptember 24. Online: https://hang.hu/belfold/tobb-virustagado-oldalt-es-csoportot-is-letiltott-a-facebook-110788

Twitter (2021): Justus Ondieki a Twitteren. Online: https://twitter.com/JustOndieki/status/1230015534944673792

Vosoughi, Soroush – Roy, Deb – Aral, Sinan (2018): The Spread of True and False News Online. *Science,* 359(6380), 1146–1151. Online: https://doi.org/10.1126/science.aap9559

Wackenreuther, Eva (2021): Az Egyesült Egyesült Államok Szenátusa nem mondta ki, hogy a koronavírus „hazugság" lenne. *AFP Ténykérdés,* 2021. június 16. Online: https://tenykerdes.afp.com/http%253A%252F%252Fdoc.afp.com%252F9CB3GZ-1

Wakabayashi, Daisuke – Alba, Davey – Tracy, Marc (2020): Bill Gates at Odds with Trump on Virus, Becomes a Right-Wing Target. *The New York Times,* 2020. április 17. Online: www.nytimes.com/2020/04/17/technology/bill-gates-virus-conspiracy-theories.html

Wakefield, Jane (2020): How Bill Gates Became the Voodoo Doll of Covid Conspiracies. *BBC News,* 2020. június 6. Online: www.bbc.com/news/technology-52833706

Warren, Tom (2020): British 5G Towers Are Being Set on Fire Because of Coronavirus Conspiracy Theories. *The Verge,* 2020. április 4. Online: www.theverge.com/2020/4/4/21207927/5g-towers-burning-uk-coronavirus-conspiracy-theory-link

Waterson, Jim – Hern, Alex (2020): How False Claims about 5G Health Risks Spread into the Mainstream. *The Guardian,* 2020. április 7. Online: www.theguardian.

com/technology/2020/apr/07/how-false-claims-about-5g-health-risks-spread-into-the-mainstream
WHO (2021a): *Coronavirus Disease (COVID-19): How Is It Transmitted.* Online: www.who.int/news-room/q-a-detail/coronavirus-disease-covid-19-how-is-it-transmitted
WHO (2021b): *Coronavirus Disease (COVID-19): Vaccines*, Online: www.who.int/news-room/q-a-detail/coronavirus-disease-(covid-19)-vaccines
WHO (2021c): *Munich Security Conference.* Online: www.who.int/director-general/speeches/detail/munich-security-conference
Zarocostas, John (2020): How to Fight an Infodemic. *The Lancet,* 395(10225), 676. Online: https://doi.org/10.1016/S0140-6736(20)30461-X

Lukács László

Szemelvények a hazai katonai robbantástechnika és a föld alatti aknaharc fejlődéstörténetéből

Az ipari robbantástechnika aktuális kérdéseit összefoglaló, a köznapi forgalomban beszerezhető művek – bár nem nagy számban, de – koronként megjelentek a hazai szakkönyvkiadásban. A honi katonai robbantástechnika múltjának feldolgozásával, rendszerező áttekintésével és a továbbfejlesztés javasolt irányaival is foglalkozó könyvet viszont Magyarországon még nem írtak. Ez változott meg 2017-ben, amikor a Nemzeti Közszolgálati Egyetem kiadta a szerző *Szemelvények a magyar robbantástechnika fejlődéstörténetéből* című könyvét.[1] Ebben fejlődésük vizsgálatán keresztül feldolgozta a magyar honvédségnél[2] alkalmazott katonai robbantástechnikai módszerek és eljárások legfontosabb kérdéseit.

Ennek a műnek mintegy folytatásaként készült el a jelen kiadvány, amelynek első részében az előző könyvből kimaradt robbantási területeket dolgozza fel: a mozgásakadályozás robbantással végrehajtható feladatait. Ezen belül az alkalmazott hazai katonai robbantóanyagok és a robbantási alapfeladatok tervezésének koronkénti összefoglalását követően bemutatja az utak és műtárgyaik, a vasutak, a repülőterek és a hidrotechnikai létesítmények robbantási szabályainak fejlődését az 1800-as évektől napjainkig. Az első részt az építmények harcászati célú robbantási szabályai zárják. A szerző a szakterület e kérdéseinek fejlődéstörténeti vizsgálata alapján is bizonyítja az előző könyvben megfogalmazott állítását, amely szerint az eddig alkalmazott robbantási elveket nem kell „elfelejteni", mert azok szervesen illeszkednek a robbantástechnika általános vonulatába, és az idők folyamán, empirikus úton szerzett ismeretekből kiindulva, a tudományos vizsgálatok eredményein nyugvó eljárásokká fejlődtek.

A könyv második részében egy olyan robbantási területet vizsgál, amelyet ilyen formában még szintén nem dolgoztak fel Magyarországon: a föld alatti aknaharcot. Ez volt történelmünk leghosszabb időn át alkalmazott eljárása az ellenség megerődített helyeinek elfoglalására, és ennek ellentettjeként a védők hasonló válasza, az ellenaknák alkalmazása. Az ókortól a középkoron át az újkori csatákig egyaránt találkozunk vele. Csúcspontját az első világháború tömeges aknaharcai jelentették, az ellenség állásai alá ásott/fúrt aknák és a védők által ennek hatástalanítására készített ellenaknák révén. Mégis viszonylag keveset tudunk róla. A föld alatti aknaharc történetéről, fejlődéséről szóló fejezet korról korra bemutatja a támadók és a védők által alkalmazott

[1] Letölthető a Közszolgálati Tudásportálról: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6916

[2] A könyvben a „magyar honvédség" alatt azt a mindenkori, központilag szervezett fegyveres erőt érti a szerző (függetlenül annak éppen aktuális megnevezésétől), amelynek feladata az ország védelme volt.

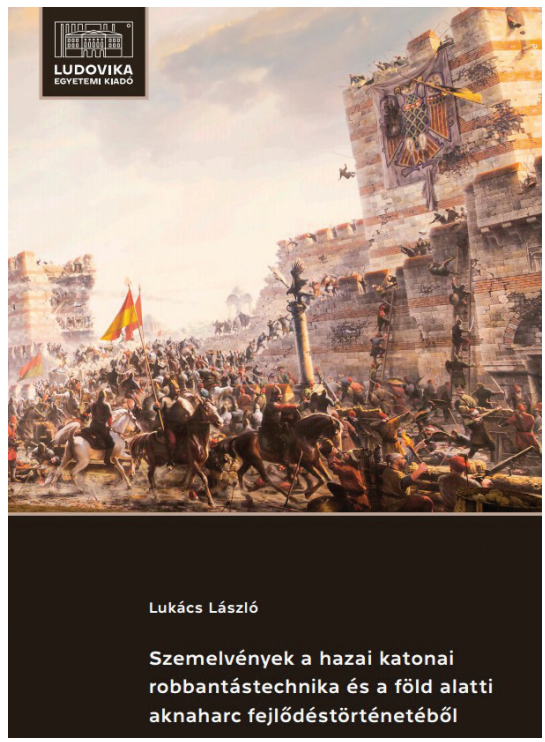
technikákat és technológiákat az adott időszak aknaharccal foglalkozó hadtudományi értekezéseiből, műveiből vett idézetekkel és megtörtént csatákról szóló beszámolókkal.

A könyv egyben emléket kíván állítani a magyar honvédségnél a robbantástechnika kutatásával, fejlesztésével, a robbantás oktatásával, a kiképzéssel és a gyakorlati munkák kivitelezésével foglalkozó műszaki katonáknak, szakembereknek.

A monográfia a Ludovika Egyetemi Kiadó gondozásában jelent meg, 576 oldal terjedelemben. ISBN: 978963531695-3

E-könyvként beszerezhető: https://webshop.ludovika.hu/termek/konyvek/hadtudomany/szemelvenyek-a-hazai-katonai-robbantastechnika-es-a-fold-alatti-aknaharc-fejlodestortenetebol/

Nyomtatott formában is hamarosan várható a könyv megjelenése.



Lukács László

Robbantástechnika a hazai katonai szakfolyóiratokban az 1800-as évek végétől napjainkig

„A mai műszaki katonai nemzedék, amely a jövőben a vezetésre hivatott, csak a múltból tanulhat. Aki pedig nem becsüli múltját, annak nincs jövője." Jacobi Ágost utász ezredesnek az első világháborúban harcoló magyar műszaki katonáknak emléket állító, 1938-ban megjelent könyvében[1] olvasható mondatai voltak azok, amelyek ennek és azt ezt megelőző két monográfiának a megírására ösztönözték a szerzőt.

Az előző két könyvében a hazai katonai robbantástechnika fejlődéstörténetét dolgozta fel, az éppen érvényes (szabályzatokban, utasításokban foglalt) előírások alakulásán keresztül.[2] A hazai katonai robbantástechnika múltjának összefoglaló bemutatásából már csak egy adóssága maradt: a katonai szakfolyóiratokban megjelent korabeli cikkek, tanulmányok feldolgozása. A legújabb kutatások és gyakorlati tapasztalatok eredményeivel mindig ezekben találkozhattak/találkozhatnak először a szakemberek. A legjelentősebb szakmai kérdések aztán – jó esetben – bekerültek az újabb szabályzatokba is, de talán ennél is nagyobb jelentőségű e kiadványoknál az olvasóik hivatalos előírásokon túlmutató szakmai ismereteinek elmélyítése a legújabb információk, tapasztalatok, kipróbált és bevált új módszerek bemutatásával.

A könyvben a szerző egy nagy történelmi kirándulásra invitálja az olvasót a hazai katonai szakfolyóiratokban megjelent, a robbantástechnikával foglalkozó cikkek világába, az 1800-as évek végétől napjainkig. A magyar katonai szaknyelv hiánya jelentette a hazai szakfolyóiratok megjelenésének első akadályát. Az első fejezetben – többek között – erről is olvashatunk.

A további fejezetekben három részre bontva mutatja be az adott témához kapcsolódó anyagokat, amelyekben az 1945-ig, az 1945–1990 között és az 1990-től napjainkig megjelent cikkek között szemlézett a szerző. Három különböző társadalmi rendszer három hadseregének robbantástechnikai történelme elevenedik meg ezekben a fejezetekben, az általa felállított szakmai rendszerezés szerint. Így olvashatunk a robbantóanyagokról, a robbanás irányított hatásáról, a szerkezeti elemek és építmények, továbbá a föld és sziklás kőzetek robbantásáról szóló anyagokat. A könyv utolsó fejezete egy szakmailag látszólag „idegen" kérdéssel foglalkozik: a robbanás egészségügyi hatásait taglaló cikkek bemutatásával. Az író azon véleménye tükröződik ebben, hogy a robbantástechnikával foglalkozó szakembereknek ismerniük kell mind a robbanás során keletkező gázok mérgező hatását, mind a robbanóanyagok gyártása, kezelése, a velük való munkavégzés során betartandó munkaegészségügyi kérdéseket.

[1] Jacobi Ágost (1938): *A Magyar műszaki parancsnokságok, csapatok és alakulatok a világháborúban 1914–1918.* Budapest: Közlekedési Nyomda K.F.T., 13.

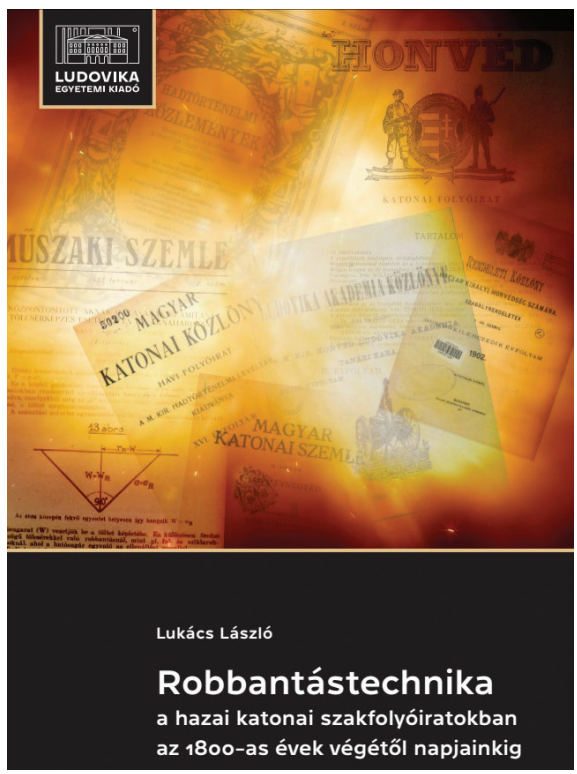
[2] *Szemelvények a magyar robbantástechnika fejlődéstörténetéből* (Dialóg Campus, 2017); *Szemelvények a hazai katonai robbantástechnika és a földalatti aknaharc fejlődéstörténetéből* (Ludovika Egyetemi Kiadó, 2023).

Ugyanígy fontos a robbanás emberi szervezetre gyakorolt hatásainak, a robbanás során keletkező sérüléseknek a megismerése, természetesen nem a sebész, hanem a parancsnok, a katonáiért felelős vezető szemszögéből.

A könyv a robbantástechnika kutatásával és fejlesztésével, a robbantás oktatásával, a kiképzéssel és a gyakorlati munkák kivitelezésével foglalkozó azon magyar műszaki katonáknak, szakembereknek kíván emléket állítani, akik értékes gondolataikat, eredményeiket a bemutatott szakfolyóiratokban osztották meg kortársaikkal.

A monográfia a Ludovika Egyetemi Kiadó gondozásában jelent meg, 432 oldal terjedelemben. ISBN 978-963-531-696-0 (elektronikus PDF) | ISBN 978-963-531-697-7 (ePub).

E-könyvként beszerezhető: https://webshop.ludovika.hu/termek/konyvek/hadtudomany/robbantastechnika-a-hazai-katonai-szakfolyoiratokban-az-1800-asevek-vegetol-napjainkig/



Tartalom