HADMÉRNÖK

Kiemelt közlemények

19. évf. (2024)
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: Bujdosó Hajnalka, Nagy Judit, Resofszki Ágnes

Tartalom

HADMÉRNÖK
BIZTONSÁGTECHNIKA

19. évfolyam (2024) 3. szám 5–16.
DOI: 10.32567/hm.2024.3.1

Horváth András[1] – Farkas Gabriella[2]

A munkahelyi egészségvédelmi és biztonsági irányítási rendszer hatékonyságának növelése

Increasing the Efficiency of the Occupational Health and Safety Management System

Absztrakt

Valamennyi vállalat elemi érdeke, hogy biztosítsa az egészséget nem veszélyeztető és biztonságos munkakörülményekre vonatkozó követelményeket. Az előrelátó vállalatok megértették, hogy a munkabalesetek vagy foglalkozási megbetegedések hatalmas kiadásokkal járnak, és felismerték a cég jó hírére gyakorolt kedvezőtlen hatásukat. Ezek elkerülésében nagy segítség lehet egy bevezetett, hatékonyan működtetett és folyamatosan fejlesztett munkahelyi egészségvédelmi és biztonsági irányítási rendszer. Cikkünkben bemutatjuk annak a kérdőíves felmérésnek az eredményeit, amelyet a MEBIR-rendszerre vonatkozóan készítettünk egy autóipari vállalat munkatársai körében. Fejlesztési javaslatokat teszünk a rendszer vállalaton belüli hatékonyságának javítására, továbbá kitérünk az integrált irányítási rendszerek előnyeire, amelyek előremutatók lehetnek a vállalat minőség- és munkavédelmi központú gondolkodásának megvalósításában.

Kulcsszavak: munkahelyi egészségvédelem, biztonság, minőségirányítási rendszerek, integrált irányítási rendszerek, munkavédelem, minőségfejlesztés

[1] Óbudai Egyetem, e-mail: horvath.andras@bgk.uni-obuda.hu
[2] Óbudai Egyetem, e-mail: farkas.gabriella@bgk.uni-obuda.hu

Abstract

The fundamental interest of all organization is to ensure the requirements for safe working conditions. Forward-thinking companies understood that accidents at work or occupational diseases involved huge costs and recognized their negative impact on the company's reputation. An established and efficiently operated and continuously improved occupational health and safety management system can be of great help in avoiding these. In our article, we present the results of a questionnaire survey conducted on the OH&S system among the automotive company's employees. We would like to make development proposals to improve the efficiency of the system within the company, and we also discuss the advantages of integrated management systems, which can help to achieve a forward-looking thinking centered on quality and occupational safety in the company.

Keywords: occupational health, safety, quality management systems, integrated management systems, occupational safety, quality improvement

Bevezetés

A minőség mellett a munkabiztonság manapság stratégiai jelentőségű kérdés a vállalatok sikeres működésében, és ebben az értelemben hatékony és megkerülhetetlen eszköz a célok elérésére, többek között a vevők és érdekelt felek elégedettségének az elnyerésére. Nemzetközi meghatározásban a minőség egy termék vagy szolgáltatás azon jellemzőinek összessége, amely megmutatja, hogy milyen mértékben képes kielégíteni a vevő kimondott és látens igényeit, elvárásait.[3] Ebből a fogalomból alakul ki a termékek és szolgáltatások értékelése, ami a felhasználói követelmények kielégítését jelenti, és amelyek meg kell hogy feleljenek a vállalat céljainak, stratégiájának.

A minőség és a munkabiztonság ma már mindenhol jelen van, jelen kell hogy legyen a vállalatok működésében. Beleépül a termékek és szolgáltatások tervezésébe, fejlesztésébe, előállítói folyamataiba, a beszerzésekbe és a termelésirányításba, amelyek a minőségcélok teljesítése érdekében történnek. Mindezek alapján olyan szervezeti szemléletmód kialakítása szükséges, amely szem előtt tartja a minőséget és a munkabiztonságot, s ezen keresztül igyekszik fejleszteni a vevők és más érdekelt felek elégedettségét, ezáltal pedig a vállalat hatékonyságát.[4]

Az integrált irányítási rendszerek bevezetésekor a legfőbb elvárás az volt, hogy olyan vállalatirányítási modell alakuljon ki, amely azonos módon és azonos időben kezeli a különböző szabványok követelményeit, s ezzel a megközelítéssel további versenyelőnyhöz juttatja a vállalatokat.[5] Az ilyen rendszerek bevezetése, működtetése és folyamatos fejlesztése minden cég számára előnyös, függetlenül a vállalat nagyságától, szakmai jellemzőitől és ipari hovatartozásától. Az irányítási rendszerek főként olyan területeken alakultak ki, ahol a biztonság kulcsfontosságú szempont, mint

[3] MSZ EN ISO 9000:2015.
[4] MSZ EN ISO 9000:2015.
[5] Moumen – El Aoufir 2014: 207–228.

például a járműipar, a repüléstechnika vagy a katonaság, később más iparágakban is alkalmazni kezdték, majd megjelentek az ehhez kapcsolódó nemzetközi szabványok is.[6]

Az integrált irányítási rendszer alkalmazása szinte minden iparágban megjelent, de a bevezetésük során kiderült, hogy nem is olyan könnyű a különböző területeken bevezetni és alkalmazni, főleg, ha a gyártás menete és tulajdonságai nagyon eltérnek az eredetileg figyelembe vett, főleg gépipari területekétől. A szabványalkotóknak viszont pont az volt a céljuk, hogy a szabvány bevezethető és alkalmazható legyen valamennyi vállalatra, függetlenül azok méretétől, tevékenységi körétől, működési módjától. A vállalatoknak a szervezeti követelményeik, kultúrájuk és partnerek elvárásai ismeretében szükséges felépíteniük munkabiztonsági és minőségirányítási rendszereiket. Ez a folyamat a felső vezetéstől származó munkabiztonsági és minőségügyi kezdeményezéssel kezdődik, amely kijelöli a prioritásokat, a kezdeti célokat, és felelősségi köröket rendel a két rendszer meghatározásához és kialakításához.

A cégek, amelyek elkötelezettek az integrált irányítási rendszer működtetésére, meg kell határozzák a hozzá szükséges erőforrásokat és a célok megvalósításáért alkalmazandó folyamatokat. A munkabiztonság és a minőség olyan elérhető, mérhető és költségmegtakarítást eredményező cél, amelyet be lehet vezetni egy szervezetbe feltéve, hogy a fogalmak megértése és az elkötelezettség a szervezetben rendelkezésre áll. Mindkét szabvány, az ISO 9001 és az ISO 45001 tartalmazza azokat az előírásokat, követelményeket, amelyeket a bevezetett irányítási rendszernek mindenképpen meg kell valósítania, illetve be kell tartania a működés, a termék vagy szolgáltatás előállítási folyamatának különböző szakaszaiban. Az előre meghatározott megrendelői vagy jogszabályi előírások szerint, illetve azok figyelembevételével kell kialakítaniuk a működésüket, hogy a meghatározott célokat minél teljesebb mértékben és minél hatékonyabban tudják teljesíteni.

Vizsgálataink alapja egy járműipari vállalat, amely mindkét minőségirányítási rendszert bevezette és működteti, érvényes tanúsítással rendelkezik. Ugyanakkor a rendszerauditok során olyan probléma merült fel, hogy a vállalaton belül a munkatársak eltérő információkkal rendelkeznek a két vállalatirányítási rendszer szükségességéről és hasznosságáról, így eltérő hangsúllyal jelenik meg a mindennapi tevékenységekben. Ennek vizsgálatára kutatásunk az alábbi területekre terjedt ki:

- Milyen kapcsolat mutatkozik a vállalaton belül a Minőségirányítási Rendszer (MIR) és a Munkahelyi Egészségvédelem és Biztonság Irányítási Rendszer (MEBIR) között?
- A vezetőség felelőssége hogyan és milyen mértékben jelenik meg a MIR-ben és a MEBIR-ben?
- A MEBIR megismeréséhez milyen tevékenységek és oktatások szükségesek?
- A két rendszer és folyamataik mely pontokon integrálhatók?

[6] Turcsányi 2014.

Vállalatirányítási rendszerek

Mind az MSZ EN ISO 9001, mind pedig az MSZ EN ISO 45001 szabvány szerint kialakított irányítási rendszer egyik központi eleme a veszély meghatározása, a kockázatértékelés és a kockázatkezelés tervezése.[7] A szabványok előre meghatározott módon és megközelítéssel azonosítják a lehetséges kockázatokat és azok mértékét, megszüntetésének, valamint csökkentésének módját. Ezen szabványok szerint bevezetett és működtetett irányítási rendszerek ezek segítségével tudják javítani, fejleszteni a minőséget, a munkabiztonságot és az egészségvédelmet.

Egy vállalat dolgozóinak egészségvédelme és a biztonságos munkavégzés körülményeinek megteremtése jogszabályok által előírt kötelessége minden munkaadónak. A szabványalapú irányítási rendszer bevezetése elősegíti a törvényi megfelelést, a tanúsítás pedig igazolja a szervezet erőfeszítéseit és intézkedéseit a törvényi előírások teljesítésére. A munkavédelem területén a vonatkozó jogszabályok és előírások eleve meghatározzák számos kötelező dokumentum meglétét. Néhány ezek közül:

- kockázatértékelés dokumentációja,
- megelőzési stratégia,
- mentési terv,
- belső rendelkezések (szabályozások),
- rendszeres belső ellenőrzések,
- munkahelyi munkavédelmi program,
- munkavállalók rendszeres munkavédelmi oktatása,
- kollektív védelem, egyéni védőeszközök biztosítása,
- munkabalesetek bejelentése, kivizsgálása, nyilvántartása,
- munkavédelmi üzembe helyezés és időszakos biztonsági felülvizsgálat (veszélyes munkaeszköz).

A fejlődés és a fenntarthatóság érdekében az egész világon szükségszerű volt az egészségvédelem és biztonság irányítási rendszerének egységes nemzetközi szabvány szerinti harmonizálása és az ehhez kapcsolódó legjobb gyakorlatok összegyűjtése, megosztása.[8] Az MSZ ISO 45001:2018 egy olyan nemzetközi szabvány, amely globálisan biztosít hivatkozási alapot a megvalósítható és egységes oktatáshoz, így a vállalatok biztosabban tudják kézben tartani a biztonsági és egészségvédelmi kockázatokat és ezek hatását.

Az alkalmazottak egészségének védelme és a biztonságos munkafolyamatok körülményeinek megteremtése törvényi előírás szerinti kötelessége az összes munkaadónak. Az MSZ ISO 45001:2018 szabvány szerinti munkavégzés elősegíti a vállalat törvényi megfelelőségét, a tanúsítása igazolja a szervezet erőfeszítését, és intézkedéseket hoz a törvényi előírások betartása érdekében. A megfelelően bevezetett és működtetett, majd tanúsított MSZ ISO 45001:2018 szabvány szerinti rendszer a működés számos területén nyújt segítséget:[9]

[7] Darabont–Antonov–Bejinariu 2017.
[8] Dzięgielewska–Konarkowska–Górny 2022.
[9] Šolc et al. 2022.

- A munkavédelmi szabályok figyelembevétele és betartása, valamint az alkalmazottak által történő betartatása révén biztosítja a munkatársak egészségének védelmét, a potenciális veszélyforrások kiküszöbölését.
- Csökkenthető a dolgozókat érő egészségkárosodások, munkabalesetek száma, ezáltal a termelékenység növekedhet.
- Minimális szintre csökkenthető a munkavállalók veszélyeztetettsége.
- Növelheti az alkalmazottak biztonságtudatosságát, javíthatja a szervezet biztonsággal kapcsolatos kultúráját.
- Költséghatékonyabb és jobb munkaminőség érhető el.
- A munkahelyi egészségvédelemmel és biztonsággal összefüggő költségek és bírságok minimalizálhatók.
- Átláthatóbbá válik a munkabiztonság és foglalkozás-egészségügy jelenlegi jogi szabályozásának való megfelelése, dokumentálható és jobban ellenőrizhetővé válik a vállalatvezetés és a hatóságok szempontjából is.
- A munkatársak, alkalmazottak elégedettsége és a vállalat iránti lojalitása nő, ha érzik munkáltatójuk figyelmét egészségi állapotuk és munkabiztonsági feltételeik javítása irányában.
- Javítja a vállalat versenyképességét.

ISO 9001 alapú minőségirányítási rendszer (MIR)

Napjainkban az ISO 9001 egy nemzetközileg elismert szabvány, amely minőségirányítási rendszerek tanúsítására vonatkozó követelményeket tartalmaz. Világszerte több mint 1,2 millió szervezet bizonyította az ISO 9001 szabványnak való megfeleléssel, hogy minőségirányítási rendszere alkalmas arra, hogy a vevői igényeket figyelembe véve, folyamatosan kiváló minőségű terméket szolgáltasson ügyfelei számára. Mindemellett úgy törekszik a vevői elégedettségre, hogy belső folyamatait állandó felügyelet alatt tartja és fejleszti, valamint csökkenti a szervezet költségeit.

A szabvány a szervezet hatékonyságának növelése érdekében útmutatást és követelményeket nyújt a folyamatszemléletű gondolkodásmód alkalmazására, valamint a korábbi verzióban megjelenő nem megfelelőségek kezelésére vonatkozó megelőző tevékenységek helyett a kockázatalapú gondolkodásmód használatát hangsúlyozza.[10]

ISO 45001 szerinti munkahelyi egészségvédelem és biztonság vállalatirányítási rendszer

A munkavédelem alapvető célja az egészséges és biztonságos munkavégzés megteremtése, az ehhez szükséges személyi, tárgyi, szervezeti feltételeinek megteremtése és szabályozása, a munkavégzők egészségének és munkavégző képességének megóvása annak érdekében, hogy a munkabaleseteket és a foglalkozási baleseteket megelőzzük. Az ISO 45001 szabványkövetelmény alapján a bevezetett MEBIR megfelelő alapot

[10] Başaran 2021.

nyújt az ezzel kapcsolatos kockázatok kezeléséhez, így hozzájárul a szervezet MEB-teljesítményének növeléséhez, biztosítja a fejlődést és a fejlesztést.

Követelményrendszerének felépítése összhangban áll az ISO 9001 alapú minőségirányítási rendszerre vonatkozó követelményekkel, így lehetőséget ad a szervezetek számára az integrált irányítási rendszerben történő alkalmazására. Bármely vállalat alkalmazhatja, függetlenül a szervezet tevékenységétől, méretétől, szervezeti felépítésétől és fejlettségi szintjétől. Az ISO 45001 bevezetése a munkatársak egészségvédelmén keresztül az üzleti siker része. A MEBIR kidolgozása biztosítja minden olyan eljárás bevezetését, amelyek szükségesek az ISO 45001 céljainak meghatározásához, és amelyekkel ezeket a célokat meg lehet valósítani.

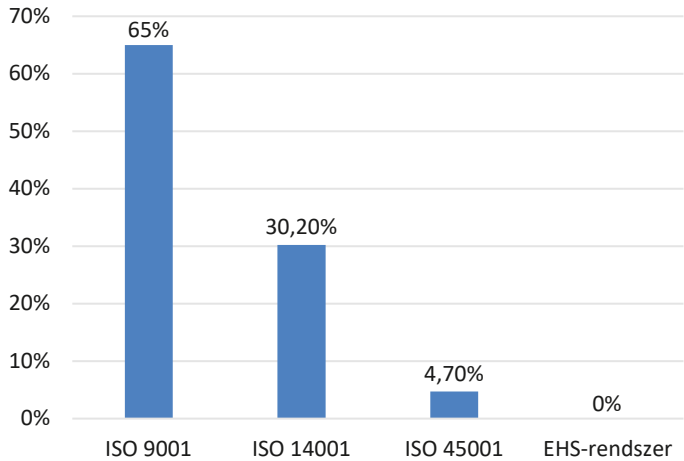
Az új 45001 szabványt a Nemzetközi Szabványügyi Szervezet (ISO) 2018-ban bocsátotta ki, ezzel együttesen az MSZ 28001 (OHSAS 18001) szerinti tanúsítványok 2021 márciusától érvényüket vesztették. Ettől az időponttól kezdve már csak az ISO 45001:2018 alapján lehet tanúsítani.

Vállalatirányítási rendszerekkel kapcsolatos követelmények vizsgálata a vállalaton belül

Kutatásunk során kérdőíves dolgozói felmérést végeztünk azzal a céllal, hogy átfogó képet kapjuk egy vállalaton belül a munkatársak ismereteiről a munkahelyi egészségvédelmi és biztonsági irányítási rendszerrel kapcsolatban. A felmérés online kérdőív formájában történt, ami lehetőséget adott az eredmények gyors kiértékelésére, a válaszok diagramban történő megjelenítésére. A kérdések a MEBIR vállalatirányítási rendszerrel összefüggésben az alábbiak voltak:

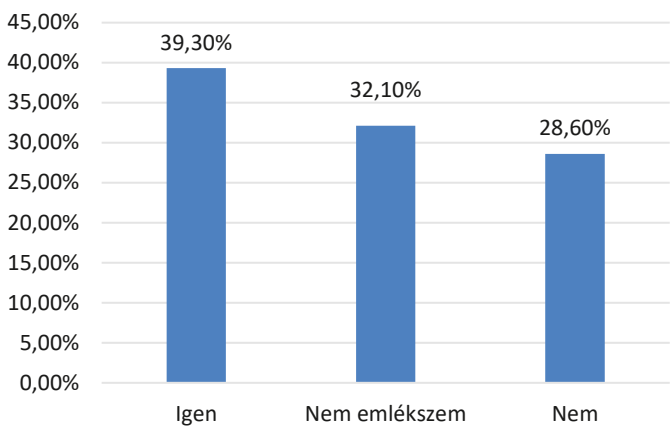
- Milyen területen dolgozik?
- Válassza ki, milyen minőségirányítási rendszert működtet a vállalat!
- Részt vett-e már munka- és egészségvédelmi oktatáson?
- A vállalathoz történő belépéskor részt vett-e minőségügyi oktatáson?
- Ön szerint miért fontos, hogy egy vállalat irányítási rendszert működtessen?

A felmérésben a vállalaton belül minden terület munkatársai részt vettek, így gyakorlatilag teljes körű képet kaphattunk a gyártási és az ahhoz kapcsolódó támogató folyamatokban részt vevőktől, valamint a vezetőktől. Az első kérdésre adott válaszok alapján megállapítható, hogy a véleményezésben részt vevők fele (50%) a fizikai munkát végzek kategóriát jelölte meg, 39,3%-a az adminisztratív munkakört választotta, és 10,7% vezető beosztásban dolgozik.



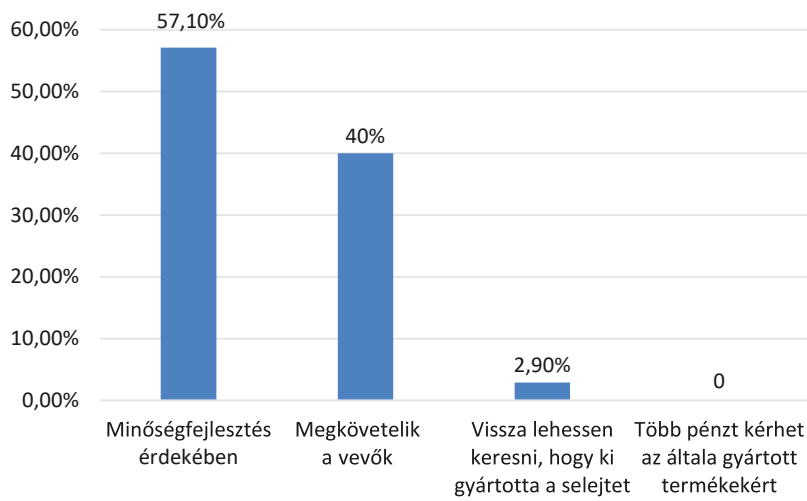
1. ábra: Minőségirányítási rendszerek ismerete a vállalaton belül
Forrás: a szerző szerkesztése

Az 1. ábra diagramja mutatja, hogy a megkérdezettek körében a MEBIR-rendszerről csak kis mértékben hallottak (4,7%), a környezetirányítási rendszerről is csak 30%, s ami sokkal érdekesebb, hogy a MIR-rendszert is csak a válaszadók 65% jelölte meg, holott ennek a rendszernek megfelelő minőségtudatosság oktatása rendszeresen, ismétlődő jelleggel megtörténik és megfelelően dokumentált is. Meglátásunk szerint ezt a nagy különbséget az indokolhatja, hogy minden egyes vevői reklamáció esetén az érintett területek valamennyi munkatársát (újra)oktatásban részesítik, ezért a MIR megléte sokkal hangsúlyosabban jelenik meg. Ez az oktatás alapvetően az elkövetett hibáról és annak rövid, valamint hosszú távú megoldásáról szól, de ilyenkor minden esetben kitérnek a minőségirányítási rendszer követelményeire, illetve a vevői elégedettség fontosságára.



2. ábra: MEBIR-oktatáson való részvétel a vállalaton belül
Forrás: a szerző szerkesztése

A következő kérdés arra vonatkozott, hogy a MEBIR-oktatás milyen hatékonysággal működik a vállalaton belül. A 2. ábra eredményeiből látható, hogy a munkatársak 60%-a nem emlékszik, vagy egyáltalán nem vett részt ilyen típusú oktatáson. Ez azért is meglepő válasz, mert a belépéskor minden dolgozó számára kötelező egy úgynevezett orientációs tréning, amelynek témája a munka- és egészségvédelem. Ezenkívül erre vonatkozóan éves ismétlő oktatások is vannak, többnyire azonban az idő hiányában nem személyes formában valósulnak meg. A vállalaton belüli gyakorlat az, hogy az oktatási anyagot a munkavédelmi felelős, szakember elektronikusan körbeküldi, illetve kiteszi a faliújságokra. Látható, hogy ennek a módszernek a hatékonysága messze nem éri el a kívánt célt. A dolgozók nem olvassák el a faliújságra kitett anyagokat, és az e-mailen érkezett oktatási anyagok nem kellő hangsúllyal rendelkeznek. Egy jól kialakított, rendszeres és gyakorlatközeli ismereteket tartalmazó képzés bevezetése és működtetése elengedhetetlen, hogy a MEBIR szükségességét és hasznosságát ugyanolyan mértékben érezzék a munkatársak, mint a MIR-rendszer esetében.



3. ábra: Az irányítási rendszerek fontossága a vállalaton belül
Forrás: a szerző szerkesztése

A felmérésben az utolsó kérdés az irányítási rendszerek működtetésének fontosságára vonatkozott, amelyre a válaszadók kötetlen formában válaszolhattak. A feldolgozás során arra törekedtünk, hogy néhány, megfelelően kezelhető csoportba soroljuk a kapott válaszokat. Ez alapján megállapítható, ahogy a 3. ábra diagramja is mutatja, hogy a munkatársak 57,1%-a egyértelműen a minőségfejlesztést fogalmazta meg mint legfontosabb célját az irányítási rendszereknek. Ez összhangban áll a MIR-re vonatkozó tréningek tartalmával, következésképpen a MEBIR célja és alkalmazásának jelentősége háttérbe szorul. 40%-a nyilatkozott úgy, hogy vevői követelményként tekint az irányítási rendszerekre, nem érzékelve a vállalati folyamatokra gyakorolt hatékonyságát.

Következtetések és javaslatok

Minden irányítási rendszerszabványnak való megfelelés egyik mérföldköve a következetesség, a vezetői aktív szerepvállalás, a munkatársak bevonása és elköteleződése, az oktatás és tudatosság, a tanulás az elkövetett hibákból és a folyamatos fejlesztés. Ez a minőségirányítási rendszer működtetése alatt folyamatosan megfigyelhető mind az új belépők esetén, mind a régi dolgozók folyamatos fejlesztésében. Ez a szervezeten belül végzett belső oktatás hatékonyságát is alátámasztja. Dokumentáltsága ugyan megfelelő, és a legtöbb dolgozó ismeri is az ehhez kapcsolódó követelményeket, folyamatokat, eljárásokat és utasításokat.

Emellett mindenhol kifüggesztették a minőségirányítási rendszerhez kapcsolódó minőségpolitikát, amelyet a munkatársak több minőségügyi dokumentummal együtt, azonosító segítségével a vállalat belső hálózatán elektronikus formában is elérhetnek. Ugyanakkor a munkahelyi egészségvédelem és biztonságirányítási rendszer esetén számos területen mutatkoztak jelentős hiányosságok a fentebb említett szempontok tekintetében. A vezetők kevésbé látszódnak elkötelezettnek, a munkatársak ezért kevéssé ismerik, értik a MEBIR célkitűzéseit. Számos helyen nem is követik vagy tartják be a vonatkozó követelményeket. A hibákból való tanulás és a folyamatos fejlődés így sokkal lassabban, nehézkesebben megy végbe.

Tudatosság, oktatás témakörében tett fejlesztési javaslatok

Az oktatási anyag összeállítására nagy hangsúlyt kell fektetni, továbbá az oktatások megvalósításában olyan rendszert kell kialakítani, amely támogatja a tudásátadás hatékonyságát és nyomonkövethetőségét. Például jelenléti ívek aláírásával lehet megtenni, ami történhet papíralapon hagyományosan vagy digitálisan valamilyen rendszeren keresztül. A külső érdekelt feleket is figyelembe kell venni mind a környezetvédelem, mind az egészség és munkabiztonság területén. Ennek érdekében be kell vonni azokat a partnereket is, akik rendszeresen látogatják a vállalatot és ott közvetlenül vagy közvetve munkát végeznek. Ezek lehetnek alvállalkozók, akik különböző javítást, karbantartást végeznek, de lehetnek a szállítók is, akik alapanyagot, alkatrészeket szállítanak.

Az oktatásnak rendszeresen ismétlődőnek kell lennie, hogy mindig frissüljenek az ismeretek, és be lehessen építeni az oktatási anyagba az évenként meghatározott új célokat és az addig felmerülő kockázatokra hozott intézkedéseket, amelyek betartása a szervezeten belül mindenki számára kötelező érvényű. Ehhez a dokumentált információkat folyamatosan karban kell tartani és módosítani annak megfelelően, ahogy változik mind a külső, mind a belső környezet.

Nyilvánosság, hozzáférhetőség tekintetében tett fejlesztési javaslatok

Kulcsfontosságú feladat, amelyet mindenképpen pótolni kell a nyilvánosság figyelembevételével és a hozzáférhetőség biztosítása mellett, hiszen a szervezet által működtetett munkavédelmi rendszert és a munkabiztonságért, egészségvédelemért

tett törekvéseket meg kell ismertetni a szűkebb és tágabb környezettel, a partnerekkel. Ehhez első lépésben javasolt a vállalat területén több helyen megjelentetni a minőségpolitikát és a minőségcélokat. A célok közzétételén túl gondoskodni kell arról is, hogy mindenki értse azokat és megfelelően informálva legyenek az aktuális teljesítésekkel.

A MEBIR-rendszer alkalmazása kapcsán felmért negatív hatások megszüntetésére vagy csökkentésére hozott intézkedéseket is szükséges megismertetni a munkatársakkal, hiszen tisztában kell lenni azzal, hogy mit tesz a vállalat a munkavállalók megóvása érdekében. Napjainkban folyamatosan nő a vállalatokra gyakorolt nyomás. Ezért egyre több szabályzatnak, jogszabálynak, illetve egyéb, a megrendelők által előírt kötelezettségnek kell megfelelni. A munkatársak sokkal elkötelezettebbek lennének, ha tudnák, értenék, hogy a különböző, elsőre akár kellemetlen intézkedéseket miért kell betartaniuk. Tehát ebből a szempontból is érdemes betartani a szabványpontokban megfogalmazott követelményeket, hogy ily módon megfeleljenek a piaci elvárásoknak, amelyeket a piac szereplői, köztük a vállalat partnerei szabnak meg.

Kockázatértékelésre tett fejlesztési javaslatok

A kockázatértékeléseket a minőségirányítási, a munkabiztonsági és egészségvédelmi területen külön-külön szükséges elvégezni, hogy megfelelően lehessen koncentrálni az egyes területekre. Érdemes ehhez akár külső szakértőt is igénybe venni. Mint például az üzemorvost az egészségvédelmi kockázatértékelésnél vagy a munkavédelmi szakembert a munkabiztonsági kockázatértékelésnél. Jelen esetben nem biztos, hogy minden területen a kockázatelemzésben munkavédelmi képzettséggel rendelkező személy vett részt. Ezek feltárása és kiküszöbölése az eredményességben is láthatóvá válik. A kockázatértékelést sosem egy személy végzi, éppen ellenkezőleg. Minden érintett, aki ezen a területen dolgozik, a saját szemszögéből nézve látja és saját tapasztalatai alapján tud a lehetséges kockázatokról dönteni. Ezért a kockázatokhoz tartozó kritériumrendszer meghatározása is közös feladat kell legyen. További javaslat ezen a területen, hogy a kockázatértékelés formátuma legyen egységes, kiegészítve az alábbi adatokkal:

- intézkedési terv felelőse (nem feltétlen név szerint megnevezve), elég a beosztás,
- intézkedési terv megvalósításának határideje, pontos dátum.

A MIR és a MEBIR integrált irányítási rendszere

Az irányítási rendszerek kétségkívül alkalmasak az összevonásra. Mára minden irányítási rendszerszabvány alkalmazza az Annex SL rendszerben megfogalmazott struktúrát, így felépítésük azonos, a szabványpontok egységesek.

Megoldás lehet a fejezetenként történő átvizsgálás és harmonizáció, amelynek megvalósítása során nem szükséges külön elvégezni a fent leírt hiányosságok pótlását, azt az integrált rendszer kiépítése során egy lépésben végre lehet hajtani.

A szabványpontok szerint az integrált kézikönyvben mindkét szabvány szerint meg kell fogalmazni a vállalat tevékenységeit, felelőseit és céljait. Majd ezek alapján az integrált politika is kialakítható, amiben ugyanúgy mindkét szabvány szerinti célok

meghatározása szükséges. Természetesen hosszabb távon, vagy akár azonnal e két rendszer integrálása előtt, el lehet gondolkodni egy harmadik, a környezetközpontú irányítási rendszer integrációjáról is. Ezzel a centralizált stratégiával, egy úgynevezett egykapus rendszer létrehozásával egyszerűbb és hatékonyabb fejlesztési terveket lehet megvalósítani, amely akár költséghatékonyságot is jelenthet, és az érdekelt felek, partnerek nagyobb megelégedettségét eredményezheti, ami egyértelmű versenyelőnyt jelent.

Összefoglalás

Az elvégzett vizsgálatok alapján és a felmérés során megállapítottuk, hogy a vizsgált szervezetnél a vezetőség nem kezeli kellő figyelemmel és elkötelezettséggel a később bevezetett munkahelyi egészségvédelmi és irányítási rendszert. Ennek megfelelően sok hiányosságot tártunk fel, amelyek azonban javíthatók, a szabványok pontjainak és a vonatkozó jogszabályok betartásával. A munkavállalók körében végzett felmérések rávilágítottak arra, hogy nincsenek tudatában a szervezet céljaival, törekvéseivel, a rendszer támasztotta követelményekkel, és nem is feltétlenül érzik magukra nézve kötelezőnek azokat.

Ahhoz, hogy a munkatársak betartsák és végrehajtsák a célok eléréséhez meghatározott tevékenységeket, továbbá az új munkabiztonság és egészségvédelem beépüljön a folyamatokba, meg kell ismertetni mind a belső, mind a külső érintett felekkel a célokat, a követelményeket, a módszereket, és általában el kell érni, hogy a munkatársak magukénak érezzék azokat. Az irányítási rendszerek egy alap szabványcsalád szerint készültek, amelyek az azonos szabványpontok alapján könnyen egymáshoz integrálhatók. Mivel az ISO 9001 alapú minőségirányítási rendszer már régóta működik a vállalatnál, és megfelelő a dokumentáltsága, nagymértékben segíthet a később kialakított rendszer hibáit kijavítani.

Fejlesztési javaslatainkban is egyértelműen megjelent a különböző menedzsmentrendszerek integrált irányítási rendszerekben történő működtetése, amelynek középpontjában az ISO:9001 szerinti minőségirányítási rendszer áll.

Felhasznált irodalom

Başaran, Burhan (2021): The Past, Present and Future ISO 9001 Quality Management System Standard. *Business & Management Studies,* 9(1), 227–247. Online: https://doi.org/10.15295/bmij.v9i1.1756

Darabont, Doru Costin – Antonov, Anca Elena – Bejinariu, A. Costiča (2017): Key Elements on Implementing an Occupational Health and Safety Management System Using ISO 45001 Standard. *MATEC Web of Conferences,* 121, 11007. Online: https://doi.org/10.1051/matecconf/201712111007

Dzięgielewska, Paulina – Konarkowska, Olga – Górny, Adam (2022): Adapting an OHS Management System to ISO 45001 Requirements: Ensuring System Management Effectiveness. *European Research Studies Journal,* 25(1), 809–819. Online: https://doi.org/10.35808/ersj/2888

MSZ EN ISO 9000:2015 Minőségirányítási rendszerek. Alapok és szótár.
MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Követelmények.
MSZ ISO 45001:2018 A munkahelyi egészségvédelem és biztonság irányítási rendszere. Követelmények alkalmazási útmutatóval.
Moumen, Mariyam – El Aoufir, Houda (2014): Quality, Safety and Environment Management Systems (QSE): Analysis of Empirical Studies on Integrated Management Systems (IMS). *Journal of Decision Systems,* 26(3), 207–228. Online: https://doi.org/10.1080/12460125.2017.1305648
Šolc, Marek et al. (2022): The Development Trend of the Occupational Health and Safety in the Context of ISO 45001:2018. *Standards,* 2(3), 294–305. Online: https://doi.org/10.3390/standards2030021
Turcsányi Károly (2014): *Minőségelmélet és -módszertan*. Budapest: NKE.

HADMÉRNÖK
HADITECHNIKA
19. évfolyam (2024) 3. szám 17–27.
DOI: 10.32567/hm.2024.3.2

István Ember[1]

Investigation of the Efficiency of Cumulative Cones Manufactured by Additive Processes from Various Materials

Abstract

There is currently little-known research on low-density cumulative cones, although they can be useful and cost-effective in a number of areas. 3D printing is providing a foundation and cohesion in this area of blasting technology that has been difficult to achieve in the past. Taking advantage of this, I have carried out prototype testing in my study, in total I have been able to create nine cumulative charges using additive manufacturing and test their effectiveness. To get a broader picture, I used several types of 3D printers and several materials for the analytical testing of the three charge types developed. The tests gave me conclusive results on the applicability of the technology and the performance of the different polymers.

Keywords: additive, 3D printing, blasting technology, cumulative, charges

Introduction

Nowadays, military research faces numerous challenges. Navigating the most important research directions is relatively simple.[2] Technical and military theoretical research encompasses the application of modern technologies, such as artificial intelligence[3] and the practical use of autonomous systems,[4] as well as what might be the greatest challenge of our time, climate change, which imposes (or will impose) an enormous

[1] Assistant Lecturer, Ludovika University of Public Service, Faculty of Military Science and Officer Training Department of Operations and Support, e-mail: Ember.Istvan@uni-nke.hu
[2] Boda et al. 2016.
[3] Fazekas 2023.
[4] Tóth–Vég 2022.

burden on all armed forces.[5] Within this broad scope, 3D printing also holds a worthy position, as most armed forces are already applying additive manufacturing technologies at a practical level.

I chose cumulative charges as a concrete research direction, focusing on this area. While cumulative liners usually emphasise high-density materials like copper, I decided to concentrate on low-density materials, specifically polymers and composite polymers. Although these materials significantly lag behind copper in terms of destruction capability, immense perforation is not always required for the target object. In certain explosive ordnance disposal tasks,[6] it can be particularly favourable if the charge only penetrates the anticipated material thickness.

In this study, I will examine cumulative cones formed from different materials and manufactured using various additive manufacturing technologies. Beyond their efficiency, it will be interesting to compare the geometry of the holes created in the target objects to identify potential future development directions. Comparing additive technologies and fundamentally similar materials is inherently intriguing, but examining the same technology with different materials can also provide forward-looking insights. All components of the examined charges have a uniform geometric shape, with only the manufacturing conditions and materials varied.

My goal is to detonate nine charges to investigate the efficiency of three variants of charges. I hypothesise that there will not be significant differences in the results, but the differences between manufacturing technologies will become clearly identifiable.

Additive manufacturing

The first technology to be demonstrated is the Fused Deposition Modelling or Fused Filament Fabrication (FDM/FFF). This is a very widely used method, even for hobby purposes, whereby wound polymers, so-called filaments, can be used as raw material.

These filament materials can be made from a wide variety of polymers and composites. Perhaps the most well-known and commonly purchased material for hobby purposes is polylactic acid (PLA), but there is a broad range of other options available, such as PET,[7] PET-G,[8] ABS,[9] ASA,[10] and PA[11] or nylon. The diameter of the filaments is crucial, as they come in two sizes (1.75 mm and 2.85 mm), and technical equipment (Figure 1) is not capable of handling a different size without significant modification or conversion.

The spooled polymer is pulled or pushed by gears into the print head, which is responsible for melting the material. The resulting melt flows through a nozzle and is deposited onto the build platform within the construction area.[12]

5 Földi–Padányi 2022; Padányi 2023.
6 E.g. some improvised explosive device disposal tasks. Daruka–Kovács 2013.
7 Polyethylene terephthalate.
8 Polyethylene terephthalate glycol.
9 Acrylonitrile butadiene styrene.
10 Acrylonitrile styrene acrylate.
11 Polyamid.
12 Gál–Németh 2019: 233.

The main principle of the technology is layer-by-layer construction, making it essential for movement to occur in three dimensions within the build chamber. One common solution is where the print head can move horizontally (two dimensions) while the build platform adjusts vertically (3rd dimension). In other variants, the print head can move in one horizontal dimension and vertically, with the build platform providing movement in the other horizontal direction. There are also solutions with a fixed build platform and others where a robotised arm enables the construction of parts from multiple directions, although the latter is not yet widely adopted by the general public.

Figure 1: FDM/FFF printers
Source: photographed by the author

The second technology I intend to introduce is Selective Laser Sintering (SLS). This method is often known as powder bed printing, a term that more clearly describes the whole process. In contrast to the widespread Fused Deposition Modelling/Fused Filament Fabrication (FDM/FFF) technology, the selection of materials is significantly more limited. Basically, a form of polyamide (PA) is used as the base material, but polypropylene (PP) can also be employed for creating lighter components, and thermoplastic polyurethane (TPU) may be used when flexibility is important.

Initially, the powder material is transferred from a container to the build chamber and spread in thin[13] layers. The evenly distributed, smoothed powder surface is then targeted by a laser at the necessary points, causing it to solidify a layer. After the plate in the build area moves downward, a new thin layer of material is applied, which is also solidified by the laser. Both the process and the material require a consistently high and uniform temperature, which is necessary for the high quality of the parts.[14]

[13] Between 50 and 200 micrometres.
[14] Gál–Németh 2019: 234.

The raw materials used in the research

The Faculty of Military Science and Officer Training (MSOT) at the Ludovika University of Public Service (LUPS) also possesses an SLS technology 3D printer. This is a Fuse 1 device manufactured by Formlabs, for which five materials are available.

The Nylon 12 (PA–12) powder used in the printer mentioned above is considered to be general purpose. It is a very versatile material that is biocompatible. It can be used to produce highly detailed and highly dimensionally accurate objects. It is also ideal for prototyping but can also be used to make complex structures that are durable and resistant to environmental influences. Of course, it is also ideal for end-use objects, i.e. for factory production.[15]

The second material used is Markforged Onyx, a special polyamide. The filament is filled with micro-carbon fibre and the end surface of the parts made from it is of high quality and can be used to make objects and parts with high dimensional accuracy. It is the matrix material of the technology and the manufacturer's proprietary continuous filament reinforcement. Even without a reinforcing insert, it provides high strength, toughness and chemical resistance. With some continuous fibres, its material properties can even rival those of aluminium, but I did not plan to use such inserts for this test.[16]

The third material used was Polimaker PolyLite ASA, which I found to be very easy to print. ASA is on the market as an alternative to ABS. It is the preferred choice when the environmental resistance of ABS is not sufficient for the object in question. It is also recommended by the manufacturer for the production of objects for everyday use. It has a density of 1.13 g/cm^3 at 23 °C and good resistance to acids and oils.[17]

I used this material in an Ultimaker S5 printer (FDM/FFF technology), which has a glass build tray and a print head optimised for water soluble supports.

Manufacturing process

The designs for all components were created using FreeCAD 0.20, a free, open-source software that is available for download. I am already familiar with this software, having used it for similar purposes before.[18] The dimensions of the shaped charges were determined through various methods,[19] incorporating my own parameters[20] that have consistently proven effective in multiple tests.[21] I kept the 20 mm diameter (internal) for the cone from the previous or base geometries, but I changed the apex angle to 90 degrees (Figure 2). While designing, I took manufacturing characteristics

[15] Formlabs Nylon 12 Powder: https://formlabs.com/store/materials/nylon-12-powder/
[16] Markforged Onyx: https://markforged.com/materials/plastics/onyx
[17] Polymaker: PolyLite ASA – Technical Data Sheet: https://cdn.shopify.com/s/files/1/0548/7299/7945/files/PolyLite_ASA_TDS_V5.1.pdf?v=1640828798
[18] Ádám–Ember 2022a; Ádám–Ember 2022b.
[19] Ember 2022a.
[20] Lukács 1992.
[21] Ember 2022b; Ember 2022c; Ember 2022d; Ember 2022e.

into account, although supports were not significant in our case since SLS technology does not require them, which allows for greater design freedom.

The finalised electronic forms were virtually arranged within the build area using the cloud-based PreForm software. This preparation tool is notably user-friendly, as it does not necessitate extensive knowledge of material science or manufacturing technology to operate. Various parameters are pre-set, so the user mainly needs to focus on maximising the use of space, which is crucial for material economy. Although the software can optimise the layout for us, I chose not to use this feature because it alters the orientation of the objects in space. This adjustment likely wouldn't cause significant differences in the blast results, but I preferred maintaining identical arrangements to ensure comparability across all aspects.

The Markforged 3D printer can also be worked using a cloud-based service which is the Eiger software. This printer is able to use Onyx material. Since it employs FDM/FFF technology, there are significantly more parameters that can be adjusted, although in this application, it is much more limited compared to a free slicing software. This limitation, however, promotes the production of very high-quality objects. Among the default or base printing settings, I only adjusted the infill to 100%, leaving the rest unchanged. The end product cones were of excellent quality; the internal supports detached almost automatically from the surface, without visible marks.

Figure 2: Onyx cumulative cone
Source: photographed by the author

For ASA material, I chose the Ultimaker S5 among several possible technical options. The "slicer" software Ultimaker Cura, offers numerous settings, but in this case, I retained the base settings recommended for the geometry, again only increasing the infill to 100%. These software programs typically recommend some infill pattern and a 15–30% infill for FDM/FFF technologies to promote low cost, efficiency and durability. However, for this research, this was not acceptable, as achieving the highest possible density required filling the entire volume to the maximum extent.

I also manufactured the other parts of the charges (Figure 3) using this device, but for those, I fully applied the recommended default settings. This approach resulted in significant material savings without compromising the quality.

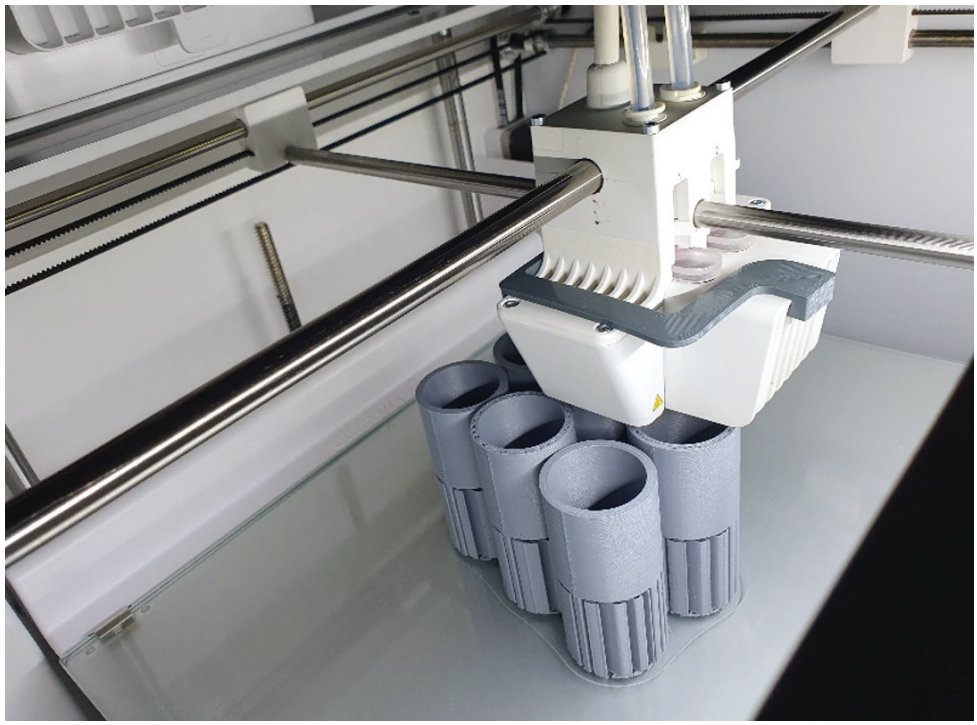


Figure 3: Charge bodies in the Ultimaker S5's buildchamber
Source: photographed by the author

Preparation for blasting

The tests were carried out with the assistance of the bomb technicians of the Hungarian Defence Forces (HDF) 1st Explosive Ordnance Disposal and River Guard Regiment (HDF 1st EOD&RG Reg.) in Táborfalva, at the designated blasting area of the HDF.

During the blasting task, more charges were detonated than those described in this article. Multiple series of blasting were conducted; however, the electrical network was configured in a series connection using the standardised electric detonators and wires of the HDF. Due to the required performance of the explosive placed in the charge body, a brisant military type[22] was chosen. This was the Semtex-H plastic explosive. A significant number of fragments were not expected due to the special implementation of the blasting and the materials. Interesting question: what changes would occur if the experiments were carried out with insensitive explosives?[23] I will be looking for the right answers to this in the future.

[22] Lukács 2017: 26.
[23] Daruka 2024: 59–61.

Figure 4: A charge placed in the blasting hole
Source: photographed by the author

We dug pits in the ground, each with a base area of 30 × 30 cm and a depth of 50 cm (Figure 4), where the target objects with the attached charges were placed. The pits were spaced far enough apart so that the detonation shockwave and other effects of blasting would not influence the process. In practice, this meant a distance of approximately 3 meters. The parameters of the configured charges can be seen in detail in Table 1.

Table 1: Data of exploded charges

No.	Type	Cone weight (g)	Explosive weight (g)	Target material
1.	Cone: 20 mm, PA–12, 90° Charge body: 40 mm stand-off, back-flow preventer	2.4	32	30 mm wide, steel disc (sawed from a single steel pole)
2.				
3.				
4.	Cone: 20 mm, ONYX, 90° Charge body: 40 mm stand-off, back-flow preventer	2.8		
5.				
6.				
4.	Cone: 20 mm, ASA, 90° Charge body: 40 mm stand-off, back-flow preventer	2.5		
5.				
6.				

Source: compiled by the author

The process of preparing the charges:

1. Assembling the charge housings
2. Filling the charges with Semtex-H explosive
3. Creating the space for the detonator
4. Attaching the charges to the target objects with superglue
5. Placing the detonator support cap
6. Inserting the secured charges into the blasting pits prepared for detonation
7. Placing the electric detonators in the charges

Results

All of the PA–12 cumulative cone-equipped charges demonstrated the expected efficiency; however, the appearance of the created holes was not entirely uniform. The height of the rim ranged between 4.5 and 5.3 mm. The upper part of the penetration formed a cavity with a wider diameter, where the rim occasionally detached. The lower part of the penetration was relatively uniform, with diameters ranging between 15 and 16.8 mm. The bottom of the cavity, measured from the original surface of the disc, was between 10.8 and 12 mm in the target objects.

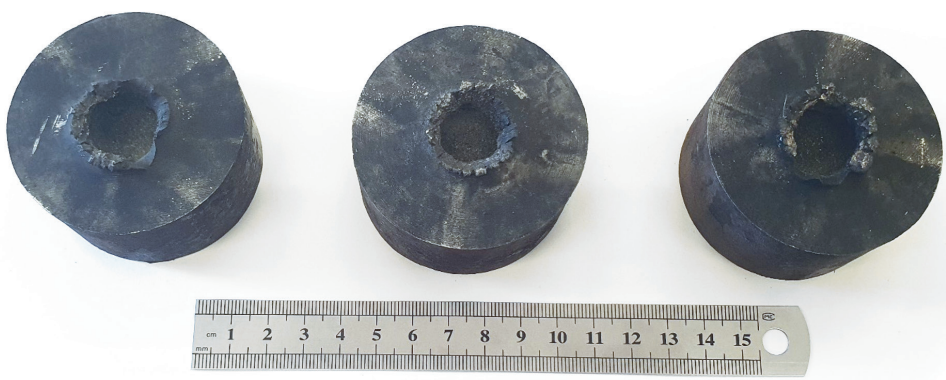


Figure 5: Target objects of charges with PA–12 cone
Source: photographed by the author

All of the Onyx cumulative cone-equipped charges also demonstrated the expected efficiency, and the appearance of the created holes was uniform. The height of the rim ranged between 3.7 and 4.3 mm. The upper part of the penetration formed a cavity with a wider diameter, where the rim occasionally detached. The lower part of the penetration was relatively uniform, with diameters ranging between 12.6 and 13 mm. The bottom of the cavity, measured from the original surface of the disc, was between 11.8 and 12.2 mm in the target objects.

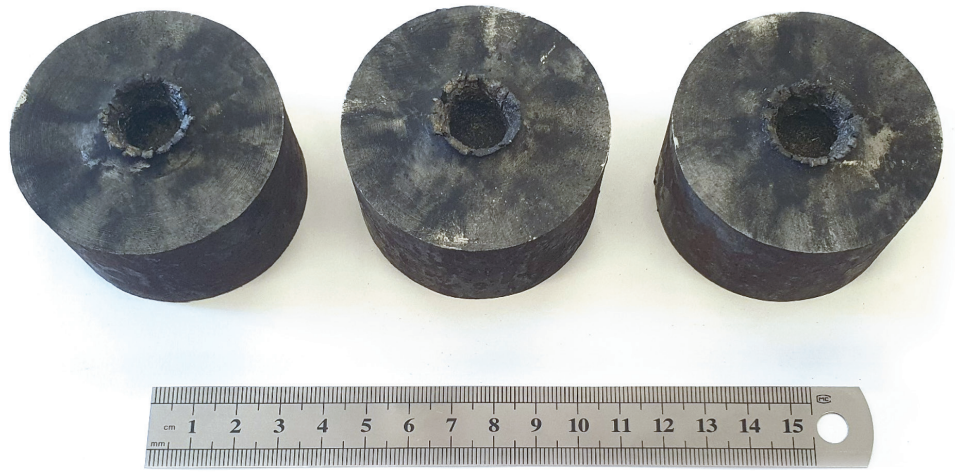


Figure 6: Target objects of charges Onyx cone
Source: photographed by the author

The ASA cumulative cone-equipped charges also demonstrated adequate efficiency, and the geometry of the cavities was uniform. The height of the rim ranged between 4 and 4.4 mm. The upper part of the penetration formed a cavity with a wider diameter, where the rim occasionally detached. The lower part of the penetration was relatively uniform, with diameters ranging between 14 and 14.7 mm. The bottom of the cavity, measured from the original surface of the disc, was between 11.8 and 11.9 mm in the target objects.

Figure 7: Target objects of charges ASA cone
Source: photographed by the author

All of the examined materials demonstrated the expected performance, although in the case of the PA–12 variants produced using SLS technology, it is visibly apparent that the geometry of the cavity is somewhat irregular. This is particularly evident when compared with the other materials, resulting in a contrasting outcome. The Onyx and ASA materials delivered nearly identical performance, with the cavities consistently forming in an orderly manner. The penetration and other parameters in these cases show relatively little variation, indicating that these charges are easily reproducible under field conditions. Additionally, this confirms that the conducted tests can be considered successful, as the charges formed were sufficiently uniform.

Summary

During the investigation, I detonated nine charges, whose design and assembly made them suitable for producing real results. The parameters established along the uniform geometry meet the requirements of scientific outcomes.

Although the nylon materials (PA–12 and Onyx) do not have completely identical properties, I considered this an acceptable variation due to the different manufacturing technologies. The disadvantage of SLS technology can be considered confirmed, likely due to the lower mass and density of the cones made from powder material.

The cones produced with FDM/FFF technology (Onyx and ASA) yielded similar results, with some differences in their efficiency and the geometry of the created holes, but overall, their performance can be described as uniform. This could also indicate that further investigations are needed, as there may be other polymers that could be more effective in piercing the target objects.

The above thus confirms my hypothesis and provides information for further studies. I find it important to test other potential materials under similar conditions in the next examination period of cumulative charges.

References

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

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

DARUKA, Norbert (2024): Érzéketlen robbanóanyagok II. Vizsgálati módszerek és alkalmazási lehetőségek. *Műszaki Katonai Közlöny,* 34(1), 47–65. Online: https//doi.org/10.32562/mkk.2024.1.4

Daruka, Norbert – Kovács, Zoltán (2013): IEDD: Improvised Explosive Device Disposal. In Krivanek, Vaclav – Stefek, Aleksandr (eds.): *International Conference on Military Technologies: ICMT 2013.* Brno: University of Defence, 383–390.
Ember, István (2022a): Modern kumulatív töltet méretezésének lehetőségei. *Műszaki Katonai Közlöny,* 32(1), 5–15. Online: https://doi.org/10.32562/mkk.2022.1.1
Ember, István (2022b): Hatásvizsgálati robbantás kumulatív töltetekkel. *Műszaki Katonai Közlöny,* 32(4), 13–23. Online: https://doi.org/10.32562/mkk.2022.3.2
Ember, István (2022c): Modern kumulatív töltetek hatékonyságának vizsgálata. *Haditechnika,* 56(6), 15–20. Online: https://doi.org/10.23713/HT.56.6.03
Ember, István (2022d): Célfeladatra készített kumulatív töltetek kialakításának vizsgálata. In Szelei, Ildikó (szerk.): *A hadtudomány aktuális kérdései 2022.* Budapest: Ludovika, 13–28.
Ember, István (2022e): 3D nyomtatott lyukasztó töltetek hatásvizsgálata. *Hadmérnök,* 17(4), 63–73. Online: https://doi.org/10.32567/hm.2022.4.5
Fazekas, Ferenc (2023): A küldetésorientált vezetés és a mesterséges intelligencia. *Hadtudományi Szemle,* 16(3), 95–109. Online: https://doi.org/10.32563/hsz.2023.3.8
Földi, László – Padányi, József (2022): Climate Change as a Challenge to the Armed Forces. *Sodboni Vojaski Izzivi/Contemporary Military Challenges,* 24(4), 37–48. Online: https://doi.org/10.33179/bsv.99.svi.11.cmc.24.4.2
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
Lukács, László (1992): *A kumulatív hatás és a kumulatív töltetek méretezése.* Jegyzet a Szárazföldi Haderőnemi Fakultás műszaki hallgatói számára. Magyar Honvédség, Zrínyi Miklós Katonai Akadémia, Műszaki tanszék.
Lukács, László (2017): *Szemelvények a magyar robbantástechnika fejlődéstörténetéből, Különös tekintettel a továbbfejlesztés várható irányaira és a kor új kihívásaira.* Budapest: Dialóg Campus.
Padányi, József (2023): Éghajlatváltozás, természeti katasztrófák, környezeti hatások, katonai képességek. *Hadtudomány,* 33(E-szám), 101–119. Online: https://ojs.mtak.hu/index.php/hadtudomany/article/view/12268/9925
Tóth, József Lukács – Vég, Róbert László (2022): Az autonóm terepjáró eszközök. *Műszaki Katonai Közlöny,* 32(2), 107–116. Online: https://doi.org/10.32562/mkk.2022.2.8

HADMÉRNÖK
HADITECHNIKA
19. évfolyam (2024) 3. szám 29–48.
DOI: 10.32567/hm.2024.3.3

István Vozsech[1]

Calculations of a Blowback System

Abstract

The paper deals with the description of the breech movement of free mass-locked weapons. The effects of the individual model elements and the limitations of the simplified computational procedures are presented using the simplest and the more complex concentrated parameter model. The computational results are compared with measurements on real weapons to determine the validity of the model. The applicability of the results of the model calculations to design problems will be evaluated.

Keywords: blowback operation weapons, automatic weapon

Introduction

An automatic or automatic weapon is a device which, by a single actuation of the firing button, can be fired continuously without interruption, i.e. in a series of shots. During a burst firing, all operational processes are automatic, except for the firing of the first round. The actuating energy is either derived directly from the energy of the propellant gases (gas-engine guns) or from the recoil impulse of the shot. One of the simplest realisations of the latter technical solution is the free mass-locking automatic.

Mass-locked weapons belong to the family of unlocked weapons. Although it may be misleading, there is a reason to call them mass-locked weapons. In a mass-locked (in older terminology, weight-locked) automatic weapon, the inertia of the bolt performs the quasi-locking action. If the mass of the bolt is sufficiently large that the gas pressure that triggers the firing, like the excitation acting on the case bottom, moves the case moving with the bolt only a short distance that the properly sized case can still bear and still provide a plug for the powder gases, then the weapon is locked with the bolt mass. So, a free mass lock is a simple mass, uninhibited in its rearward movement, which, because of its inertia, provides reduced rearward movement of the case.[2] This extremely simple technical solution is nowadays only used/applied

[1] Engineer, Gestamen Kutatás Fejlesztés Zrt., e-mail: vozsech.istvan@dianaszki.hu
[2] More precisely, only the force of the positioning spring and the friction forces prevented the lock from moving.

to machine guns, and in the past to submachine guns and machine guns with a lower specific power.[3]

Benefits of the system:

- the simplest and therefore most reliable weapon design
- requiring few components, therefore a low-cost technical solution
- the barrel is rigidly mounted, there is no gas engine, therefore the barrel deflections are negligibly small, and the theoretical dispersion of such weapons is thus also exceptionally low compared to other serial firing weapons

Disadvantages of the system:

- the high mass of the bolt
- considerable mass forces for larger calibres
- large practical variation due to the large variation in the centre of gravity of the weapon during firing
- requires a special, short and cylindrical cartridge case; firing a high-capacity (bottle-shaped) cartridge is generally not possible

The HK G3 self-loading rifle, developed from the MP45, is a uniquely designed weapon that fires a 7.62 × 51 NATO calibre, bottle-shaped cartridge. However, this rifle uses a chamber with longitudinal grooves, known as Rewelli channels, to loosen the case, so that the powder gases entering between the case cavity and the chamber partially relieve the case wall, thus reducing the tensile stress on the case cavity. In this weapon, a semi-rigid roller bolt also provides additional delay and thus reduces the load on the case. Figure 1 clearly shows the grooves on the fired cartridge case.

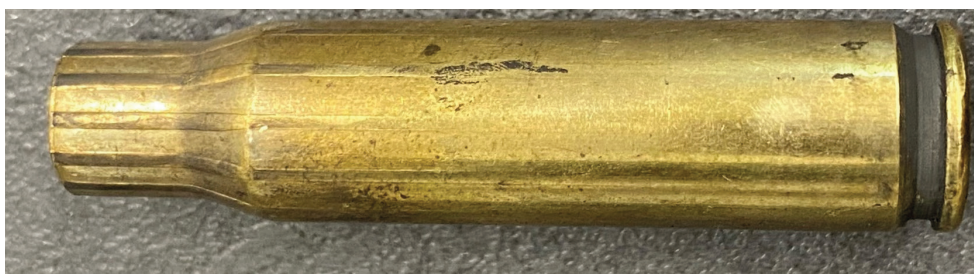


Figure 1: The fired case of the HK G3 automatic rifle
Source: photographed by the author

To examine the change in the state of motion of the bolt during the firing process, consider a schematic sketch of such a design around the chamber (see Figure 2).

[3] There are exceptions of course, see HK G3 automatic rifle.

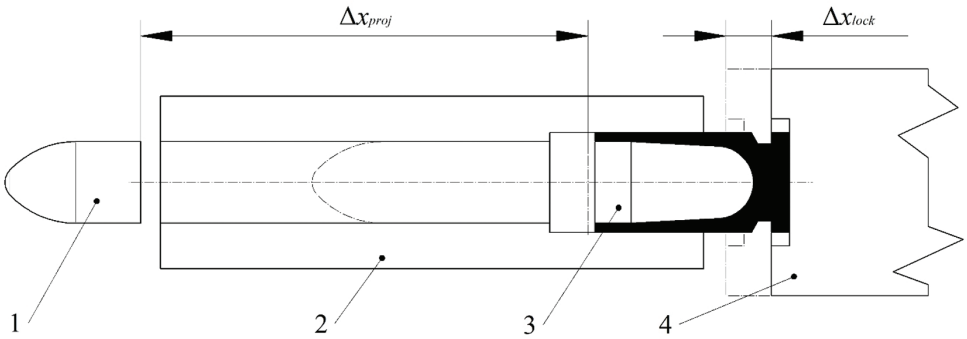


Figure 2: Characteristics of a free mass lock and the limits of exclusion (1) projectile, (2) stationary gun barrel, (3) cartridge case, (4) mass lock
Source: compiled by the author

It is also very important to note that from now on our discussions will be limited to weapons firing from the closed bolt position, i.e. the single degree of freedom models described in the following are not suitable for the discussion of automatic weapons with a firing system and fixed firing pin, which can only be dealt with effectively by means of considerably more complex multi-degree of freedom models.

The four most important components of the simplest five-element model of a free mass lock can be seen in Figure 2. These components are the breech (4), the case (3), the projectile (1) and the stationary case assembly (2), represented in the figure by the rigidly clamped gun barrel. The system element not shown is the positioning spring, which is negligible in the initial, excited phase of the recoil, as will be seen later. Interestingly, for the one more complex model, the number of system components is reduced because, given the gas pressure function, we do not need to know the projectile motion to calculate the motion of the bolt, with a small approximation.

Of course, it is also possible to describe very complicated, multi-degree-of-freedom models of the pendulum system, where the simultaneous volume-increasing effect of the ballistic gas pressure curve and the projectile motion should not be neglected, but we will not go into this in depth here.

The technical problem

The system has five components, of which up to four can be neglected, depending on the complexity of the model, but one can never be neglected, and that is the lock.

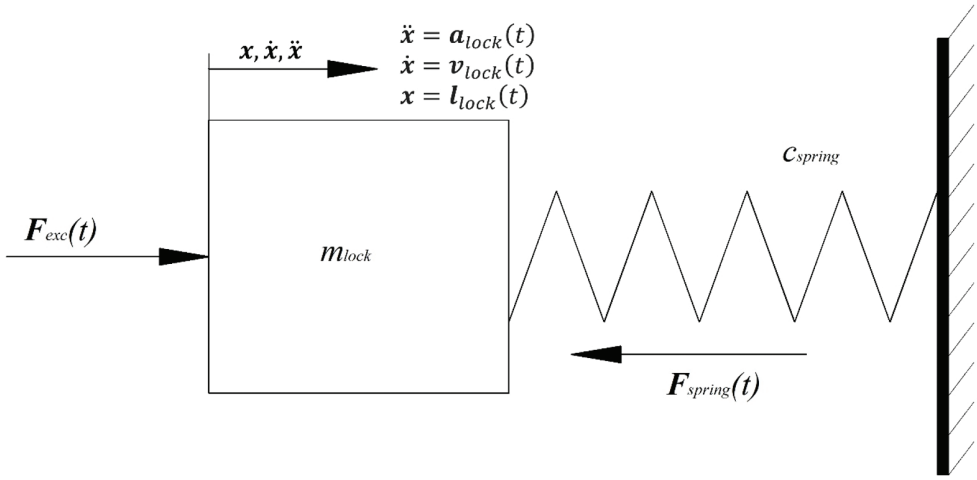


Figure 3: Dynamical model of a free mass lock as a single degree of freedom, undamped oscillating system
Source: compiled by the author

Figure 3 shows one simple model, where the free mass lock is assumed to be a single degree of freedom, undamped rocking system. If we mentally remove the spring and wall on the right side of the mass from the figure, we obtain the simplest possible model with only one system element, the lock. The equation of motion of this system is the basic equation of dynamics, which with these simplifications is a scalar equation:

$$F_{exc}(t) = \frac{d}{dt} I(t) = m_{lock} \frac{d}{dt} v_{lock}(t) = m_{lock} \frac{d^2}{dt^2} x_{lock}(t) \qquad (1)$$

where $I(t)$ is a function of the amount of lock movement.

Depending on the nature of the excitation function, this equation can be solved either analytically or numerically. The excitation function is given by the gas pressure

$$F_{exc}(t) = p(t) A_{barr} \qquad (2)$$

where A_{barr} is the cross-sectional area of the gun barrel and $p(t)$ is the time dependence of the gas pressure.

The instantaneous velocity of the lock can be determined using the force theorem:

$$A_{barr} \int_0^t p(\tau) d\tau = m_{lock} v_{lock}(t) \qquad (3)$$

at the moment when the gas pressure in the gun barrel equals the atmospheric pressure (t_5):

$$A_{barr} \int_0^{t_5} p(\tau) d\tau = m_{lock} v_{lock}(t_5) \tag{4}$$

Since the system, consisting of the projectile, the propellant gas and the bolt, is closed, its overall momentum is unchanged throughout the firing process. If the mass of the powder charge is neglected, and the equalisation of the muzzle pressure after the projectile is ejected (time t_4) is considered instantaneous, the absolute value of the projectile's momentum will be equal to the absolute value of the breech's momentum:

$$A_{barr} \int_0^{t_4} p(\tau) d\tau = m_{proj} v_{proj}(t_4) = m_{lock} v_{lock}(t_4) \tag{5}$$

We also know (because we have measured or calculated) that the projectile left the barrel at velocity v_0, and that our muzzle velocity[4] reaches its maximum at this point, so equation (5) takes the simple form:

$$m_{proj} v_0 = m_{lock} v_{lock\_max} \tag{6}$$

The maximum shutter speed can be a design parameter or a quantity to be calculated for an existing weapon, so equation (5) has to be ordered in two ways:

$$m_{lock} = m_{proj} \frac{v_0}{v_{lock\_max}} \tag{7}$$

$$v_{lock\_max} = \frac{m_{proj}}{m_{lock}} v_0 \tag{8}$$

From this simplest model (7) it is possible to determine the required lock weight, or to calculate the maximum lock speed for a given design (8). For a given calibre, the lock weight calculated in this way is approximately the same as the weight of locks in existing guns, but the lock speed obtained differs from the measured values, so after this brief analysis we will turn our investigations to an explanation of this empirical fact.

[4] In our current study, we neglect the gas path effects.

Objective and tasks

When designing a blowback weapon, we need to be able to determine from the calibre data the locking weight at which neither a case rupture nor a case break will occur. Knowing the lock weight, the breech speed, the recoil length and the expected rate of fire, we also need to calculate the recoil spring.

In order to provide an efficient method for determining the required closing mass and the equations of motion with as little simplification as possible, we need to build a model with sufficient depth but not too much complexity.

Our goal is to construct a dynamical model that is tractable at the engineering level for the most common blowback weapons firing from a closed bolt position. The calculations of the model should not require knowledge of internal ballistic processes and systems of equations, but should be able to calculate the response functions of the model using only digital data from internal ballistic gas pressure measurements.

Furthermore, our aim is to verify and validate the established model by means of a rapid-filming procedure for two different friction coefficients of the case-fill-space pairing, in the metal-clean and thinly silicon grease-coated states of the case-fill-space pairing.

The tasks to be carried out can be sequenced, as they are chronologically sequential:

1. identify the model elements to be used and assemble them in the correct order
2. write down the dynamic equation system of the model and solve it
3. take measurements and then determine the values of the free model parameters fitted to the measurement results

Literature used

Solutions to free mass-locked systems are (also) discussed by Peter Dannecker, whose schematic diagrams were a great help in preparing our own diagrams.

A more detailed discussion of the subject can be found in the work of V. M. Kirillov, where sample computational procedures supported by sample problems are available, but from the pre-digital computing era, based on models optimised for analogue computers.

For the solution of the vibration problems, we consulted the book of Gábor Csernák and Gábor Stépán, written with the mathematical formalism of the present day.[5] The model and its calculations describing the man-weapon system as a multi-freedom degree of freedom system can be found in Dziopa et al.,[6] where the authors do not discuss the internal oscillation system built from the components of the weapon in detail, but we aimed at describing it.

[5] Csernák–Stépán 2019.
[6] Dziopa et al. 2023.

The solutions of the systems of equations and the diagrams of the problem were obtained with the Maple symbolic mathematical editor, for the programming of which we used the work of André Heck.[7]

Model making

When building our model, we need to decide the very important question of how we want to generate our internal ballistic excitation function – the gas pressure function $p(t)$ – and we have two options. Either we generate it ourselves by solving the internal ballistics equations or we obtain it from measured data. At the design level, the former is not usually expected, but measurement data or simulation results from commercial ballistics software are always available to those who are more concerned with this. We will use the latter, in line with our objective.

When using an external data source, the gas pressure curve is given, so any system element that only affects it can be neglected or ignored. These are the gun barrel, the powder charge and the projectile. Our model is from now on purely mechanical, more precisely a concentrated parameter damped single degree of freedom swing system. This system needs to be further subdivided, because the backward and forward movement of the bolt are treated separately to account for the different conditions of forward and backward movement, but in this paper, we will only deal in detail with the backward movement of the bolt under the effect of firing. The vibration model of the backward motion oscillation system is shown in Figure 4.

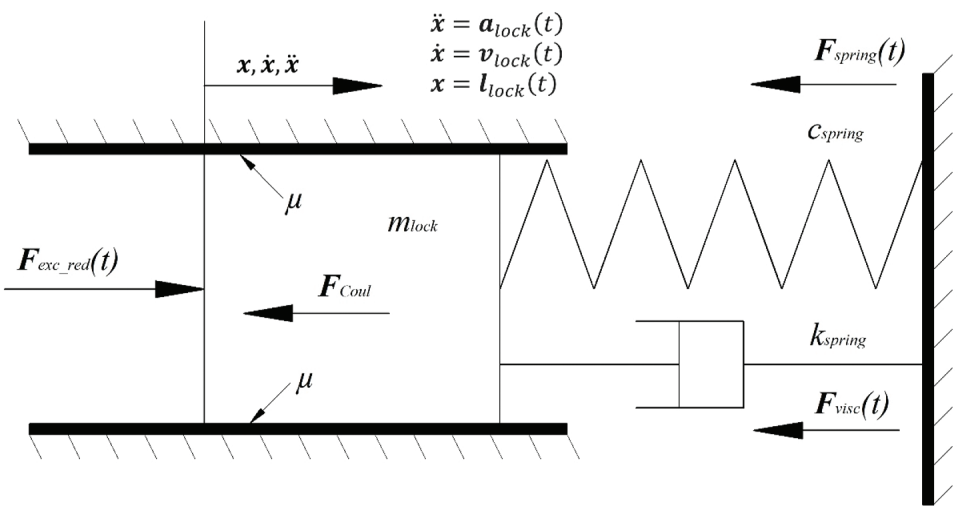


Figure 4: Dynamic model of the mass lock when the lock is moved backwards
Source: compiled by the author

[7] Heck 1999.

The main constraints and neglect of our swinging system:

- The positioning spring has linear characteristics and zero mass
- The friction force is constant (the external Coulomb friction coefficient is constant)
- The effect of the gravity field is neglected
- The viscous damping coefficient is constant
- The masonry is ideal, no displacement
- The lock is rigid

The forces acting on the mass lock and the equation of motion

The equation of motion of a constrained pendulum system with the notations in Figure 4:

$$F_{exc\_red}(t) = m_{lock}\ddot{x}(t) + \left(c_{spring}x(t) + F_1 + F_{Coul}\right) + m_{lock}k_{spring}\dot{x}(t) \qquad (9)$$

which, after naming the time derivatives and transforming them into first order equations, takes the following forms in our example:

$$\frac{d}{dt}v_{lock}(t) = \frac{F_{exc\_red}(t) - c_{spring}l_{lock}(t) - F_1 - F_{Coul}}{m_{lock}} - k_{spring}\frac{d}{dt}l_{lock}(t) \qquad (10)$$

$$\frac{d}{dt}l_{lock}(t) = v_{lock}(t) \qquad (11)$$

where:

$F_{exc\_red}(t)$ is the function of the reduced excitation force, unit N,
$v_{lock}(t)$ is the velocity function of the lock, unit $\frac{\mathrm{m}}{\mathrm{s}}$,
$l_{lock}(t)$ is the displacement function of the lock, unit m,
m_{lock} is the mass of the lock, unit: kg,
c_{spring} is the spring stiffness of the positioning spring, unit $\frac{\mathrm{N}}{\mathrm{n}}$,
F_1 is the preload of the positioning spring, unit N,
F_{Coul} is the Coulomb friction force, unit N ,
k_{spring} is the viscous damping coefficient of the positioning spring, unit $\frac{1}{\mathrm{s}}$.

It can be seen that after a reasonable choice of parameters and the determination of the reduced excitation force function, the problem can be solved both analytically and numerically. Without going into the specification of the parameters, let us define the reduced excitation force function, for which see Figure 5.

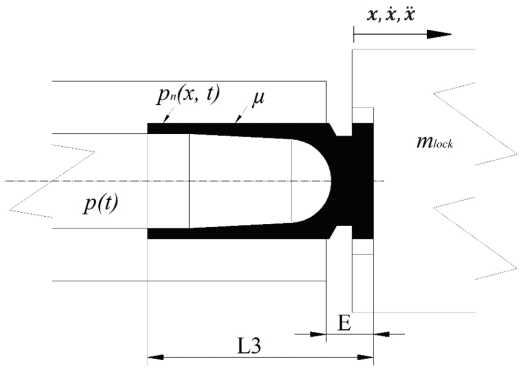


Figure 5: Bivariate surface pressure on the vaginal surface
Source: compiled by the author

The time-varying gas pressure generates a spatially varying surface pressure along the sleeve casing, from which the Coulomb friction force function on the casing can be calculated. The resulting surface pressure decreases steadily towards the bottom of the sleeve, i.e. the wall thickness of the sleeve increases steadily in this direction. The resulting bivariate surface pressure function can be calculated in principle (under equilibrium conditions), but for simplicity, let us use the approximation that in the deformable section $L_3 - E$ of the sleeve, both the thickness of the sleeve wall and the gap between the shell space and the sleeve casing are assumed to be zero. However, this latter simplification causes a problem. The model cannot take into account the fact that in reality the gunpowder gases can penetrate between the casing and the chamber, counteracting the effect of the gas pressure on the casing. This can be taken into account by varying the value of the friction coefficient and/or the length of the freely deformable casing section (as free model parameters) by fitting the simulation results to the measurement results. The pressure compressing the surfaces will then be independent of the location and equal to the gas pressure (Figure 6).

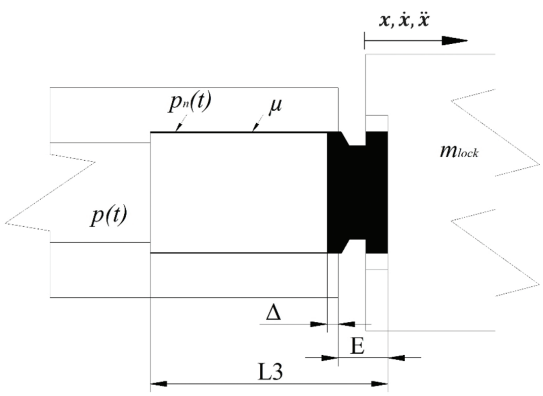


Figure 6: Univariate surface pressure on the vaginal surface
Source: compiled by the author

We know that the freely backward moving shutter is accelerated by the gas pressure through the bottom of the sleeve, so it is necessary that the function of the shutter travel is the same as the function of the displacement of the sleeve as long as the sleeve is directly exposed to the gas pressure. From this consideration, the current contact casing surface can be defined.

At the start of the shot, the contact surface area of the casing:

$$A_{surf\_0} = (L_3 - E - \Delta) d_{case} \pi \tag{12}$$

where d_{case} is the outer diameter of the sleeve, measured in m.

This is the current contact surface area of the casing:

$$A_{surf}(t) = \begin{cases} A_{surf\_0} & t < t_\Delta \\ A_{surf\_0} - l_{lock}(t) d_{case} \pi & t \geq t_\Delta \; and \; t \leq t_{L3} \\ 0 & otherwise \end{cases} \tag{13}$$

where t_Δ is the time instant associated with the condition $l_{lock}(t) = \Delta$ and t_{L3} is the time instant associated with the condition $l_{lock}(t) = L_3 - E$, unit s.

Knowing the contact slab surface function, we can write the friction force function on the slab:

$$F_{Coul\_surf}(t) = p(t) A_{surf}(t) \mu \tag{14}$$

where μ is the coefficient of sliding friction between the case and the chamber, measured in units.

From these, the complex force function that excites our vibration system:

$$F_{exc\_red}(t) = p(t) A_{case\_int} - F_{Coul\_surf}(t) \tag{15}$$

where A_{case_int} is the area of the cross-section defined by the projectile diameter in m^2.

Now that we have all the necessary parameters and functions, our problem is solvable.

Measurement results for 9 × 19 mm NATO calibre

The measurements were carried out in the ballistics laboratory of the Civilian Small Arms and Ammunition Testing Ltd. Our measurements can be divided into two parts, an internal ballistic gas pressure measurement combined with an initial velocity measurement and a rapid filming of the breech movement of a CZ EVO submachine gun. Both the recorded gas pressure data and the rapid film recordings were processed using proprietary software. The gas pressure and projectile velocity measurements provided the basic characteristics of the ammunition used, as well as the exact value of the excitation function for the swing system. The gas pressure measurement of the ammunition used and the initial velocity measurement, carried out simultaneously with the gas pressure measurement, were performed using a NATO AEP-97 standard measuring tube, which is essentially identical to the CZ EVO tube from a ballistic point of view.

We were not able to prepare the weapon in the usual way for the production of the short films, so we only made reversible modifications to the weapon. As the breech mechanism of the gun is only visible in the opening of the ejector window, the full range of breech movement cannot be recorded, only the approximate first 35 mm of the movement. This can be filmed during both forward and backward movement, but for our task the forward movement is irrelevant and the first 12 mm of movement is sufficient to simulate the excitation that occurs. The right thumb release port of the gun and the observed edge are shown in Figure 7.

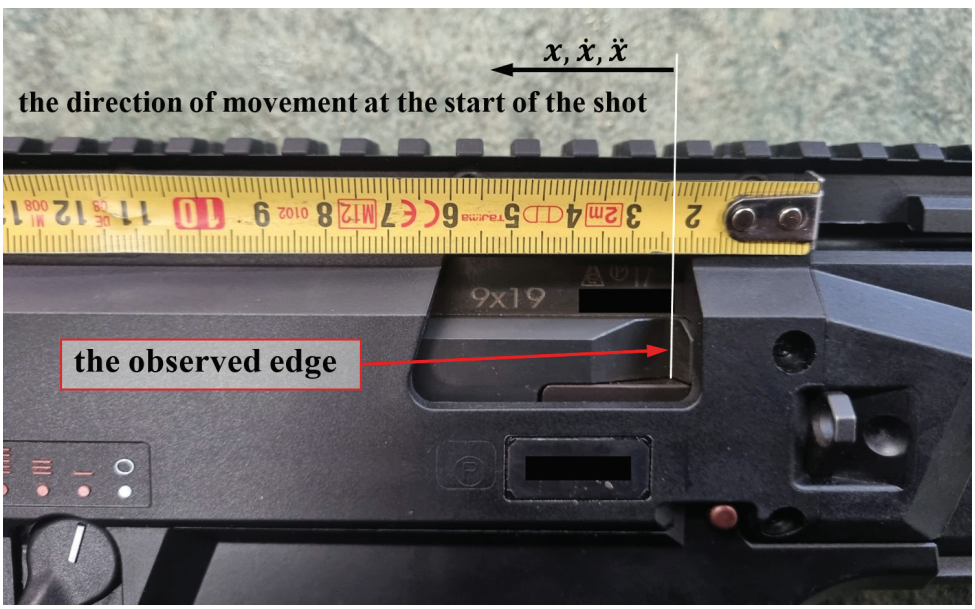


Figure 7: Right side view of the unprepared CZ EVO submachine gun included in the study, with the ejection port in focus
Source: photographed by the author

From digitally recorded short film files, digital frames of video can also be extracted as image files. The image files were processed using a proprietary analysis algorithm written in the symbolic math program Maple. Figure 8 shows the 45th control frame generated by the program for a shot taken with a degreased (dry) shell casing and shell casing pair.

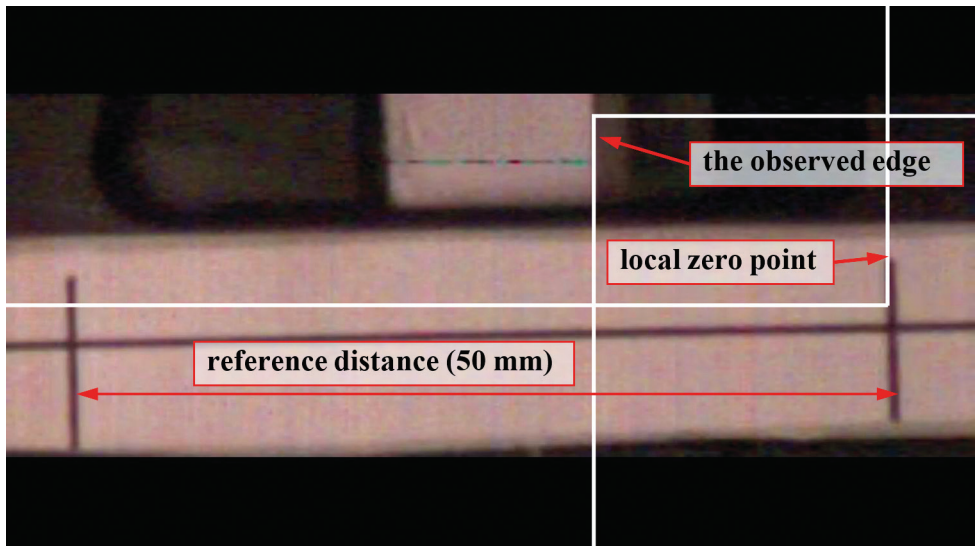


Figure 8: Control frame 45 of the dry firing on the prepared gun
Source: compiled by the author

The result of the gas pressure measurement and the fitted function are illustrated in Figure 9. (The left side of Figure 9 shows the gas pressure measurement report diagram, the right side shows the fitted spline function.)

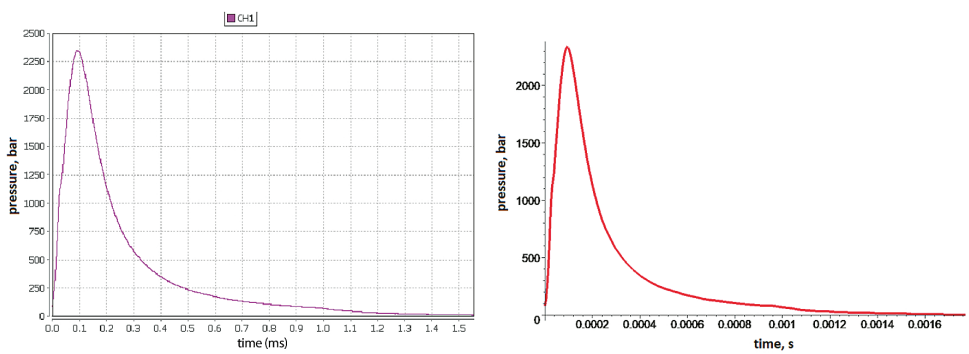


Figure 9: Univariate surface pressure on the vaginal surface
Source: compiled by the author

High-speed filming was performed at 32,667 fps or 320 × 120 resolution, which was already relatively usable and provided a sufficient number of frames for motion analysis.[8] However, although a telephoto lens was used to film the motion, the horizontal resolution for observing the initial (1-2 mm) phase of the motion is only acceptable with compromises, as the excessive pixel sizes result in a relatively high uncertainty of the readout compared to the relative displacement at that time instant. For more accurate studies of the excitation phase, a camera with a minimum vertical resolution of 1,280 pixels at 50,000 fps is required.[9]

These fluctuations due to increased reading uncertainty had to be filtered out, since with high-speed filming we are recording the instantaneous position of the shutter, which is significantly burdened by reading uncertainty. The numerical derivation of noisy displacement-time value pairs without filtering can already render the velocity-time values almost unusable, but this is even more true for the second derivative acceleration, since the derivation operator amplifies errors due to the fluctuations.

The displacement-time point pairs recorded by filming were filtered twice, taking care to minimise data loss. The best results were obtained using the moving average filter (first filter) and the logarithmic filter (second filter). The maximum velocity value was obtained from the analytical function obtained by regressing the filtered measurement points, which were loaded by the longitudinal oscillation of the spring-lock system. The unsmoothed discrete velocity function is shown in Figure 11 by the black diagram similar to the black sawtooth signal, and the filtered measurement points by the blue diagram, which was approximated by a similar analytical function, now detached from its actual physical content.

It is useful to plot the regression objective function on the shutter speed because it is easier to visually judge the "goodness" of the regression than for directly measured displacement-time pairs.[10] The nature of the graph given by the velocity-time point pairs is similar to that of an exponential function describing a single-loop system.[11] This function still needs to be corrected by the method of least squares to change the strict monotonic increase in the function to a strict monotonic decrease after the maximum shutter speed is reached. A polynomial of degree one is the most appropriate for this purpose, based on the runs, and this gives the best fit. This gives a parametric function approximating the shutter speed-time value pairs:[12]

[8] The video recordings were made with a CHRONOS colour high-speed camera, type CH14-1.0-C.

[9] The vertical resolution (perpendicular to the direction of motion) was measured to be 320-pixel columns, resulting in a scaling factor of 0,179 $\frac{\text{mm}}{\text{pixel}}$ for a reference distance of 50 mm. This discretisation imposed a measurement uncertainty of $\pm$ 0,0895 mm on all displacement values of our measurements (analogous to the measurement uncertainty component due to the finite resolution of digital instruments).

[10] When evaluating the measurements, the moving average filter window size was 20 measurement points, and the logarithmic filtering parameter was 0.2.

[11] This can be observed in the blue graph in Figure 11 as a periodic variation in velocity.

[12] Although our function $v_{reg}(t)$ is difficult to integrate analytically, the differential equations are solved numerically, so analytical integrability is not a consideration here.
You can also choose a higher order polynomial as the regression function, in which case integrability is ensured, but pure regression algorithms cannot be used because of the bias in the initial and final values. In this case, the initial and final values are either bound as interpolation points, or the set of regression point pairs is extended by extrapolation to define virtual measurement points.

$$v_{reg}(t) = b_0 v_{max} \cdot \mathrm{e}^{-\frac{1}{c_0 + c_1 t} \cdot (a_0 + a_1 t)} \tag{16}$$

where:

b_0 is the multiplier for the asymptotic shutter speed, there is no unit of measurement,

v_{max} is the maximum closing velocity averaged over the maximum velocity values, unit $\frac{\mathrm{m}}{\mathrm{s}}$,

c_0, c_1 are the parameters of the single storage system fitted to the measurement points, units: none, $\frac{1}{\mathrm{s}}$,

a_0, a_1 are the parameters of the first degree polynomial determined by the method of least squares, units: none, $\frac{1}{\mathrm{s}}$.

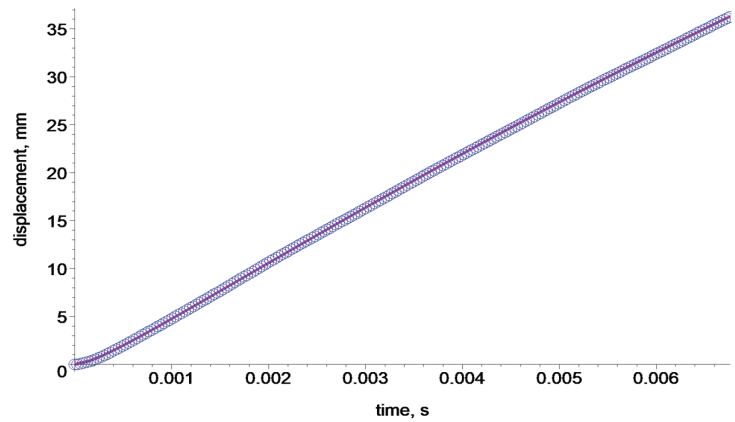


Figure 10: Shutter positions obtained by processing frames from a shot fired in the dry state (circles on the diagram), using the integral function of the regression function

Source: compiled by the author

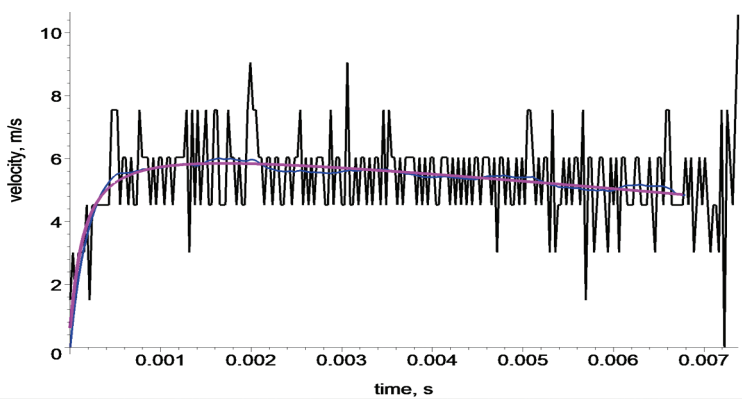


Figure 11: Shutter speed calculated numerically from the frames, from a shot fired in dry conditions

Note: The black noisy velocity is the unfiltered velocity, the blue smoother is the velocity produced from the filtered data, the purple is a regression analytical approximation.

Source: compiled by the author

Calculation results for 9 × 19 mm NATO calibre

Let's look at the results of running the above model for a machine gun firing 9 × 19 mm NATO ammunition, where the main model parameters are as follows:

Table 1: Main parameters of the simulation with projectile data

Name	Value	Unit of measurement
lock road	75	mm
the mass of the lock	600	g
spring force, lock in forward position	25	N
spring force, lock in rear position	60	N
viscous damping factor	2	1/s
friction force of the lock	5	N
dome-steel coefficient of friction (literature value)	0.120	unit
dome-steel coefficient of friction in dry condition (fitted parameter)	0.049	unit
dome-steel coefficient of friction in the greased condition (fitted parameter)	0.010	unit
length of the deformable sheath of the case	10	mm
outer diameter of the case	10	mm

Source: compiled by the author

The excitation gas pressure curve was obtained by interpolation of the measured data, the first order interpolation spline curve is illustrated in Figure 9, Figure 12, Figure 13 and Figure 14 show the response function plots obtained. In the figures, the excitation phase – when the gas pressure in front of the sleeve is not zero – is uniformly marked in red, the greenish yellow is the sleeve still in the charge space but not under gas pressure, the blue is the damped backward displacement and the black is the forward displacement of the lock.

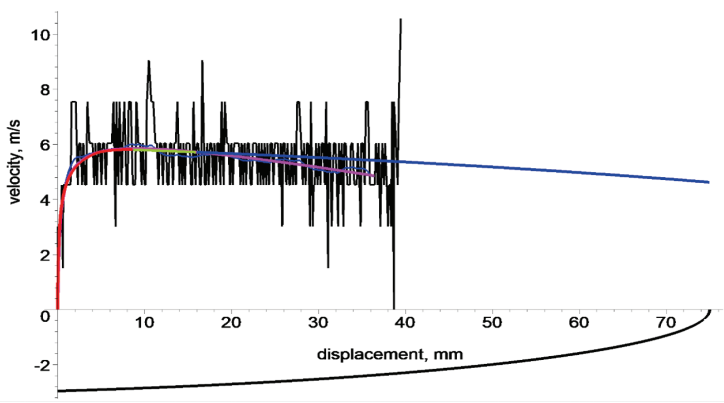


Figure 12: Closing velocity – closing displacement function from dry fired shots, with values from Table 1 and calculated closing velocity from measurement, and regressed closing velocity

Source: compiled by the author

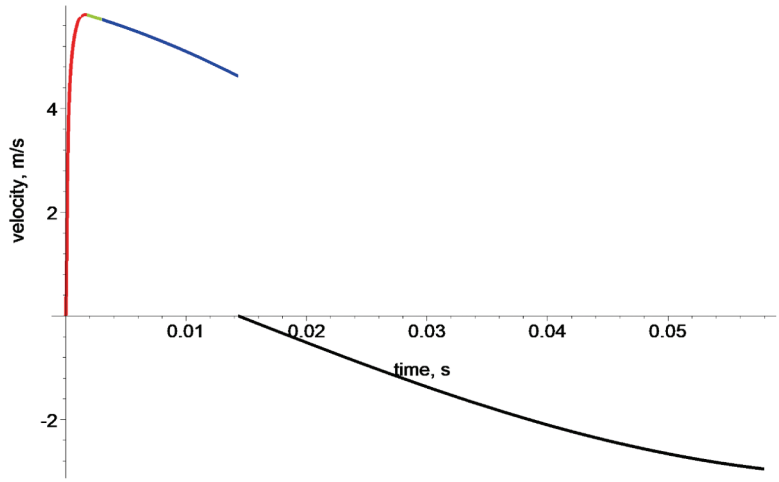


Figure 13: Closing velocity-time function from a shot fired in the dry state, with the values shown in Table 1
Source: compiled by the author

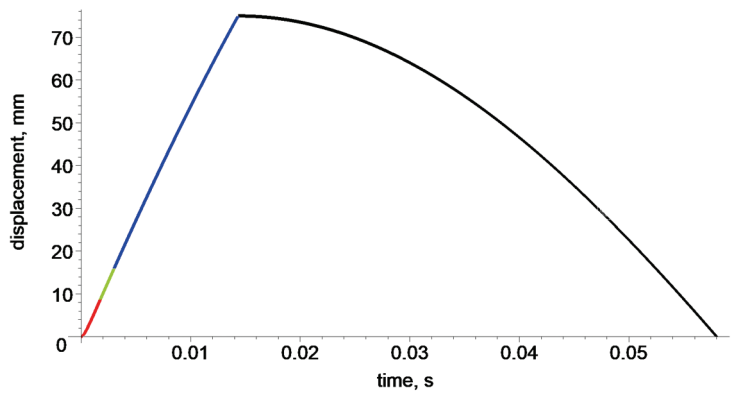


Figure 14: Closing displacement-time function from a shot fired in the dry state, with the values shown in Table 1
Source: compiled by the author

It can be seen that with the given parameters, the simulation is a good approximation of reality, the automatics work, there is locking energy for the impact.

Let's now look at the case where friction is strongly reduced by thin lubrication of the case and chamber. Now the calculated shutter speeds and regression from the measurement are illustrated in Figure 15.

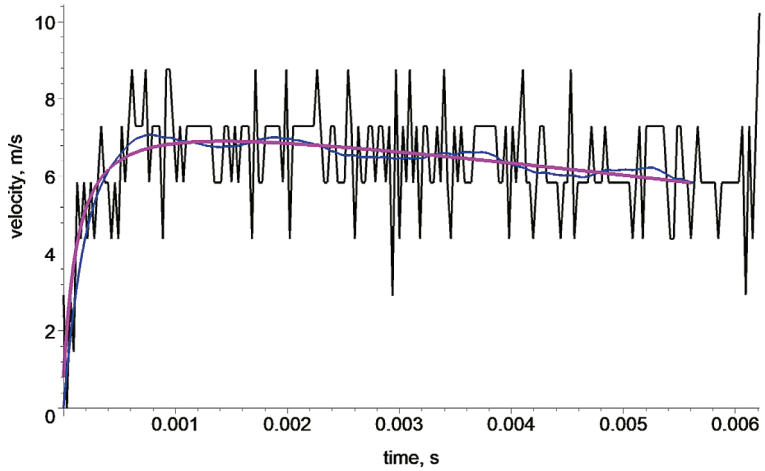


Figure 15: Numerically calculated shutter speed from frames, fired in a greased condition

Note: The black noisy velocity is the unfiltered velocity, the blue smoother is the velocity produced from the filtered data, the purple is a regression analytical approximation.

Source: compiled by the author

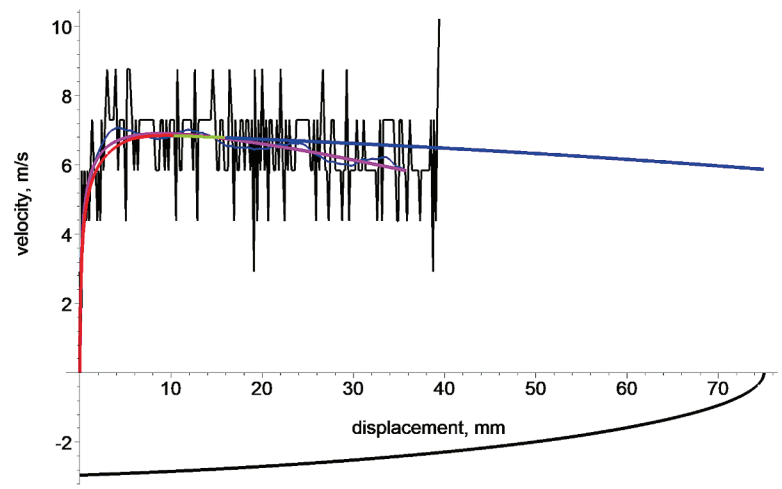


Figure 16: Closing velocity-closure displacement function in the greased state

Source: compiled by the author

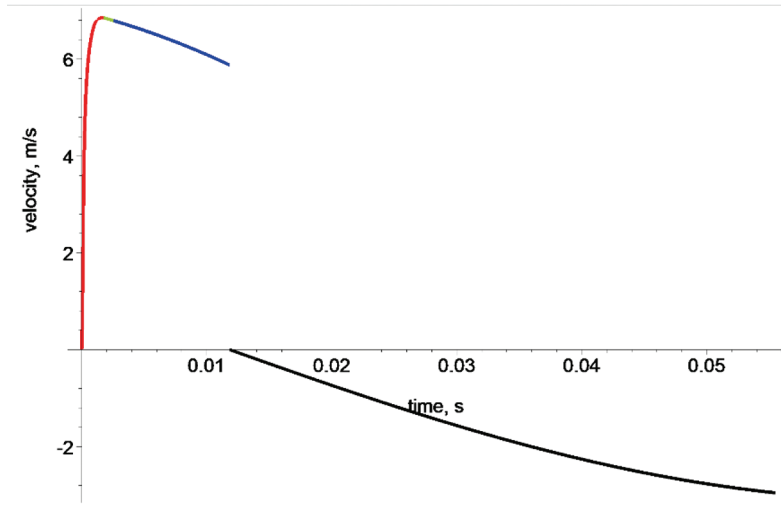


Figure 17: Closing speed-time function in the greased state
Source: compiled by the author

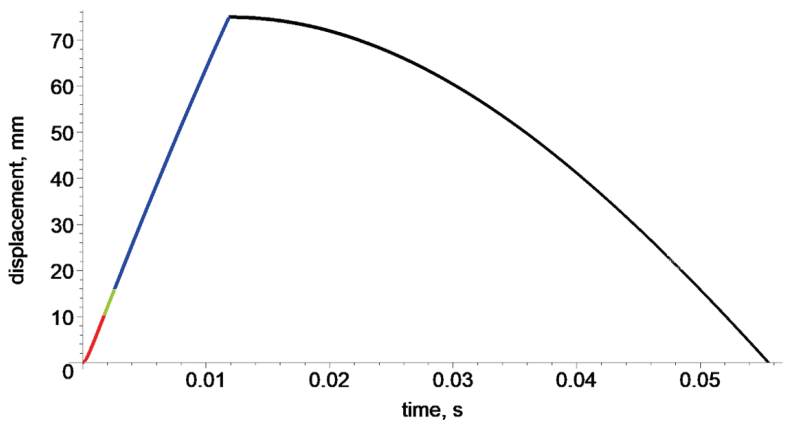


Figure 18: Closed-motion-time function in the greased state
Source: compiled by the author

Now we can also conclude that the simulation is a good approximation of reality with the given parameters, and the simulated shutter speed can be exactly matched to the one calculated from the measurement results.

Let us consider the case where we do not take into account the sleeve-loosening effect of the gases flowing between the casing and the chamber. In this case the friction coefficient can be determined from the literature. Figure 16 illustrates the simulation of the closure displacement-closure velocity function. It can be clearly seen that the results obtained are far from reality.

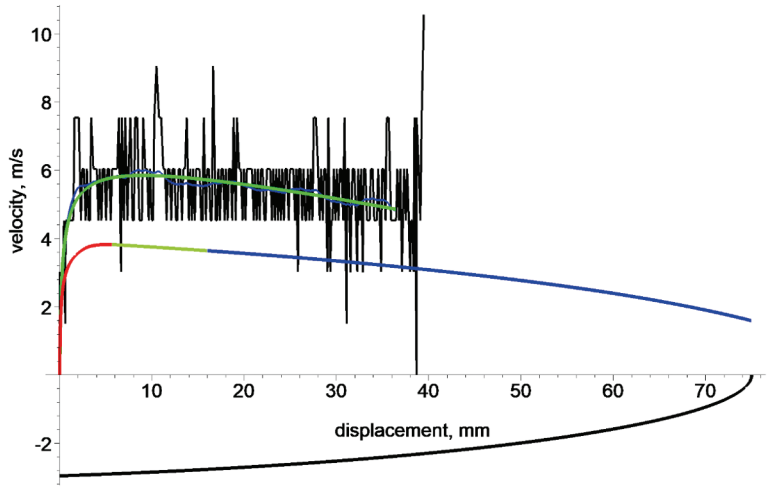


Figure 19: Closing velocity-closing displacement function with the literature friction coefficient values according to Table 1 and the closing velocity calculated from the measurement, as well as the regressed closing velocity

Source: compiled by the author

Remarkably, this seemingly insignificant neglect[13] means that our calculations will have little to do with the movements that occur in reality. It should be seen that by treating the walls of the sheath as a membrane of zero thickness and by excluding the inflow of gases between the surfaces, we have made a significant simplification which, although it would save costly and time-consuming measurements, is not allowed by the validity of the model. Although the membrane approximation of the sleeve wall can be solved, the excitation function in our equation (9) is now bivariate and our equation is transformed into an integro-differential equation, but we still cannot deal with the relaxing effect of the inflowing gases with this model. It is also important to see that, for free mass-locked systems, the design, quality and sliding characteristics of the sleeve and the friction surfaces are very sensitive, which cannot be taken into account at all by the simpler models.

Summary

- The mass locks (by design) are not capable of arbitrarily high backward velocities,[14] which limits their rate of fire and makes them susceptible to filling-discharge problems.

[13] With which we can "save" on measurements.

[14] In the case of machine guns, even 1,000 rpm a rate of fire can be achieved that is considered high, but note that this is only due to the short recoil distance resulting from the relatively short case length.

- The design of weapons with this system should always be based on models that can at least take into account the effects of friction. Their free model parameters should be fitted to the results of measurements carried out at least on an existing weapon, but preferably on a technological demonstrator, in order to achieve the lowest possible simulation error.
- The quality of the cartridge case used is of paramount importance, both in terms of the raw material and the surface quality.
- The ammunition and cartridge cases of free-floating weapons must not be altered from their factory condition, i.e. neither oiled, nor polished, nor "tuned" by any efficiency-enhancing process, because the case-cartridge pair is the most critical point of this system.
- The manufacturers minimise the sealing weight, therefore any gun barrel that does not have a factory silencer connection is an accident hazard to retrofit a silencer to that gun due to its gas retention effect. The consequence of such retrofitting is a drastic increase in gas backflow.
- In particular, the use of reloaded ammunition (once or more than once reshaped cartridge case) for this type of weapon is contraindicated because it increases the risk of case rupture, which is an increased risk of accident.

References

Csernák, Gábor – Stépán, Gábor (2019): *Rezgéstan.* Budapest: Akadémiai Kiadó. Online: https://doi.org/10.1556/9789634544739

Dannecker, Peter (1992): *Verschlußsysteme von Feuerwaffen.* Schwäbisch Hall: Journal Verlag Schwend GmbH.

Dziopa, Z. J. – Lenarcik, A. – Zdeb, K. (2023): Modelling and Testing the Dynamic Properties in a Submachine Gun-Man System. *Problems of Mechatronics Armament, Aviation, Safety Engineering,* 14(3), 25–40. Online: https://doi.org/10.5604/01.3001.0053.8818

Heck, André (1999): *Bevezetés a Maple használatába.* Szeged: Juhász Gyula Felsőoktatási Kiadó.

Kirillov, V. M. (1973): *Teorija i raszcset avtomaticseszkovo oruzsija.* Penza: PVAIU.

HADMÉRNÖK
KATONAI LOGISZTIKA ÉS KÖZLEKEDÉS

19. évfolyam (2024) 3. szám 49–66.
DOI: 10.32567/hm.2024.3.4

Ardai István Tamás[1] – Tóth Bence[2]

A Magyar Honvédség szállítási képességeinek elemzése villamosítatlan vasútvonalakon

The Transportation Capabilities of the Hungarian Army using Unelectrified Railway Lines

Absztrakt

A Magyar Honvédség saját célú vasúti pályái mind villamosítatlanok. Emiatt a dízelvontatás alkalmazása elkerülhetetlen, miközben a nemzetközi trend a vasútvonalak villamosítása annak környezetbarát volta miatt. Ugyanakkor különleges jogrendi helyzetben fel kell készülni a villamos vontatás zavarára is megfelelő mennyiségű és képességű dízelmozdony fenntartásával. Cikkünkben megvizsgáljuk a hálózat átbocsátóképességének növekedését, ha a villamosított vonalak mellett a villamosítatlanokat is figyelembe vesszük. Továbbá meghatározzuk a Magyar Honvédség (MH) maximális szállítási kapacitását, és javaslatot teszünk a kapacitás növelésének módjaira.

Kulcsszavak: vasúthálózat, gráfelmélet, átbocsátóképesség, kapacitás, Magyar Honvédség, villamosítás

Abstract

The railway sidings owned by the Hungarian Army are not electrified. This makes the use of diesel engines unavoidable while the international trend is to electrify as many lines as possible due to its environment friendly nature. However, in the case of an emergency situation one must be prepared for the disruption of the power supply by maintaining

[1] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, e-mail: aistvan26@gmail.com
[2] Nemzeti Közszolgálati Egyetem, e-mail: toth.bence@uni-nke.hu

enough diesel locomotives. In this paper, the increase in the capacity of the railway network of Hungary is determined if not only the electrified but also the unelectrified lines are taken into account. Furthermore, the maximal transportation capacity of the Hungarian Army is determined suggestions are made to improve it.

Keywords: railway network; graph theory; flow; capacity; Hungarian Army; electrification

Bevezetés

Napjainkban a katonai logisztikai műveleteket egyre nagyobb mértékben a polgári infastruktúra- és szállítóeszköz-állományra hagyatkozva tervezik. Ez igaz az olyan létfontosságú rendszerelemekre is, mint a vasúti közlekedési hálózat és az azon közlekedő gördülőállomány.[3] A polgári vasúti szállítás pedig egyre inkább áttér a villamos vontatásra, amely olcsóbb, mint a dízelvontatás és emellett környezetbarátabb is annál. Az egyes országok vasúthálózatának fejlettségét éppen ezért annak villamosítottsági arányával is szokás jellemezni. Ez az érték Magyarország esetében 40,8%, amivel tizenhatodikok vagyunk az EU-n belül. A mutató a legalacsonyabb Írország esetén (2,6%), míg a kontinensen Svájc esetében a legmagasabb (99,8%).[4] Ugyanakkor a védelmi szempontok meghatározásakor az egyes alrendszerek sérülésével is számolni kell, ami a vasúti közlekedésben a villanymozdonyok megfelelő dízelmeghajtású helyettesíthetőségének biztosítását jelenti.

A Magyar Honvédség (MH) rendelkezik 12 iparvágánnyal, úgynevezett saját célú vasúti pályával (scvp) [277/2014. (XI. 14.) Korm. rendelet], amelyek mind villamosítatlanok, ezért az ezen iparvágányokat érintő szállításoknál elkerülhetetlen a dízel vontatójárművek alkalmazása.

A magyarországi vasúthálózat jelentősebb vonalai (többnyire) villamosítottak,[5] és a villamos vontatás lényegesen olcsóbb is, mint a dízel, ezért a használható dízelmozdonyok száma a vasútvillamosítás előrehaladtával csökken.[6] Az előzőek alapján azonban honvédelmi érdek legalább annyinak a rendszerben tartása, amennyivel a szükséges szállítások a felsővezeték-hálózat nélkül is elvégezhetők lennének.

Cikkünkben megvizsgáljuk a magyarországi vasúthálózat átbocsátóképességét a határátmenetek között arra az esetre, amikor csak a villamosított vonalakat vesszük figyelembe, valamint meghatározzuk a kapacitásnövekményt, ha a villamosítatlan vonalakat is használhatjuk. Meghatározzuk továbbá az MH scvp-k között lebonyolítható maximális forgalmat különböző forgatókönyvek esetén. Célunk annak feltárása egy matematikai modell alapján, hogy mi(k) a vasúti közlekedési rendszer szűk keresztmetszete(i): a pálya és/vagy a gördülőállomány és/vagy a humán erőforrás (rakodási kapacitás)? Szem előtt kell tartani ugyanakkor, hogy a katonai szállítási feladatok végrehajtása során ezen elemzési eljárások sok esetben csak a speciális honvédelmi igények figyelembevétele mellett, azok integrálásával alkalmazhatók.

[3] Szászi 2013a.
[4] Eurostat 2024a; Eurostat 2024b.
[5] Tóth 2018.
[6] Szászi 2013b.

A magyarországi vasúthálózat térköz szintű gráfmodellje

A számítások elvégzéséhez egy súlyozott irányított gráfot használtunk. A modellt egy korábbi publikációban részletesen bemutattuk,[7] ezért itt csak a megértéshez elengedhetetlenül szükséges részletességgel ismertetjük azt.

Jelzők és vágánykapcsolataik

A hálózati modell 5188 gráfcsúcsot tartalmazott, amelyekből 1491 csúcs állomási kijárati jelzőt, 1687 csúcs bejárati jelzőt, 1896 csúcs térközjelzőt, 114 csúcs pedig egyéb vágánykapcsolati pontot (például határátmenet, iparvágány) reprezentált.

A fenti gráfpontok közti vágánykapcsolatokat 6803 gráfbeli éllel írtuk le. Két jelző között a menetidőt az egyes csúcsok valós fizikai távolságából és a köztük lévő vasúti pályára engedélyezett sebességből számítottuk ki. Ezen adatok nagyrészt nyilvánosan elérhetőek a VPE Kft. weblapján;[8] az itt nem szereplő iparvágányok hosszadatait a vonatkozó kormányrendelet [277/2014. (XI. 14.) Korm. rendelet] alapján, illetve saját távolságmérés alapján[9] építettük be a modellbe.

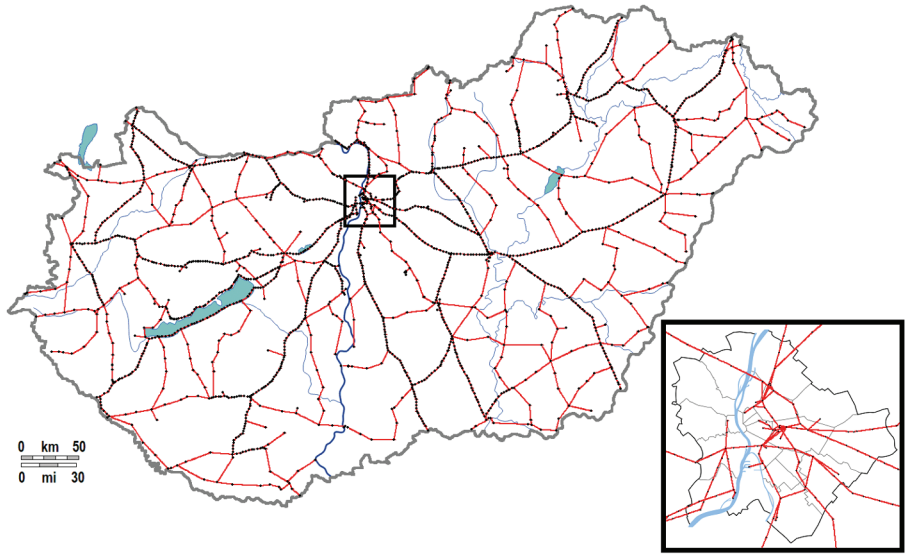
Ezen távolság- és menetidőértékeket rendeltük hozzá az egyes vasútvonalszakaszokat reprezentáló gráfbeli élekhez mint súlyokat (természetesen egy számításnál egyszerre csak az egyiket). Ebből következően a menetvonalak számított hosszai néhány méteres pontossággal megegyeznek a valós értékekkel. A számított menetidőértékek ugyanakkor a valós értékeknek egy abszolút alsó korlátját jelentik, mivel például a pálya állapotából fakadóan kitűzött lassújeleket nem építettük be a modellbe. Ahol kisebb engedélyezettsebesség-érték vonatkozott a nagyobb tengelyterhelésű vagy a mozdonnyal továbbított szerelvényekre, ott ezt az alacsonyabb sebességértéket vettük alapul a számításokhoz.

Állomások

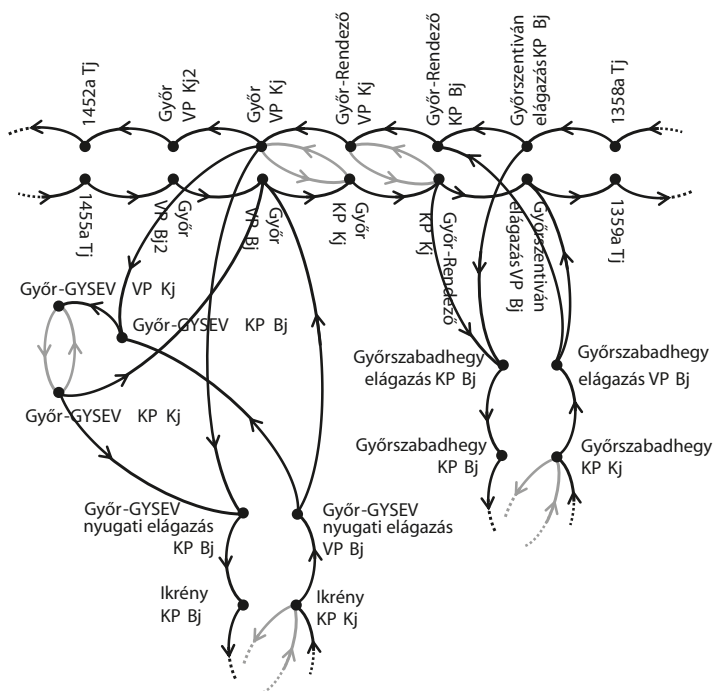
Egy állomás területét a végein található bejárati jelzők definiálják.[10] Egy szerelvény azonban nem bejárati jelzőtől bejárati jelzőig közlekedik, hanem azon túl, de legfeljebb a megfelelő kijárati jelzőig. Ezért az egyes menetvonalakat minden esetben a kiinduló- és a célállomás megfelelő kijárati jelzői között értelmeztük. A menetirányváltást is csak az arra alkalmas állomásokon (a modellben 710 ilyen szerepel) tettük lehetővé. Ilyen esetekben a menetvonalak hosszát nem növeltük meg irányváltáskor, de menetidő-számításnál minden egyes irányváltás esetén 10 percet hozzáadtunk a menetidőhöz, mivel ez a megállástól a menesztésig terjedő időtartamnak egy alsó korlátja.

A teljes hálózat diagramja az 1. ábrán látható Magyarország térképére vetítve. A gráf felépítésének elvét Győr állomás és környékének diagramján szemléltetjük (2. ábra).

[7] Tóth 2023.
[8] VPE 2023, 2024.
[9] Google 2024.
[10] MÁV 2018: 21.



1. ábra: A magyarországi vasúthálózat gráfjának diagramja
Forrás: Tóth 2023

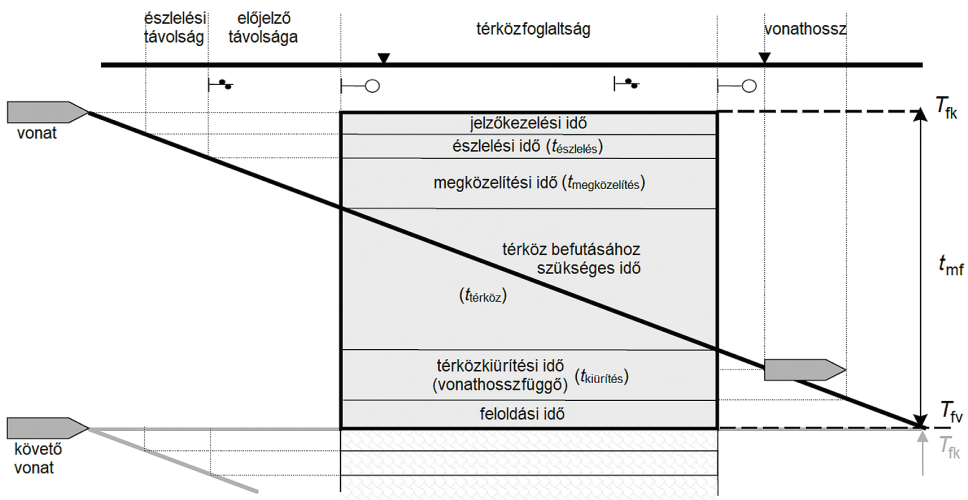


2. ábra: Győr állomást és környékét leíró részgráf diagramja
Forrás: Tóth 2023

Követési időköz

Állomásközi követés esetén a követő vonat csak akkor indulhat el az állomásról (azaz annak megfelelő irányú kijárati jelzője akkor állítható szabad állásba, és a vonat akkor haladhatja azt meg), ha a megelőző vonat teljes hosszában meghaladta a következő állomás bejárati jelzőjét. Annak a feltétele azonban, hogy minden vonat maximális sebességgel közlekedjen, különösen térközi közlekedésre berendezett pályán, ennél összetettebb.

Tegyük fel, hogy a térközjelzők távolsága nagyobb, mint az általános fékúttávolság. Ekkor a követő vonat akkor tud végig a megengedett maximális sebességgel közlekedni, ha (önműködő térközjelzőkkel felszerelt pálya esetén) akkor érkezik a következő térközjelző észlelési pontjához, amikor az éppen zöldre vált. Ez azt is jelenti, hogy az ezt követő térközjelző pont ekkor vált vörösről sárgára, azaz a megelőző vonat ekkor haladt ki az ezen jelző által fedezett térközből.[11] Ezek alapján az adott térköz úgynevezett mértékadó foglaltsági ideje (t_{mf}) a következőképpen számítható (3. ábra).[12]



3. ábra: A követési távolság meghatározása
Forrás: UIC 2013; Lévai 2022

A mértékadó foglaltsági idő (tmf) a foglaltsági idő kezdete (T_{fk}) és a foglaltsági idő vége (T_{fv}) közötti időtartam. A foglaltsági idő az a teljes idő, amely ahhoz szükséges, hogy egy vonat áthaladjon a térközön, amely a következő időket tartalmazza:

- biztonsági tartalék, amely az az idő, ami alatt a vonat fizikailag belép a térközbe. Ennek része a jelzőkezelési idő, az észlelési idő ($t_{észlelés}$) és a megközelítési szakasz befutásához szükséges idő ($t_{megközelítés}$); helyből induló vonatnál ez az érték 0. A jelzőkezelési időt a számításokban zérusnak vettük;

[11] MÁV 2023a: 36.
[12] UIC 2013; Lévai 2022.

- az az idő, amíg a vonat eleje áthalad a térközön: a foglalt térköz befutási ideje ($t_{\text{térköz}}$);
- a térköz kiürítéséhez szükséges idő, ami a vonat kihaladásához és a biztonsági szakasz befutásához kellő idő ($t_{\text{kiürítés}}$);
- a jelzők kezeléséhez szükséges idő, hogy a következő vonat behaladhasson a térközbe. Ez önműködő térközjelzők esetében szintén zérus, ezért a számításokban az egyszerűség kedvéért ezt az értéket is nullának vettük.

Ezekből a mértékadó foglaltsági idő:

$$t_{\text{mf}} = t_{\text{észlelés}} + t_{\text{megközelítés}} + t_{\text{térköz}} + t_{\text{kiürítés}} \tag{1}$$

Az észlelési távolság a MÁV F.1. sz. jelzési utasítása alapján határozható meg: „a főjelzőket úgy kell elhelyezni, hogy jelzéseik a mozdonyról, vezérlőkocsiról folyamatosan láthatók legyenek a vasúti pályára engedélyezett, km/h-ban kifejezett sebesség tízszeresének 1/3 részével egyenlő, méterben mért távolságból, de legalább 200 m-től."[13]

A kapacitáskihasználtság a vonatkozó UIC-döntvény[14] alapján az alábbi módon számítható:

$$K_{\text{k}} = \frac{t_f \cdot (1 + t_p)}{t_N} \tag{2}$$

ahol K_{k} a kapacitáskihasználtság (ezt az UIC által javasoltak alapján 0,7-nek vettük), t_{f} a foglaltsági idő, t_{p} az állandó jellegű időfelhasználásnak a teljes foglaltsághoz viszonyított értéke (ennek értékét 0,18-nak vettük),[15] t_{N} pedig a naptári időalap, ami esetünkben 1440 perc.

Az (1) és (2) összefüggésekből meghatározva a t_{mf} és t_{f} értékeket, az egy vágányon közlekedtethető vonatdarabszám (N) ezek hányadosaként számítható:[16]

$$N = \frac{t_f}{t_{mf}} \tag{3}$$

Mindezek figyelembevételéhez minden egyes főjelzőre meghatároztuk az azt követő összes lehetséges két térközt, és kiválasztottuk azokat, amelyekre az összmenetidő a legkisebb. Hasonlóan meghatároztuk a jelzőt megelőző térközre az észlelési távolságot, és ennek, illetve a maximális engedélyezett vonathossznak a figyelembevételével kiszámítottuk az egyes térközökhöz a mértékadó foglaltsági időket, ezekből pedig meghatározható az adott vonalszakasz egy napra vetített átbocsátóképessége. Ez az érték ezért egy abszolút felső határ az egyes vonalszakaszok átbocsátóképességére.

[13] MÁV 2023b: 16.
[14] UIC 2013.
[15] Lévai 2022.
[16] Lévai 2022.

Számítási módszerek

Szoftverkörnyezet

A számításokat az R programozási nyelven és környezetben[17] végeztük el a Csárdi Gábor és Nepusz Tamás által kifejlesztett *igraph* csomaggal.[18] A menetidők, illetve menetvonalhosszak szempontjából legrövidebb utakat a csomag distances() függvényével határoztuk meg, amely olyan élsúlyozott gráfok esetében, amelyek csak nemnegatív súlyú éleket tartalmaznak (mint esetünkben is), a Dijkstra-algoritmust[19] használja ehhez. Két gráfpont között a programcsomag shortest_paths() függvényével meghatározhatók a pontos útvonal által érintett egyes gráfélek ($epath).

Mozdonyflotta

Mivel a Magyar Honvédség tulajdonában nincs vasúti vontatójármű, ezért azokat a katonai szállításokhoz is bérelni kell. Vizsgálatunkban csak nyilvánosan elérhető adatokra támaszkodva[20] azon normál nyomtávú (1435 mm) dízelmozdonyait vizsgáltuk, amikkel bármilyen jellegű kocsitovábbítás lehetséges. Ezekből összesen 444 darab van, a mozdonyok maximális menetsebességét is minden esetben figyelembe vettük a számításokban.

Mivel elsősorban különleges jogrend idején kívántuk vizsgálni a szállítási kapacitásokat, az áramellátás esetleges zavara miatt a szerelvények továbbítása ilyen esetben csak dízelüzemmel lehetséges. A kérdés, hogy elegendő-e ebben az esetben is a rendelkezésre álló flotta (feltételezve, hogy a pálya nem sérült).

Emellett az MH saját célú vasúti pályái (scvp) kivétel nélkül villamosítatlanok, azaz berakodás után, illetve lerakodás előtt az elegy továbbítását mindenképpen dízelmozdonnyal kell végezni legalább az iparvágány és a legközelebbi villamosított vasútállomás között. Emellett a legrövidebb/leggyorsabb útvonalnak villamosítatlan vonal(szakasz)ok is részei lehetnek, ahol legalább dízel előfogatra is szükség van.[21]

A maximális folyam

Minden gráfélhez kiszámítottuk annak kapacitását, azaz esetünkben az azon időegység alatt közlekedtethető vonatok maximális számát. Ekkor bármely két gráfcsúcs között meghatározható az úgynevezett folyam, amely azt mutatja meg, hogy mennyi azon két csúcs (azaz az általuk reprezentált jelző) között egységnyi idő (esetünkben egy nap) alatt leközlekedtethető vonatok maximális száma, és mi ezeknek a pontos útvonala. Ez utóbbi azért lényeges, mert lehet, hogy két nagyobb kapacitású vonalszakasz között

[17] R Core Team 2012.
[18] Csardi–Nepusz 2006.
[19] Dijkstra 1959.
[20] Vonat-összeállítás 2023.
[21] Vörös 2014.

több kisebb átbocsátóképességű található, amelyek mindegyike igénybe veendő a maximális folyam átbocsátásához.

A maximális folyam értéke, azaz hogy két gráfcsúcs között mekkora a hálózat maximális átbocsátóképessége és ennek a gráf élein való eloszlása, az *igraph* csomag maxflow() függvényével határozható meg.

A teljes hálózat átbocsátóképességének meghatározásához először kiszámítottuk minden határátmenetpár között a lehetséges maximális kapacitást úgy, hogy a nem villamosított vonalak kapacitását 0-ra állítottuk a számítás elején, és a kapott értékeket összegeztük (kumulált átbocsátóképesség). Ezután elvégeztük a számítást a villamosítatlan vonalak valós kapacitásértékével is.

Az MH iparvágányai közötti folyamokat kétféleképpen számítottuk, amelyek a szállítások szélsőséges példáit modellezik. Először a rövid távú szállításokat szimuláltuk úgy, hogy meghatároztuk a két (időben, illetve távolságban) legközelebbi MH-iparvágány távolságát és kiszámítottuk közöttük a maximális folyamot. Ezzel az értékkel csökkentettük az útvonalra eső pályaszakaszok elérhető szabad kapacitását, majd meghatároztuk a második két legközelebbi MH-iparvágány távolságát és kiszámítottuk közöttük a maximális folyamot stb.

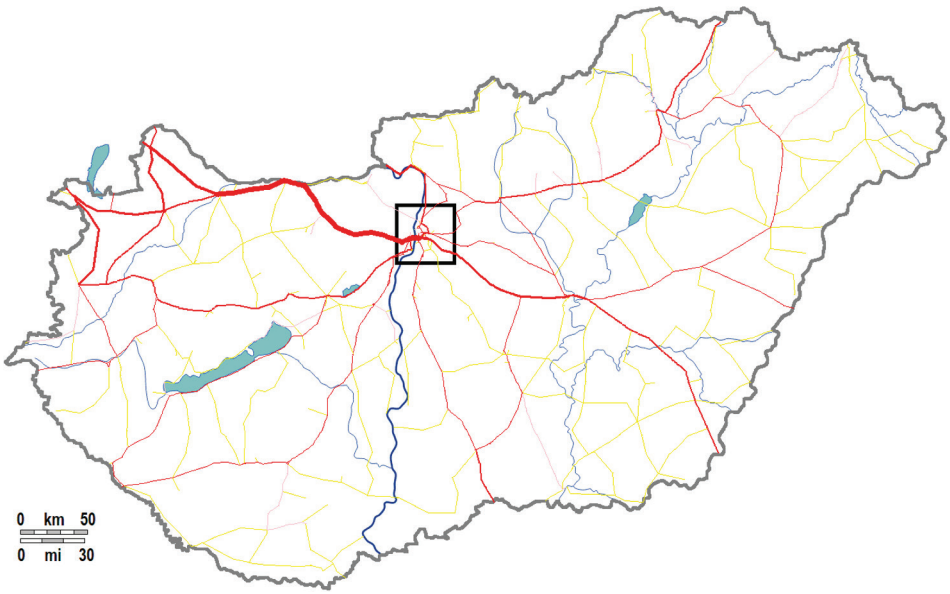
Másodszor a nagy távolságú szállításokat szimuláltuk: most a két legtávolabbi MH-iparvágány között számítottuk ki a folyamot, majd a második két legközelebbi között stb. Itt tehát az volt a különbség az előző számításhoz képest, hogy mindig a két (időben vagy távolságban) legtávolabbi MH scvp-k között számoltuk a folyamot. Ez természetesen azt is jelentette, hogy az igénybe vett vasútvonalszakaszok is sokkal hosszabbak voltak, mint az előző számításnál.

Eredmények

A számítások eredményeit a következőkben térképeken szemléltetve mutatjuk be.

A magyarországi vasúthálózat átbocsátóképessége

Először a villamosított határátmenetek között határoztuk meg a lehetséges maximális forgalmat. A 27 határátmenet közül csak 13 (Biharkeresztes, Fertőújlak, Gyékényes, Harka, Hegyeshalom, Hidasnémeti, Kelebia, Komárom, Lőkösháza, Őriszentpéter, Rajka, Sopron és Szob) villamosított, 14 (Ágerdőmajor, Ágfalva, Bánréve, Eperjeske, Hídvégardó, Ipolytarnóc, Kötegyán, Magyarbóly, Murakeresztúr, Nógrádszakál, Nyírábrány, Röszke, Sátoraljaújhely, Somoskőújfalu, Szentgotthárd, Záhony) nem. Bár a 150. sz. Budapest-Kelebia vonal jelenleg teljes átépítés alatt van, és annak felújítás utáni pontos térközkiosztása sem ismert, ennek ellenére nem akartuk ezen vonalat figyelmen kívül hagyni. A számításokhoz ezért a felújítás előtti paramétereket használtuk, tehát a vonal forgalomnak való átadása után annak szerepe ennél jelentősebb lesz. A kapott eredmények a 4. ábrán láthatók.



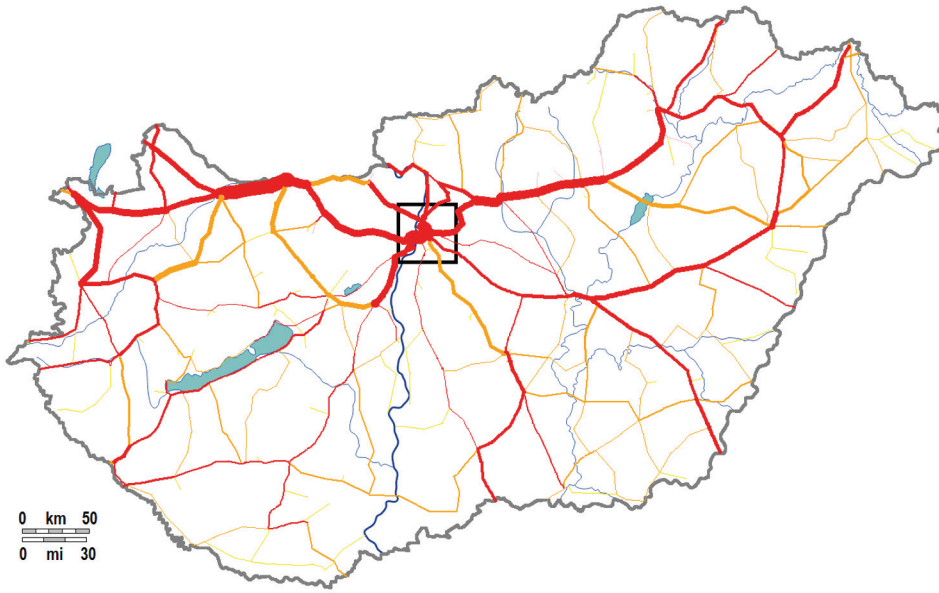
4. ábra: A magyarországi vasúthálózat kumulált átbocsátóképessége kizárólag villamos vontatás esetében. A vonalak vastagsága az átbocsátott forgalommal és nem az adott vonalszakasz kapacitásával arányos. Piros: villamosított vonal nemnulla forgalommal, rózsaszín: villamosított vonal nulla forgalommal, sárga: villamosítatlan vonal

Forrás: a szerzők szerkesztése

Azt látjuk, hogy például a 40. sz. Pusztaszabolcs–Pécs-vasútvonal Dombóvártól délre eső szakasza vagy a 100. sz. Szolnok–Debrecen–Nyíregyháza–Záhony-vonal Nyíregyházától keletre eső szakasza villamosítás szempontjából zsákvonal, hiszen bár ezek a vonalak villamosítottak, a megfelelő határátmenet (Magyarbóly, illetve Záhony) villamosítatlansága miatt nem elérhetők.

A nemzetközi forgalom szempontjából a legjelentősebb az 1. sz. Budapest–Hegyeshalom-vonal, különösen annak Győrtől keletre eső szakasza. Ennek elsődleges oka, hogy bár a vonal kapacitása végig nagyjából állandó, a Győrtől nyugatra eső határátmeneteknek a pályánál alacsonyabb engedélyezett sebessége miatt az itt csatlakozó 8. sz. Győr–Sopron-vonal forgalma is hozzáadódik a Budapest felé vezető irányhoz.

Alapvetően megváltozik a kép, ha a villamosítatlan vonalakat is figyelembe vesszük (5. ábra). A kumulált átbocsátott forgalom 57%-kal nő meg a villamosítatlan határátmenetek forgalmának köszönhetően, azaz a lehetséges forgalom 64%-a bonyolódik csak a villamosított vonalakon, annak harmada a villamosítatlan határátmeneteken zajlik.



5. ábra: A magyarországi vasúthálózat kumulált átbocsátóképessége villamos és dízelvontatás esetében. A vonalak vastagsága az átbocsátott forgalommal és nem az adott vonalszakasz kapacitásával arányos. Piros: villamosított vonal, sárga: villamosítatlan vonal

Forrás: a szerzők szerkesztése

A legjelentősebb forgalmat bonyolító villamosítatlan vonalak a villamosított vonalak között található, magas engedélyezett sebességű vonalak. Ezek a 10. sz. Győr–Celldömölk-vonal, a 2. sz. Budapest–Esztergom-vonal, az 5. sz. Székesfehérvár–Komárom-vonal, a 142. sz. Budapest–Lajosmizse–Kecskemét-vonal és a 108. sz. Debrecen–Füzesabony-vonal.

Ez az eredmény is kiemeli az 5. sz. vonal meghatározó szerepét Budapest elkerülésében, amely a tervezett V0 vasútvonal több korábbi nyomvonaltervében is a vonal részeként szerepelt.[22]

A 142. sz. vonal honvédelmi szerepét a hálózatban már korábban kimutatták,[23] és jelen vizsgálat megerősítette helyettesítő szerepét a 100. és 150. sz. vonalak tekintetében.

A 108. sz. vonal a 80a és 80. sz. Budapest–Hatvan–Miskolc–Szerencs–Sátoraljaújhely-vonal és a 100. sz. vonal közötti átjárhatóságot biztosítja,[24] ezáltal lehetőséget teremt a két fővonal bármelyikének sérülése esetén a forgalom másikra való terelésére.

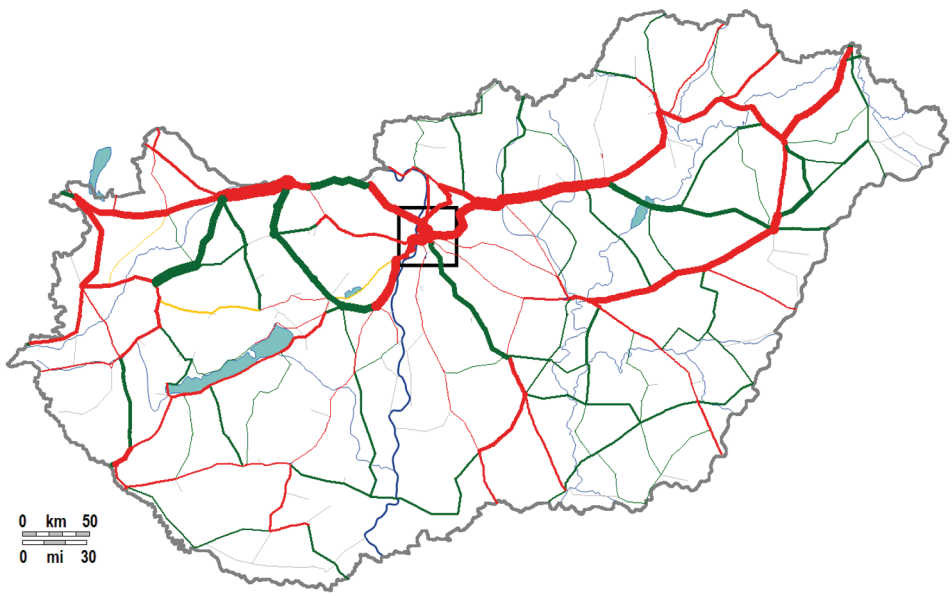
A számítás azt is kimutatta, hogy a 4. sz. Esztergom–Almásfüzitő- és a 2. sz. Budapest–Esztergom-vonal megfelelő paraméterek esetén valós helyettesítője lehetne az 1. sz. fővonalnak, azonban az itt található műtárgyak és a vonalak berendezése

[22] Somogyvári–Tóth 2023.
[23] Szászi 2013b.
[24] Lévai 2023.

miatt jelenleg nem alkalmas erre a funkcióra, és csak irreálisan magas költségekkel lehetne alkalmassá tenni.

Feltűnően alacsony a 20. sz. Székesfehérvár–Szombathely-vonal forgalma, annak ellenére, hogy a vonal villamosított. Ennek oka abban keresendő, hogy több szakaszán csak 80 km/h a rajta engedélyezett sebesség, valamint hogy a Celldömölk és Boba közötti szakasza kivételével egyvágányú. Emiatt az 1. sz. vonal (különösen annak Győr és Komárom közötti szakasza) az Északnyugat-Magyarország és Budapest közötti forgalom fő útvonala.

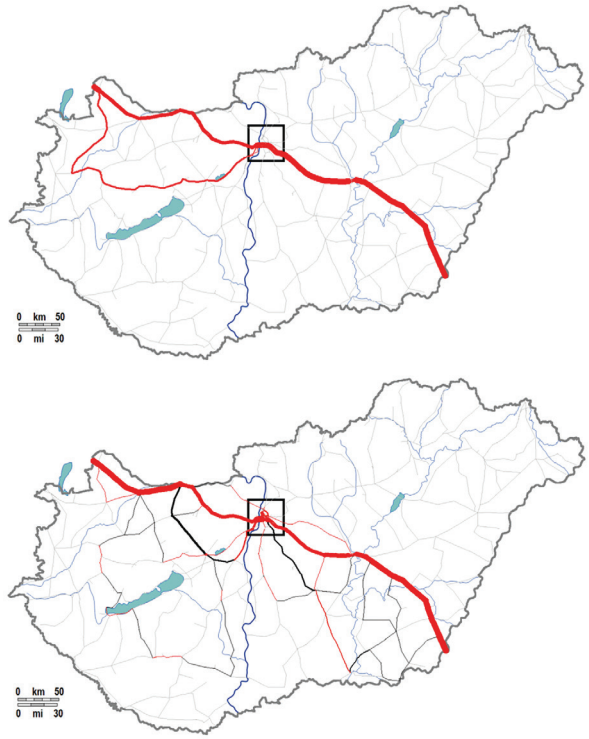
Ábrázolva a 4. és az 5. ábra forgalomértékeinek a különbségeit, a 6. ábrán bemutatott eredményeket kapjuk.



6. ábra: A magyarországi vasúthálózat kumulált átbocsátóképességének változása a villamosítatlan vonalak figyelembevételének hatására. Piros: villamosított vonal, forgalomnövekedés; sárga: villamosítatlan vonal, forgalomnövekedés; narancs: villamosított vonal, forgalomcsökkenés
Forrás: a szerzők szerkesztése

A várakozásoknak megfelelően majdnem mindenhol forgalomnövekedést tapasztalunk, három vonalszakaszt kivéve. Az egyik a már említett 20. sz. vonal Boba és Veszprém közötti szakasza, a másik a 30a Budapest–Székesfehérvár-vonal Székesfehérvár és Érd alsó elágazás, illetve Érd elágazás közötti szakasza, amelyek forgalma a 10. sz., illetve az 5. sz. vonalak igénybevételével halad.

Ennek szemléltetésére vizsgáljuk meg a Hegyeshalom–Lőkösháza-viszonylatot (7. ábra).



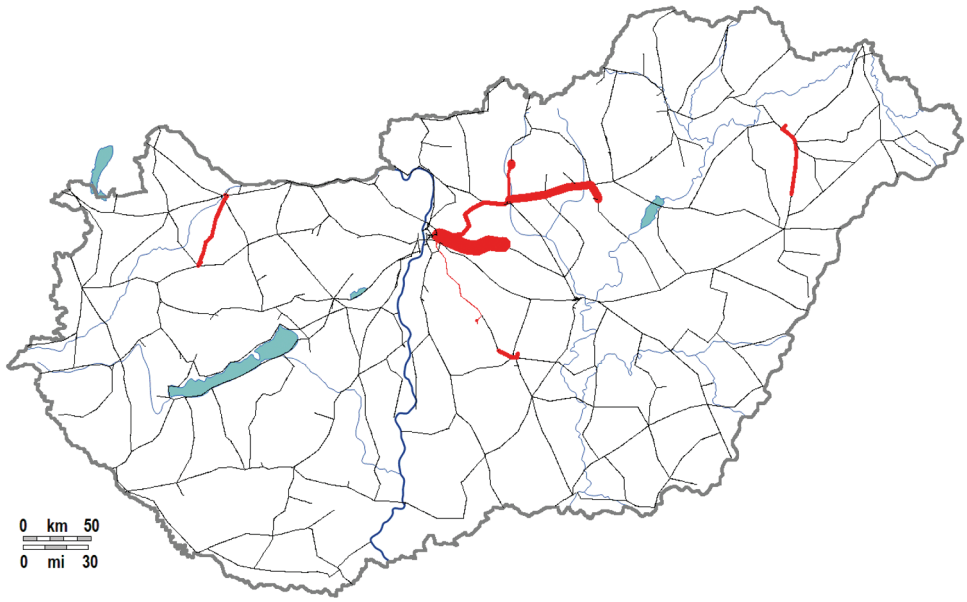
7. ábra: A Hegyeshalom és Lőkösháza közötti kumulált átbocsátóképesség csak villamosított vonalakra (fent) és villamosított és villamosítatlan vonalak figyelembevételével (lent). A vonalak vastagsága az átbocsátott forgalommal és nem az adott vonalszakasz kapacitásával arányos. Piros: villamosított vonal, fekete: villamosítatlan vonal

Forrás: a szerzők szerkesztése

Csak villamosított vonalakat igénybe véve a folyam egy része a nyilvánvaló 1., 100a és 120. sz. Szolnok–Békéscsaba–Lőkösháza-vonalak által alkotott útirány mellett a 16. sz. Hegyeshalom–Szombathely és a 20. és 30a vonalakon halad Budapestig. A villamosítatlan vonalakat is figyelembe véve több jelentéktelen (köztük egy Bátaszéket és egy Szegedet is érintő) útvonal mellett a legjelentősebb az 5., 44. sz. Pusztaszabolcs–Székesfehérvár- és 40a Budapest–Pusztaszabolcs-vonalakat érintő útirány, amely a hosszú porpáci kitérőt (és irányváltást) váltja ki a többnyire villamosítatlan alternatív útvonalon.

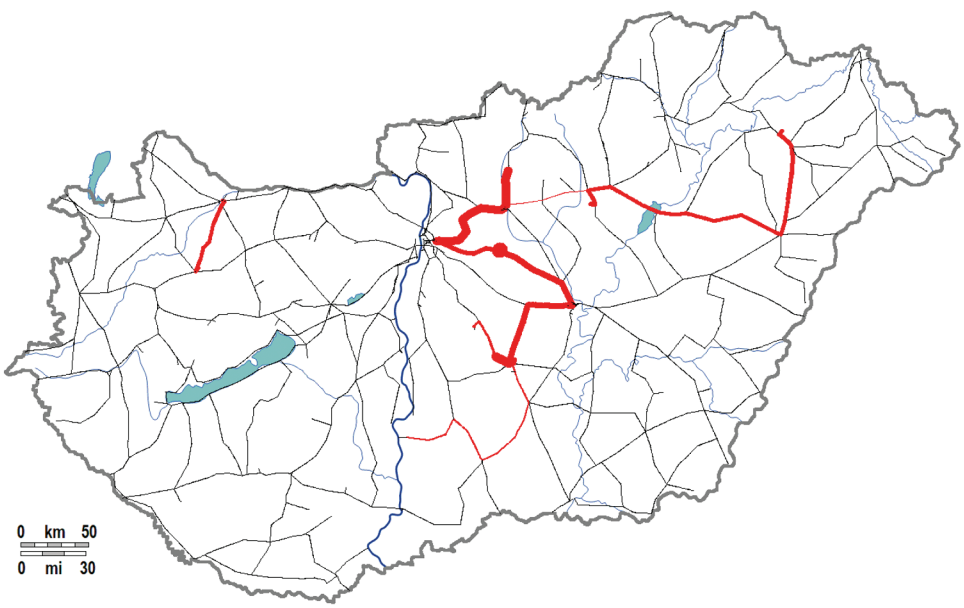
Az MH iparvágányai közötti szállítások

Az előzőekben tárgyalt módon elosztva a mozdonyokat, az alábbi eredményeket kapjuk a legközelebbi MH scvp-k közötti közlekedtetés esetén minimális menetvonalhosszakra (8. ábra) és minimális menetidőkre (9. ábra).



8. ábra: A menetvonalhossz szerint legközelebbi MH-iparvágányok között közlekedtethető dízelvontatású vonatok eloszlása

Forrás: a szerzők szerkesztése



9. ábra: A menetidő szerint legközelebbi MH-iparvágányok között közlekedtethető dízelvontatású vonatok eloszlása

Forrás: a szerzők szerkesztése

A számítások alapján a szállítások minimális menetvonalhosszak esetén a leközlekedtetett vonatok darabszámának csökkenő sorrendjében a Rákos–Tápiószecső, Jobbágyi–Erdőtelek, Jobbágyi–Rákos, Kecskemét–Hetényegyháza, Nyírtelek–Hajdúhadház, Győr–Pápa, a táborfalvai iparvágányok között, valamint Táborfalva–Rákos között, minimális menetidők esetén pedig Tápiószecső–Jobbágyi, Tápiószecső–Hetényegyháza, Hetényegyháza–Kecskemét, Jobbágyi–Erdőtelek, Nyírtelek–Hajdúhadház, Győr–Pápa, Rákos–Tápiószecső, a táborfalvai iparvágányok között, Táborfalva–Hetényegyháza és Tápiószecső–Kecskemét viszonylatokban történnek.

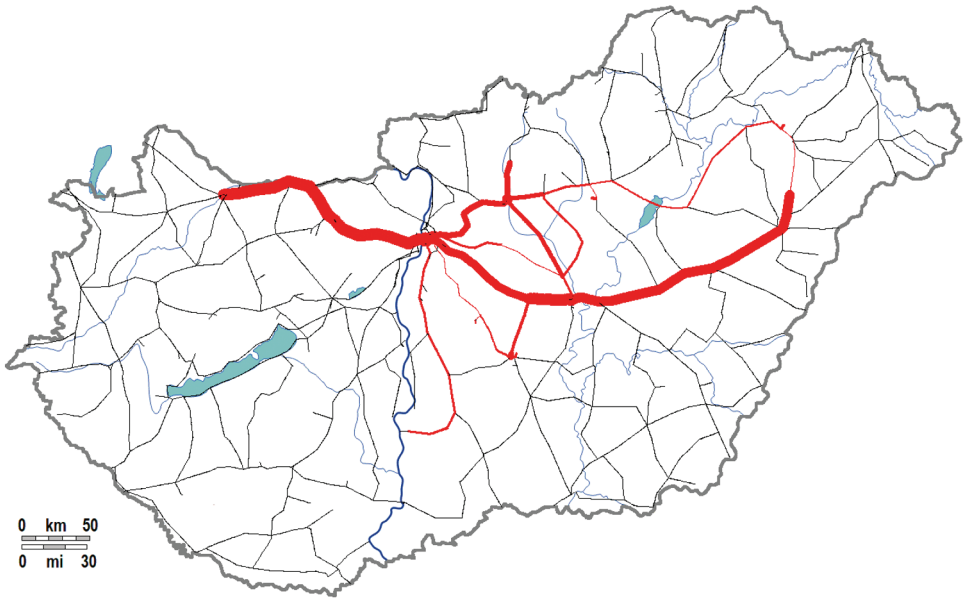
Az eredmények azt mutatják, hogy rövid távú szállítások esetében a hálózat kapacitása megfelelő, ha a legrövidebb úton akarjuk a szállítást lebonyolítani. Ennek legfőbb oka, hogy az útvonalak, amelyeken a szállítás történik, nem fednek át. Ekkor tehát, ha elegendő vontatójármű és rakodási kapacitás áll rendelkezésre (amik korlátait ezen számításban nem vettünk figyelembe), a szállítások kivitelezhetők.

Azonban a rövid távú szállítások minimális menetidők esetében nem végezhetők el teljes mértékben, csak a vonatok 87%-a közlekedtethető le. Mivel az iparvágányok néhány kivétellel fővonalak mellett helyezkednek el, amelyekre magas az engedélyezett sebesség, ez a hálózat telítődését okozza, ugyanis minden menetvonal ezekre a vonalakra „törekszik" a menetidő minimalizálása érdekében. Ahogy a 8. ábrán látszik is, a szerelvények a fővonalak néhány rövidebb szakaszát annak kapacitáshatáráig veszik igénybe, és ezért további menetvonalak már nem vezethetők arra.

Tovább romlik a kép, ha elvégezzük a számítást az egymástól legmesszebb levő MH scvp-k esetére is, amikor minden lépésben térben és időben legmesszebbi, de még nem nulla kapacitású scvp-k között szállítunk. Bár ezek meglehetősen ritka szállítási viszonylatnak számítanak, hiszen ezen vágányok alapvetően a gyakorlatban inkább a helyszíni rakodást követően a fővonalak elérését támogatják, és nem egy másik HM scvp elérése a cél, de mégsem példa nélküliek.[25] Célunk ezen viszonylatok elemzésével ezért inkább annak vizsgálata, hogy ilyen alacsony kapacitású, de egymástól távol eső pályák esetében milyen a hálózat teljesítőképessége. Az eredmények minimális menetvonalhosszakra a 9. ábrán, minimális menetidőkre a 10. ábrán láthatók.

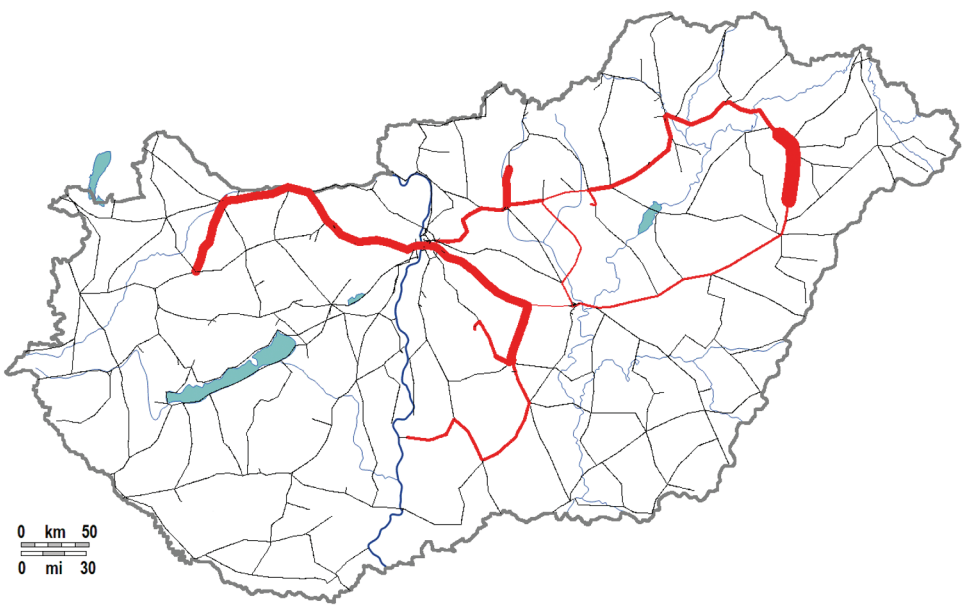
A számítások alapján a szállítások maximális menetvonalhosszak esetén a leközlekedtetett vonatok darabszámának csökkenő sorrendjében a Győr–Hajdúhadház, Győr–Erdőtelek, Győr–Nyírtelek, Nyírtelek–Táborfalva, valamint Győr–Kalocsa között, maximális menetidők esetén pedig Pápa–Hajdúhadház, Nyírtelek–Rákos, Nyírtelek–Pápa, Nyírtelek–Táborfalva, Nyírtelek–Kalocsa, Nyírtelek–Győr, Győr–Hetényegyháza és Hetényegyháza–Pápa viszonylatokban történnek.

[25] Vörös 2014.



10. ábra: A menetvonalhossz szerint legtávolabbi MH-iparvágányok között közlekedtethető dízelvontatású vonatok eloszlása

Forrás: a szerzők szerkesztése



11. ábra: A menetidő szerint legtávolabbi MH-iparvágányok között közlekedtethető dízelvontatású vonatok eloszlása

Forrás: a szerzők szerkesztése

A maximális menetvonalhosszak esetében a hálózat erősen kapacitáshiányosnak bizonyult. A szerelvényeknek mindössze 52%-át lehetett leközlekedtetni és az Összekötő vasúti híd is elérte áteresztőképességének határát. Ez azt is jelenti, hogy nagy távolságú szállítások esetén nem elsősorban a vontatójárművek darabszáma jelenti a korlátozó tényezőt, hanem a magyarországi pályahálózat szűk keresztmetszetei, ahol különböző irányból érkező és különböző irányokba tartó menetvonalak találkoznak. Ilyenek különösen a nagyfolyami hidak,[26] amelyek többvágányúvá bővítésük esetén is érzékenyek maradnak a szomszédos állomások forgalmi zavaraira.[27]

Maximális menetidők esetében ugyan a szerelvények 70%-a leközlekedtethető, de ekkor pedig a Hajdúhadház–Nyíregyháza-állomásköz telítődik. Ez hasonló, de a hálózat szerkezetéből adódóan kisebb probléma, mint az előző esetben az Összekötő vasúti híd átbocsátóképességének teljes kihasználása, mivel a 100. sz. fővonalon Debrecentől és a 80. sz. fővonalon még az egyvágányú Mezőzombor–Nyíregyháza-szakaszon is marad kapacitás az esetleges további keleti irányú igény átbocsátására. Ebben az esetben azonban a fővonalak kölcsönös helyettesítőképessége leromlik az alacsony kapacitású transzverzális vonalak miatt.

Konklúzió

Megvizsgálva a magyarországi vasúthálózat határátmenetek közötti forgalmi teljesítőképességét azt találtuk, hogy a forgalom harmada villamosítatlan vonalakon futna. Villamos vontatás esetében a 20. sz. vasútvonal a hálózat lényeges eleme, azonban dízelvontatás alkalmazása esetén léteznek kedvezőbb útirányok.

A Magyar Honvédség szállításaira nézve azt találtuk, hogy minimális távolságú szállítások esetén a pályakapacitás elégséges, a korlátozó tényezőt a gördülőállomány mennyisége jelenti. Bár minimális menetidejű szállítások esetén már telítődött a hálózat, feltételezhető, hogy hosszabb kerülőutakkal a szállítás még megoldható lenne. Maximális távolságú és menetidejű szállítások esetén a pályakapacitás bizonyult elégtelennek. Maximális menetvonalhosszak esetén nem lehetett az összes vonatot leközlekedtetni az Összekötő vasúti híd telítődése miatt. Maximális menetidők esetén minden vonat le tudott közlekedni, a Hajdúhadház–Nyíregyháza-állomásköz telítődött, azonban itt rendelkezésre álltak szabad kapacitású alternatív útvonalak.

A leközlekedtetett szerelvények darabszáma viszont azt sejteti, hogy ennyi vonat be- és kirakása ennyi idő alatt a rendelkezésre álló honvédségi rakodókon nem megoldható, azonban ennek egzakt igazolása további kutatást igényel.

[26] Szászi 2013b.
[27] Szászi 2014.

Felhasznált irodalom

277/2014. (XI. 14.) Kormányrendelet a vasúti közlekedési hatóság által kiszabható bírság mértékéről és megfizetésének részletes szabályairól. Online: https://net.jogtar.hu/jogszabaly?docid=a1400277.kor

Csárdi, Gábor – Nepusz, Tamás (2006): The Igraph Software Package for Complex Network Research. *InterJournal, Complex Systems,* 1695. Online: https://igraph.org/

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

Eurostat (2024a): *Total Length of Railway Lines*. Online: https://ec.europa.eu/eurostat/databrowser/view/TTR00003/default/table?lang=en&category=rail.rail_if

Eurostat (2024b): *Length of Electrified Railway Lines by Type of Current*. Online: https://ec.europa.eu/eurostat/databrowser/view/rail_if_electri/default/table

Lévai Zsolt (2022): A BAVS által javasolt új budapesti vasúthálózat helyettesíthetőségének vizsgálata. In Horváth, Gábor – Horváth, Balázs (szerk.): *XX. European Transport Congress/XII. International Conference on Transport Sciences.* Győr. 342–354.

Lévai Zsolt (2023): A fővonali vasúti Tisza-hidak helyettesíthetőségének kérdései. *Műszaki Katonai Közlöny,* 33(2), 59–74. Online: https://doi.org/10.32562/mkk.2023.2.5

MÁV (2023a): *F. 2. sz. Forgalmi Utasítás*. MÁV Zrt. Pályavasúti Üzletág Forgalmi Főosztály. Online: https://bit.ly/41b2qCn

MÁV (2023b): *F. 1. sz. Jelzési Utasítás*. MÁV Zrt. Pályavasúti Üzletág Forgalmi Főosztály. Online: https://bit.ly/3CHygMw

MÁV-Start mozdonyok (2023). Online: www.vonatosszeallitas.hu/jarmuvek_mav_mozdonyok.html

R Core Team (2012). *A Language and Environment for Statistical Computing.* Vienna: R Foundation for Statistical Computing. Online: www.R-project.org/

Somogyvári Bence Miklós – Tóth Bence (2023): A V0 vasútvonal új nyomvonalának hatása a Magyar Honvédség saját célú vasúti pályáinak kapcsolatára. In Horváth, Balázs – Horváth, Gábor (szerk.): *XIII. International Conference on Transport Sciences.* Győr. 335–346.

Szászi Gábor (2013a): *A vasúti hálózati infrastruktúrával szemben támasztott újszerű védelmi követelmények kutatása, a továbbfejlesztés feltételrendszerének vizsgálata.* PhD-disszertáció. Budapest: Nemzeti Közszolgálati Egyetem. 103–104. Online: https://doi.org/10.17625/NKE.2014.028

Szászi Gábor (2013b): A vasúti közlekedési alágazat, mint kritikus infrastruktúra. In Horváth Attila (szerk.): *Fejezetek a kritikus infrastruktúra védelemből*. Budapest: Magyar Hadtudományi Társaság, 167–190. Online: www.mhtt.eu/hadtudomany/KIV_tanulmanykotet.pdf

Szászi Gábor (2013c): Long-Span Railway Bridges in the Transport System of Hungary. *Hadmérnök,* 8(2), 98–107. Online: http://hadmernok.hu/132_09_szaszig.pdf

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

Budapest: Nemzeti Közszolgálati Egyetem, 83–99. Online: https://real.mtak.hu/94343/1/Kozlekedj_okosan-_A_kozlekedest_tamogato.pdf

TÓTH Bence (2018): A magyarországi vasúthálózat zavarainak gráfelméleti alapú vizsgálata. In HORVÁTH Balázs – HORVÁTH Gábor – GAÁL B. (szerk.): *Közlekedéstudományi Konferencia. Győr 2018*. 505–519. Online: http://real.mtak.hu/78843/1/2018b_KTK.pdf

TÓTH Bence (2023): Állomásközök és térközök hatása a vasúthálózat modelljének pontosságára. *Hadtudomány,* 33(E-szám), 137–156. Online: https://doi.org/10.17047/Hadtud.2023.33.E+137

UIC (2013): *Union International des Chemins de fer: Capacity (UIC Code R 406)*. Paris. Online: https://tamannaei.iut.ac.ir/sites/tamannaei.iut.ac.ir/files/files_course/uic406_2013.pdf

VÖRÖS Attila (2014): Valamit rakodnak Táborfalván. *Iho.hu,* 2014. június 15. Online: https://iho.hu/hirek/valamit-rakodnak-taborfalvan-140614

VPE (2023): *Vasútvonalak*. Online: www.kapella.hu/takt/vonal_lista.php

VPE (2024): *Vasúthálózati térkép*. Online: https://takt.kapella2.hu/metronom-server/map

HADMÉRNÖK
KATONAI LOGISZTIKA ÉS KÖZLEKEDÉS

19. évfolyam (2024) 3. szám 67–83.
DOI: 10.32567/hm.2024.3.5

Szajkó Gyula[1] – Pap Andrea[2] – Gulyás György[3]

A FOURLOG 2024 logisztikai kiképzés magyarországi szakaszának tapasztalatai és újszerű elemei

The Experience and New Elements of Hungarian Part of FOURLOG 2024 Logistic Training

Absztrakt

Napjainkban a felsőoktatásban is egyre nagyobb jelentőségű a nemzetköziesítés. A Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék által az elmúlt több mind két évtizedben megrendezett FOURLOG többnemzeti logisztikai kiképzés is részben ezt a célt szolgálja. A kiképzésen rendszerint az Osztrák Szövetségi Haderő Logisztikai Iskolájának, a brnói Védelmi Egyetem Katonai Vezetői Karának, valamint a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar katonai logisztika alapképzési szak három specializációjának végzős hallgatói vesznek részt. A gyakorlatot három országban (Ausztria, Magyarország, Csehország) és ütemben, civil és katonai objektumok igénybevételével bonyolítják le. A kiképzés fő célkitűzése, hogy a honvédtisztjelöltek tapasztalatot szerezzenek a többnemzeti munkacsoportokban történő feladatkidolgozásokban, megismerkedjenek a műveletervezés logisztikai támogatásának alapjaival, valamint bővítsék a szakmai idegen nyelvi tudásukat. A gyakorlat ideje alatt a hallgatóknak komplex feladatokat kell megoldaniuk, amelyek a későbbiekben katonatisztként a beosztásuk betöltésekor is megjelenhetnek mind országvédelmi, mind válságreagáló műveletekben. Ezért is fontos a felsőoktatási intézmények számára, hogy

[1] Tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék, e-mail: szajko.gyula@uni-nke.hu
[2] Egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék, e-mail: pap.andrea@uni-nke.hu
[3] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék; tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: gulyas.gyorgy@uni-nke.hu

az érintett szervezeti elemek folytassák az együttműködést és fejlesszék a kiképzési programot, amely igazodik a biztonságpolitikai helyzetben bekövetkezett változáskhoz.

Kulcsszavak: logisztikai kiképzés, felsőoktatás, törzsmunka, együttműködés, felkészítés

Abstract

Nowadays internationalization has a great importance in the higher education. FOURLOG Multinational Logistic Traning is organized every year by the Department of Supply, Finance and Military Transportation, Faculty of Military Science and Officer Training, of Ludovika University of Public Service with two other foreign higher educations institutions which is in line with these objectives. Cadets of the Logistics School of the Austrian Bundesheer and the Department of Logistics, Faculty of Military Leadership, Defence University in Brno and the graduating cadets of the abovementioned Hungarian University take part in this training. The exercise takes place in different military barracks and civilian facilities in three countries (Austria, Hungary and the Czech Republic). The main objective of this training is cadets to gain experience with the multinational stuff work and to get acquainted with basics of logistic support of the operational planning also to improve their professional English language skills. Complex tasks have to be carried out during this training by cadets, which can be appeared later both in crisis response and conventional operation when they will serve as a military officer. It is very important for the higher education institutions, their organization elements to continue the cooperation and improve the training program which follows the changes of security situation.

Keywords: logistic training, higher education, stuff work, cooperation, preparation

Bevezetés

A FOURLOG Logisztikai Kiképzés 20 éves történelmi múlttal rendelkezik. A 2000-es évek elején az akkori Zrínyi Miklós Nemzetvédelmi Egyetem Vezetés- és Szervezéstudományi Kar Hadtáp és Pénzügyi Tanszék oktatói felismerték, hogy a tananyag részeként kidolgozott magyar nyelvű harcászati feladatok mellett szükség van az angol nyelven történő gyakorlási lehetőség biztosítására is. Ennek érdekében 2001-ben a Cseh Hadsereg Szárazföldi Haderőnemi Egyeteme és a Bolyai János Katonai Műszaki Főiskola[4] együttműködési megállapodást kötött a Cooperative Training 2001 Bilaterális Békefenntartói Logisztikai Képzési Program elindítására vonatkozóan.[5] A kiképzés 14 nap időtartamban zajlott, amelynek keretében az első héten Magyarországon logisztikai szemrevételezést, a művelet szakági biztosításával kapcsolatos tervezési feladatokat hajtották végre a kadétok, míg a második ütemben Csehországban a logisztikai szakalegységek funkcionális tábori elemei telepítésével és működtetésével ismerkedtek meg a hallgatók. A képzési programot 2004-ben változtatták

[4] 2001-ben önálló felsőoktatási intézményként működött.
[5] Venekei 2015.

meg a szervezők és nevezték át FOURLOG Logisztikai Kiképzési Programmá, amikor csatlakozott a részt vevő nemzetekhez az Osztrák Szövetségi Haderő Logisztikai Iskolája, valamint a liptószentmiklósi Katonai Akadémia.[6] Az eltelt időszakban a szervezők folyamatosan fejlesztették a programot figyelembe véve a logisztikai eljárásrendekben bekövetkezett változásokat. Példaként lehet említeni, hogy 2008-tól új elemként bekerült a feladatok közé a LOGFAS[7] moduljainak alkalmazása, így az erők állománytábláinak és eszközeinek összeállítását, a készletek számvetését, a digitális térképen a mozgatás szállítási útvonalainak kijelölését, a vasúti, valamint a közúti átcsoportosítások tervezését már (a NATO által is használt) logisztikai információs rendszer támogatásával végezték a hallgatók.

A FOURLOG 2024 többnemzeti logisztikai kiképzés tervezésekor is fontos szempont volt az oktatók és mentorok részéről, hogy olyan felkészítést biztosítsanak a hallgatók számára, amely igazodik az új kihívásokhoz és a logisztikai tisztekkel szemben támasztott követelményekhez. Habár a Covid–19-világjárvány miatt 2020–2021-ben a gyakorlat teljes egészben elmaradt, 2022-ben csak a hazai ütemet hajtották végre, külföldi résztvevők nélkül, 2023-tól is a cél az, hogy a hallgatók olyan képzésben részesüljenek, aminek birtokában fiatal tisztként megfelelnek korunk elvárásainak. A cikkünkben bemutatjuk a képzés programját és az új elgondolások lényegét, majd a hallgatói kérdőívek alapján elemezzük – az incidens- és eseménylistába (MEL/MIL List) integrált új feladatokkal együtt – a kiképzés eredményességét.

FOURLOG logisztikai kiképzés

A 2004-ben elindított együttműködés fő célkitűzése az volt, hogy a katonai intézményekben tanulmányokat folytató hallgatók megismerkedjenek a többnemzeti műveletek logisztikai támogatását érintő feladatokkal. A részt vevő iskolák által tartott felkészítést úgy alakították ki a szervezők, hogy az tartalmazza:

- a lövészzászlóalj felelősségi körzetében a logisztikai alegységparancsnoki kötelmek gyakorlását (például a műveletek kezdete előtt a feladat megértését, értelmezését, a logisztikai alegységek elhelyezésével, telepítésével, az erők megóvásával, a döntés-előkészítő tevékenységgel kapcsolatos feladatokat);
- az erők hadszíntéri telepítésének elkészítése érdekében végzendő logisztikai tervezésben való részvételt, a szükséges programrendszerek alkalmazását, a dandár vezetési szintjén a szakági ellátási feladatok megtervezését;
- a műveleti támogatási lánc egyes elemei funkcióinak és működési elveinek megértését, az együttműködés gyakorlását.[8]

[6] Bár a szlovák iskola csak 2004-ben tudott delegálni kadétokat a kiképzésre, a szervezők nem változtatták meg a későbbiekben a program nevét.

[7] A LOGFAS *(Logistics Functional Area Services)* a NATO logisztikai információs rendszereinek az összessége, amely alkalmas az adatáramlás biztosítására és a jelentések megtételére a NATO-parancsnokságok, a katonai szervezetek és a nemzetek között a műveletek logisztikai támogatásának tervezési és végrehajtási fázisaiban. Szabados 2018.

[8] Pap–Venekei 2018.

A gyakorlati feladatok végrehajtása érdekében a szcenáriót egy ENSZ-felhatalmazás alapján folyó, válságreagáló műveletre építették, amelynek lényege, hogy a hadszíntér egy fiktív európai állam, Eastland területén helyezkedik el, és az infrastruktúrája megegyezik a mai kelet-közép-európai országok jellemzőivel. Az országban kibontakozó nemzetiségi konfliktusok etnikai tisztogatásokhoz vezettek, így a katonai szövetség ENSZ-felhatalmazás alapján légicsapásokat mért a kormányerőkre.[9] A konfliktusban részt vevő felek tűzszüneti megállapodást kötöttek, és a béke érdekében engedélyezték a két hadosztályból álló kontingensnek (Eastland Forces) az ország területére történő telepítését.

A rend helyreállítása érdekében a béketámogató erők kiemelt feladatai közé tartozott a szemben álló felek lefegyverzése, a fegyverek begyűjtése, a tűzszüneti megállapodás betartatása és bármely fél részére nyújtott külső fegyveres támogatás megakadályozása.[10]

Az eredeti szcenárió alapján kialakított műveleti környezetben kell minden évben a hallgatóknak logisztikai feladatokat megoldaniuk, amelyeket folyamatosan aktualizálnak a mindenkori biztonsági kihívásoknak és műveletтervezési feladatoknak megfelelően.

A tényleges végrehajtás angol nyelven, három ütemben zajlik 2004 óta. Az első ütemben a többnemzeti munkacsoportokba[11] beosztott hallgatók megismerkednek a béketámogató műveletek alapfelkészítésének sajátosságaival, például az ellenőrző-áteresztő pontok telepítésével és működtetésével, a robbanótestek azonosításával, terepen történő megjelölésével. A foglalkozások rendszerint a Grossmittelben állomásozó 35. Páncélgránátos Ezred kiképző bázisán zajlanak. A második ütemben Magyarországon a munkacsoportok – a kiadott közlések alapján – elemzést végeznek a kialakult helyzetre vonatkozóan, megtervezik az erők telepítését, átcsoportosítását, az alegységek várható anyagfelhasználását, prognosztizálják a haditechnikai eszközök meghibásodásának darabszámát, majd a felelősségi körzet logisztikai felderítését követően jelentik csoportonként a parancsnokok, mentorok, oktatók részére az elgondolásaikat. A harmadik ütemben a hallgatók a lövészzászlóaljak logisztikai alegységeinek tábori körülmények közötti telepítését és működtetését gyakorolják, majd az ellátó pontok kiépítésével kapcsolatos javaslataikat prezentáció formájában jelentik az elöljáró felé.

A FOURLOG 2024 fordulópont volt a kiképzés történetében, mivel az oktatók teljesen új elemekkel bővítették a program magyarországi szakaszát, bízva abban, hogy a módosítások hozzájárulnak a végzős hallgatók első tiszti beosztásra történő felkészítéséhez.

[9] Operational Scenario of Logistics Training Fourlog.
[10] Operational Scenario of Logistics Training Fourlog.
[11] A létszámadatok függvényében 4 vagy 6 munkacsoportba *(syndicate),* vegyes elrendezéssel osztják be a hallgatókat. A munkacsoportok egyben az alegységek megjelölésére is szolgálnak, mivel a szcenárió alapján a hadosztály alárendeltségében egy többnemzeti dandárt is (osztrák, cseh, magyar és szlovák elnevezésű zászlóaljakkal) megalakítanak.

Új elgondolások

A részt vevő nemzetek mindig szem előtt tartották, hogy a kiképzés az aktuális katonai és szakmai kihívásokra készítse fel a tisztjelölteket. Különösen igaz ez a gyakorlat magyar szakaszára, amelynek fókuszában a logisztikai tervezési tevékenység áll. A szcenáriót még a 2000-es évek első harmadában készítették el a HHK Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék munkatársai, amely alapját képezte az akkoriban jellemző béketámogató műveletek logisztikai támogatásával kapcsolatos feladatokra való felkészülésnek. Mivel napjainkban hazánknak és egész Európának új, a korábbiaknál meghatározóbb kihívásokkal kell szembenéznie, a gyakorlat logisztikai tervező tevékenységének alapját jelentő szcenáriót is meg kell változtatni, hogy az jobban tükrözze a jelenlegi valós biztonsági helyzetet és a nemzetközi katonai és politikai viszonyokat.[12] Habár a különböző nemzetek iskolai tanterve, illetve a tisztképzésben megjelenő hangsúlyok eltérők, a fenti módosítás szükségességével mindhárom nemzet képviselői egyetértenek. Ezen felül azoknak a NATO és nemzeti haderők által levont következtetéseknek is meg kell jelenniük a kiképzés anyagában, amelyek a jelenlegi konfliktusok és biztonsági veszélyek kapcsán születtek a műveletek logisztikai támogatásával összefüggésben. Ilyen például a többnemzeti logisztikai megoldások hatékony igénybevételének szükségessége, a beszállítók bevonása a műveletekbe a logisztikai támogatás tervezésétől a feladatok végrehajtásáig[13] vagy a megfelelő kommunikáció a különböző vezetési szintek között. Éppen ezért a magyar fél a fentiekre igyekezett nagy hangsúlyt fektetni már a felkészülési időszakban az iskolai tananyag megfelelő módosításával, valamint a gyakorlat alatt végrehajtandó feladatok átalakításával. Mivel a három nemzet tisztjelöltjei vegyes munkacsoportokban hajtották végre feladataikat, így kénytelenek voltak együttműködni a sikeres végrehajtás céljából. A különböző szintű katonai ismeretek és szakmai háttér rá is kényszerítette őket a kooperációra, de a külföldi hallgatók néhány feladat esetén meglehetősen bizonytalannak mutatták magukat, mondván, hogy „ők erről nem tanultak". A korábbi évek tapasztalataiból kiindulva a magyar gyakorlattervezők igyekeztek figyelembe venni ezeket az eltéréseket is bizonyos mértékig, hiszen a saját kadétokra vonatkozó kiképzési célok sem sérülhettek.

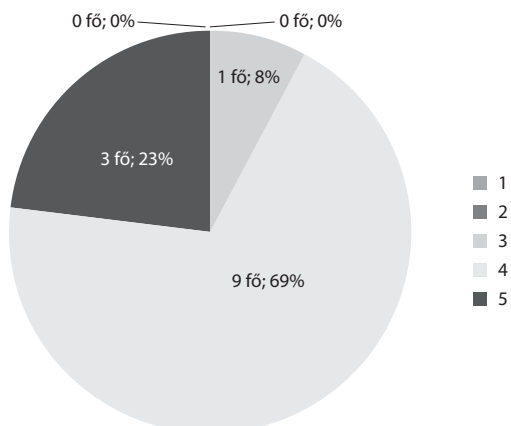
A felkészülési szakasz

A FOURLOG többnemzeti logisztikai kiképzésen történő részvételt hosszú tanulási folyamat előzi meg, amelynek része, hogy a tisztjelöltek jártasságot szerezzenek a logisztika és a művelettervezés területén is. Ennek érdekében vettek részt Tatán és Táborfalván kétszer egyhetes gyakorlaton harmad- és negyedévben. Előbbi esetében egy lövészzászlóalj átcsoportosítását, elhelyezését és ellátását kellett megtervezniük, míg utóbbi alkalommal egy Konvoj Támogató Központ létrehozása és a működtetés közbeni úgynevezett Main Events List/ Main Incidents List (MEL/MIL) közléseire

[12] Járdi 2024.
[13] Snoj 2023.

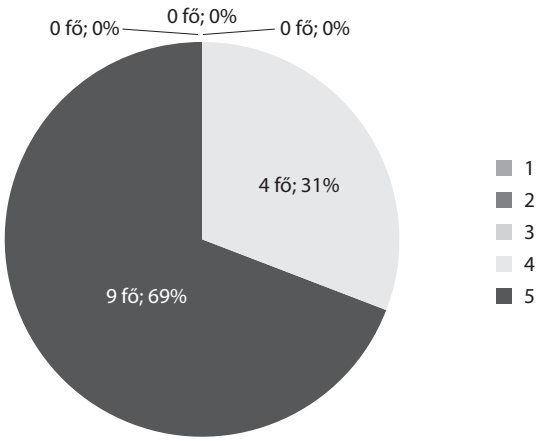
történő reagálás volt a feladatuk. Mindkét esetben munkacsoportokban történt a munkavégzés. A tisztjelöltek felkészítését segítette még egy új, műveletek logisztikai támogatásának tervezésével kapcsolatos tantárgy bevezetése a végzős évfolyamnak a 2023/2024-es tanév első szemeszterétől. Ezzel a hadműveletitől a harcászati (szakasz) szintig betekintést nyertek a logisztikai tervezői tevékenységbe, és gyakorlati feladatok megoldásával bizonyították az elméleti ismeretek elsajátítását. A harmadik, de különösen a negyedik évben a hallgatók egyre több szakmai tárgy keretében ismerkedtek meg a hazai, a NATO, továbbá más külföldi logisztikával és műveletervezéssel kapcsolatos doktrinális anyaggal és szabályzóval. Ezek a dokumentumok mindenképp hozzájárultak ahhoz, hogy a különböző nemzetek tisztjelöltjei együtt tudjanak működni a tervezési feladatok végrehajtása során. A kiképzés alkalmával a munkacsoportok részére kiadott munkaállomásokra egy könyvtárat is telepítettek alkönyvtárral, amelyek tartalmazták a vonatkozó szabályzókat, a tervezési tevékenységet elősegítő térképeket, a fiktívharcérték-táblázatot, a szcenáriót, a hadszínteret bemutató OLRT-[14] jelentést, a harcparancsot és a kitalált képességkatalógust.

Mindezek eredményét elég jól visszatükrözik a gyakorlat hazai szakaszára vonatkozó, a magyar hallgatók által kitöltött kérdőív releváns pontjai is. A felkészítési időszakot illetően a feladatok tisztázására, az oktatók tevékenységére és a rendelkezésre bocsátott szakirodalom használhatóságára vonatkozó kérdésekben, az egytől ötig terjedő skálán a legtöbb esetben „4" (jó) és „5" (jeles) értékelések születtek, amit az 1., 2., 3. ábra is mutat.

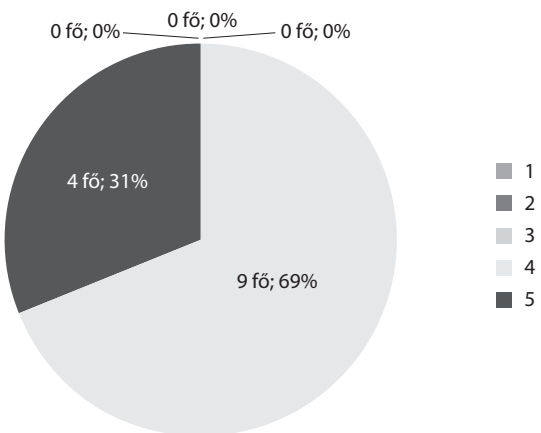


1. ábra: A feladat értelmezése, tisztázása az oktatói állomány részéről a hallgatók részére
Forrás: saját szerkesztés a kitöltött kérdőívek alapján

[14] OLRT: Operational Liaison and Reconnaissance Team.



2. ábra: Az oktató által rendelkezésre bocsátott irodalom, dokumentáció használhatósága
Forrás: saját szerkesztés a kitöltött kérdőívek alapján



3. ábra: Az oktatók tevékenysége a gyakorlatra való felkészülés időszakában
Forrás: saját szerkesztés a kitöltött kérdőívek alapján

Az eredmény jónak mondható, de még lehet rajta javítani, amit az is alátámaszt, hogy a hallgatók gyakran igényelték a mentorok segítségét és iránymutatását a munkacsoportban tevékenységük során.

A végrehajtási szakasz

A fentebb említett magyar szakaszra vonatkozó kérdőív eredményei több szempontból is meglepőek voltak, de van rájuk logikus magyarázat. Elöljáróban meg kell jegyezni, hogy a korábban több évig kiadott feladatok egy részében változtatásokat kellett

eszközölni. Ilyenek voltak a logisztikai tervezés bizonyos speciális területeivel, az előzetes hadműveleti értékeléssel és lehetőségelemzéssel, valamint a helyzetértékeléssel kapcsolatosak (például Center of Gravity Analysis, Factor Analysis).[15] Habár a fentebb már említett műveletтervezési ismereteket is tartalmazó, hetedik szemeszterben oktatott tantárgy tárgyalta ezeket a témákat – ellentétben több más hadtáp vagy közlekedési tárggyal –, ezt a speciális szakterületet ezt a félévet leszámítva korábban nem kellő részletességgel oktattuk. Ennek okán valószínűleg nem is ágyazódott be kellőképpen a hallgatók tudásába. Továbbá a cseh és osztrák fél jelezte az előző évben is, hogy az ő tantervük ilyen ismereteket egyáltalán nem tartalmaz, tehát először találkoztak ilyen kihívással a külföldi kadétok.

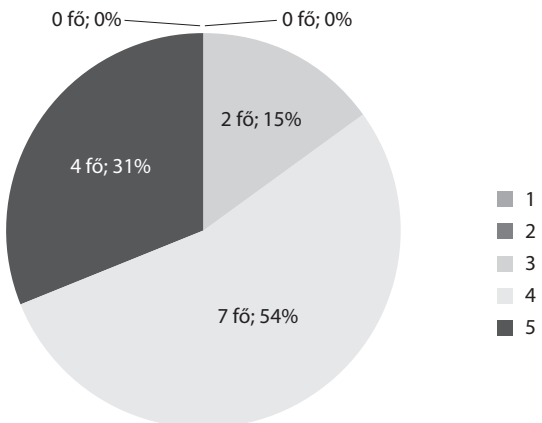
Az idei évben a magyar rész szervezői nagyobb hangsúlyt fektettek a gyakorlati tevékenységre. Így került be új elemként egy szemrevételezés, amelyet a lövészzászlóaljakat alakító négy munkacsoport négy különböző helyszínen hajtott végre, amelynek célja egy Konvoj Támogató Központ létrehozása, az ehhez és a működéshez szükséges képességek, kapacitások, valamint infrastruktúra-elemek felmérésével és tervezésével. Ennek alapján el kellett készíteniük egy komplett Szükségleti Jegyzéket (*Statement of Requirement,* SOR), a lehető legrészletesebb módon, amelyet azután megküldtek a Nemzeti Támogató Elemük (NTE) részére (két munkacsoport játszotta ezt a szerepet), akik feladata a szükséges képességek és kapacitások beszerzési forrásainak azonosítását követően a Támogatási Táblázat *(Support Matrix)*, valamint a beszerzett anyagok és szolgáltatások költségeinek elemzését követően a kalkulációk elkészítése volt. Ehhez a gyakorlat levezetését segítő mentorok, akik a lövészszászlóaljak felett elhelyezkedő dandárparancsnokság szerepét töltötték be, nyújtottak adatokat, fiktív helyi szolgáltatók profiljainak és a NATO Support and Procurement Agency (NSPA) által kiképzési célból kimunkált árainak megküldésével.[16] Ezzel a hallgatók gyakorolták a vertikális és horizontális kommunikációs csatornák alkalmazását is egyrészt a parancsnoki struktúra elemeivel, másrészt az NTE munkatársaival való együttműködés keretében. A feladat egyik célja az volt, hogy modellezze a beszerzési eljárás azon szakaszát, amikor az igény megérkezik egy katonai parancsnokságtól (jelen esetben zászlóalj-parancsnokságtól) a beszerzést végző szervezethez, és megkezdődik annak tisztázása. Ez a rész az eljárás meghatározó és kiemelten fontos eleme, hiszen a végén olyan minőségű szolgáltatást szereznek be, amilyen részletességgel és pontossággal megfogalmaztuk az igényt. Szintén ekkor dől el a SOR életképessége, hiszen ha a beszállítók számára nem lesz elég vonzó (például túl sok energiabefektetés kevés haszonnal), vagy nem lesz végrehajtható (például a túl rövid határidők miatt), akkor nem érkeznek majd ajánlatok a számunkra fontos szükséglet kielégítésére. Mint az várható volt, a szokásos problémák elő is jöttek, amikor az NTE nem tudta értelmezni a megküldött igényeket azok pontatlansága vagy hiányos meghatározása miatt. Ez sajnos éppen így történik a valóságban is. Ezért fontos, hogy a tisztjelöltek megismerkedjenek a beszerzési eljárásokkal legalább alapszinten, és bizonyos fokig tisztában legyenek a folyamat nehézségeivel és buktatóival, amire nagyobb figyelmet

[15] Ált. 2015: 216.

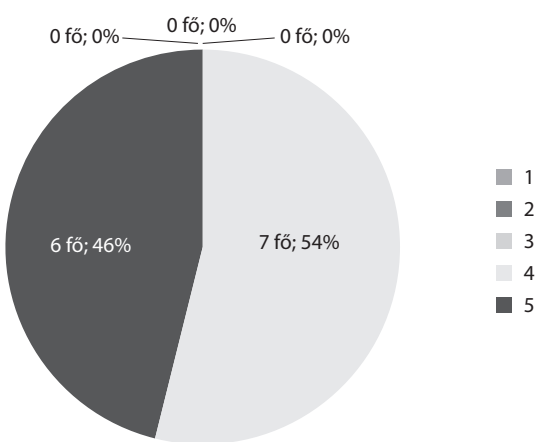
[16] Az NSPA is támogatta a gyakorlatot pl. azáltal, hogy életszerű, de nem valós szolgáltatásárakat generált számunkra.

szükséges majd fordítaniuk. Hiszen előfordulhat, hogy egy-két éven belül már egy béketámogató misszió kontingensében hajtanak végre hasonló feladatot, ahogyan az meg is történt az elmúlt években több frissen végzett tiszttel is.

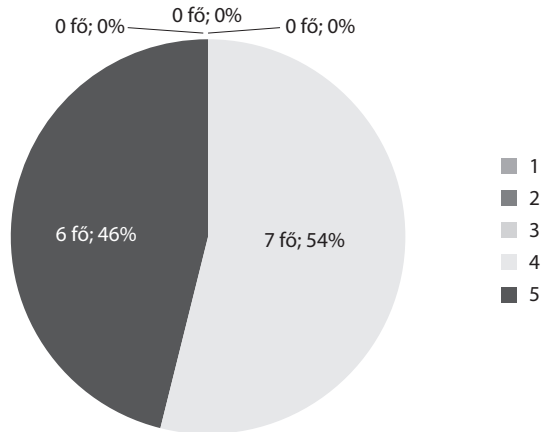
Ahogyan azt fentebb már említettük, ez az új és elég komplex feladat, amely a helyszíni szemrevételezéstől a szolgáltatásbeszerzés költségeinek meghatározásáig terjedt, a hazai tisztjelöltek számára is kihívást jelentett, hiszen több tárgyból tanult ismereteiket is alkalmazniuk kellett, ami a korábbi tanulmányok során megismert információk és a megszerzett tudás adekvát felhasználását kívánta meg. Ezt mindenképp elősegítette volna egy bizonyos szintű tervezői rutin, ami viszont valószínűleg még nem alakult ki náluk. Alapvetően ez lehet az oka annak, hogy a kérdőív vonatkozó kérdéseire kevésbé jó értékelést adtak a hallgatók, amit a 4–7. ábrák tartalmaznak.



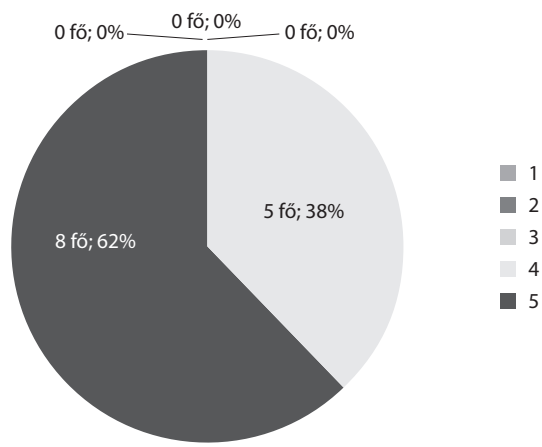
4. ábra: A kiadott feladat érthetősége
Forrás: saját szerkesztés a kitöltött kérdőívek alapján



5. ábra: A kiadott feladatok illeszkedése a korábban oktatott ismeretekhez
Forrás: saját szerkesztés a kitöltött kérdőívek alapján



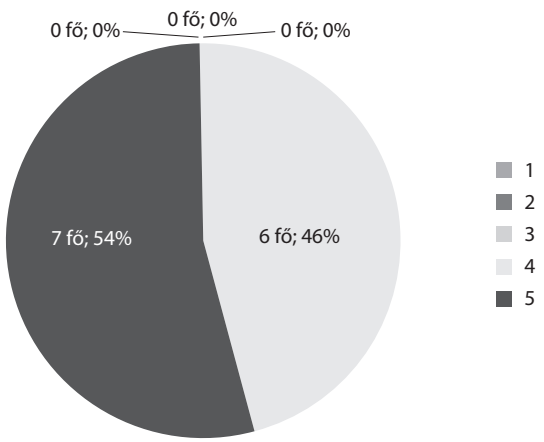
6. ábra: Az angol nyelvű szakmai terminológia érthetősége
Forrás: saját szerkesztés a kitöltött kérdőívek alapján



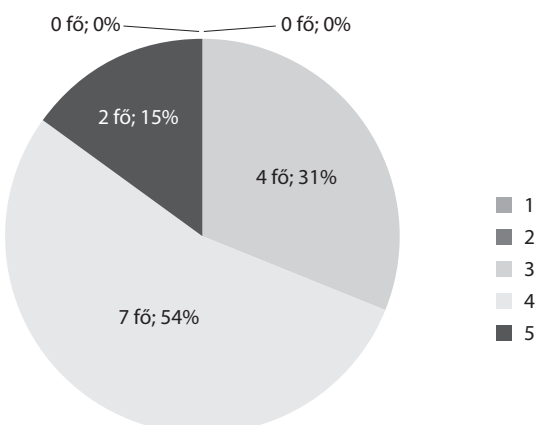
7. ábra: Az angol nyelvű szakmai terminológia hasznosíthatósága
Forrás: saját szerkesztés a kitöltött kérdőívek alapján

A Covid–19-járvány egyik következményeként 2020-ban és 2021-ben elmaradt a FOURLOG. 2022-ben az NKE HHK egy „mini" gyakorlatot vezetett le, mert a külföldi nemzetek a pandémia újbóli megjelenése feletti bizonytalanság miatt nem vettek részt. 2023-ban és 2024-ben már újra, az eredeti felállásnak megfelelően rendezték meg a kiképzést, de a személyes jelenléttel járó gyakorlatot megelőző tervezői értekezleteket nem tartották meg. A szervezés, a gyakorlat szakaszainak meghatározása és a kapcsolatos teendők koordinálása, valamint a feladatok kidolgozása informatikai és telekommunikációs eszközök alkalmazásának útján történt. Ráadásul mind a magyar, mind pedig a külföldi mentorállomány legalább fele kicserélődött. Ennek egyik eredménye az lett, hogy a gyakorlattervező és tisztjelölteket kísérő tisztek leginkább

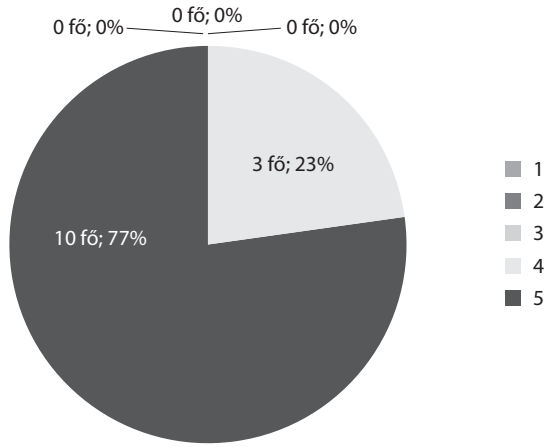
csak a saját nemzeti szakaszuk kiképzési tevékenységeivel voltak teljesen mértékig tisztában. Így a magyar szakasz során kiadott logisztikai tervezési feladatok kidolgozásakor csak korlátozott mértékben tudták ismereteiket vagy javaslataikat megosztani a saját és az idegen hallgatókkal. Az is világossá vált a végrehajtás időszakában, hogy a komplex módon felépített szcenárió és az abból következő feladatok összefüggéseinek átlátása és megértése sem sikerült minden külföldi oktatónak maradéktalanul, amit jelentős részben a felkészülési szakaszban elmaradt személyes megbeszélések hiánya okozott. Ezzel is magyarázható, hogy amíg a hazai mentorok tevékenységét a magyar hallgatók legnagyobb részben jelesre értékelték, addig a külföldi gyakorlatvezetők és oktató tisztek hozzájárulását nem minősítették ennyire pozitívan (8–10. ábrák).



8. ábra: A beosztott segítő oktató(k) hozzájárulása a feladat sikeres megoldásához
Forrás: saját szerkesztés a kitöltött kérdőívek alapján



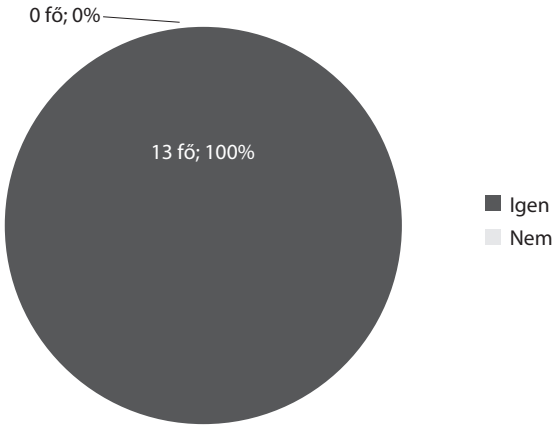
9. ábra: A külföldi gyakorlatvezető (osztrák, cseh) tevékenységének értékelése
Forrás: saját szerkesztés a kitöltött kérdőívek alapján



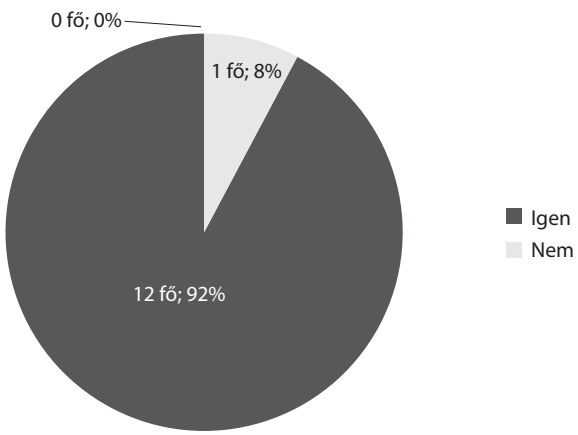
10. ábra: A magyar gyakorlatvezető tevékenységének értékelése
Forrás: saját szerkesztés a kitöltött kérdőívek alapján

Összegzés

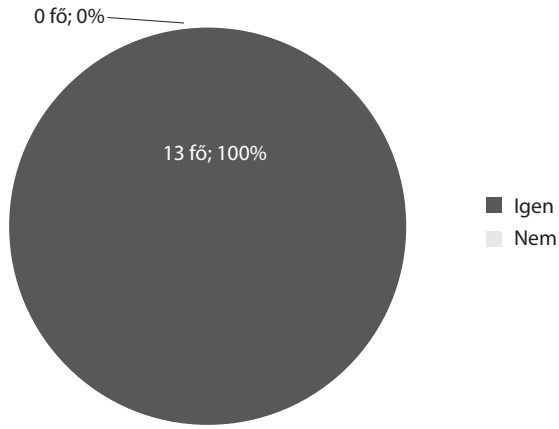
Kétségtelen, hogy a gyakorlat felkészülési szakaszában a szorosabb nemzetek közötti együttműködéssel jó esélyeink vannak a még eredményesebb végrehajtásra, bár a hallgatói munkacsoportok végső jelentései alapján az értékelő elöljárók így is megelégedéssel nyilatkoztak a kadétok teljesítményéről. Mindenesetre a FOURLOG továbbra is tökéletes platform a nyelvi képességek fejlesztésére, a különböző vezetési szintek közti együttműködés és a törzsfunkciók megértésére, a nemzetközi törzsmunkába történő betekintésre, a logisztikai támogatás erőforrásai azonosításának és kiválasztási szempontjainak megismerésére, a kulturális különbségekből adódó kihívások megismerésére és azok kezelésére alkalmazható módszerek elsajátítására, valamint a tisztjelöltek és mentorok közötti tapasztalatcserére. Az bizonyos, hogy a munkacsoportok sikeresen végrehajtották feladataikat a gyakorlat mindhárom szakaszában, a hallgatók nyelvi képességei is fejlődtek, és sok barátság szövődött közöttük. Mindezt visszatükrözik a kérdőívre adott válaszok is, amelyeket a következő öt ábra szemléltet.



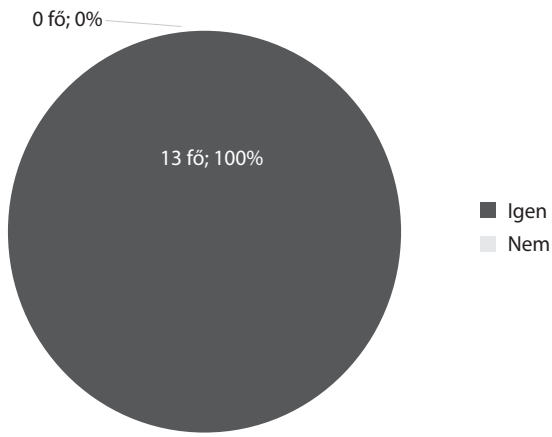
11. ábra: Hozzájárult-e a gyakorlat szakmai angolnyelv-tudásának fejlesztéséhez?
Forrás: saját szerkesztés a kitöltött kérdőívek alapján



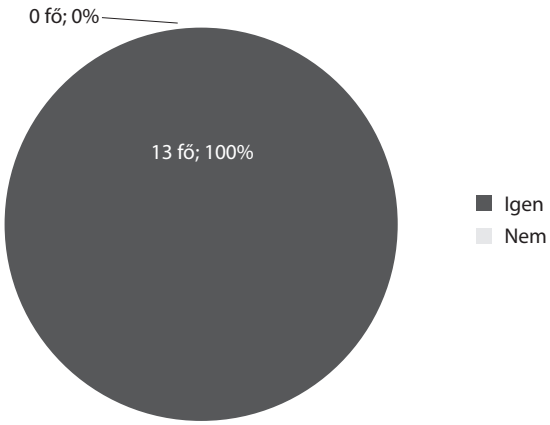
12. ábra: Hozzájárult-e a gyakorlat általános katonai szakmai ismereteinek bővítéséhez?
Forrás: saját szerkesztés a kitöltött kérdőívek alapján



13. ábra: Hozzájárult-e a gyakorlat a harcászati szintű (logisztikai) törzsmunka, valamint az egyes törzsfunkciók együttműködésének megértéséhez és elsajátításához?
Forrás: saját szerkesztés a kitöltött kérdőívek alapján



14. ábra: Hozzájárult-e a gyakorlat a műveleti parancsnoki lánc működésének, valamint a harcoló, harctámogató, harci kiszolgáló támogató erők, a befogadó nemzet és a polgári beszállítók kapcsolatának és együttműködésének megismeréséhez és megértéséhez?
Forrás: saját szerkesztés a kitöltött kérdőívek alapján



15. ábra: Hozzájárult-e a gyakorlat a nemzetközi környezetben történő törzsmunka nyelvi, kulturális, valamint szakmai különbségekből adódó kihívásainak megismeréséhez, továbbá az ezek kezelésére alkalmas magatartás és módszerek elsajátításához?
Forrás: saját szerkesztés a kitöltött kérdőívek alapján

A jövőre nézve mindenképpen vissza kell térni a Covid–19-járvány előtti FOURLOG tervezői értekezletek megtartásának gyakorlatához. Így a gyakorlati és valós biztosítás kérdésein túl lehetőség van jobban elmerülni a szcenárió főbb elemeiben, a logisztikai tervezéssel kapcsolatos feladatok megértésében, ha kell, átdolgozásában. Különös tekintettel azokra a feladatokra, amelyek majd megfelelően reflektálnak az új biztonsági kihívásokra, valamint a NATO és a magyar katonai vezetés által feldogozott tapasztalatokra és iránymutatásokra, mint például a beszállítókkal történő szorosabb együttműködés. Mindez elősegíti a külföldi oktató tisztek magyar szakaszba történő hatékonyabb bevonását és hallgatóik eredményesebb mentorálását is. Mindezeken túl a hazai ütem elején annak eredményes végrehajtásához szükséges lenne egy, a korábbi rövid prezentációs előadásokon keresztül történő bemutatás gyakorlatától eltérő, hosszabb, akár félnapos tréning megtartása is a résztvevőknek. A katonai parancsnokságokon bevett elem a műveletek vagy gyakorlatok előtti felkészítés *(battle staff training),* amely elősegíti a szcenárió megértését, illetve a különböző nemzetek eltérő szakmai szintű felkészültségének vagy hátterének kiegyenlítését. Ugyanis a tisztjelöltek hiába rendelkeztek minden szükséges dokumentummal és írásban kiadott tervezési segédlettel, a hadszíntér megismerésére és a helyzetelemzésre nincs elegendő idő a feladatok kidolgozása mellett. A sok adat feldolgozásához a komplex helyzetek áttekintésének és értékelésének képességét pedig tovább kell fejleszteni a vonatkozó tantárgyak gyakorlati óráin, valamint a hazai kiképzési eseményeken is. Szintén nagy hangsúlyt kell fektetni a csoportmunkában történő feladat-végrehajtásra is, amely a jövőben nagyobb önbizalmat ad majd hallgatóinknak. A FOURLOG több évtizedes múltja is bizonyítja, mennyire hasznos a tisztjelöltek kiképzésében és felkészítésében ez a gyakorlat, és mennyi használható tudást nyújt részükre a hazai és nemzetközi katonai szolgálatuk ellátásához aktív tiszti karrierjük során.

Felhasznált irodalom

Ált. 216. A Magyar Honvédség Törzsszolgálati Szabályzata II. rész. 2015. április 14.
Járdi Roland (2024): Vészjósló üzenet a magyar katonai vezetőtől: nem béketámogató műveletekre, hanem konfliktusokra kell felkészülni. *Vg.hu,* 2024. május 11. Online: www.vg.hu/kozelet/2024/05/magyar-katonai-vezeto-konfliktusok
Kérdőív a FOURLOG 2024 Logisztikai Kiképzés hazai ütemének értékelésére.
Operational Scenario of Logistics Training Fourlog 2004–2024. Budapest, NKE HHK.
Pap Andrea – Venekei József (2018): The Innovative Elements of the Conduct of Fourlog Logistics Training 2018 and Their Application in Military Higher Education. *Hadmérnök,* 13(2), 105–116. Online: http://hadmernok.hu/182_08_pap.pdf
Snoj Péter (2023): Az ellenálló képesség közös feladat. *Honvedelem.hu,* 2023. október 2. Online: https://honvedelem.hu/hirek/az-ellenallo-kepesseg-kozos-feladat.html
Szabados János József (2018): A Logisztikai Információs Rendszer szükségessége és fejlesztési lehetőségei a Magyar Honvédségben. *Hadtudományi Szemle,* 146(4), 89–102. Online: https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/365/349
Venekei József (2015): *A katonai logisztikai ellátási lánc koncepció fejlesztésének és alkalmazásának lehetőségei a Nemzeti Közszolgálati Egyetem alap- és mesterszakjainak multinacionális gyakorlati képzési programjaiban*. PhD-disszertáció. Budapest: NKE. Online: https://doi.org/10.17625/NKE.2015.018

Melléklet

Kérdőív a FOURLOG 2024 logisztikai kiképzés hazai szakaszának értékeléséhez					
I. Felkészítési időszak	**Értékelés**				
	1	**2**	**3**	**4**	**5**
1.) A feladat értelmezése, tisztázása az oktatói állomány részéről a hallgatók részére					
2.) Az oktatók által rendelkezésre bocsátott irodalom, dokumentáció használhatósága					
3.) Az oktatók tevékenysége a gyakorlatra való felkészítés időszakában					
II. Végrehajtási időszak					
1.) A kiadott feladat érthetősége					
2.) A kiadott feladatok illeszkedése a korábban oktatott ismeretekhez					
3.) Az oktatók által meghatározott/hallgatók által választott törzsmunka módszer hatékonysága					
4.) A külföldi munkacsoportokkal való együttműködés hatékonysága					
5.) Az angol nyelvű szakmai terminológia érthetősége					

6.) Az angol nyelvű szakmai terminológia hasznosíthatósága					
7.) A beosztott segítő oktató(k) hozzájárulása a feladat sikeres megoldásához					
8.) A külföldi (osztrák, cseh) gyakorlatvezető tevékenységének értékelése					
9.) A magyar gyakorlatvezető tevékenységének értékelése					

III. Befejező időszak	**Értékelés**	
	Igen	**Nem**
1.) Történt-e gyakorlatvezetői értékelés a hallgatók számára?		
2.) Hozzájárult-e a gyakorlat szakmai angolnyelv-tudásának fejlesztéséhez?		
3.) Hozzájárult-e a gyakorlat általános katonai szakmai ismereteinek bővítéséhez?		
4.) Hozzájárult-e a gyakorlat a harcászati szintű szakmai ismereteinek bővítéséhez?		
5.) Hozzájárult-e a gyakorlat a harcászati szintű (logisztikai) törzsmunka, valamint az egyes törzsfunkciók együttműködésének megértéséhez és elsajátításához?		
6.) Hozzájárult-e a gyakorlat a műveleti parancsnoki lánc működésének, valamint a harcoló, harctámogató, harci kiszolgáló támogató erők, a befogadó nemzet és a polgári beszállítók kapcsolatának és együttműködésének megismeréséhez és megértéséhez?		
7.) Hozzájárult-e a gyakorlat a nemzetközi környezetben történő törzsmunka nyelvi, kulturális, valamint szakmai különbségekből adódó kihívásainak megismeréséhez, továbbá az ezek kezelésére alkalmas magatartás és módszerek elsajátításához?		
8.) Hozzájárult-e a helyszíni szemrevételezés a tervezési feladatok sikeres végrehajtásához?		

9.) Milyennek ítéli meg a gyakorlat valós logisztikai biztosítását?	**Nem megfelelő**	**Megfelelő**	**Jó**	**Kiváló**
Élelmezés				
Elhelyezés				
Informatika				
Térképészet				

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
19. évfolyam (2024) 3. szám 85–95.
DOI: 10.32567/hm.2024.3.6

Lilla Horváth[1] – Péter Pántya[2]

New Methods of Maintenance and Cleaning of Firefighter's Protective Clothing by Dry Cleaning

Abstract

The condition of personal protective equipment (PPE) worn by firefighters has always been of paramount importance. In this article, the authors briefly describe the work of firefighters, based on analysis of domestic and international literature and their own professional practices, and then the types of contamination of clothing and the health risks they pose. A number of new technologies for the complete removal of contaminants from protective clothing are already on the market, but due to their higher cost, they are unlikely to fully replace the traditional cleaning currently used, but can be an excellent complement to current cleaning processes. The authors then proceed to examine the innovative technological solutions that are currently available in the field of cleaning firefighter protective clothing, before finally proposing the introduction of certain methods.

Keywords: firefighter, personal protective equipment, contamination, cleaning, washing

Introduction

The work of firefighters is more dangerous than everyday life, but this does not end when the duty is finished. In order to ensure the safety of firefighters and the public, it is essential that they have adequate theoretical and practical knowledge, experience, high mental and physical endurance and communication within the team. In addition to these, the personal protective equipment (PPE) and fire equipment they wear complement the previously listed conditions for accident-free and healthy work.[3]

[1] Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: lilla.horvath@katved.gov.hu
[2] Associate Professor, Ludovika University of Public Service, e-mail: pantya.peter@uni-nke.hu
[3] Pántya–Horváth 2023b: 88.

For preparing this article, the authors used the methods of analysing selected literature as international and Hungarian scientific papers, examining international wide databases about fire cases and product data about their capabilities from producers in the field of protective clothing. The authors used their own experience in fire safety from both the occupational health and intervention side. Given the scarcity of publications in this area of research, the available resources were limited.

Following the conclusion of an intervention and the departure from the scene of an accident, there are still a number of tasks that must be completed. Failure to do so could have a detrimental effect on the physical integrity and health of the firefighters. In addition to the inspection of professional equipment and the subsequent professional analysis of the case, the proper handling and cleaning of PPE plays a prominent role. This is because countless contaminants that are harmful to the human body can get on its surface or get into the fabrics (e.g. protective jacket).[4] Before embarking on an explanation of the topic of cleaning, it is advisable to take a brief detour into the realm of firefighters' daily work and the potential pollutants that they may encounter.

In addition to extinguishing fires, firefighters are also responsible for carrying out technical rescue and fire investigation tasks. The exact definition of these tasks in Hungary is provided by Act XXXI of 1996 on Fire Protection, Technical Rescue and Fire Brigades. Different activities involve various sources of danger, and PPE offers sufficient protection against most of them. Horváth briefly explains this topic, mentioning the dangers and psychological stress that arise during the performance of sports tasks required to maintain physical condition.[5]

For a detailed overview of the firefighter's job and the associated dangers, the risk assessment at the employer can provide adequate help, which is provided in Hungary by the Act XCIII of 1993 on Labour Safety. Furthermore, the document delineates the specific dangers associated with each job, the circumstances that exacerbate these risks, and the measures implemented to mitigate them. By furnishing the employer with a comprehensive understanding of the occupational hazards faced by employees, this document facilitates the procurement of the requisite PPE.

Following the purchase of this equipment, it is of the utmost importance to disseminate comprehensive information to all staff members regarding the correct use, cleaning and storage of the provided clothing. As the manufacturer always prepares a comprehensive user manual, its content can be integrated into the subject matter of the educational material (in addition to general practical experience). Although this may not appear to be a significant factor at first glance, it is nevertheless a necessary condition for everyday life. This is because any object that is used on a regular basis and that is subjected to professional maintenance will inevitably increase its quality of life. This is also true of personal protective equipment, which will maintain its ability to protect for a longer period if it is subjected to the correct maintenance procedures, which is also economically advantageous, since it reduces the number of purchases. The International Association of Fire Services (CTIF) provides statistical data on fires

[4] Fent et al. 2017: 801–802.
[5] Horváth 2022: 50–52.

in different countries for several years. Highlighting one of them, Figure 1 shows that the number of injured firefighters increased during the period under review. Although the reasons are not indicated, the increasing trend certainly provides a basis for the development of personal protective equipment.

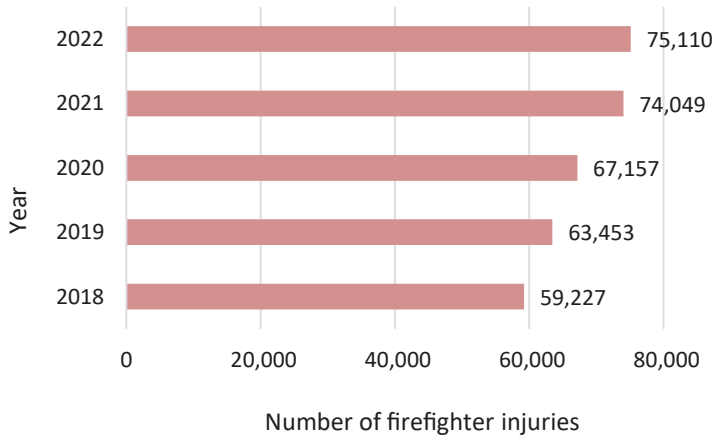


Figure 1: Trends in firefighter injuries in the countries of the World in 2018–2022
Source: compiled by the authors based on www.ctif.org/world-fire-statistics

It's important to note that different types of contamination require different cleaning methods. This is why it is also important that the staff receives adequate information in advance and regularly about the handling of personal protective equipment. Protective clothing may also become contaminated with substances of medium or high risk to human health, including blood, urine, faeces, and various chemical substances. In such instances, it is recommended (or indeed obligatory) to remove the protective clothing immediately and place it in a securely sealed bag for subsequent decontamination or to perform the decontamination procedure on-site.[6]

A significant number of international literatures address the issue of pollutants affecting firefighters, which can result in long-term illness due to their carcinogenic properties. One such group is the group of polycyclic aromatic hydrocarbons (PAHs), which are predominantly formed during the incomplete combustion of organic substances. Their natural sources of origin are, for instance, forest fires, but they can also be found in tobacco smoke and exhaust gas, and can also enter the human body during grilling of meat products.[7] A number of studies have reported the presence of PAHs and other pollutants on the PPE of firefighters, which subsequently enter the body through inhalation or contact with the skin. It is therefore important to pay sufficient attention to the proper cleaning and disinfection of clothing. In their experiment, Mayer et al. examined the effect of washing on the PAH concentration

[6] Decontamination is a combination of processes that removes or destroys contamination so that infectious agents or other contaminants cannot reach a susceptible site in sufficient quantities to initiate infection, or other harmful response.
[7] See: www.cdc.gov/biomonitoring/PAHs_FactSheet.html

on the given clothing. It was demonstrated that the concentration of PAHs could be significantly reduced by washing a contaminated garment, however, its presence could be detected on the new garment after washing, indicating cross-contamination.[8]

Regardless of the chosen method, the primary objective is to safeguard human health, with prevention being contingent upon economic and technical feasibility. The authors' objective is to present, through the examination and analysis of the methods presented in the following chapters, technological achievements that have long provided a satisfactory level of solution or have not yet been widely used as novum, but show convincing results.

Washing

The use of household and industrial washing machines has become widespread in most fire departments for the cleaning of firefighting protective clothing. Due to their smaller capacity, household washing machines can only wash a maximum of one item of clothing (trousers or jacket) at a time. This is not necessarily the most optimal solution in terms of time required and amount of water used, but it is sufficient to remove minor, non-infectious types of dirt. In contrast, industrial washing machines are now capable of accommodating multiple items of clothing. Their robust construction also allows for a longer expected fault-free lifespan. Furthermore, some manufacturers offer users the option to select an appropriate washing programme for the specific clothing in question (e.g. Protective Apparel programmes).[9] This is particularly beneficial for firefighting protective clothing, as preserving its protective ability for as long as possible is of paramount importance.[10]

In the case of washing protective clothing with a washing machine, it is also necessary to add an impregnating agent to the detergent at intervals recommended by the manufacturer. In order to understand the process of impregnation, it is first necessary to clarify the concepts involved. Firstly, it is worth mentioning the term water repellent. The materials in this group (clothing in this case) have the least protection against water. The addition of nylon or polyester during the mixing process is typically employed to enhance the water repellence of the material. The greater the density of the weave, the more challenging it is for water to penetrate. However, this provides only temporary protection. The next group includes water-repellent materials, in which case water is less able to enter the fabrics, thanks to the reinforced structure. The last group with the greatest protection is waterproof, where the given material is able to prevent the entry of water for a longer period of time.[11]

Textile impregnation is a process by which textiles are treated with a coating or substance in order to enhance their properties. This may include the addition of water resistance, stain resistance, flame resistance, or other desirable properties to

[8] Mayer et al. 2019: 139.
[9] See: www.dupont.com/personal-protection/nomex-industrial.html
[10] Bralewska et al. 2024: 1.
[11] See: https://manteco.com/what-is-the-difference-among-water-repellent-water-resistant-and-water-proof-clothing/

the fabric. The impregnation process can be carried out using a number of methods, including spraying, soaking or coating the fabric with a special solution. One common method of impregnation is the application of a chemical coating to the fabric, which is then cured by heat or pressure. This process creates a barrier on the surface of the fabric that repels liquids and prevents stain build-up. Another method of impregnation is lamination, where a thin film is applied to the fabric to provide greater protection and durability. Lamination can be employed to enhance the strength, flexibility, and resistance to tearing or wear of the fabric. This process is frequently utilised to manufacture technical fabrics for sportswear, outdoor equipment and medical textiles.[12]

The application of nanotechnology to the field of textile impregnation has led to the development of superhydrophobic fabrics that repel water and dirt at the molecular level. This cutting-edge technology enables the fabrics to retain their breathability and elasticity while providing excellent protection against stains and moisture. Furthermore, nanotechnology can be employed to create self-cleaning materials that require minimal maintenance and retain their properties after repeated washing.[13]

In the user information document of the Fire Fit 2 protective clothing sold by Rosenbauer, the manufacturer recommends the use of the impregnating agent at least after every second wash.[14] In their list, specific products are displayed (TX-Direct Wash, Hydrob Easydry), so it is possible to choose the right product for us on the manufacturer's website. The Nikwax website states that the TX 10i water repellent elastomer was developed based on EVA (ethylene vinyl acetate), and later became the primary active ingredient in all their products.[15]

In order to maintain the water repellent properties of firefighting protective clothing, it is essential to apply an impregnating treatment to the material on a regular basis. This is typically done during the washing process, which restores the fabric's ability to repel water and other substances. The water repellent surface plays a vital role in keeping firefighters dry and comfortable, and it is therefore crucial to ensure proper maintenance and washing of these garments in order to maintain protection and longevity.

In addition to impregnation, it is worth noting the significance of vapour diffusion, which is also an important aspect of firefighters' lives during an intervention. Physical activity raises body temperature, and the body responds by sweating to expel extra heat. This job is much more crucial in high outside temperatures, where intense physical labour is conducted under severe conditions. Clothing must consequently be fashioned of a material that is both water repellent and vapour permeable. This property is already present in firefighting protective apparel, although there has been extensive national and international research in this field.[16]

Moisture barriers, as a critical component in several applications, are principally constituted of slender, semi-permeable membranes, which are meticulously laminated onto a base fabric that is inherently resistant to fire. This base fabric may either be woven or nonwoven, depending on the specific requirements of the application.

[12] Smith 2010: 3–9.
[13] Jeyasubramanian et al. 2016.
[14] See: www.rosenbauer.com/en/int/rosenbauer-world/products/equipment/protective-clothing/fire-fit-2
[15] See: www.nikwax.com/en-us/how-nikwax-works/
[16] Pántya–Horváth 2023a.

Presently, the technology underpinning these membranes can be classified into three distinct categories: microporous membranes, solid hydrophilic membranes, and bicomponent membranes. These categorisations encapsulate the existing diversity in membrane technology, each with its unique method of moisture regulation, catering to various performance demands in industrial and consumer products. Within the realm of microporous membranes, expanded polytetrafluoroethylene (e-PTFE) membranes are extensively employed in the fabrication of firefighting apparel. Nonporous films, including polyurethanes (PUs) with hydrophilic components, are extensively employed as breathable and waterproof membranes in firefighter suits. Vapour transmission over solid film barriers involves an absorption–diffusion–desorption mechanism. Bicomponent membranes consist of a microporous membrane and a solid hydrophilic film. Most commercially available moisture barriers in firefighter uniforms are bicomponent e-PTFE barriers. Adding a solid hydrophilic layer improves moisture barrier longevity and resistance to water penetration. However, it also increases evaporative resistance, which is highly reliant on moisture content. The study of Gao et al. examines heat transfer via firefighter protective clothing by contrasting several moisture barrier technologies. The findings of this study provide conclusive evidence that hotter environments result in reduced water accumulation within moisture barriers, leading to significantly higher evaporative resistance with bicomponent moisture barriers.[17]

So, in addition to impregnation, research is also looking at heat transfer and vapour permeability, both of which are important in the design of a firefighter protective suit.

Dry cleaning

In the previous sections, the authors briefly described the possibilities and characteristics of traditional washing with water regarding the protective clothing of firefighters. In the following, the so-called dry-cleaning procedures will be discussed, which does not necessarily mean that the contaminated textiles are cleaned in an almost sterile environment.

Dry cleaning is a process that involves cleaning clothes and fabrics without the use of water. This cleaning method is preferred for materials that are less resistant to conventional washing in a washing machine. The process can extend the life of these garments by preventing shrinkage, fading or damage from regular washing. Dry cleaning has a long history dating back centuries. While the modern dry cleaning process was only invented in the 19th century, the concept of cleaning clothes without water has been around for much longer. Its origins can be traced back to the ancient Romans, who used ammonia extracted from urine to clean their clothes. The practice of dry cleaning continued into the Middle Ages and the Renaissance, with various materials such as clay, ash, and even sawdust being used to clean fabrics. The most significant revolution occurred at the beginning of the 19th century, when in 1825 a maid accidentally knocked over a lamp and spilled turpentine on a dirty

[17] Gao et al. 2021.

tablecloth. French-born Jean Baptiste Jolly noticed that after the turpentine dried, the resulting stains disappeared from the tablecloth. After that, he experimented by filling the bathtub with turpentine and then soaking the tablecloth, which became clean after being removed and dried. Dry cleaning soon became popular in Europe and the United States, as it was an effective method for cleaning delicate materials that could not withstand traditional washing methods. During the procedure, the clothes were placed in the machine and then a solvent was added to dissolve the dirt without water. Over the years, technology has developed, becoming more efficient and environmentally friendly. New solvents that are less harmful to the environment have been developed, and machines have been designed to use less energy and produce fewer emissions.[18]

Perchlorethylene (PER) is most often used in traditional dry cleaning. Despite its excellent cleaning performance, PER has several disadvantages, such as its toxic effect on the human body.[19] To avoid this, many alternative solvents are used for textile dry cleaning: hydrocarbon solvents, silicon-based solvents and carbon dioxide (CO_2).[20] In this article, the authors will describe the CO_2 dry cleaning process, as the technology for cleaning protective clothing has appeared in more and more countries.

The use of liquid carbon dioxide in the process of dry cleaning represents a more environmentally friendly alternative to traditional dry cleaning methods that utilise chemicals. This method involves the utilisation of liquid CO_2 as a solvent to clean clothes, rather than the use of toxic chemicals such as perchlorethylene. It is a colourless, odourless, non-toxic and non-flammable gas. In the liquid CO_2 dry cleaning process, this is employed in its supercritical state, whereby it simultaneously exists as a liquid and a gas. Liquid carbon dioxide is combined with a small quantity of detergent and then pumped into a chamber where it is utilised to clean clothes. The solvent is capable of penetrating the fibres of the fabric, removing dirt and stains without damaging the material. The process ensures that the clothes retain their original shape and colour.[21]

A number of international studies have addressed the issue of cleaning firefighter protective gear using carbon dioxide due to concerns about residual impurities from conventional washing methods. These impurities, including potential cross-contamination, can have long-term detrimental effects on firefighters' health. Arjunsing et al. conducted a comparative study examining the effectiveness of traditional washing versus dry cleaning with CO_2 on firefighter protective clothing.

The findings indicated that traditional washing was less efficient in removing high molecular weight pollutants such as PAHs and phthalates compared to lower weight pollutants like phenols. In contrast, dry cleaning with CO_2 consistently achieved high efficiency levels (averaging 95.36%).

[18] See: https://drycleaningca.com/blog/who-invented-dry-cleaning/
[19] Ceballos et al. 2021: 1.
[20] Sutanto et al. 2014.
[21] Madsen et al. 2021: 3–4.

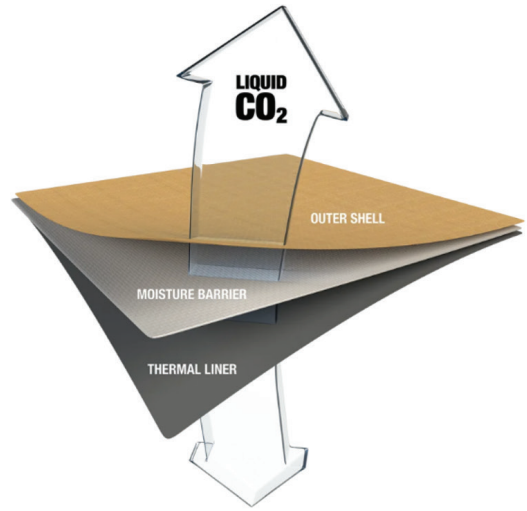


Figure 2: CO_2 cleaning machine and cleaning method
Source: Fire Engineering Staff 2024

It is important to note that the experiment focused solely on liquid pollutants, limiting the ability to draw broad conclusions since firefighters are also exposed to solid pollutants like soot during their duties. Nevertheless, the results provide valuable insights for future research endeavours in this area.[22]

On a domestic scale, the utilisation of dry ice for cleaning purposes has been witnessed in various industries such as plastics and automotive, enabling the cleaning of equipment without disassembly or the use of additional chemicals.[23] In Hungary, ozone-based disinfection is employed for clothes, effectively eliminating diverse pathogens without the need for water or other additives. While ozone disinfection may serve as a beneficial supplementary method for general clothing care, its innovative impact is limited when it comes to firefighter protective gear. Although carbon dioxide dry cleaning services are not yet widely accessible domestically, several international manufacturers have begun offering this option. Notably, Decontex is one such company operating across numerous European countries, specialising in decontamination cleaning services for fire departments. Their website highlights that carbon dioxide dry cleaning not only cleans firefighter protective clothing more effectively than traditional washing methods but also removes dirt from the intermediate membrane material (Deco2 Fire Technology®).[24]

The dry cleaning procedure necessitates a solution for businesses that not only eliminates surface dirt from clothing but also cleanses the fabrics, including the membrane, while maintaining their protective qualities. While the technology's efficiency is not currently economically justifiable for widespread adoption, there are instances, such as when there is a risk of biological contamination, where utilising this method may be advantageous.

[22] Girase et al. 2022.
[23] Tang et al. 2020.
[24] See: https://decontex.com/decon-solution/

Drying

The drying methods employed after traditional laundering play a significant role in the longevity of garments and overall operational efficiency. Following household or industrial washing, fire departments have various options for drying attire. When weather conditions permit and spare clothing is available, it can be advantageous to air dry outdoors. However, caution must be exercised due to intense UV radiation which can compromise material quality and lead to colour fading. Indoor drying reduces this risk but may result in slower drying times and increased humidity levels to consider. A common remedy is the use of a dryer, which effectively mitigates the aforementioned drawbacks either partially or entirely.

A drying cabinet or a free-standing/wall-mounted open dryer is utilised in multiple fire stations. In both instances, the drying process involves the circulation of warm air, powered by electricity. These technological solutions offer expedited and delicate drying, proving beneficial for fire departments facing challenges such as limited space and high humidity that hinder traditional drying methods. This innovation becomes essential when there is a need to dry a larger quantity of protective clothing within a constrained timeframe.

Figure 3: Powered drying cabinet and dryer

Source: https://unimac.com/product/firefighters-ppe-system/firefighter-ppe-drying-cabinet/; www.ppedryers.com/dryers/turnout-gear-dryers/model-ps4-r8/

Summary

Proper maintenance of firefighter turnout gear is essential for safeguarding the health and safety of those working in hazardous conditions. Historically, washing these garments with water has been the conventional approach. Nonetheless, studies indicate that these techniques are often inadequate for the removal of carcinogenic contaminants, such as polycyclic aromatic PAHs and phthalates, which accumulate

in the multilayer materials of firefighting apparel. In contrast, liquid carbon dioxide cleaning technology has emerged as a promising alternative, demonstrating superior contaminant removal capabilities compared to conventional methods.

Liquid CO_2 cleaning functions on principles that exploit its solvent properties, reducing water consumption and environmental impact. Unlike traditional methods that heavily depend on water and detergents, liquid CO_2 utilises a non-toxic solvent that effectively penetrates fabric layers to dissolve and extract contaminants without compromising the protective qualities of the gear. Studies have demonstrated that liquid CO_2 significantly surpasses aqueous washing in decontamination efficiency, thereby enhancing firefighters' safety by reducing long-term health risks linked to contaminated clothing. Furthermore, the environmentally friendly profile of liquid CO_2 positions it advantageously within modern sustainable practices. However, while this method demonstrates potential, continuous research is vital to facilitate widespread adoption among fire departments striving for optimal gear maintenance and firefighter safety.

References

Bralewska, Karolina – Bralewski, Adrian – Wolny, Piotr – Chiliński, Błażej (2024): Size-Resolved Particulate Matter Inside Selected Fire Stations and Preliminary Evaluation of the Effectiveness of Washing Machines in Reducing Its Concentrations. *Scientific Reports,* 14, Online: https://doi.org/10.1038/s41598-024-69268-9

Ceballos, Diana M. – Fellows, Katie M. – Evans, Ashley E. – Janulewicz, Patricia A. – Lee, Eun Gyung – Whittaker, Stephen G. (2021): Perchloroethylene and Dry Cleaning: It's Time to Move the Industry to Safer Alternatives. *Frontiers in Public Health,* 9. Online: https://doi.org/10.3389/fpubh.2021.638082

Fent, Kenneth W. – Alexander, Barbara – Roberts, Jennifer – Robertson, Shirley – Toennis, Christine – Sammons, Deborah – Bertke, Stephen – Kerber, Steve – Smith, Denise – Horn, Gavin (2017): Contamination of firefighter Personal Protective Equipment and Skin and the Effectiveness of Decontamination Procedures. *Journal of Occupational and Environmental Hygiene,* 14(10), 801–814. Online: https://doi.org/10.1080/15459624.2017.1334904

Fire Engineering Staff (2024): Gear Wash Introduces the Power of CO_2 Cleaning Services. *Fire Engineering,* 17 May 2024. Online: www.fireengineering.com/industry-news/gear-wash-introduces-the-power-of-co2-cleaning-services/#gref

Gao, Huipo et al. (2021): Effects of Environmental Temperature and Humidity on Evaporative Heat Loss through Firefighter Suit Materials Made with Semi-Permeable and Microporous Moisture Barriers. *Textile Research Journal,* 92(1–2), 219–231. Online: https://doi.org/10.1177/00405175211026537

Girase, Arjunsing – Thompson, Donald – Ormond, Robert Bryan (2022): Comparative Analysis of the Liquid CO_2 Washing with Conventional Wash on Firefighters' Personal Protective Equipment (PPE). *Textiles,* 2(4), 624–632. Online: https://doi.org/10.3390/textiles2040036

Horváth, Lilla (2022): Examination of the Application of Currently Used, New or Additional Firefighting Personal Protective Equipment, *AARMS*, 21 (3), 50–52. Online: https://doi.org/10.32565/aarms.2022.3.3

Jeyasubramanian, K. – Hikku, G. S. – Preethi, A. V. M. – Benitha, V. S. – Selvakumar, N. (2016): Fabrication of Water Repellent Cotton Fabric by Coating Nano Particle Impregnated Hydrophobic Additives and Its Characterization. *Journal of Industrial and Engineering Chemistry,* 37, 180–189. Online: https://doi.org/10.1016/j.jiec.2016.03.023

Madsen, Steve – Robbins, Christopher – Robbins, Alyson (2021): *Carbon Dioxide-Based Cleaning of Military Textiles.* Energy Research and Development Division. Final Project Report. Online: www.energy.ca.gov/sites/default/files/2021-12/CEC-500-2021-056.pdf

Martinizing Dry Cleaning: Who invented dry cleaning? https://drycleaningca.com/blog/who-invented-dry-cleaning/

Mayer, C. Alexander – Fent, Kenneth W. – Bertke, Stephen – Horn, Gavin P. – Smith, Denise L. – Kerber, Steve – La Guardia, Mark J. (2019): Firefighter Hood Contamination: Efficiency of Laundering to Remove PAHs and FRs. *Journal of Occupational and Environmental Hygiene,* 16(2), 129–140. Online: https://doi.org/10.1080/15459624.2018.1540877

Pántya, Péter – Horváth, Lilla (2023a): Analysis of the Material Characteristics of Firefighter Personal Protective Clothing. *Hadmérnök,* 18(2), 73–81. Online: https://doi.org/10.32567/hm.2023.2.4

Pántya, Péter – Horváth, Lilla (2023b): Presentation of the Hazardous Environment in the Light of Firefighting Activity. *Műszaki Katonai Közlöny,* 33(1), 85–93. Online: https://doi.org/10.32562/mkk.2023.1.6

Smith, William C. ed. (2010): Overview of Textile Coating and Lamination. In *Smart Textile Coatings and Laminates.* Boca Raton: CRC Press, 3–9. Online: https://doi.org/10.1533/9781845697785.1.3

Sutanto, Stevia – Roosmalen, M. J. E. van – Witkamp, G. J. (2014): Mechanical Action in CO_2 Dry Cleaning. *The Journal of Supercritical Fluids,* 23, 138–143. Online: https://doi.org/10.1016/j.supflu.2013.09.019

Tang, Shufeng – Zhou, Pengfei – Wang, Xu – Yu, Yue – Li, Hualei (2020): Design and Experiment of Dry-Ice Cleaning Mechanical Arm for Insulators in Substation. *Applied Sciences,* 10(7). Online: https://doi.org/10.3390/app10072461

Legal sources

Act XCIII of 1993 on Labour Safety (Hungary)
Act XXXI of 1996 on Fire Protection, Technical Rescue and Fire Brigades (Hungary)

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 3. szám 97–118.
DOI: 10.32567/hm.2024.3.7

Bányász Péter[1]

Dezinformáció az Ipar 4.0 kontextusában

Disinformation in the Context of Industry 4.0

Absztrakt

Az Ipar 4.0 technológiái, különösen az 5G-hálózatok, jelentős előrelépést jelentenek az ipari automatizáció és az okoseszközök integrációja terén. Azonban az új technológiák bevezetését gyakran kísérik álhírek, intenzív dezinformációs kampányok, amelyek aláássák a közvélemény bizalmát, és félelmet keltenek a felhasználók körében, ami kihat a technológia társadalmi elfogadására. Jelen tanulmány célja az 5G-vel kapcsolatos álhírek elemzése, különös tekintettel azok tartalmára és az Ipar 4.0 technológiáival való kapcsolatukra. E tanulmányban a szerző a Snopes.com tényellenőrző oldalon található, 5G kulcsszóval ellátott cikkeket elemezte különböző statisztikai módszertanok segítségével. A tanulmány rámutat arra, hogy az 5G-technológiával kapcsolatos álhírek jelentős hatással lehetnek az Ipar 4.0 technológiák elfogadására és bevezetésére. Az álhírek terjedésének megakadályozása és a közvélemény hiteles tájékoztatása kulcsfontosságú az új technológiák sikeres integrációja érdekében. Az eredmények alapján javaslatokat fogalmazunk meg az álhírek elleni küzdelemre és az Ipar 4.0 technológiáival kapcsolatos dezinformációk kezelésére.

Kulcsszavak: Ipar 4.0, 5G-technológia, dezinformáció, Covid, álhírek, tartalomelemzés

Abstract

The advancement of Industry 4.0 technologies, especially 5G networks, represents a substantial leap in industrial automation and the amalgamation of intelligent devices. However, the introduction of new technologies often accompanies the dissemination of

[1] Egyetemi docens, Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Kiberbiztonsági Tanszék, e-mail: banyasz.peter@uni-nke.hu

false information and deliberate disinformation campaigns that erode public trust and instill apprehension among users, influencing the societal acceptance of the technology. This paper aims to examine disinformation pertaining to 5G and its impact on Industry 4.0 technologies. The author conducted an analysis of articles containing the keyword 5G on the fact-checking site Snopes.com using various statistical approaches. The study illustrates that false information about 5G technology can significantly impede the adoption and implementation of Industry 4.0 technologies. Halting the proliferation of fake news and furnishing reliable information to the public are pivotal for the successful assimilation of new technologies. The findings prompt recommendations to combat misinformation and address fake news concerning Industry 4.0 technologies.

Keywords: industry 4.0, 5G technology, disinformation, COVID, fake news, content analysis

Bevezetés

Az Ipar 4.0 szerepe és jelentősége a modern társadalmakban alapjaiban határozza meg a gazdasági és technológiai fejlődést, amely új kihívások és lehetőségek elé állítja a vállalatokat és a munkavállalókat. Az Ipar 4.0, amelyet gyakran a negyedik ipari forradalomként is emlegetnek, az automatizáció, a digitalizáció és az intelligens technológiák integrációjának köszönhetően újítja meg a gyártási folyamatokat és az üzleti modelleket. Ez a változás nem csupán technológiai, hanem társadalmi és gazdasági szempontból is komoly hatásokkal jár, mivel az új technológiák bevezetése átalakítja a munkaerőpiacot, a munkavégzés módját és a vállalatok közötti versenyt.[2]

A modern társadalmakban az Ipar 4.0 technológiáinak elterjedése elősegíti a termelés hatékonyságának növelését és a költségek csökkentését, miközben lehetővé teszi a termékek és szolgáltatások testreszabását a fogyasztói igényekhez. Az intelligens gyártási rendszerek, a dolgok internete (IoT), a nagy adatok elemzése (big data) és a mesterséges intelligencia (AI) alkalmazása révén a vállalatok képesek valós idejű adatok alapján döntéseket hozni, ami növeli a termelékenységet és csökkenti a hibák számát.[3] Az Ipar 4.0 jelentősége azonban nem merül ki a technológiai fejlődésben. A társadalmi aspektusok is kiemelt figyelmet kapnak, mivel a munkaerő átképzése és a digitális kompetenciák fejlesztése elengedhetetlen a munkaerőpiac változásaihoz való alkalmazkodásban. Az automatizáció és a robotizáció terjedése ugyanis egyes munkahelyek megszűnéséhez vezethet, miközben új munkakörök és szakmák jönnek létre, amelyek magasabb szintű digitális készségeket igényelnek.[4] Az Ipar 4.0 társadalmi jelentőségét tovább növeli az a tény, hogy a technológiai innovációk nem csupán a termelés és a gazdaság területén fejtenek ki hatást, hanem a fenntarthatóság és a környezetvédelem szempontjából is fontos szerepet játszanak. Az intelligens rendszerek és a digitalizáció alkalmazása lehetővé teszi a természeti erőforrások hatékonyabb felhasználását és a hulladéktermelés csökkentését, ami hozzájárul a fenntartható fejlődési célok eléréséhez.[5]

[2] Schwab 2017.
[3] Crawford–Khayyam–Milani 2021.
[4] Brynjolfsson–McAfee 2014.
[5] Wang et al. 2016.

Az 5G-technológia kulcsfontosságú szerepet játszik ebben az átalakulásban, mivel olyan fejlett kommunikációs infrastruktúrát biztosít, amely lehetővé teszi az adatok gyors és megbízható továbbítását, valamint az eszközök és rendszerek valós idejű összekapcsolását. Az 5G-technológia egyik legnagyobb előnye a rendkívül alacsony késleltetés és a magas adatátviteli sebesség. Az 5G-hálózatok képesek másodpercenként akár több gigabitnyi adatot is továbbítani, ami jelentősen meghaladja a korábbi mobilhálózatok képességeit.[6] Ez a megnövekedett sávszélesség és a csökkentett késleltetés lehetővé teszi a gyártási folyamatok valós idejű monitorozását és irányítását, valamint az intelligens eszközök közötti kommunikációt. Az ilyen képességek elengedhetetlenek az Ipar 4.0 számára, ahol az automatizáció és a digitalizáció központi szerepet játszik. Az 5G-technológia támogatja a dolgok internetét, amely az Ipar 4.0 egyik alapvető eleme. Az IoT révén a gyártási eszközök és rendszerek intelligens érzékelőkkel és kommunikációs modulokkal vannak felszerelve, amelyek folyamatosan gyűjtik és továbbítják az adatokat a hálózaton keresztül. Az 5G-hálózatok képesek egyszerre nagyszámú IoT-eszköz támogatására, biztosítva a stabil és gyors adatátvitelt.[7] Ez lehetővé teszi a prediktív karbantartást, ahol az érzékelők által gyűjtött adatok alapján előre jelezhetők a gépek meghibásodásai, így minimalizálva a leállásokat és optimalizálva a termelési folyamatokat.

Az 5G-technológia további előnye a megnövekedett hálózati kapacitás és a sűrűbb hálózati lefedettség, ami különösen fontos a gyártási környezetekben, ahol számos eszköz és rendszer működik egyszerre. Az 5G-hálózatok képesek a hagyományos vezetékes hálózatok teljesítményét nyújtani, miközben rugalmasságot biztosítanak a vezeték nélküli kapcsolat révén. Ez különösen előnyös az ipari automatizáció és a robotizáció területén, ahol a vezeték nélküli kapcsolatok lehetővé teszik a gyártási folyamatok gyors átalakítását és optimalizálását.[8]

A technológiai innovációk gyors ütemű fejlődése alapvetően formálja a modern társadalmakat, ám ezek az újítások csak akkor érhetik el teljes potenciáljukat, ha a társadalom széles körben elfogadja és integrálja őket a mindennapi életbe. Ezt a jelenséget Farkas Tibor is hangsúlyozta a 2023-ban megjelent közleményében.[9]

A technológia társadalmi elfogadása ezért kulcsfontosságú tényező a technológiai fejlesztések sikerében és fenntarthatóságában. Az elfogadás folyamata azonban komplex és számos tényezőtől függ, beleértve a technológia hasznosságának és használhatóságának percepcióját, a felhasználók attitűdjeit, a társadalmi normákat, valamint a gazdasági és politikai környezetet.[10] A technológiai elfogadás egyik alapvető modellje, a *technology acceptance model* (TAM), két fő tényezőt emel ki, amelyek befolyásolják a technológia elfogadását: az észlelt hasznosságot és az észlelt könnyű használhatóságot. Az észlelt hasznosság azt jelenti, hogy a felhasználók mennyire tartják hasznosnak a technológiát saját céljaik elérésében, míg az észlelt könnyű használhatóság azt mutatja meg, hogy mennyire egyszerűnek találják a technológia

[6] Li–Xu–Zhao 2018.
[7] Wollschlaeger–Sauter–Jasperneite 2017.
[8] Park et al. 2018.
[9] Farkas 2023.
[10] Davis 1989.

használatát.[11] Ezek a tényezők közvetlenül befolyásolják a felhasználók szándékát a technológia használatára, ami végső soron meghatározza az elfogadás mértékét.

A társadalmi normák és a társadalmi hatások szintén jelentős szerepet játszanak a technológia elfogadásában. Az egyének hajlamosak figyelembe venni a környezetük véleményét és viselkedését, amikor új technológiát fontolgatnak. A közösségi média és az online platformok korában a társadalmi hatások még erőteljesebbé váltak, mivel az információ gyorsan terjed, és az emberek könnyen befolyásolhatók mások tapasztalatai által.[12] Ezért a pozitív tapasztalatok és visszajelzések elősegíthetik a technológia széles körű elfogadását, míg a negatív tapasztalatok akadályozhatják azt. A technológiai elfogadás gazdasági és politikai tényezői szintén meghatározók lehetnek. A kormányzati támogatások, szabályozások és ösztönzők jelentős mértékben befolyásolhatják a technológia elterjedését. A megfelelő szabályozási keretek és támogatási rendszerek elősegíthetik az új technológiák integrációját, míg a túlzott szabályozás és a támogatások hiánya akadályozhatják azt.[13] A gazdasági tényezők, mint például a technológia ára és a hozzáférhetőség, szintén kritikusak, mivel a magas költségek és az elérhetőség hiánya gátolhatja az elfogadást. A technológia társadalmi elfogadásának jelentősége abban rejlik, hogy ez az elfogadás alapvetően befolyásolja a technológiai innovációk sikerét és fenntarthatóságát. Az elfogadás hiánya nemcsak a technológia elterjedését akadályozza, hanem hosszú távú gazdasági és társadalmi következményekkel is járhat. Az elfogadás elősegítése érdekében fontos, hogy a technológia fejlesztői és bevezetői figyelembe vegyék a felhasználók igényeit és elvárásait, valamint a társadalmi, gazdasági és politikai környezetet is. A felhasználói oktatás és a tudatosság növelése, a pozitív tapasztalatok megosztása, valamint a megfelelő szabályozási keretek kialakítása mind hozzájárulhatnak a technológiai elfogadás növeléséhez és a technológiai innovációk sikeréhez. Az új technológiák elfogadását számos tényező befolyásolja, köztük a közvélemény, a társadalmi normák és a médiában megjelenő információk. Az utóbbi években az álhírek és összeesküvés-elméletek egyre nagyobb szerepet játszanak a közvélemény formálásában, különösen a közösségimédia-platformok terjedésével. Az álhírek és összeesküvés-elméletek jelentős mértékben befolyásolhatják az új technológiák elfogadását, mivel torzítják a valóságot és hamis információkat terjesztenek, amelyek félelmet és bizalmatlanságot keltenek az emberekben.

Az álhírek és összeesküvés-elméletek egyik fő hatása a technológiai innovációkkal szembeni bizalmatlanság növelése. Például az 5G-technológiával kapcsolatban terjedő összeesküvés-elméletek, amelyek szerint az 5G-sugárzás egészségkárosító hatású, vagy akár a Covid–19 terjedéséért is felelős, jelentős mértékben hozzájárulnak ahhoz, hogy az emberek bizalmatlanokká váljanak az új technológiai fejlesztésekkel szemben.[14] Az ilyen típusú információk gyakran gyorsan terjednek a közösségi médiában, és a széles körű elérésük miatt sokan elhiszik őket, még akkor is, ha nincs tudományos alapjuk. Az online közösségi platformokon egyre több bizonytalan hitelességű információ terjed, különösen olyan események kapcsán, mint a Covid–19-járvány vagy az orosz–ukrán konfliktus, ahol a felhasználók ugyan sok információhoz jutnak, de ezek

[11] Venkatesh–Davis 2000.
[12] Ajzen 1991.
[13] Rogers 1983.
[14] Ahmed et al. 2020.

valóságtartalmát gyakran nem ellenőrzik megfelelően.[15] A félelem és bizonytalanság, amelyet az álhírek és összeesküvés-elméletek keltenek, közvetlenül befolyásolja a technológia elfogadását. Az emberek hajlamosak elutasítani vagy vonakodva elfogadni azokat az újításokat, amelyekről negatív vagy ijesztő információkat hallanak. Ez a jelenség különösen igaz lehet olyan technológiákra, amelyek összetettek és nehezen érthetők a nagyközönség számára. A bizonytalanság és a félelem miatt az emberek inkább ragaszkodnak a jól bevált, hagyományos módszerekhez, és ellenállnak az új technológiák bevezetésének.[16] Az álhírek és összeesküvés-elméletek terjedése emellett az észlelt kockázat növekedéséhez vezethet. Az emberek hajlamosak túlbecsülni azokat a kockázatokat, amelyeket gyakran és hangsúlyosan említenek a médiában. Amikor az álhírek és összeesküvés-elméletek folyamatosan negatív következményekről számolnak be, a közvélemény nagyobb kockázatot lát az új technológiákban, mint amennyit valójában jelentenek. Ez a fokozott kockázatészlelés pedig csökkenti az elfogadási hajlandóságot.[17] A technológiai elfogadás szempontjából különösen káros, ha a dezinformáció kormányzati intézkedések vagy hivatalos szervek hitelességét is aláássa. Ha a közvélemény úgy érzi, hogy a kormány vagy más hatóságok nem megbízhatók, vagy hogy ezek az intézmények részesei valamilyen összeesküvésnek, akkor az emberek még inkább ellenállnak az új technológiák bevezetésének. Ez különösen igaz lehet olyan esetekben, amikor a technológiai újítások közvetlen kormányzati támogatást vagy szabályozást igényelnek.[18]

Az 5G-technológia fejlesztése és bevezetése nem csupán technológiai, hanem geopolitikai kérdések szempontjából is relevánsnak tekinthető, különösen az Amerikai Egyesült Államok és Kína közötti versengés fényében. Az 5G-technológia, amely lehetővé teszi a rendkívül gyors adatátvitelt és az alacsony késleltetést, alapvetően átalakíthatja a globális kommunikációs és információs infrastruktúrát, ami stratégiai előnyt jelenthet annak az országnak, amely vezető szerepet tölt be ezen a területen.[19] Az Egyesült Államok és Kína közötti ellentét az 5G-technológia kapcsán elsősorban a nemzetbiztonsági aggályokból fakad. Az amerikai kormány aggodalmát fejezte ki amiatt, hogy a kínai vállalatok, különösen a Huawei, amelyek jelentős szerepet játszanak az 5G-infrastruktúra kiépítésében, potenciális kockázatot jelenthetnek az Egyesült Államok és szövetségesei számára. Az amerikai hatóságok szerint a Huawei eszközei lehetővé tehetik a kínai kormány számára, hogy kémkedjenek az amerikai hálózatokban, és hozzáférjenek érzékeny adatokhoz.[20] Ezen aggodalmak nyomán az Egyesült Államok számos intézkedést hozott a Huawei és más kínai technológiai vállalatok ellen, beleértve a kereskedelmi korlátozásokat és az exporttilalmakat. Kína viszont elutasítja ezeket a vádakat, és azt állítja, hogy az Egyesült Államok geopolitikai okokból próbálja visszaszorítani a kínai technológiai cégek globális térnyerését. Kína azzal érvel, hogy az 5G-technológia terén elért eredményei nemzetközi szabványoknak megfelelően történtek, és hogy a Huawei és más kínai cégek világszerte

15 Ináncsi–Farkas 2022.
16 Sunstein–Vermeule 2008.
17 Allcott–Gentzkow 2017.
18 Flynn–Reifler 2017: 127–150.
19 *America does not want China to dominate 5G mobile networks* 2020.
20 Segal 2020.

versenyképes áron nyújtanak minőségi szolgáltatásokat.[21] Kína továbbá hangsúlyozza, hogy az 5G-technológia fejlesztése és terjesztése kulcsfontosságú a globális gazdasági növekedés és a digitális átalakulás szempontjából, és hogy az Egyesült Államok intézkedései gátolják az innovációt és a globális együttműködést.

Az amerikai–kínai ellentét az 5G-technológia kapcsán nemcsak a két ország közötti viszonyokat befolyásolja, hanem globális szinten is komoly következményekkel jár. Számos ország kénytelen választani az amerikai és a kínai 5G-megoldások között, ami geopolitikai feszültségeket okoz és megosztja a nemzetközi közösséget. Ezen kívül a technológiai szektor szereplői számára is kihívást jelent, hogy hogyan kezeljék a két nagyhatalom közötti versengést és a kapcsolódó szabályozási környezetet.[22] Az 5G-technológia kapcsán kialakult amerikai–kínai ellentét rámutat arra, hogy a technológiai innovációk nem csupán gazdasági és technológiai, hanem politikai és stratégiai szempontból is jelentősek. A versengés kimenetele alapvetően befolyásolhatja a globális technológiai fejlődés irányát és ütemét, valamint a nemzetközi hatalmi egyensúlyt. Ahhoz, hogy a technológiai fejlődés előnyeit maximálisan kihasználhassuk, szükség van a nemzetközi együttműködés és a bizalom erősítésére, valamint a szabályozási keretek és a biztonsági protokollok fejlesztésére.[23]

A fentiek alapján megállapíthatjuk, hogy a koronavírus-járvány idején az 5G-technológia körüli álhírek és dezinformációs kampányok jelentős mértékben befolyásolták a közvélemény percepcióját, ami akadályozza az Ipar 4.0 technológiák elfogadását és bevezetését. A dezinformáció hatására kialakult félelem és bizalmatlanság nemcsak a technológiai innovációk terjedését gátolja, hanem a társadalmi és gazdasági fejlődést is veszélyezteti. Ezen álhírek és összeesküvés-elméletek tartalmi elemzése segít abban, hogy megértsük, hogyan befolyásolják az emberek hozzáállását az 5G és az Ipar 4.0 technológiáihoz.

Ebből fakadóan e tanulmány kutatási célkitűzései ekképp foglalhatók össze:

1. Azonosítani és elemezni az 5G-technológiával kapcsolatos álhírek és dezinformációk főbb narratíváit, különös tekintettel a Covid–19-járvány idején megjelenő tartalmakra.
2. Az 5G-technológiával kapcsolatos álhírek tartalmi elemzése és a Covid–19 előtti és utáni időszakok közötti változások vizsgálata.
3. A leggyakrabban előforduló témák és narratívák feltárása az 5G-technológiával kapcsolatos álhírekben.

A kutatásban három kutatási kérdést jártam körül:

1. Milyen típusú álhírek terjednek leginkább az 5G-technológiával kapcsolatban a Covid–19-járvány idején?
2. Hogyan változott az 5G-technológiával kapcsolatos álhírek gyakorisága és tartalma a Covid–19-járvány előtti és utáni időszakokban?
3. Milyen jellemző témák és narratívák dominálnak az 5G-technológiával kapcsolatos álhírekben?

[21] Segal 2020.
[22] Medeiros 2019.
[23] Maxigas–Oever 2023.

A fentiek alapján a kutatáshoz az alábbi hipotéziseket fogalmaztam meg:

H1: Az 5G-technológiával kapcsolatos álhírek száma jelentősen megnőtt a Covid–19-járvány idején.

H2: Az 5G-technológiával kapcsolatos álhírek többsége egészségügyi kockázatokat és összeesküvés-elméleteket tartalmaz.

H3: Az 5G-technológiával kapcsolatos álhírek gyakran kapcsolódnak sürgősségi helyzetekhez.

Módszertan

Kutatásom első lépéseként a *Snopes.com* nevű tényellenőrző oldalon megjelent cikkeket gyűjtöttem össze és elemeztem különböző statisztikai módszerek segítségével. A *Snopes* 1994-ben indult, kezdetben városi legendák, átverések vizsgálatával, de ahogy nőtt a megbízható tényellenőrzés iránti igény, úgy bővült a *Snopes* csapata is. A *Snopes* a The International Fact-Checking Network része, és megfelel a Hálózat legmagasabb szintű normáinak az online félretájékoztatás elleni küzdelemben.

Az álhírek terjedésének növekedésével párhuzamosan a tényellenőrzés szerepe és jelentősége is egyre hangsúlyosabbá vált a modern információs társadalomban. A tényellenőrzés célja, hogy kiszűrje és cáfolja a hamis információkat, ezáltal helyreállítva a közvélemény hitelességét és bizalmát. A tényellenőrzés rendszere számos feladatot és kihívást foglal magában, amelyek hatékonysága és megbízhatósága döntően befolyásolja a dezinformáció elleni küzdelem eredményességét.

A tényellenőrzés elsődleges feladata a potenciálisan hamis információk azonosítása és kiválasztása. Ez a folyamat magában foglalja a közösségimédia-platformokon és más online forrásokon megjelenő tartalmak szisztematikus áttekintését, amelyek közül azokat választják ki, amelyek nagy valószínűséggel hamis információkat tartalmaznak vagy széles körben terjednek. Az azonosított tartalmakat ezt követően alapos vizsgálatnak vetik alá, amely során különféle módszereket alkalmaznak az információk hitelességének és pontosságának ellenőrzésére.[24] A tényellenőrzés második lépése a források és bizonyítékok elemzése. Ez a folyamat magában foglalja az eredeti források felkutatását és azok hitelességének értékelését, valamint a rendelkezésre álló tudományos és szakmai bizonyítékok összevetését a vizsgált állításokkal. A tényellenőrök különös figyelmet fordítanak a források megbízhatóságára és a bizonyítékok minőségére, hogy biztosítsák az ellenőrzés objektivitását és pontosságát.[25] A tényellenőrzés harmadik lépése az eredmények közzététele és kommunikálása. Az ellenőrzött információkat világosan és érthetően kell bemutatni, hogy a nagyközönség könnyen megérthesse azokat. Az eredmények kommunikációja különféle platformokon történhet, beleértve a tényellenőrző weboldalakat, közösségimédia-felületeket és hagyományos médiumokat is. A tényellenőröknek folyamatosan frissíteniük kell az információkat, hogy reagáljanak az új fejleményekre és biztosítsák az aktuális és releváns tájékoztatást.[26]

[24] Moran 2018.
[25] Vosoughi–Roy–Aral 2018.
[26] Lazer et al. 2018.

Bár a tényellenőrzés számos előnnyel jár, és alapvető fontosságú a dezinformáció elleni küzdelemben, a módszerrel kapcsolatban kritikák is felmerültek. Az egyik leggyakoribb kritika a tényellenőrzés szubjektivitásával és politikai elfogultságával kapcsolatos. Egyes vélemények szerint a tényellenőrök politikai vagy ideológiai meggyőződéseik alapján válogathatnak a vizsgált témák és források között, ami torzíthatja az eredményeket és alááshatja a folyamat hitelességét.[27] További kritika éri a tényellenőrzés hatékonyságát is, különösen a dezinformáció gyors terjedése és az algoritmusok által vezérelt online platformok működése miatt. Az álhírek gyakran gyorsabban terjednek, mint ahogy a tényellenőrök reagálni tudnak rájuk, így a tényellenőrzés gyakran csak utólagos korrekciót jelent, amely nem mindig éri el a széles közönséget.[28] A tényellenőrzés harmadik kritikája az információk komplexitásával és a közönség információfeldolgozási képességeivel kapcsolatos. Az álhírek és összeesküvés-elméletek gyakran egyszerű, érzelmileg töltött narratívák, míg a tényellenőrzés során bemutatott információk bonyolultak és részletesek lehetnek, ami nehezíti azok megértését és elfogadását a közönség számára. Ezenfelül az emberek hajlamosak a már meglévő hiedelmeikhez ragaszkodni, és ellenállnak az ellentétes információknak, még akkor is, ha azok megbízható forrásból származnak.[29] A globális hatalmi elittel kapcsolatos összeesküvés-elméletekben hívők ilyen esetben gyakran racionalizálják az elméleteket, „tudjuk, kik állnak a média mögött, és hogy miért akarják elhallgattatni az igazságot szólókat" – ahogy a gyakori vélemény hangzik el esetükben.

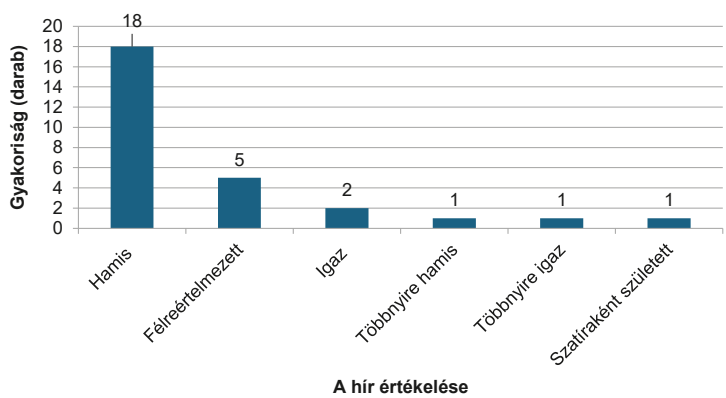
Kutatásom során a *Snopes* adatbázisában szereplő cikkeket vizsgáltam tartalomelemzéssel. A keresés során az 5G és az „5G technology" keresőkifejezéseket alkalmaztam. Az idézőjel operátor alkalmazására azért volt szükség az 5G technology keresőkifejezés esetén, hogy a keresés során a találatoknál figyelembe vegye a két szó közti kontextust, és ne kapjak olyan találatokat, amelyekben a technology kifejezés szerepel, de az 5G nem. A keresést tovább szűkítettem a tényellenőrzés kategóriákra, így az egyéb típusú cikkeket nem vontam be a vizsgálatba. Természetesen az általam definiált keresési kifejezésekre számos kapcsolódó álhír létezik az internet különböző oldalain, jelen kutatásban azonban nem képezte a vizsgálat fókuszát ezen hírek permutációinak, illetve azok terjedésének vizsgálata, kizárólag a tényellenőrzésen átesett hírek elemzését tűztem ki célomul. Ezt követően adattisztítást végeztem, és kiszűrtem a nem releváns találatokat. Az eredeti találati listában számos olyan cikk is megjelent, amelyekben vagy más kontextusban szerepelt az 5G (például a *Margarine vs. Butter: What's Better?*[30] című cikk, amelyben az 5g mint mértékegység jelent meg az összetevők felsorolásakor), vagy az eredeti cikk eltérő témával foglalkozott, és csupán utaltak benne, hogy a bizonyos összeesküvés-elméletben hívők többek között hisznek még az 5G-vel kapcsolatos összeesküvés-elméletekben is (például *Is Beyoncé an Italian Woman Named Ann Marie Lastrassi?*[31]). Ily módon 28 5G-vel kapcsolatos tényellenőrzött cikkből álló adatbázist hoztam létre, amelyben különböző szempontok szerint dolgoztam fel a cikkek tartalmát. Fontos hangsúlyozni, hogy ezt

[27] Lewis–Marwick 2017.
[28] Friggeri et al. 2014.
[29] Nyhan–Reifler 2010.
[30] Mikkelson 2003.
[31] Evon 2020.

a 28 elemből álló mintát nem lehet megfelelően arányosítani az egyébként 5G-vel kapcsolatos álhírek számosságával. Ennek oka, hogy az egyes álhírek folyamatosan mutálódnak, gondoljunk csak az olyan jellegű álhírre, mint hogy az 5G-technológia megöli a madarakat. Az álhírek gyakran oly módon mutálódnak, hogy a „bekövetezett" eseményt egy adott helyszínre lokalizálják, azonban egy másik hírben a helyszín eltérhet. Akárcsak a dátum, amelyre a beszámolóban hivatkoznak. Ebből kifolyólag rendkívül nehéz meghatározni, hogy egy adott témában hány álhírrel is találkozunk. Nem említve itt a nyelvi sajátosságokat, hiszen egy angol nyelven megjelenő álhírt gyakran fordítanak át különböző nyelvekre. Mindez a nagy nyelvi modellek körébe sorolható generatív mesterséges intelligencia megjelenésével nagyobb varianciát tesz lehetővé más nyelvekre való átfordítással. Éppen ezért a kutatásban szükségesnek láttam limitálni a fókuszt kizárólag a tényellenőrzésen átesett tartalmak elemzésére. Ilyen elemzési szempont volt többek között a megjelenés ideje, a tényellenőrzés eredménye, a felhasznált források, illetve az állítások és tényellenőrzés főbb kifejezései, az ellenőrzött hírek kapcsolódó tématerületei. E tanulmányban a tartalomelemzés kapcsán szógyakoriság-vizsgálatokat, illetve klaszteranalízist végeztem Python programnyelv segítségével, amelynek részletesebb ismertetését az adott résznél látom el.

Eredmények

Az 5G-technológiával kapcsolatos álhírek száma a Covid–19 hatására jelentős mértékben megemelkedett. A *Snopes* adatbázisában a 28 tényellenőrzött hírből 4-et azonosíthatunk 2020 előtt. Az első ilyen cikk 2018. november 13-ára datálható *Did a 5G Cellular Network Test Cause Hundreds of Birds to Die?* címmel, ami már a technológia egészségkárosító hatásáról szól, amelynek következtében madarak tömeges pusztulása következett be.[32] A hírt a *Snopes* tényellenőrzői többnyire igazként értékelték. Az 1. ábrán látható az oldal által vizsgált hírek értékelésének eloszlása.



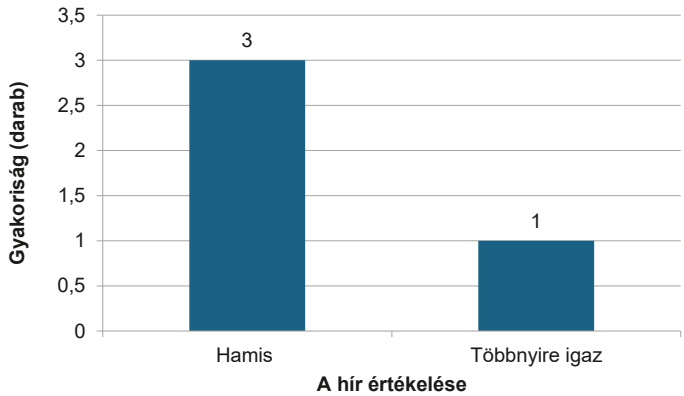
1. ábra: A hírek értékelésének eloszlása
Forrás: a szerző szerkesztése a Snopes alapján

[32] Kasprak 2018.

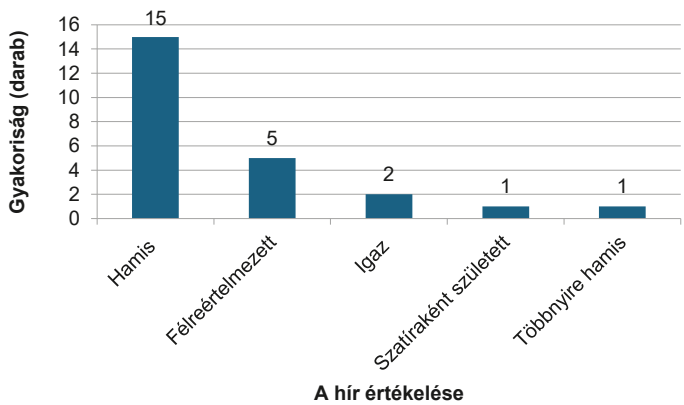
Az 1. ábra az 5G-technológiával kapcsolatos különböző típusú álhírek gyakoriságát szemlélteti. Jól látható, hogy a hamis információk dominálnak (18 darab), messze meghaladva a többi kategóriát. Ez az eloszlás arra utal, hogy az 5G-technológiával kapcsolatos álhírek többsége teljesen hamis állításokat tartalmaz, amelyek torzítják a közvéleményt, és félrevezetik az embereket. A félreértelmezett információk szintén jelentős számban jelennek meg (5 darab), ami arra enged következtetni, hogy az 5G-technológiáról szóló képek és videók gyakran kerülnek ki kontextusukból, hogy megtévesztő narratívákat támogassanak. Az igaz információk alacsony gyakorisága továbbá azt sugallja, hogy a dezinformációs kampányok hatásosak a valódi tények elnyomásában és eltorzításában.

Az álhírekkel kapcsolatos diskurzust nagyban nehezíti a megfelelő fogalmi keret kijelölése, hogy egyáltalán mit értünk álhír alatt. Jelen tanulmánynak ez nem témája, így a *Snopes* meghatározásait veszem alapul. Az értékelések minden esetben az állítás pontos megfogalmazását vizsgálják. Ez alapján a hamis azt jelzi, hogy az állítás elsődleges elemei bizonyítottan hamisak. A többnyire hamis azt jelenti, hogy az állítás elsődleges elemei bizonyítottan hamisak, de az állítást kísérő néhány további részlet pontos lehet. A félreértelmezett minősítést olyan fényképek és videók esetében alkalmazzák, amelyek „valódiak" (azaz részben vagy egészben nem digitális manipuláció termékei), de ennek ellenére félrevezetők, mivel olyan magyarázó anyaggal vannak ellátva, amely hamisan írja le eredetüket, kontextusukat és/vagy jelentésüket. Értelemszerűen az igaz minősítés arra utal, hogy az állítás elsődleges elemei bizonyíthatóan igazak, míg a többnyire igaz esetén azt mutatja, hogy az állítás elsődleges elemei bizonyíthatóan igazak, de az állítást érintő néhány egyéb részlet pontatlan lehet. Az oldal több kategóriát is megkülönböztet, az általam vizsgált tartalmak esetében még csak a szatíraként született értékelés jelenik meg. Ez a minősítés olyan tartalomra vonatkozik, amely eredetileg egy olyan oldalról származik, amelyet úgy jellemeznek, mint szatírát, de később eltávolították belőle a szatirikus jegyeket, átalakították, és máshol tették közzé. A minősítés olyan tartalmakra is vonatkozik, amelyeket nem feltétlenül szatíraként jelöltek meg, de a közönség mégis szatirikusnak érzékelt, mint például a The Onion tartalma. A szatíraként indult kategória jelenléte arra hívja fel a figyelmet, hogy egyes esetekben az eredetileg igaz információk is átalakulnak álhírekké, amikor azokat félreértelmezik vagy szándékosan manipulálják. Ez a jelenség különösen veszélyes, mivel az ilyen típusú álhírek hitelesebbnek tűnhetnek a nagyközönség számára. Összességében kijelenthető, hogy az 5G-technológiával kapcsolatos álhírek többsége hamis vagy félrevezető információkat tartalmaz, ami jelentős kihívást jelent a technológia elfogadása és elterjedése szempontjából. A hamis és félreértelmezett információk nagy száma aláássa a közbizalmat, és növeli a technológia iránti félelmet és ellenállást. Ezen álhírek hatékony kezelése és cáfolata elengedhetetlen ahhoz, hogy az 5G-technológia előnyeit széles körben elismerjék és elfogadják a társadalomban.

A 2. és 3. ábra a vizsgált hírek Covid–19 előtti és utáni időszakok szerinti megoszlását mutatja be.



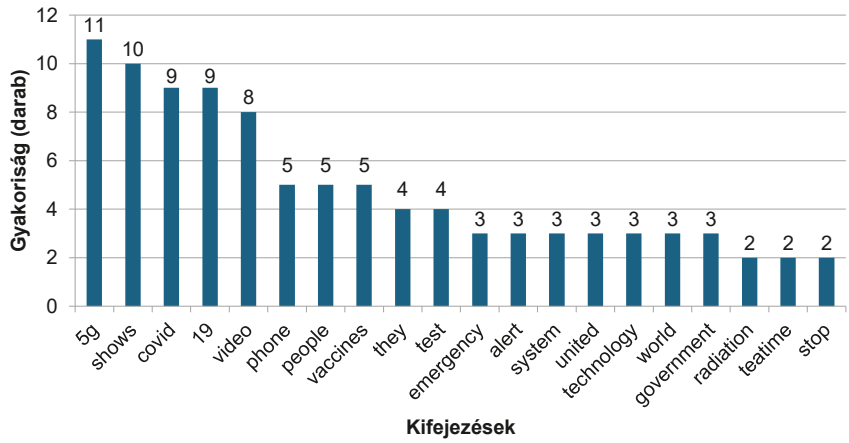
2. ábra: A hírek értékelésének eloszlása a Covid–19 előtti időszakban
Forrás: a szerző szerkesztése a Snopes alapján



3. ábra: A hírek értékelésének eloszlása a Covid–19 utáni időszakban
Forrás: a szerző szerkesztése a Snopes alapján

Következő lépésként az 5G-technológiával kapcsolatos állításokban leggyakrabban előforduló kifejezéseket, illetve bigramokat és trigramokat vizsgáltam. A bigramok olyan szókapcsolatok, amelyek két egymást követő szóból állnak, míg a trigramok három egymást követő szóból állnak, és segítenek feltárni az állítások központi témáit és narratíváit. A vizsgálat eredményei esetében nem fordítottam le magyar nyelvre a kapott kifejezéseket, így az ábrákon eredeti formában, angol nyelven szerepelnek.

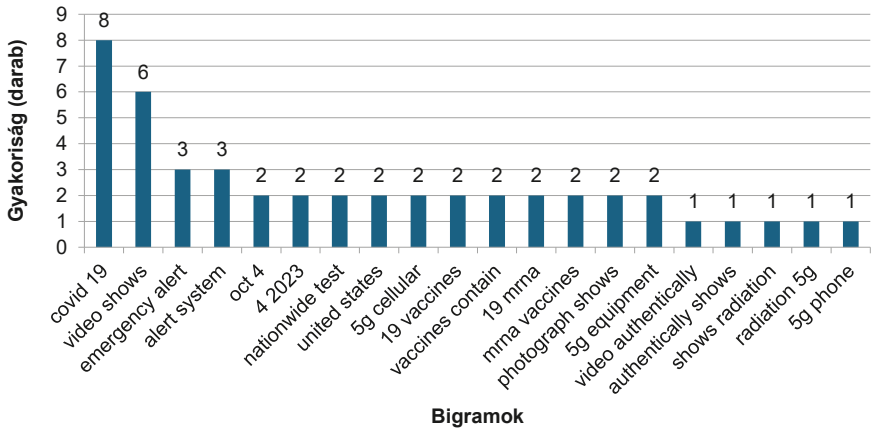
A 4. ábra az 5G-technológiával kapcsolatos állításokban leggyakrabban előforduló szavakat mutatja be, ami betekintést nyújt az álhírek központi témáiba és narratíváiba. Az adatok alapján egyértelműen látható, hogy az „5G" kifejezés dominál, ami természetes, tekintve, hogy ez a technológia áll az álhírek középpontjában. Az „G" mellett a „shows" és a „covid" szavak gyakorisága is kiemelkedő, jelezve, hogy az álhírek gyakran vizuális bizonyítékokra hivatkoznak, és szoros kapcsolatban állnak a Covid–19-járvánnyal.



4. ábra: A 20 leggyakoribb kifejezés
Forrás: a szerző szerkesztése a Snopes alapján

A „video" kifejezés jelenléte arra utal, hogy az állítások gyakran olyan formátumokban jelennek meg, amelyek könnyen hozzáférhetők és megoszthatók a közösségi médiában. Az ilyen vizuális tartalmak erőteljes hatást gyakorolhatnak a közönségre, mivel a videók és képek meggyőzőbbek és emlékezetesebbek lehetnek, mint a szöveges információk. A „people" és a „vaccines" szavak gyakori előfordulása azt jelzi, hogy az álhírek nemcsak az 5G-technológiával, hanem a közegészségügyi kérdésekkel, különösen az oltásokkal kapcsolatos dezinformációs tartalmakat is magukban foglalnak. Az „emergency" és az „alert" kifejezések jelenléte azt mutatja, hogy az állítások gyakran sürgősségi helyzetekre hivatkoznak, hogy fokozzák a közönség érzékenységét és figyelmét. Az ilyen narratívák célja az emberek érzelmi reakcióinak kiváltása, ami növeli az álhírek terjedésének sebességét és hatékonyságát. A „technology" és a „world" szavak gyakorisága arra utal, hogy az álhírek globális perspektívában tárgyalják az 5G-technológiát, és gyakran általánosítanak a technológiai innovációk potenciális hatásairól. A „government" és a „radiation" szavak jelenléte pedig arra utal, hogy az álhírek gyakran kormányzati intézkedésekkel és az 5G-sugárzás állítólagos egészségügyi kockázataival kapcsolatos narratívákat tartalmaznak, amelyek célja a közönség félelmeinek kihasználása.

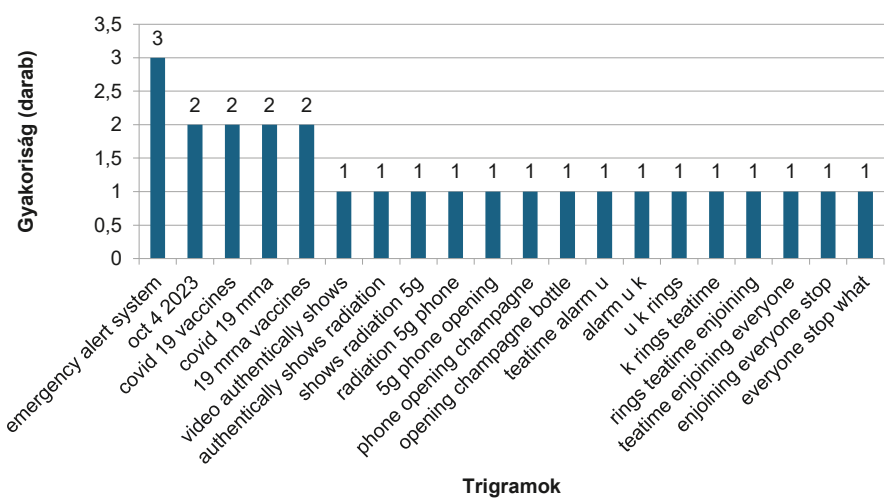
Az 5. ábrán a kiemelt bigramok közül a „covid 19" azonosítható a leggyakoribbnak, ami arra utal, hogy az 5G-technológiával kapcsolatos álhírek szorosan összefonódnak a koronavírus-járvánnyal. Ez az összefüggés megerősíti azt a megfigyelést, hogy a Covid–19-járvány idején az 5G-technológia elleni dezinformációs kampányok jelentős mértékben felerősödtek, és a vírus terjedését gyakran az új technológiával hozták összefüggésbe.



5. ábra: A 20 leggyakoribb bigram
Forrás: a szerző szerkesztése a Snopes alapján

A diagramon látható további gyakori bigramok, mint például a „video shows" és az „emergency alert" és „alert system", azt jelzik, hogy az állítások gyakran vizuális tartalmakra és sürgősségi helyzetekre hivatkoznak. Az ilyen típusú narratívák célja általában az, hogy megerősítsék az álhírek hitelességét és sürgősségét, ezáltal nagyobb hatást gyakorolva a közönségre. Érdekes módon a „19 vaccines" és az „mrna vaccines" bigramok jelenléte azt mutatja, hogy az álhírek nemcsak az 5G-technológiát, hanem az oltásokkal kapcsolatos dezinformációkat is magukban foglalják. Ez a jelenség arra utal, hogy az összeesküvés-elméletek gyakran több, egymással összefüggő témát is felölelnek, és komplex narratívákat építenek fel, amelyek szélesebb közönséget céloznak meg. Az „authenticity shows" és a „video shows" bigramok azt jelzik, hogy az állítások gyakran a hitelesség és a vizuális bizonyítékok bemutatására törekednek. Az ilyen típusú állítások célja, hogy növeljék a közönség bizalmát és meggyőződését az álhírek igazságtartalmáról, miközben gyakran manipulatív technikákat alkalmaznak a meggyőzés érdekében. A „radiation 5g" és az „5g phone" bigramok gyakorisága arra utal, hogy az álhírek gyakran összpontosítanak az 5G-technológia állítólagos egészségügyi kockázataira, főként a sugárzással kapcsolatos félelmekre. Ez a narratíva különösen hatásos lehet, mivel az emberek egészségügyi aggodalmai könnyen kihasználhatók a dezinformációs kampányok során.

A 6. ábra adatai alapján az „emergency alert system" trigram a leggyakoribb, ami arra utal, hogy az 5G-technológiával kapcsolatos álhírek gyakran köthetők sürgősségi helyzetekhez és riasztórendszerekhez. Ez a kombináció valószínűleg célzott pánikkeltést szolgál, mivel az emberek érzékenyen reagálnak a vészhelyzetekkel kapcsolatos információkra.



6. ábra: A 20 leggyakoribb trigram
Forrás: a szerző szerkesztése a Snopes alapján

A „covid 19 vaccines" és a „19 mrna vaccines" trigramok valószínűsítik, hogy az 5G-technológiával kapcsolatos álhírek szorosan összefonódnak a koronavírus-járvánnyal és az oltásokkal. A „video shows authentically" trigram jelenléte megerősíti a szógyakoriság, illetve a bigramok hasonló eredményeit, akárcsak a „shows radiation 5g" és az „5g phone opening" trigramok. Ezek arra utalhatnak, hogy az állítások gyakran konkrét technológiai eszközökre és azok bevezetésére összpontosítanak, különösen a sugárzással kapcsolatos félelmek és a telefonok használata révén. Ez az aspektus valószínűleg arra irányul, hogy közvetlenül befolyásolja a közönség technológiával kapcsolatos percepcióját és felhasználási szokásait.

A „teatime alarm uk" trigram jelenléte pedig arra utalhat, hogy az álhírek gyakran geopolitikai kontextusban jelennek meg, különös tekintettel az Egyesült Királyságra és annak technológiai fejlesztéseire. Érdekes módon a „rings teatime enjoining" és az „enjoining everyone stop" trigramok gyakorisága jelezheti, hogy az álhírek bizonyos kulturális vagy regionális specifikumokra is hivatkoznak, amelyeket a helyi közönség jobban megérthet és elfogadhat. Az ilyen narratívák célja valószínűleg az, hogy növeljék a dezinformáció hitelességét és relevanciáját a célcsoport számára. Korábbi kutatásaim alapján az Egyesült Királyság ilyen irányú szereplése nem tűnik véletlennek, ugyanis a Covid–19 és 5G kifejezések szentimentanalízissel való elemzése azt mutatta, hogy az Egyesült Királyságban jelentősen nagyobb számban terjedtek a témával kapcsolatos álhírek, ami arra vezetett, hogy 2020 áprilisában 77 5G átjátszó tornyot gyújtottak fel az országban a Covid–19 miatti félelem okán.[33]

Összességében e három diagram eredményei azt mutatják, hogy az 5G-technológiával kapcsolatos álhírek többféle narratívát és témát ölelnek fel, amelyek célja a közönség félelmeinek és bizonytalanságainak kihasználása. Az ilyen típusú dezinformációs

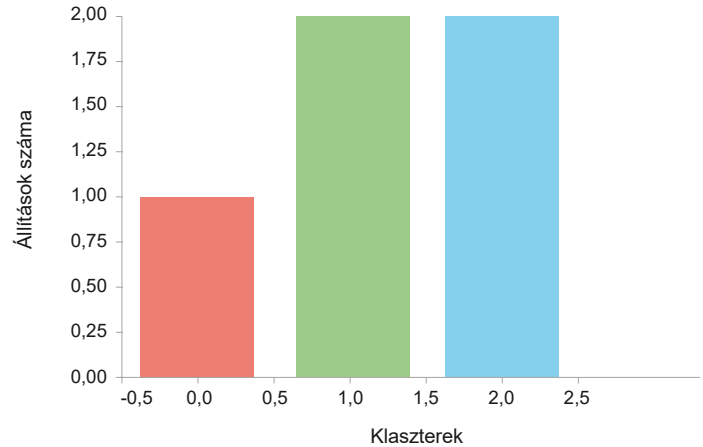
[33] Bányász–Tóth–László 2022.

tartalmak terjedésének megakadályozása érdekében elengedhetetlen a folyamatos oktatás és tájékoztatás, valamint a hiteles információk terjesztése, hogy ellensúlyozzuk az álhírek negatív hatásait és támogassuk a technológiai innovációk társadalmi elfogadását.

A klaszterelemzés célja az volt, hogy azonosítsam a hasonló jellegű állításokat az 5G-technológiával kapcsolatos álhírek között. Az elemzéshez az állításokban szereplő szöveges adatokat használtam fel, és Pyhtonban először szöveges adatokat TF-IDF- *(term frequency-inverse document frequency)* mátrixszá alakítottam, hogy a szavak előfordulási gyakorisága és fontossága alapján számszerűsíthetővé alakítsa az adatokat. A TF-IDF egy súlyozási technika, amely meghatározza egy szó fontosságát egy dokumentumban a teljes dokumentumgyűjtemény figyelembevételével. A TF-IDF két fő összetevőből áll: a *term frequency* (TF), amely a szó gyakoriságát méri a dokumentumban, és az *inverse document frequency* (IDF), amely a szó ritkaságát méri a teljes dokumentumgyűjteményben. A TF-IDF-súlyt úgy számítják ki, hogy a TF értékét megszorozzák az IDF értékével, ezáltal nagyobb súlyt adva a ritkább és gyakrabban előforduló szavaknak. Előnyei közé tartozik, hogy hatékonyan azonosítja a fontos szavakat és egyszerűen implementálható. Hátrányai között szerepel, hogy nem kezeli a szinonimákat és többjelentésű szavakat, valamint nagy dokumentumgyűjtemények esetén számításigényes lehet. A TF-IDF széles körben alkalmazható keresőmotorok optimalizálására, dokumentumok szegmentálására és kulcsszavak azonosítására.

Ezt követően k-means algoritmust alkalmaztam a TF-IDF-mátrixon. A k-means algoritmus egy népszerű klaszterezési módszer, amely az adatpontokat \(k\) darab előre meghatározott számú klaszterbe rendezi, minimalizálva a klasztereken belüli adatpontok közötti távolságot. Az algoritmus kezdetben véletlenszerűen választ ki \(k\) adatpontot klaszterközéppontként, majd minden adatpontot a legközelebbi centroidhoz rendel. Az új centroidokat a klaszterekben lévő pontok átlagaként számítja ki, és ezt a folyamatot iterálja a konvergenciáig. Előnyei közé tartozik az egyszerűsége és gyorsasága, valamint az eredmények könnyű értelmezhetősége. Hátrányai között szerepel a klaszterszám előzetes meghatározásának szükségessége és az érzékenység a kezdeti értékekre. A k-means algoritmust széles körben alkalmazzák a marketingszegmentációtól kezdve a kép- és videófeldolgozásig. Az algoritmus feltételezi, hogy a klaszterek gömb alakúak és hasonló méretűek, ami korlátokat jelenthet bizonyos adathalmazok esetén. Az iteratív folyamat a klaszterek homogenitásának növelésére szolgál. Az alkalmazási területek sokfélesége mellett fontos figyelembe venni az algoritmus sajátosságait és korlátait.

Az optimális klaszterek számát (k=3) választottam, amely három jól elkülöníthető csoportot eredményezett (lásd 7. ábra).



7. ábra: Az 5G-vel kapcsolatos állítások klaszterei
Forrás: a szerző szerkesztése Python használatával, Snopes alapján

A 7. ábrán az alábbi három klasztert azonosíthatjuk:

1. Fantasztikus és abszurd állítások (piros oszlop, klaszter 0): az első klaszterhez tartozó állítások, amelyek fantasztikus vagy abszurd elemeket tartalmaznak, viszonylag kevesebb előfordulással jelennek meg az ábrán. Az elemzés során 1 elemet azonosítottam ebben a klaszterben, az összes elem 20%-át teszi ki. Ezek az állítások gyakran látványos, de valóságtól elrugaszkodott elemeket tartalmaznak, és céljuk a szenzációkeltés. Ilyen például az a hír, ami videós bizonyítékot ígér, hogy az 5G okozta sugárzás felrobbant egy üveg pezsgőt (*Champagne Bottle Exploded Due to 5G Phone Radiation?*[34]).
2. Politikai és egészségügyi dezinformáció (zöld oszlop, klaszter 1): a második klaszterhez tartozó állítások száma jelentős, és ezek főként politikai vagy egészségügyi vonatkozású dezinformációkat tartalmaznak. Ez a klaszter 2 elemet tartalmaz, amelyek az összes elem 40%-át képviselik. Ezek az állítások gyakran politikai célokat szolgálnak, vagy félelmet keltenek az egészségügyi kockázatokkal kapcsolatban. Példaként említhető a hír, ami szerint Vlagyimir Putyin orosz elnök betiltja az 5G-tornyok kiépítését egészségügyi megfontolásokból (*Did Putin Ban 5G in Russia Due to Health Concerns?*[35]).
3. Tényalapú információk (kék oszlop, klaszter 2): a harmadik klaszterhez tartozó állítások száma szintén jelentős, és ezek valós eseményeken alapulnak, valamint hiteles forrásokat is megjelölnek. A klaszter szintén 2 elemet tartalmaz, az összes elem 40%-át. Ezek az állítások hiteles információkat közvetítenek és gyakran tájékoztató jellegűek. Például, amiben szakértőkre hivatkozva tanácsolják a családon belüli erőszak áldozatainak, hogy az amerikai katasztrófavédelem,

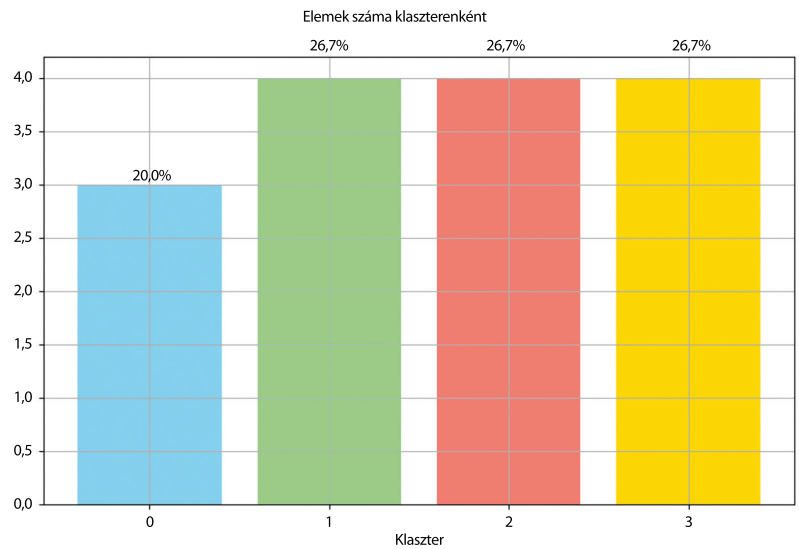
[34] Eifert 2024.
[35] Kasprak 2023b.

a FEMA vészhelyzeti gyakorlata idején ne használják a telefonjukat (*FEMA To Test Emergency Alert System Nationwide on Oct. 4, 2023?*[36]).

Az ábrán látható klaszterek eloszlása azt jelzi, hogy az 5G-technológiával kapcsolatos álhírek többsége politikai és egészségügyi dezinformáció (zöld oszlop), míg a fantasztikus és abszurd állítások száma (piros oszlop) kisebb. A tényalapú információk (kék oszlop) szintén jelentős számban vannak jelen, ami arra utal, hogy ezek a hiteles információk is fontos szerepet játszanak az álhírek kontextusában.

A klaszterelemzést elvégeztem az Ipar 4.0 kontextusában is. Ennek érdekében a fenti eljárásba egy plusz lépést illesztettem, ami az Ipar 4.0-hoz kapcsolódó kifejezések azonosítására vonatkozott. Emellett az úgynevezett Elbow-módszert is alkalmaztam, ami segített a klaszterek számának meghatározásában.

A 8. ábrán tüntettem fel a klaszterelemzés eredményeit.



8. ábra: Az 5G-vel kapcsolatos állítások klaszterei az Ipar 4.0 kontextusában
Forrás: a szerző szerkesztése Python használatával, Snopes alapján

Az Ipar 4.0 kontextusában négy klasztert azonosíthatunk:

1. Politikai álhírek (kék oszlop, klaszter 0): ez a klaszter főként politikai vezetőkkel és döntéshozókkal kapcsolatos hamis állításokat tartalmaz. Az ilyen típusú álhírek célja gyakran a politikai szereplők hiteltelenítése vagy népszerűsítése, illetve a közvélemény manipulálása. Az elemzés során 3 elemet azonosítottam ebben a klaszterben, amelyek az összes elem 20%-át teszik ki. Példa erre az a hír, amely szerint Vlagyimir Putyin orosz elnök betiltotta az 5G-mobilhálózatokat (*Did Putin Ban 5G in Russia Due to Health Concerns?*[37]).

[36] Emery 2023.
[37] Kasprak 2023b.

2. Egészségügyi álhírek (zöld oszlop, klaszter 1): ebben a klaszterben találhatók azok az álhírek, amelyek az egészségüggyel kapcsolatban téves információkat terjesztenek. Különösen gyakoriak a vakcinákkal és azok hatásaival kapcsolatos álhírek. Ez a klaszter 4 elemet tartalmaz, amelyek az összes elem 26,7%-át képviselik. Példaként említhető az a hír, amely szerint a Covid–19-vakcinával oltakozott emberek feje felrobban (*Does Video Show Vaxxed Heads Exploding Due to 5G in Israel?*[38]).
3. Összeesküvés-elméletek (piros oszlop, klaszter 2): ez a klaszter különféle összeesküvés-elméleteket tartalmaz, amelyek gyakran globális konspirációkra és a technológia veszélyeire összpontosítanak. Az ilyen típusú álhírek célja általában a félelemkeltés és a bizonytalanság terjesztése. A klaszter szintén 4 elemet foglal magában, az összes elem 26,7%-át. Ilyen például az az álhír, amely az ENSZ Agenda 21/2030 programját hamisan új világrendként értelmezi (*Is 'UN Agenda 21/2030' Proposing 'End of Family Unit' and 'Government Raised Children' Real?*[39]).
4. Technológiai álhírek (sárga oszlop, klaszter 3): Ebben a klaszterben találhatók azok az álhírek, amelyek a technológiai fejlesztésekkel és azok állítólagos negatív következményeivel kapcsolatosak. Az ilyen álhírek gyakran az új technológiák iránti bizalmatlanságot és félelmet igyekeznek kihasználni. A klaszter szintén 4 elemet tartalmaz, az összes elem 26,7%-át. Példa erre az az álhír, amely szerint az 5G-technológia komoly egészségügyi problémákat okoz (*Did a 5G Cellular Network Test Cause Hundreds of Birds to Die?*[40]).

Diszkusszió

A kutatás eredményei megerősítették, hogy az 5G-technológiával kapcsolatos álhírek és dezinformációs tartalmak jelentős mértékben elterjedtek a Covid–19-járvány idején. Az 5G-technológiáról szóló álhírek gyakorisága és intenzitása nagymértékben nőtt a pandémia idején, ami összhangban áll az első hipotézissel, miszerint az álhírek száma jelentősen emelkedett a Covid–19-járvány alatt. Az elemzett adatokból kiderült, hogy a *Snopes* adatbázisában található 28 tényellenőrzött hír közül 24-et a Covid–19-járvány idején vagy azt követően publikáltak, ami egyértelműen mutatja az álhírek számának növekedését ebben az időszakban. Az álhírek tartalmi elemzése során az is világossá vált, hogy ezek nagy része egészségügyi kockázatokra és összeesküvés-elméletekre fókuszált. Az álhírek jelentős része az 5G-technológia állítólagos egészségügyi kockázatait emelte ki, különösen a sugárzás hatásaival kapcsolatban, és gyakran kapcsolta össze a technológiát a Covid–19-járvány terjedésével. Ez az eredmény alátámasztja a második hipotézist, miszerint az 5G-technológiával kapcsolatos álhírek többségében egészségügyi kockázatok és összeesküvés-elméletek szerepeltek. Az álhírek 40%-a politikai és egészségügyi dezinformációkat tartalmazott, míg 26,7%-a

[38] Evon 2022.
[39] Kasprak 2023a.
[40] Kasprak 2018.

összeesküvés-elméleteket propagált, ami megerősíti ezen narratívák dominanciáját az álhírekben.

Az álhírek narratíváinak részletes vizsgálata azt is kimutatta, hogy gyakran sürgősségi helyzetekhez és riasztórendszerekhez kapcsolódnak, hogy növeljék a pánikkeltés hatékonyságát. Az elemzés során a leggyakrabban előforduló trigramok között az „emergency alert system" szerepelt a legtöbbször, jelezve, hogy az álhírek gyakran használják a sürgősségi helyzetekhez kapcsolódó narratívákat a közönség befolyásolására. Ez az eredmény alátámasztja a harmadik hipotézist, miszerint az 5G-technológiával kapcsolatos álhírek gyakran kapcsolódnak sürgősségi helyzetekhez.

A kutatás további eredményei azt mutatják, hogy az álhírek terjedése és a tényellenőrzés között fennálló időbeli különbségek kihívást jelentenek a dezinformáció hatékony kezelésében. Az álhírek gyakran gyorsabban terjednek, mint ahogy a tényellenőrök reagálni tudnak rájuk, így a tényellenőrzés gyakran csak utólagos korrekciót jelent, amely nem mindig éri el a széles közönséget. Ezenkívül a tényellenőrzés során bemutatott információk bonyolultsága és részletessége is nehezíti azok megértését és elfogadását a közönség számára, különösen azokban az esetekben, amikor az álhírek egyszerű, érzelmileg töltött narratívákat kínálnak.

Ily módon a kutatás tézisei ekképp foglalhatók össze:

T1: A *Snopes* adatbázisában található 28 tényellenőrzött hír közül 24-et a Covid–19-járvány idején vagy azt követően publikáltak, ami jelentős növekedést mutat az álhírek számában ebben az időszakban.

T2: Az elemzett álhírek 40%-a politikai és egészségügyi dezinformációkat tartalmazott, míg 26,7%-a összeesküvés-elméleteket propagált, amelyek főként az 5G-technológia egészségügyi kockázataira és globális összeesküvésekre fókuszáltak.

T3: Az elemzés során a leggyakrabban előforduló trigramok között az „emergency alert system" szerepelt a legtöbbször, jelezve, hogy az álhírek gyakran használják a sürgősségi helyzetekhez kapcsolódó narratívákat a közönség befolyásolására.

A dezinformáció elleni küzdelem hatékonyságának növelése érdekében elengedhetetlen a közvélemény folyamatos és hiteles tájékoztatása, valamint a tényellenőrzési módszerek fejlesztése. A hiteles információk terjesztése, a közösségimédia-platformok megfelelő szabályozása és a folyamatos oktatás mind hozzájárulhatnak az álhírek negatív hatásainak csökkentéséhez és az 5G-technológia társadalmi elfogadásának növeléséhez. Összességében a kutatás rámutatott arra, hogy az 5G-technológiával kapcsolatos álhírek jelentős kihívást jelentenek az Ipar 4.0 technológiák elfogadása és bevezetése szempontjából. Az álhírek hatékony kezelése és cáfolata kulcsfontosságú ahhoz, hogy az 5G-technológia előnyeit széles körben elismerjék és elfogadják a társadalomban. A további kutatások célja lehet a dezinformáció elleni stratégiák kidolgozása és a tényellenőrzési módszerek hatékonyságának növelése, hogy a technológiai innovációk sikeresen integrálódhassanak a társadalomba.

Felhasznált irodalom

Ahmed, Wasim et al. (2020): COVID-19 and the 5G Conspiracy Theory: Social Network Analysis of Twitter Data. *Journal of Medical Internet Research,* 22(5), e19458. Online: https://doi.org/10.2196/19458

Ajzen, Icek (1991): The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes,* 50(2), 179–211. Online: https://doi.org/10.1016/0749-5978(91)90020-T

Allcott, Hunt – Gentzkow, Matthew (2017): Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives,* 31(2), 211–236. Online: https://doi.org/10.1257/jep.31.2.211

America Does Not Want China to Dominate 5G Mobile Networks. *The Economist*, 2020. április 8. Online: www.economist.com/business/2020/04/08/america-does-not-want-china-to-dominate-5g-mobile-networks

Bányász Péter – Tóth András – László Gábor (2022): A koronavírus oltással kapcsolatos állampolgári attitűd vizsgálata szentimentanalízis segítségével. *Információs Társadalom,* 22(1), 99. Online: https://doi.org/10.22503/inftars.XXII.2022.1.6

Brynjolfsson, Erik – McAfee, Andrew (2014): *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. W. W. Norton.

Crawford, Bryan – Khayyam, Hamid – Milani, Abbas (2021): A Mini-Review and Perspective on Current Best Practice and Emerging Industry 4.0 Methods for Risk Reduction in Advanced Composites Manufacturing. *Open Journal of Composite Materials,* 11(2), 31–45. Online: https://doi.org/10.4236/ojcm.2021.112004

Davis, Fred D. (1989): Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly,* 13(3), 319–340. Online: https://doi.org/10.2307/249008

Eifert, Sean (2024): Champagne Bottle Exploded Due to 5G Phone Radiation? *Snopes,* 2024. június 24. Online: www.snopes.com/fact-check/5g-radiation-champagne/

Emery, David (2023): FEMA To Test Emergency Alert System Nationwide on Oct. 4, 2023? *Snopes,* 2023. szeptember 6. Online: www.snopes.com/fact-check/fema-to-test-emergency-alert-system-nationwide-on-oct-4/

Evon, Dan (2020): Is Beyoncé an Italian Woman Named Ann Marie Lastrassi? *Snopes,* 2020. július 7. Online: www.snopes.com/fact-check/beyonce-is-italian/

Evon, Dan (2022): Does Video Show Vaxxed Heads Exploding Due to 5G in Israel? *Snopes,* 2022. január 4. Online: www.snopes.com/fact-check/5g-israel-heads-explode/

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.

Flynn, Brendan N. – Reifler, Jason (2017): The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics. *Political Psychology,* 38(S1), 127–150. Online: https://doi.org/10.1111/pops.12394

Friggeri, Adrien et al. (2014): Rumor Cascades. *Proceedings of the International AAAI Conference on Web and Social Media,* 8(1), 101–110. Online: https://doi.org/10.1609/icwsm.v8i1.14559

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
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/
Kasprak, Alex (2023a): Did Putin Ban 5G in Russia Due to Health Concerns? *Snopes,* 2023. augusztus 7. Online: www.snopes.com/fact-check/putin-ban-5g/
Kasprak, Alex (2023b): Is 'UN Agenda 21/2030' Proposing 'End of Family Unit' and 'Government Raised Children' Real? *Snopes,* 2023. április 27. Online: www.snopes.com/fact-check/un-agenda-21-2030/
Lazer, David M. et al. (2018): The Science of Fake News. *Science,* 359(6380): 1094–1096. Online: https://doi.org/10.1126/science.aao2998
Lewis, Becca – Marwick, Alice E. (2017): Media Manipulation and Disinformation Online. *Data & Society,* 2017. május 15. Online: https://datasociety.net/library/media-manipulation-and-disinfo-online/
Li, Shancang – Xu, Li Da – Zhao, Shanshan (2018): 5G Internet of Things: A survey. *Journal of Industrial Information Integration,* 10, 1–9. Online: https://doi.org/10.1016/j.jii.2018.01.005
Maxigas – Oever, Niels ten (2023): Geopolitics in the Infrastructural Ideology of 5G. *Global Media and China,* 8(3), 271–288. Online: https://doi.org/10.1177/20594364231193950
Medeiros, Evan S. (2019): The Changing Fundamentals of US-China Relations. *The Washington Quarterly,* 42(3), 93–119. Online: https://doi.org/10.1080/0163660X.2019.1666355
Mikkelson, Barbara (2003): Margarine vs. Butter: What's Better? *Snopes,* 2003. július 18. Online: www.snopes.com/fact-check/the-butter-truth/
Moran, Rachel E. (2018): Deciding What's True: The Rise of Political Fact-Checking in American Journalism. *New Media & Society,* 20(12), 4832–4834. Online: https://doi.org/10.1177/1461444818795694
Nyhan, Brendan – Reifler, Jason (2010): When Corrections Fail: The Persistence of Political Misperceptions. *Political Behavior,* 32(2), 303–330. Online: https://doi.org/10.1007/s11109-010-9112-2
Park, Pangun et al. (2018): Wireless Network Design for Control Systems: A Survey. *IEEE Communications Surveys & Tutorials,* 20(2), 978–1013. Online: https://doi.org/10.1109/COMST.2017.2780114
Rogers, Everett M. (1983): *Diffusion of Innovations*. 3rd ed. New York – London: Free Press – Collier Macmillan.
Schwab, Klaus (2017): *The Fourth Industrial Revolution*. [h. n.]: Crown Currency.
Segal, Adam (2020): The Coming Tech Cold War With China. *Foreign Affairs,* 2020. szeptember 9. Online: www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china
Segal, Adam (2024): Year in Review: Huawei and the Technology Cold War. *Council on Foreign Relations*. www.cfr.org/blog/year-review-huawei-and-technology-cold-war (2024. július 24.).

Sunstein, Cass R. – Vermeule, Adrian (2008): Conspiracy Theories: Causes and Cures. *Journal of Political Philosophy,* 17(2), 202–227. Online: https://doi.org/10.1111/j.1467-9760.2008.00325.x

Venkatesh, Viswanath – Davis, Fred D. (2000): A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science,* 46(2), 186–204. Online: https://doi.org/10.1287/mnsc.46.2.186.11926

Vosoughi, Soroush – Roy, Deb – Aral, Sinan (2018): The Spread of True and False News Online. *Science,* 359(6380): 1146. Online: https://doi.org/10.1126/science.aap9559

Wang, Shiyong et al. (2016): Towards Smart Factory for Industry 4.0: A Self-Organized Multi-Agent System With Big Data Based Feedback and Coordination. *Computer Networks,* 101, 158–68. Online: https://doi.org/10.1016/j.comnet.2015.12.017

Wollschlaeger, Martin – Sauter, Thilo – Jasperneite, Juergen (2017): The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. *IEEE Industrial Electronics Magazine,* 11(1), 17–27. Online: https://doi.org/10.1109/MIE.2017.2649104

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 3. szám 119–135.
DOI: 10.32567/hm.2024.3.8

Bederna Zsolt[1]

A mesterségesintelligencia-rendszerek megfelelősége

Compliance of Artificial Intelligence Systems

Absztrakt

A különféle mesterségesintelligencia- (MI) alapú megoldások terjedése következtében elengedhetetlenné vált az MI-rendszerek által jelentett kockázatok megértése és menedzselése. A tanulmány szisztematikusan vizsgálja az MI által képviselt kockázati profilokat, hangsúlyozva a személyre szabott kockázatkezelési stratégiák és etikai megközelítések jelentőségét.
Az elemzés feltárja a magas kockázatú MI-rendszerek kihívásainak jellegét, amelyek szigorú szabályozási megfelelést tesznek szükségessé a lehetséges káros következmények megakadályozása, illetve mérséklése érdekében, míg a jogalkotó ösztönzi a vonatkozó kötelezettségek teljesítését az alacsonyabb kockázatú MI-rendszerek esetén az átláthatóság és az elszámoltathatóság vonatkozásában.
Jelen tanulmány részletes áttekintést nyújt az MI kockázati tényezőiről, amelyek befolyásolják az adatok integritását, a modellek pontosságát, a folyamatok és eredmények megbízhatóságát, valamint a felhasználói interakciót.

Kulcsszavak: mesterséges intelligencia, Európai Unió, kockázatok, irányítási rendszerek, kiberbiztonság

Abstract

Due to the proliferation of various artificial intelligence (AI) solutions, understanding and managing the risks posed by AI systems has become essential. This study systematically

[1] Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Kiberbiztonsági Tanszék, e-mail: bederna.zsolt@bederna.hu

examines the risk profiles represented by AI, emphasizing the importance of personalized risk management strategies and ethical approaches.
The analysis reveals the nature of challenges posed by high-risk AI systems, which require strict regulatory compliance to prevent or mitigate potential harmful consequences, while lawmakers encourage the fulfilment of relevant obligations regarding transparency and accountability for lower-risk AI systems. The AI legislation mandates that providers of high-risk AI systems establish and operate an AI governance system that integrates quality management, information security, and data protection.
The paper provides a detailed overview of AI risk factors that affect data integrity, model accuracy, the reliability of processes and outcomes, as well as user interaction.

Keywords: artificial intelligence, European Union, risks, management systems, cybersecurity

Bevezetés

A mesterséges intelligencia (MI) múltját jellemző fellendülések és hullámvölgyek változó természete ellenére a jelenlegi trendek azt mutatják, hogy az MI-t az élet egyre több területén alkalmazzák, mint például az ipar, a gyártás, az egészségügy, az adatelemzés. Ennek oka az MI képességbeli és teljesítményét érintő fejlődése, amelynek alapját a mögöttes elmélet és algoritmus, valamint az információs és kommunikációs technológia (IKT) számítási kapacitásának fejlődése képezi.[2]

Az Európai Unió a mesterséges intelligenciát a digitális stratégiája részeként szabályozza azzal a céllal, hogy jobb feltételeket biztosítson a technológia fejlesztéséhez és használatához, illetve csökkentse az MI-rendszerek által jelentett kockázatokat. Az Európai Bizottság 2022-ben terjesztette elő az Európa digitális évtizede szakpolitikai programját,[3] amely konkrét célokat és célkitűzéseket tartalmaz 2030-ra az EU egyik prioritásának számító digitális átalakulással kapcsolatos területeken. A program magában foglalja (1) a digitális készségekbe való befektetést Európa új digitális technológiákkal kapcsolatos kapacitásainak megerősítése érdekében, (2) az emberek kiberfenyegetésekkel szembeni védelmét, a kiberbiztonsági szint és a kapcsolódó képességek javítását, (3) az ultragyors széles sávú internet elterjedésének felgyorsítását, (4) Európa szuperszámítógép-kapacitásának bővítését az orvostudomány, a közlekedés és a környezetvédelem terén történő innovatív megoldások kidolgozása érdekében és (5) annak biztosítását, hogy az MI fejlesztése az emberek jogainak tiszteletben tartásával történjen.

2021 áprilisában az Európai Bizottság javaslatot tett az MI szabályozási keretére.[4] A Mesterséges intelligenciáról szóló jogszabály[5] javaslatát várhatóan 2024 harmadik negyedévében fogadják el. Uniós szinten létrejött a tagállamok és a Bizottság képviselőiből álló Mesterséges Intelligenciával Foglalkozó Európai Hivatal, amely összegyűjti és megosztja a legjobb gyakorlatokat a tagállamok között. Nemzeti

[2] Jiang et al. 2022.
[3] *Az Európai Parlament és a Tanács (EU) 2022/2481 határozata.*
[4] Council of the European Union 2024.
[5] Európai Parlament 2024.

szinten a tagállamoknak ki kell jelölniük egy vagy több nemzeti illetékes hatóságot, amelyek közül a nemzeti felügyeleti hatóság felügyeli a jogszabály alkalmazását és a végrehajtását.

Jelen tanulmánnyal a szerző az MI-rendszerek ellenében az Európai Unió által megfogalmazott jogszabályi kötelezettségek, valamint az MI-rendszerek által jelentett és a működésüket jellemző kockázatok áttekintését és elemzését tűzi ki célul.

E célok elérése érdekében a szerző előbb a módszertant ismerteti, majd áttekinti a mesterséges intelligencia kockázati profiljait, a kötelezettségeket és a vonatkozó irányítási rendszereket. Ezután az MI-rendszerekkel összefüggésbe hozható információbiztonsági, adatvédelmi, illetve minőségi elvárásokat, a kapcsolódó irányítási rendszerek összefüggéseit elemzi. Továbbá az MI-rendszerek által jelentett, valamint az MI-rendszerekre hatással lévő kockázatokat vizsgálja. A cikk összegzéssel és konklúzióval zárul.

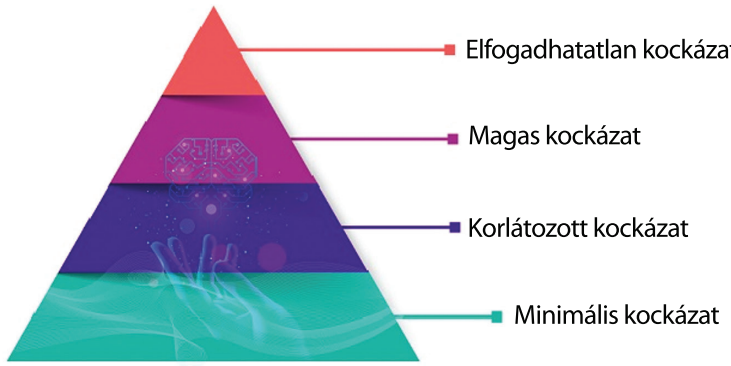
Módszertan

Elsődlegesen az MI-vonatkozású európai uniós jogszabályok, nemzetközi szabványok, illetve a hazai és nemzetközi releváns szakirodalom feldolgozásával azonosítjuk és rendszerezzük a jogszabályi kötelezettségeket. A jogalkotó által a Mesterséges intelligenciáról szóló jogszabályban megfogalmazott elvárt kötelezettségek és az ISO/IEC 42001 szabvány tekintetében összehasonlító elemzést végzünk annak érdekében, hogy azonosítani tudjuk más szakterületekkel (úgymint adatvédelem és kiberbiztonság) a kapcsolódási pontokat, valamint az elvárt kockázatkezelési megközelítést. Végezetül az MI-rendszerek által jelentett és a működésüket jellemző kockázatok átfogó elemzését, kategorizálását valósítjuk meg.

Jogszabályi áttekintés

Mesterséges intelligencia kockázati profilok

A Mesterséges intelligenciáról szóló jogszabály kimondja, hogy a különböző alkalmazásokban használható MI-rendszereket négy kockázati osztályba kell besorolni aszerint, hogy milyen kockázatot jelentenek a felhasználók számára. A jogalkotó négy kockázati szintet határozott meg: (1) minimális kockázat, (2) korlátozott kockázat, (3) magas kockázat és (4) elfogadhatatlan kockázat (1. ábra).



1. ábra: Mesterséges intelligencia kockázati profilok
Forrás: a szerző szerkesztése European Commission 2024 alapján

Minimális és alacsony kockázati profil

A jogszabály megfogalmazása szerint minimális kockázatot azok az MI-rendszerek jelentenek, amelyek nem tartoznak magasabb biztonsági osztályba. E rendszerek alkalmazására nincs korlátozás vagy kötelező tevékenység, mindenesetre javasolt az általános elvek követése, mint az emberi felügyelet, az egyenlő bánásmód és a méltányosság.

Alacsony kockázat esetén felmerül az MI-rendszerek által kivitelezhető manipuláció vagy megtévesztés lehetősége. Az általános célú MI (*general purpose artificial intelligence,* GPAI) nagy mennyiségű adatot felhasználva képes önálló döntések megalkotására, különböző feladatok kompetens végrehajtására. Egy GPAI-t önállóan vagy más rendszerbe vagy alkalmazásba integrált módon is kiadhatnak.

A GPAI-rendszerek kapcsán biztosítani kell a transzparenciát, azaz egyértelművé kell tenni a felhasználók számára, hogy MI-rendszerrel vagy MI-rendszer által létrehozott tartalommal dolgoznak (hacsak ez nem nyilvánvaló). Ennek megfelelően az MI segítségével generált vagy módosított tartalmat, például képeket, hang- vagy videófájlokat egyértelműen jelölni kell. Ezeknek a rendszereknek meg kell felelniük a digitális egységes piacon a szerzői és szomszédos jogokról szóló irányelvnek,[6] valamint meg kell akadályozni az illegális tartalom létrehozását.

Ezenkívül a GPAI-modellek valamennyi szolgáltatójának műszaki dokumentációt kell biztosítania, beleértve a képzési és tesztelési folyamatokat, valamint az értékelési eredményeket, továbbá azokat az információkat, amelyek a más szolgáltatók számára nyújtanak információt a GPAI-modell saját MI-rendszerbe történő integrálásához. Az ingyenes és nyílt licencű GPAI-rendszerek abban az esetben tartoznak a jogszabály hatálya alá, amennyiben nagy kockázatú MI-rendszerek részét képezik, illetve értelemszerűen ugyanúgy vonatkoznak rájuk a tiltott gyakorlatokkal kapcsolatos előírások és az átláthatósági kötelezettségi elvárások. E kategóriába a GPAI akkor tartozik, amennyiben a betanításhoz felhasznált számítások kumulatív mennyisége meghaladja

[6] Európai Parlament és a Tanács (EU) 2019/790 irányelve.

a 10^{25} lebegőpontos műveletet. A rendszerkockázattal járó GPAI-modellek szolgáltatóinak a korábbi kötelezettségeken túl a modellértékeléseket is el kell végezniük, továbbá megfelelő szintű kiberbiztonsági védelmet kell kialakítaniuk és fenntartaniuk, az incidensekről és az esetleges korrekciós intézkedésekről indokolatlan késedelem nélkül tájékoztatni kell az illetékes nemzeti hatóságokat.

Magas kockázati profil

A magas kockázatú MI-rendszerek negatívan befolyásolhatják egy természetes személy vagy egy csoport alapvető jogait, egészségét és biztonságát vagy a környezetet. A jogszabály III. melléklete szerint magas kockázatú MI-rendszernek minősülnek a) a biometrikus és biometria-alapú rendszerek; b) a kritikus infrastruktúra kezelésében és működtetésében közreműködő rendszerek; c) oktatást és szakképzést megvalósító rendszerek; d) foglalkoztatás és munkavállalók kezelését biztosító rendszerek; e) alapvető magán- és közszolgáltatásokhoz és juttatásokhoz való hozzáférést nyújtó rendszerek; f) bűnüldözést támogató rendszerek; g) migráció, menedékjog és határigazgatás kezelésében részt vevő rendszerek, valamint h) igazságszolgáltatást és demokratikus folyamatokat támogató rendszerek. Azonban kivételnek számítanak azok az MI-rendszerek, amelyek szűk feladatot látnak el, céljuk javítani egy korábban elvégzett emberi tevékenység eredményét, illetve döntéshozatali mintákat vagy eltéréseket észlelnek korábbi döntésekhez képest. További feltételként jelenik meg, hogy az MI-rendszer nem helyettesíti vagy befolyásolja a korábban elvégzett emberi értékelést megfelelő emberi felülvizsgálat nélkül, vagy mindössze előkészítő feladatot lát el.

Ahhoz, hogy az unió egységes piacán forgalomba vagy üzembe kerüljön egy magas kockázati besorolással bíró MI-rendszer, a szolgáltatónak meg kell felelnie a 8–25. cikkekben meghatározott követelményeknek. Ezek a kötelezettségek megkövetelik a mindenkori MI-szolgáltatótól, hogy hozzon létre kockázatkezelési és minőségirányítási rendszert, valamint megfelelő adatvédelmi megoldást, biztosítva, hogy a képzési, validációs és tesztelési adathalmazok relevánsak, megfelelően reprezentatívak és lehetőség szerint hibamentesek. Ezzel összefüggésben a kötelezően készítendő műszaki dokumentáció képes bizonyítani a rendszer megfelelőségét. Az ilyen rendszert úgy kell kialakítani, hogy a felhasználók emberi felügyeletet tudjanak megvalósítani, és elérjék a megfelelő mértékű pontosságot, robusztusságot és kiberbiztonságot.

A jogszabály további szereplőkre is kötelezettségeket ró. A magas kockázatú MI-rendszerek felhasználóinak megfelelő technikai és szervezeti intézkedéseket kell tenniük annak érdekében, hogy az ilyen rendszereket a rendelkezésre álló használati utasításoknak megfelelően használják (26. cikk). Az importőröknek ellenőrizniük kell, hogy (1) a szolgáltató elvégezte az adekvát megfelelőségértékelési eljárást, (2) a műszaki dokumentáció elkészült, (3) a rendszer viseli a szükséges CE-jelölést, és mellékelve van az EU megfelelőségi nyilatkozata, valamint (4) a szolgáltató kinevezett egy meghatalmazott képviselőt (23. cikk). Még a forgalmazók (24. cikk) és az értéklánc más szereplői (25. cikk) is felelősek azért, hogy ellenőrizzék és biztosítsák, hogy a szolgáltatók elvégezték a jogi kötelezettségeiket.

Nem elfogadható kockázati profil

A nem elfogadható kockázat a legmagasabb kockázati szint, amelyet a II. fejezet 5. cikke határoz meg. Értelemszerűen az e kategóriába tartozó tevékenységek tiltottak az EU értékeivel és alapvető jogaival való összeegyeztethetetlenség miatt. Ezek az alkalmazások a következőkhöz kapcsolódnak:

- Szubliminális technikák, amelyek túlmutatnak egy személy tudatosságán vagy célzottan manipulatívak vagy megtévesztők, és jelentősen rontják egy személy vagy csoport döntéshozatali képességét, aminek eredményeként olyan döntést hoznak, amelyet egyébként nem hoztak volna meg, és amely jelentős kárt okoz vagy valószínűsíthető módon okozhat annak a személynek, más személynek vagy csoportnak.
- Egy személy vagy egy adott csoport sebezhetőségének kihasználása koruk, fogyatékosságuk, szociális vagy gazdasági helyzetük miatt, azzal a céllal vagy eredménnyel, hogy jelentősen torzítsák a viselkedésüket, ami jelentős kárt okoz vagy okozhat annak a személynek vagy más személynek.
- Szociális pontozás MI-rendszerek használatával, amelyek a személyeket vagy csoportokat személyes jellemzőik, társadalmi viselkedésük és tevékenységeik alapján értékelik és jellemzik, ami a kezdeti kontextustól független vagy indokolatlan és aránytalan következtetésekhez vezethet.
- Prediktív bűnüldözés, amely természetes személyek kockázatának felmérésére vagy bűncselekmény elkövetésének előrejelzésére szolgáló profilozás személyiség és jellemzők felmérése alapján, kivéve, ha az ilyen MI-rendszert egy személy bűncselekményhez való kapcsolódása emberi értékelésének támogatására használják, amelynek igazolható kapcsolata van a bűncselekménnyel.
- Arcképekből álló adatbázisok létrehozásához vagy bővítéséhez az interneten elérhető arcképek vagy videómegfigyelési felvételek felhasználásával.
- Személy érzelmi állapotának felmérése, amely vonatkozik a munkahelyi vagy oktatási MI-rendszerekre, kivéve egészségügyi vagy biztonsági okokból, például annak észlelésére, hogy egy sofőr elalszik-e.
- Személyek biometrikus kategorizálása érzékeny jellemzők alapján, beleértve a nemi, faji, politikai irányultságot, vallást, nemi életet, szexuális irányultságot és filozófiai meggyőződéseket.
- Valós idejű távoli biometrikus azonosítás nyilvános helyeken, amely magában foglalja a biometrikus azonosító rendszerek teljes tilalmát, beleértve az utólagos azonosítást is, kivéve a bűnüldözést bírói jóváhagyással és a Bizottság felügyelete mellett előre meghatározott célokra, mint például bűncselekmény áldozatainak célzott keresése, terrorizmus megelőzése, súlyos bűncselekmények vagy gyanúsítottak célzott keresése, beleértve az emberkereskedelmet, szexuális kizsákmányolást, fegyveres rablást és környezet és természet elleni bűncselekményeket.

Kiberbiztonsági és adatvédelmi kötelezettségek a mesterségesintelligencia-rendszerekben

A Mesterséges intelligenciáról szóló jogszabály kötelezi a magas kockázatú MI-rendszerek szolgáltatóit és a rendszerszintű GPAI-szolgáltatókat a kiberbiztonsági kockázatok kezelésére egy mesterségesintelligencia-irányítási rendszer részeként.[7] A magas kockázatú MI-rendszereket a kiberbiztonsági követelményeknek megfelelően tanúsítani kell az (EU) 2019/881 rendelet szerint, a rendelet 15. cikkében meghatározott kiberbiztonsági követelmények alapján. A kapcsolódó szabványosítási kérelmet az Európai Szabványügyi Bizottság (European Committee for Standardization, CEN) és az Európai Elektrotechnikai Szabványügyi Bizottság (European Committee for Electrotechnical Standardization, CENELEC) kapta, azzal a követelménnyel, hogy a szabványosítás egyes területein konzultáljon az Európai Távközlési Szabványosítási Intézettel (European Telecommunications Standards Institute, ETSI).[8]

Másrészről a Mesterséges intelligenciáról szóló jogszabály kimondja, hogy a kritikus infrastruktúra üzemeltetésében részt vevő MI-rendszerek magas kockázatú kategóriába tartoznak. Ezáltal a rendelet egyértelműen megteremti a kapcsolatot a 2022/2557/EU irányelvvel,[9] amely a kritikus entitások rezilienciáját (*critical entities resilience,* CER) szabályozza hatálybalépését követően, felváltva az elavulttá vált korábbi irányelvet.[10] A kritikus entitások alapvető szolgáltatásokat nyújtanak a társadalmi funkciók fenntartásában, a gazdaság támogatásában, a közegészség és biztonság biztosításában, valamint a környezet megőrzésében.

Tekintettel arra, hogy a NIS2 irányelv[11] megteremti a kapcsolatot a CER irányelvvel, azaz a NIS2 irányelv I. és II. mellékletében meghatározott ágazatok és kapcsolódó alágazatok jelentős hányada kritikus infrastruktúraként jelenik meg, a kritikusinfrastruktúra-szolgáltatók kötelesek a NIS2 irányelvben meghatározott kiberbiztonsági követelményeket teljesíteni.

A NIS2 irányelv célja a kiberbiztonsági képességek fejlesztése az Európai Unió, a tagállamok és a hatályba tartozó vállalatok tekintetében, ezáltal a jogalkotó célja a jogszabállyal az egységes kiberbiztonsági szint növelése. Ennek értelmében e vállalatoknak meg kell felelniük a követelményeknek függetlenül attól, hogy használnak-e MI-rendszert vagy sem, illetve függetlenül az alkalmazott MI-rendszer kockázati szintjétől. A NIS2 hatálya alá tartozó szervezeteknek megfelelő és arányos intézkedéseket kell tenniük a hálózati és információs rendszereik biztonságát jellemző kockázatok kezelésére, valamint az incidensek megelőzésére és az incidensek hatásainak enyhítésére adminisztratív és kikényszerítő technológiai és fizikai kontrollok formájában. Ennek megfelelően ezeknek az intézkedéseknek a részét képezi a kockázatelemzés, az információs rendszerek biztonsági politikája és szabályzata, kockázatalapú biztonsági program kitűzése és megvalósítása, az incidenskezelés, üzletmenet-folytonosság, ellátási lánc biztonsága, kiberhigiéniai gyakorlatok

[7] Junklewitz et al. 2023; Soler Garrido et al. 2023.
[8] Junklewitz et al. 2023.
[9] Európai Parlament és a Tanács (EU) 2022/2557 irányelve.
[10] A Tanács 2008/114/EK irányelve.
[11] Európai Parlament és a Tanács 2022/2555 irányelve.

és kiberbiztonsági képzés, titkosítás, humánerőforrás-biztonság, hozzáférés-ellenőrzési politikák és eszközgazdálkodás, többfaktoros hitelesítés vagy folyamatos hitelesítési megoldások, biztonságos hang-, video- és szöveges kommunikációk, valamint biztonságos vészhelyzeti kommunikációs rendszerek használata. Emellett a vezetőknek elegendő ismeretekkel és készségekkel kell rendelkezniük ahhoz, hogy azonosítani tudják a szervezetükre vonatkozó kockázatokat, és értékelni tudják a kiberbiztonsági intézkedéseket és azok hatását a szervezetükre.

Továbbá, bár a NIS2 meghatározza a biztonsági szolgáltatókra vonatkozó követelményeket, a Cyber Solidarity Act javaslata kifejezetten előírja számukra a követelményeket, amelyek szerint az Európai Kiberpajzsban részt vevő entitásoknak korszerű és rendkívül biztonságos eszközökkel, felszerelésekkel és infrastruktúrákkal kell rendelkezniük. Ez lehetővé teszi a kollektív észlelési képességek, valamint a hatóságoknak és releváns entitásoknak szóló időben történő figyelmeztetések javítását, különösen a legújabb mesterséges intelligencia és adatelemzési technológiák használatával.[12]

Ahogy a NIS2 irányelv, úgy a Mesterséges intelligenciáról szóló jogszabály is meghatározza az adatvédelemhez való viszonyát is, hivatkozva a 2016/679/EU rendeletre,[13] azaz az Általános adatvédelmi rendeletre (GDPR). A GDPR az adatkezelési műveletekre vonatkozóan alapvető elveket, illetve az érintettek számára alapvető jogokat határoz meg. A személyes adatok kezelésére vonatkozó elveket az 5. cikk definiálja, amelyek:

- Jogszerűség, tisztességes eljárás és átláthatóság: a személyes adatokra vonatkozó adatkezelést jogszerűen, tisztességesen és az érintettek számára átlátható módon kell végezni.
- Célhoz kötöttség: a személyes adatok gyűjtése csak előre meghatározott, egyértelmű és jogszerű célból történjen.
- Adattakarékosság: az adatkezelési tevékenység csak és kizárólag a szükséges személyes adatokra korlátozódjon.
- Pontosság: biztosítani kell az adatkezelési tevékenységben érintett személyes adatok naprakészségét.
- Korlátozott tárolhatóság: a személyes adatokat csak az adatkezelés meghatározott céljainak megfelelő ideig szabad tárolni.
- Integritás és bizalmas jelleg: a személyes adatok kezelése során megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítani kell a személyes adatok bizalmasságát, sértetlenséget és rendelkezésre állását.

[12] Európai Bizottság 2023.
[13] Európai Parlament és a Tanács 2016/679 rendelete.

Az adatkezelő és az adatfeldolgozó tevékenysége során végzett adatkezelési műveletek a 6. cikk értelmében akkor tekinthetők jogszerűnek, ha:

- az érintett hozzájárulását adta;
- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél;
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, vagy
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Irányítási rendszerek

A Mesterséges intelligenciáról szóló jogszabály megköveteli a magas kockázatú MI-rendszerek szolgáltatóitól, hogy hozzanak létre és kezeljenek egy MI-irányítási rendszert (*artificial intelligence management system,* AIMS), amely a minőségirányítással, az információbiztonsággal vagy kiberbiztonsággal, valamint a személyes adatokra vonatkozó adatkezeléssel és adatfeldolgozással is együtt dolgozik. Ezek a követelmények nyilvánvaló hasonlóságot mutatnak az ISO/IEC 42001 szabványban meghatározottakkal.

Az ISO/IEC 42001[14] az AIMS követelményeit határozza meg, azaz útmutatást nyújt egy ilyen irányítási rendszer létrehozásához, megvalósításához, fenntartásához és folyamatos fejlesztéséhez. Átfogó keretet biztosít az MI-rendszerek etikus kialakításához, és biztosítja, hogy az MI-technológiák megfeleljenek az átláthatóság, elszámoltathatóság és adatvédelem elveinek. Az AIMS együttműködik a minőségirányítási rendszerrel (*quality management system,* QMS), az információbiztonsági irányítási rendszerrel (*information security management system,* ISMS) és a személyes adatkezelési rendszerekkel (*privacy information management system,* PIMS). Ennek megfelelően az AIMS integrálódik a szervezeti folyamatokba, illetve több ISO szabvánnyal, úgymint az ISO/IEC 27001[15] az ISMS, az ISO 9001[16] a QMS és az ISO/IEC 27701[17] a PIMS tekintetében. (Az ISO/IEC 27701 az ISO/IEC 27001 kiterjesztése, amelyet a jövőben a független ISO/IEC DIS 27701 vált fel.) Az ilyen integrációs képességek nem meglepők, mivel az ISO 42001 nagy hangsúlyt fektet arra, hogy az MI-rendszerek megfeleljenek a jogszabályi elvárásoknak, közte az adatvédelmi

[14] ISO/IEC 42001:2023.
[15] ISO/IEC 27001:2022.
[16] ISO 9001:2015.
[17] ISO/IEC 27701:2019.

követelményeknek, valamint kiberbiztonsági intézkedések végrehajtását követeli meg az MI-rendszerek fenyegetettségek elleni védelme érdekében.

Irányítási rendszer lévén az AIMS alapvető eleme a kockázatmenedzsment, amely rendszerezett megközelítést biztosít az MI életciklusa során felmerülő kockázatok azonosítására, elemzésére és mérséklésére, felhasználva az MI hatásvizsgálat-eredményeit. A szabvány technikai útmutatást nyújt az irányítási rendszer szervezeti célokból és etikai normákból történő származtatásához, beleértve az MI-rendszerek folyamatos monitorozására és fejlesztésére vonatkozó eljárásokat. Ez biztosítja, hogy az etikai megfontolások integrálódjanak az irányítási rendszerbe, beleértve az MI-megoldás fejlesztését és használatát szabályozó etikai irányelveket és egy felügyeleti mechanizmust. Mivel egy MI-rendszer tanítása torzított adatkészlet miatt helytelen módon is végbemehet, az AIMS alapja a különböző és reprezentatív adatkészlet használata az MI-algoritmusok működése torzításának csökkentése érdekében. Végül az átláthatósági és elszámoltathatósági követelmények megkövetelik az MI-algoritmusok, adatforrások és döntéshozatali folyamatok dokumentálását.

A mesterséges intelligencia kockázatai

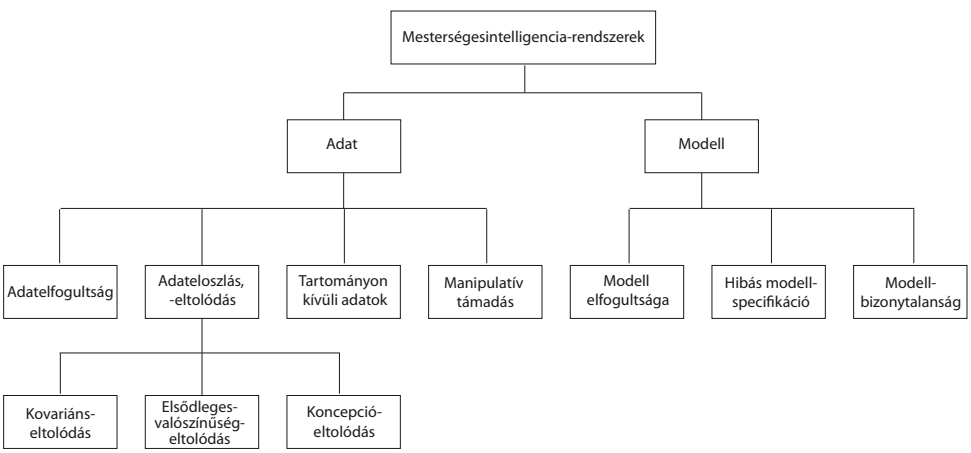
A NIST MI Kockázatkezelési Keretrendszere (*artificial intelligence risk management framework,* AI RMF) önkéntes használatra készült, és célja, hogy javítsa a megbízhatósági szempontok beépítésének képességét az MI-termékek, szolgáltatások és rendszerek tervezésébe, fejlesztésébe, használatába és értékelésébe. Az irányítás kritikus szerepet játszik az MI-kockázatkezelés minden más szakaszában, egy olyan kultúra kialakításával, amely felismeri a mesterséges intelligenciával kapcsolatos potenciális kockázatokat. Az irányítás lépése magában foglalja a kockázatok kezelésére és hatásuk felmérésére szolgáló folyamatok és dokumentációk kidolgozását és megvalósítását.[18]

A kockázatmenedzsment ennélfogva magában foglalja az átfogó MI-kockázatelemzést a felhasználókra, a társadalomra és még a környezeti hatásokra vonatkozó lehetséges hatások azonosítása érdekében, valamint az azonosított kockázatok mérséklése és a negatív hatások minimalizálása érdekében az intézkedések kidolgozását és végrehajtását. Az MI-kockázatértékelésnek tartalmaznia kell az MI-rendszert használó vállalatnak a rendszerre vonatkozó kiberbiztonsági és adatvédelmi kockázatkezelését, valamint a teljes vállalati kockázatkezelés részét kell képeznie. Mint általában, a kapcsolódó kockázatokat a fenyegetés valószínűsége és a hatás súlyossága alapján számoljuk, alkalmazva a Mesterséges intelligenciáról szóló jogszabály 3. cikk (2) bekezdésében foglaltakat, a kockázat az ártalom bekövetkezési valószínűségének és az ártalom súlyosságának kombinációja.[19]

[18] Tabassi 2023.
[19] Európai Parlament 2024.

Az MI-rendszereket célzó, illetve általa jelentett kockázatokat technikai, operatív, etikai és szabályozási kockázatok széles körébe lehet sorolni. Technikai kockázatot jelent például egy MI-rendszer bemeneteinek manipulálása a rendszer megtévesztésére, az algoritmusokban található hibák vagy gyengeségek, a modell kimenetének korrupttá tétele adatmérgezés útján. Operatív kockázatok közé tartozik egy MI-rendszer telepítése, frissítése és karbantartása során fellépő hibák, az adathalmazok vagy összetettebb feladatok skálázására vonatkozó hiányosságok, illetve a meglévő technológiák vagy folyamatok közötti inkompatibilitás. Etikai kockázatot jelent például a rendszer tanításához felhasznált adatokban meglévő elfogultság, részrehajlás továbbvitele vagy felerősítése, a döntéshozatali folyamatok megértésének vagy magyarázatának képtelensége (feketedoboz-probléma), az MI által vezérelt döntések és cselekvések felelősségének megállapításával kapcsolatos problémák, valamint összefüggésben az adatvédelmi kérdésekkel, az egyének magánéletének megsértése túlzott adatgyűjtés és megfigyelés révén. Szabályozási (vagy jogszabályi megfelelés) kockázatok közé sorolandó a jogszabályi előírások és szabványok követelményeitől való eltérés, azok ellenében történő nem megfelelés, az MI-rendszerek által okozott károk miatt indított jogi eljárások és bírságok.[20]

Zhang és munkatársai[21] az MI-rendszerek kapcsán felmerülő kockázatokat forrásuk szerint két nagy csoportra osztották (2. ábra): az adat és a modell. Az egyes kockázatok leírását az 1. táblázat ismerteti.



2. ábra: Mesterséges intelligencia kapcsán felmerülő kockázatok osztályozása
Forrás: a szerző szerkesztése Zhang et al. 2022 alapján

[20] Európai Parlament 2024.
[21] Zhang et al. 2022.

1. táblázat: Mesterséges intelligencia kapcsán felmerülő adat- és modellkockázatok

Kockázat	**Leírás**
Adatelfogultság	Az adatelfogultság arra utal, amikor az MI-modellekben egyes csoportok vagy elemtípusok túl- vagy alulreprezentáltak. A túlreprezentált jelleg esetén az adott csoport- vagy elemtípus nagyobb súlyt kap, mint mások. Ha egy adott osztály vagy csoport alulreprezentált, a modell gyengén teljesíthet ezen csoport kapcsán. Tekintettel arra, hogy az MI-modellek általában múltbeli adatok alapján tanulnak döntéseket hozni, gyakran az adott adatokban meglévő elfogultságokat továbbörökítik.
Adateloszlás, -eltolódás	Az adateloszlás, -eltolódás azt a helyzetet jellemzi, amikor az MI-modell tanítási és futásidőbeli adatai eltérő eloszlásokat mutatnak: • Kovarianciaeltolódás esetén a címkeelosztások eltérők, de a címkék jellemzői megegyeznek. • Elsődleges valószínűség eltolódása esetén a jellemzők eloszlása eltérő, de a jellemzőkhöz adott címkék azonosak. • Koncepcióeltolódás esetén a jellemzők ugyanazok, de a jellemzőkkel rendelkező címkék eltérők.
Tartományon kívüli adatok	Az inputadatokra vonatkozó nem megfelelő validálás és kezelés esetén nagy a valószínűsége annak, hogy a betanított modell téves előrejelzéseket ad magas bizonyossággal.
Manipulatív támadás	A manipulatív támadás célzott és nem célzott támadást foglal magában. A célzott támadás célja, hogy az MI-modell egy olyan ellenkező képet osztályozzon be célzott osztályként, amelynek valódi címkéje eltér ettől, ezt szándékos tervezéssel érik el (például adatmanipulációval). A nem célzott támadás célja, hogy az MI-modell olyan előrejelzést adjon, amely eltér a valódi címkétől anélkül, hogy meghatározott célt állítanának fel.
Modell elfogultsága	A tanítási adatokra jellemző elfogultság vagy hibás algoritmus következtében a betanított MI-modell elfogulttá válik.
Hibás specifikáció	A modell rossz specifikációja akkor következik be, ha a modell feltételezései nem megfelelők a tanítás során használt adatokhoz. A modell rossz specifikációját három tényező okozhatja: • Modellformalizálási hiba: a megadott funkcionális forma nem megfelelő a valódi kapcsolat jellemzéséhez, azaz bár minden magyarázó változó rendelkezésre áll, de a modell nem képes helyesen jellemezni a magyarázó változók és a magyarázott változó közötti kapcsolatot. • Modell túltanulása: a feladathoz mérten a szükségesnél összetettebb modell illesztése miatt a modell, bár kiválóan teljesít a tanítási adatok illesztésében, a tanítási adatokon túli teljesítménye az elvártakhoz képest alulmarad. • Változóbevonási hiba: változóbevonási hiba merül fel, amikor egy szükséges változó a modellből kimarad, vagy egy nem szükséges változó szerepel a modellben (tévedésből vagy szándékosan). A kimaradt jelentős változó eredményeként a modell nem képes megfelelően jellemezni az adatokat, ami végül elfogultságot eredményez. Az irreleváns változó bevonása a modell túltanulásához vezethet.
Modellbizonytalanság	Minden előrejelzési modell definíció szerint a valóság idealizált reprezentációja, és ezért eredendően nem képes tökéletesen reprezentálni a valódi rendszer viselkedését. A modell előrejelzési bizonytalansága a modell paramétereiben és szerkezetében rejlő sajátosság.

Forrás: a szerző szerkesztése Zhang et al. 2022 alapján

A MITRE ATLAS (MITRE 2024) hatás (impact) taktika részét képező technikák számos módszert részletesen tárgyalnak (2. táblázat). Az egyes technikák a modell, illetve az MI-rendszer hibás működéséből fakadó addicionális hatásokat („Külső hatás") fedik le. Az adatokra és a modellt megvalósító algoritmusra vonatkozó bizalmasság, sértetlenség és rendelkezésre állás kérdésével a MITRE ATLAS további taktikái foglalkoznak (például „ML Model Access", azaz „Gépi tanulás modell hozzáférés").

2. táblázat: MITRE ATLAS hatás- (impact) technikák

Technika	Leírás
Gépi tanulási modell kijátszása	A támadó megakadályozza, hogy a gépi tanulási modell helyesen azonosítsa az adatok tartalmát. Ez a technika felhasználható a gépi tanulást alkalmazó feladatok kijátszására.
Gépi tanulás megtagadása	A támadó szándékosan olyan bemeneteket hoz létre, amelyek nagy mennyiségű haszontalan számítást igényelnek a gépi tanulási rendszertől, ezzel lerontva vagy leállítva a szolgáltatást.
Gépi tanulás modell integritásának erodálása	A támadó manipulált adatokkal lerontja a modell teljesítményét, ezzel idővel megingatva a rendszerbe vetett bizalmat.
Költségnövelés	A támadó különböző gépi tanulási szolgáltatásokat célozhat meg haszontalan kérdésekkel vagy számításigényes bemenetekkel, hogy növelje a szolgáltatások futtatásának költségeit az áldozatszervezet számára.
Gépi tanulási rendszer hamis adatokkal történő bombázása	A támadó a gépi tanulási rendszert hamis adatokkal arra kényszerítheti a rendszert használó felett, hogy helytelen következtetések felülvizsgálatára és kijavítására fordítsa erőforrásait.
Külső károk	A támadó egy MI-rendszer erőforrásait vagy képességeit felhasználhatja saját céljának elérésére, miközben külső károkat okoz. Ezek a károk érinthetik a szervezetet (például pénzügyi károk, hírnévrombolás), annak felhasználóit (például felhasználói károk) vagy egy tágabb közösséget (például társadalmi károk). A pénzügyi kár magában foglalhatja a vagyon, tulajdon vagy egyéb pénzügyi eszközök elvesztését lopás, csalás vagy hamisítás miatt, vagy a nyomásgyakorlást, hogy pénzügyi erőforrásokat biztosítsanak a támadó számára. A hírnévrombolás a közvélemény és a szervezet iránti bizalom csökkenését jelenti. A társadalmi károk olyan negatív hatásokat eredményezhetnek, amelyek a közvéleményt vagy specifikus sebezhető csoportokat érinthetnek, mint például a gyermekek káros tartalommal való találkozása. A felhasználói károk magukban foglalhatnak pénzügyi és hírnévkárosodást, amelyeket az egyéni áldozatok éreznek, nem pedig szervezeti szinten jelentkeznek. A támadó az MI-rendszerek modelljének és a bemeneti, illetve kimeneti adatok által jelentett szellemi tulajdont lophatnak, gazdasági kárt okozva az áldozat szervezetnek.

Forrás: a szerző szerkesztése MITRE 2024 alapján

Kutatási eredmények

Ennek értelmében további kategóriaként jelennek meg az adatvédelmi és a kiberbiztonsági kockázatok. Az adatvédelemi kockázatok alatt többek közt a személyes adatok jogosulatlan felhasználása, nem megfelelő intézkedések az adatvédelem biztosítására, valamint a nem megfelelő jogalap alkalmazása értendő. Kiberbiztonsági kockázatként

jelenik meg az adott információs és kommunikációs technológia (IKT) vonatkozásában, például a jogosulatlan hozzáférés, az adatszivárgás, illetve a szolgáltatásmegtagadás-jellegű támadás formájában. A fenyegető tényezők mindehhez kihasználhatják a fizikai környezet, az emberek (alkalmazottak és harmadik felek), a technológia vagy akár a folyamatok gyengeségeit. A kiberbiztonsági területen végzett tevékenységek közvetlen hatást gyakorolhatnak egy IKT-rendszer integritására vagy rendelkezésre állására, ugyanakkor közvetlenül befolyásolhatják az adatok bizalmasságát, valamint az IKT-rendszerek integritását és rendelkezésre állását. Az IKT-rendszer szintjén felmerülő problémák negatív hatással lehetnek az adatokra, és ilyen problémák könnyen érinthetik az MI-szintet az MI-algoritmus integritása vagy a tanulási adatok mérgezése révén. A költség begyűjtése ezen a szinten jelentős közvetlen hatást gyakorol. A legfelső szinten, amely az üzleti hatásokat képviseli, mindezek pénzügyi hatásokkal járhatnak. A jogszabályi követelmények e kockázatok tükrében szükségesek és a kockázati profilokhoz rendelt elvárások miatt arányosak is.

Mindezek értelmében az MI-rendszerek minőségi kockázatai szerteágazók (3. táblázat), befolyásolják az adatok integritását, a modellek pontosságát, a folyamatok megbízhatóságát, az eredmények megbízhatóságát és a felhasználói interakciót.

3. táblázat: Az MI-rendszerek minőségi kockázatai

Kockázat	**Leírás**
Adatok minőségi kockázatai	• Adatelfogultság: a valós élethelyzeteket nem tükröző adathalmaz elfogult MI-modellekhez vezethet. • Adatinkonzisztencia: az inkonzisztens adatformázás, címkézés vagy kategorizálás hibákat okozhat az MI-modell tanításában. • Adathiányosság: a hiányos vagy nem teljes adathalmaz olyan MI-modellekhez vezethet, amelyek nem képesek hatékonyan kezelni bizonyos helyzeteket. • Adatpontosság: a pontatlan adatok helytelen döntésekhez vezethetnek.
Modell minőségi kockázatai	• Modell túltanulása: az MI-modellek, amelyek túl szorosan illeszkednek a tréningadatokhoz, nem általánosíthatók jól az új, ismeretlen adatokra. • Modell alultanulása: az egyszerűsített modellek, amelyek nem képesek megragadni az adatok mögöttes mintázatait, gyenge teljesítményt eredményezhetnek. • Algoritmus elfogultsága: az algoritmusokban lévő hibák elfogult, hibás döntéshozatalt eredményezhetnek. • Robusztusság hiánya: az MI-modellek, amelyek nem robusztusak, nem képesek ellenállni az enyhe változásoknak vagy támadásoknak. • Magyarázhatóság és értelmezhetőség: a modellek döntéshozatali folyamatai megértésének nehézsége (feketedoboz-jelenség) csökkentheti a bizalmat és a felelősséget.

Kockázat	Leírás
Folyamat minőségi kockázatai	• Rossz tréningfolyamatok: az elégtelen tanítási eljárások szuboptimális-modell-teljesítményhez vezethetnek. • Elégtelen validáció és tesztelés: a szigorú validáció és tesztelés hiánya hibás modellekhez vezethet. • Elégtelen monitorozás: az MI-rendszerek folyamatos monitorozásának elmulasztása idővel észrevétlen minőségi romláshoz vezethet. • Változáskezelési problémák: Az MI-rendszerek frissítésének és változtatásainak kezelési folyamatai hiányosak lehetnek, ami a minőség degradálásához vezethet.
Eredmény minőségi kockázatai	• Teljesítményromlás: idővel az MI-modellek teljesítménye romolhat, ha nem megfelelő a karbantartás és a frissítés. • Nem szándékolt következmények: az MI-rendszerek olyan következtetést tehetnek, amelyek technikailag helyesek, de kontextuálisan nem megfelelők vagy károsak. • Megbízhatósági problémák: azok az MI-rendszerek, amelyek nem teljesítenek következetesen, aláásható a bizalmat és a megbízhatóságot. • Méretezhetőségi problémák: a hatékony skálázódásra nem képes MI-rendszerek nehézségekbe ütközhetnek a növekvő adatmennyiségek vagy felhasználók kezelésében.
Felhasználói interakció kockázatai	• Felhasználói félreértés: a felhasználók félreérthetik a kimenetet, ami helytelen döntésekhez vagy cselekvésekhez vezethet. • Felhasználói bizalom hiánya: ha a felhasználók nem bíznak az MI-rendszerben, vonakodhatnak használni azt, csökkentve annak hatékonyságát. • Használhatósági problémák: rosszul tervezett interfészek és interakciók akadályozhatják az MI-rendszerek hatékony használatát.

Forrás: a szerző szerkesztése

Összegzés és konklúzió

A tanulmány betekintést nyújtott a mesterségesintelligencia- (MI-) rendszerek megvalósításának az Európai Unióban körvonalazódó jogi keretébe. A jogszabályi környezet átfogó megközelítést alkalmaz, amely definiálja a különböző kockázati profilokat, amelyekhez a kockázati szint függvényében kötelezettségeket ír elő.

A Mesterséges intelligenciáról szóló jogszabály megköveteli a magas kockázatú MI-rendszerek szolgáltatóitól egy MI-irányítási rendszer (AIMS) létrehozását és működtetését, amely integrálja a minőségirányítást, az információbiztonságot és az adatvédelmet. A jogszabályi kötelezettségek felépítése és jellege és az ISO/IEC 42001 szabvány között jelentős átfedés azonosítható, így a szabvány útmutatást nyújt az AIMS létrehozásához, fenntartásához és fejlesztéséhez. Egy AIMS célja, hogy biztosítsa egy MI-rendszer etikus, átlátható működését, amely megfelel az adatvédelmi törvényeknek, integrálódva más irányítási rendszerekhez, mint az ISO/IEC 27001 (ISMS), ISO 9001 (QMS) és ISO/IEC 27701 (PIMS).

Mint minden irányítási rendszer, így az AIMS egyik alapvető eleme a kockázatmenedzsment, amely az MI életciklusa során felmerülő kockázatok kezelésére és mérséklésére szolgál. A NIST MI Kockázatkezelési Keretrendszere (AI RMF) önkéntes

használatra készült, és célja a megbízhatóság növelése az MI-rendszerek tervezése, fejlesztése és használata során. A kockázatmenedzsment magában foglalja a kockázatok azonosítását, elemzését és a mérséklő intézkedések kidolgozását, figyelembe véve a technikai, operatív, etikai és szabályozási kockázatokat. A kockázatok közé tartoznak például a bemeneti adatok manipulálása, algoritmikus hibák, adatelfogultság és a döntéshozatali folyamatok átláthatatlansága.

Az MI-rendszerek minőségi kockázatai szerteágazók, befolyásolják az adatok integritását, a modellek pontosságát, a folyamatok megbízhatóságát, az eredmények megbízhatóságát és a felhasználói interakciót. Ezek közé tartozik az adatelfogultság, adatinkonzisztencia, adathiányosság, modell túltanulása vagy alultanulása, algoritmikus elfogultság és az MI-rendszerek folyamatos monitorozásának elmulasztása. Az eredmények minőségi kockázatai között szerepel a teljesítményromlás, nem szándékolt következmények és megbízhatósági problémák. A felhasználói interakció kockázatai közé tartozik a felhasználói félreértés, bizalom hiánya és használhatósági problémák.

Felhasznált irodalom

Council of the European Union (2024): *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Analysis of the Final Compromise Text with a View to Agreement.* Online: https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf

Európai Bizottság (2023): *Javaslat. Az Európai Parlament és a Tanács rendelete a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról*. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52023PC0209

Európai Parlament (2024): *HELYESBÍTÉS az Európai Parlament által 2024. március 13-án a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról.* Online: www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_HU.pdf

Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete.

Európai Parlament és a Tanács 2019/881 rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról. Az Európai Parlament és a Tanács (EU) 2019/881 rendelete.

Európai Parlament és a Tanács 2022/2481 határozata a Digitális évtized 2030 szakpolitikai program létrehozásáról.

Európai Parlament és a Tanács 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről.

Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról.

Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról.

European Commission (2024): *AI Act.* Online: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

ISO 9001:2015 Quality Management Systems — Requirements.

ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection. Information Security Management Systems. Requirements.

ISO/IEC 27701:2019 Security Techniques Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management Requirements and Guidelines.

ISO/IEC 42001:2023 Information Technology Artificial Intelligence Management System.

ISO/IEC DIS 27701 Information Security, Cybersecurity and Privacy Protection Privacy Information Management Systems Requirements and Guidance.

Jiang, Yuchen et al. (2022): Quo Vadis Artificial Intelligence? *Discover Artificial Intelligence,* 2(4). Online: https://doi.org/10.1007/s44163-022-00022-8

Junklewitz, Henrik et al. (2023): *Cybersecurity of Artificial Intelligence in the AI Act*. Luxembourg: Office of the European Union. Online: https://doi.org/10.2760/271009

MITRE (2024): MITRE ATLAS. Online: https://atlas.mitre.org/

Soler Garrido, Josep et al. (2023): *Analysis of the Preliminary AI Standardisation Work Plan in Support of the AI Act*. Luxembourg: Office of the European Union. Online: https://doi.org/10.2760/5847

Tabassi, Elham (2023): *Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST Trustworthy and Responsible AI, National Institute of Standards and Technology.* Gaithersburg. Online: https://doi.org/10.6028/NIST.AI.100-1

Tanács 2008/114/EK irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. 2008/114/EK (2008).

Zhang, Xiaoge et al. (2022): Towards Risk-Aware Artificial Intelligence and Machine Learning Systems: An Overview. *Decision Support Systems, 159*, 113800. Online: https://doi.org/10.1016/j.dss.2022.113800

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 3. szám 137–163.
DOI: 10.32567/hm.2024.3.9

Ináncsi Mátyás Ottó[1] – Dub Máté[2]

Dezinformáció az Ipar 4.0 rendszerek elleni támadásokban

Az elektromos autók dezinformációs csapdái a szélsőséges közösségimédia-platformokon (Telegram, 4chan, Truth Social) – A félrevezető tartalmak vizsgálata,[3] 1. rész

Disinformation in Attacks against Industry 4.0 Systems

Electric Car Disinformation Traps on Extremist Social Media Platforms (Telegram, 4chan, Truth Social) – Investigation of Misleading Content, Part1

Absztrakt

A két kutatás célja az volt, hogy bemutassa a dezinformáció szerepét az Ipar 4.0 rendszerek elleni támadásokban, különös tekintettel a klímaváltozás és az elektromos autók témaköre körüli szélsőséges közösségimédia-platformokon megjelenő szentimentekre. A kutatás során részletesen bemutattuk a misinformation, malinformation és disinformation fogalmainak különbségeit, hogy jobban megértsük ezen jelenségek mechanizmusait és következményeit. A European Digital Media Observatory által feltárt dezinformációkat elemeztük, amelyek

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Kiberbiztonsági Tanszék Hadtudományi Doktori Iskola, e-mail: inancsi.matyas@uni-nke.hu
[2] Doktori hallgató, Nemzeti Közszolgálati Egyetem Kiberbiztonsági Tanszék Hadtudományi Doktori Iskola, e-mail: dub.mate.98@gmail.com
[3] A TKP2021-NKTA-51 számú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP2021-NKTA pályázati program finanszírozásában valósult meg.

a közösségi médiában terjedtek, különösen a klímaváltozás és az elektromos autók témájában. Vizsgálataink során szélsőséges közösségimédia-platformokat, mint a 4chan, Truth Social és Telegram, vettünk górcső alá, hogy feltérképezzük a dezinformációs tartalmak elérését és azok hatását a közösségre. Különös figyelmet fordítottunk a kommentek szentimentjének elemzésére, hogy megértsük a felhasználói reakciók érzelmi töltetét és polarizációját. Kutatásunk rávilágít arra, hogy a dezinformáció milyen mértékben befolyásolja az Ipar 4.0 rendszerek biztonságát és a társadalmi percepciót a klímaváltozás és az elektromos autók vonatkozásában, valamint javaslatokat fogalmaz meg a dezinformáció elleni hatékonyabb küzdelem érdekében.

Kulcsszavak: Ipar 4.0, dezinformáció, EWS

Abstract

The aim of the two studies was to showcase the role of disinformation in attacks against Industry 4.0 systems, with a particular focus on the sentiments appearing on extremist social media platforms surrounding the topics of climate change and electric vehicles. During the study, we provided a detailed explanation of the differences between misinformation, malinformation, and disinformation to better understand the mechanisms and consequences of these phenomena. We analyzed the disinformation uncovered by the European Digital Media Observatory that spread on social media, particularly concerning climate change and electric vehicles. In our investigations, we scrutinized extreme social media platforms such as 4chan, Truth Social, and Telegram to map the reach of disinformation content and its impact on the community. Special attention was given to analyzing the sentiment of comments to understand the emotional charge and polarization of user reactions. Our research highlights the extent to which disinformation affects the security of Industry 4.0 systems and public perception regarding climate change and electric vehicles, and it also offers recommendations for more effective measures against disinformation.

Keywords: Industry 4.0, disinformation, EWS

Bevezető

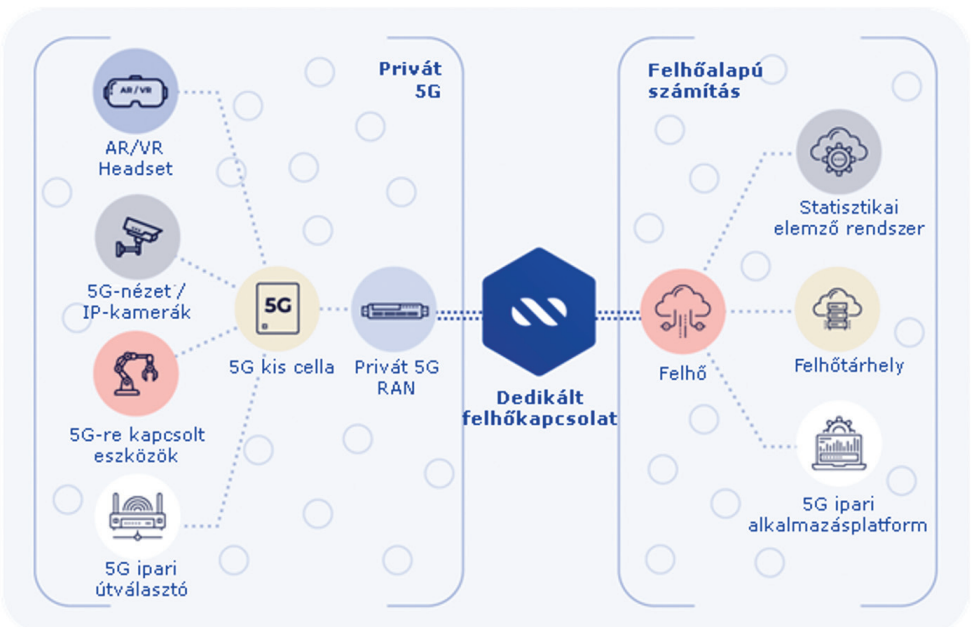
Napjainkban az internetes álhírek, megtévesztő tájékoztatások kifejezetten szerteágazók. Elmondhatjuk, hogy szinte bármilyen kérdéskörben felmerülnek álhírek, megtévesztő tartalmak a digitális felületeken, kifejezetten a közösségi médiában. A digitális álhírek sajátossága, hogy

„Az információ forrása például rejtve maradhat a többszöri megosztás eredményeként; az üzenet felerősített érzelmi vagy értékelő jellemzőkkel jelenhet meg a kapott tetszések vagy nemtetszések száma, vagy a megosztások száma miatt. Az üzenet címzettje elfogultan választhatja ki a tájékoztatásokat, amit a platform felismer, így a hírfolyam a preferenciáikhoz igazodik. A legproblémásabb a felhasználó referenciapontjának eltolódása a szövegkörnyezetben:

a természetes interperszonális kommunikációban ez magában foglalja az üzenet küldőjét és címzettjét, valamint találkozásuk helyzetét."[4]

A digitális világban azért kifejezetten aggasztó az álhírek terjedése, mert sokkal tágabb az információ terjedése, illetve a felhasználói visszajelzések (például tetszések/nem tetszések) száma.

A Covid–19-járvány idején a védőoltás körül több egyértelmű álhír is keringett. Az egyik ilyen jelentős híresztelés – ami főleg közösségimédia-platformokon bukkant fel –, hogy az oltás autizmust okoz.[5] Az állításnak tudományos bizonyítéka jelenleg nincs, ugyanakkor az oltásellenes csoportokban közkedvelt az oltás és autizmus kapcsolatának boncolgatása, és a kettő közötti párhuzam bemutatása. A járványhoz hasonlóan az álhírek sajnos nagyon hamar kapcsolódni kezdtek az Ipar 4.0 rendszerekhez is. 2019-ben nem sokkal a Covid kitörése előtt Európában és az Egyesült Államokban megkezdődött a 4G telekommunikációs rendszerek bővítése és ennek keretében 5G-rendszerek kiépítése. A fejlesztés vezető hírnek számított, jelentős médiavisszhangnak is örvendett, hiszen mind a felhasználóknak, mind pedig az ipari felhasználóknak bővült a kommunikációs lehetősége. Ez szorosan kapcsolódik az Ipar 4.0 térnyeréséhez, mint az első ábrán is látható elengedhetetlen lépés, hiszen a rendszereknek folyamatosan szükséges a hálózati kommunikáció.



1. ábra: Az Ipar 4.0 és az 5G-hálózat kapcsolatának fontossága
Forrás: saját fordítás a Flō Networks 2023 alapján

[4] Jakusné Harnos – Demeter – Bányász 2023: 134.
[5] Yandell 2024.

Sajnos a technológia térnyerése nem volt zökkenőmentes, a koronavírus-járványt és az 5G-hálózatok terjedését a felhasználók hamar összekötötték. Több közösségimédia-felületen is megjelentek olyan bejegyzések, amelyek az 5G és a vírus/oltás kapcsolatát fejtegették. Többek szerint az 5G-hálózat elterjedése okozta a járványt. Ez a képtelen álhír nagy népszerűségnek örvendett közösségimédia-platformokon. Összeesküvés-elméletekre nyitottabb emberek pedig pár esetben 5G-tornyokat gyújtottak fel, hogy megállítsák a vírus terjedését.[6] Az Egyesült Királyságban 77 darab 5G-adótornyot érintett valamilyen jellegű gyújtogatás, amely a járvánnyal kapcsolatos 5G-összeesküvés-elmélethez köthető.[7] Most hasonló jellegű híreket láthatunk az orosz–ukrán konfliktus esetében is, olyan csavarral, hogy itt már az állami szereplők is érdekeltté váltak a megtévesztő információk terjesztésében.

Az Ipar 4.0 akár közvetve, akár közvetett módon kitett a közösségi médiában jelen lévő álhíreknek. A Covid–19-járvány során keletkezett tanulmányok rávilágítottak arra is, hogy az ellátási lánc mennyire érzékeny az álhírek terjedésére és az ehhez kapcsolódó hatásokra. A félretájékoztatás és az álhírek terjesztése közvetlenül járult hozzá ahhoz, hogy bizalmatlanság alakuljon ki az emberekben.[8] Az Ipar 4.0 pedig pontosan erre az érzékeny ellátóláncra épül, szorosan összekapcsolva más technológiákat, hálózatokat és eszközöket, ezért több szempontból is felmerül a kitettség veszélye.

Az 5G-technológia IoT-eszközökkel gazdagítva pedig lehetőséget nyújt arra, hogy a termelési folyamatokat forradalmasítsa kifejezetten a kritikus infrastruktúrákban.[9] Az így látható technológiából eredő fejlődés, illetve fejlesztés (kifejezetten: fenntartható gyártási folyamatok, okos-energiarendszerek, környezetbarátabb termelési módszerek és logisztikai folyamatok) lehetőséget fog nyújtani a klímaváltozással szembeni harcban. Ugyanakkor ennek alapfeltétele az, hogy a társadalom bízzon a technológiában, mert láthattuk az 5G-tornyok felgyújtása kapcsán, hogy a társadalmi bizalom kizökkenése súlyos negatív következményeket hoz.

A dezinformáció lényegében ezt a társadalmi bizalmat gyengíti el, ami megnehezíti az emberek számára, hogy megbízható információk alapján hozzanak döntéseket, és akadályozza a hatékony politikai döntéshozatalt. Az alábbi publikációban az elektromos autók kapcsán felmerülő felhasználói megítélést, illetve dezinformációs témákat vizsgáljuk. A téma kapcsán két kérdésre keressük a választ:

- Milyen mértékben jelennek meg az elektromos autókkal kapcsolatos témák a közösségi médiában, különös tekintettel azok népszerűségére és elterjedtségére?
- Milyen attitűdök és vélemények figyelhetők meg az elektromos autók kapcsán a szélsőséges közösségimédia-platformokon, különösen a dezinformáció és a felhasználói megítélés szempontjából?

Mielőtt továbblépünk, a második kérdés esetében fontos tisztázni, mit tekintünk szélsőséges közösségimédia-platformnak. Tanulmányunkban azon platformokat tekintjük szélsőségesnek, ahol a moderáció teljes hiánya merül fel a bejegyzésekkel

[6] Chan–Dupuy–Lajka 2020.
[7] Reichert 2020.
[8] Chatterjee–Chaudhuri–Vrontis 2023; Li et al. 2020.
[9] Toth 2024.

kapcsolatban. Kifejezetten ilyen platform a 4chan, a Truth Social és a Telegram. A Twitter/X esetében csökkent a moderációs jelenlét, viszont a Birdwatch (jelenlegi verzióban közösségi komment) lehetőséget nyújt a felhasználóknak, hogy nyíltan ellenmoderációt hozzanak létre a dezinformatív tartalommal szemben.

Vizsgálatunk középpontjában a klímaváltozás és az elektromos autók dezinformációs csapdái állnak. Azért választottuk az elektromos autók kapcsolatát, mert a téma rendkívül időszerű és jelentős figyelmet kap a közösségimédia-felületeken, ahogyan azt az ábrák is mutatják. Az álhírek és a felhasználói bizonytalanság azonban továbbra is komoly kihívást jelentenek ezen a területen. Úgy látjuk, hogy az Ipar 4.0 és a hozzá kapcsolódó technológiák, különösen az 5G-hálózat, alapvető fontosságúak a klímaváltozás elleni küzdelemben. Az elektromos autók ebbe a technológiai forradalomba kapcsolódnak be azzal a céllal, hogy csökkentsék a károsanyag-kibocsátást, ezzel hozzájárulva a környezettudatossághoz. Továbbá az Ipar 4.0 technológiái, mint az automatizáció, a digitalizáció és az IoT,[10] lehetővé teszik az energiahatékonyabb gyártási folyamatokat és a környezetbarát termelési módszereket. Ezek a technológiai fejlesztések nemcsak a gyártás és az energiafelhasználás optimalizálását teszik lehetővé, hanem a valós idejű adatgyűjtés révén a klímaváltozással kapcsolatos kutatásokat is támogatják. Az elektromos autók elterjedése pedig kulcsfontosságú a károsanyag-kibocsátás csökkentésében, amely az egyik legfontosabb lépés a klímaváltozás hatásainak mérséklésében.

Ezért fontosnak tartjuk, hogy figyelmünket e technológiák és az elektromos autók (illetve klímaváltozással kapcsolatos) dezinformáció elleni küzdelmére irányítsuk, mivel a pontos és hiteles tájékoztatás elősegíti a hatékony döntéshozatalt és felhasználói bizalmat.

Bevezetőül és az első kutatási kérdéshez kapcsolódóan bemutatjuk az elektromos autók kérdéskörének népszerűségét választott közösségimédia-platformokon:

- Milyen mértékben jelennek meg a klímaváltozással és elektromos autókkal kapcsolatos témák a közösségi médiában, különös tekintettel azok népszerűségére és elterjedtségére?

A mérés módszeréül a közösségimédiaelérés-vizsgálatot választottuk.

A vizsgálat időtartamát az elérhető adatok határozták meg, így a május 19. és június 18. közötti időszakot tudtuk vizsgálni. Több közösségimédia-platform az AI elterjedése miatt (azért, hogy modelleket ne taníthassanak a felhasználók bejegyzéseiből) letiltotta az automatizált lekérdezéseket, ezért kifejezetten nehéz nagy mennyiségű adatot letölteni. A kutatási adathalmazt ennek következtében az határozza meg, hogy tulajdonképpen hol érhető el gyűjtött adat. Fontos kiemelnünk, hogy az adatok így semmilyen módon nem tekinthetők reprezentatívnak. A tiltás előtt lehetőség volt szoftver segítségével (például Facepager) letölteni nagy mennyiségű adatot a saját paramétereink szerint, most csak más weboldalakról tudjuk beszerezni az adatokat. Ez felvet pontatlanságot, viszont jelenleg más megoldást nem tudunk adatgyűjtésre, és a téma folytonos aktualitására tekintettel nem akarjuk hanyagolni a téma kutatását.

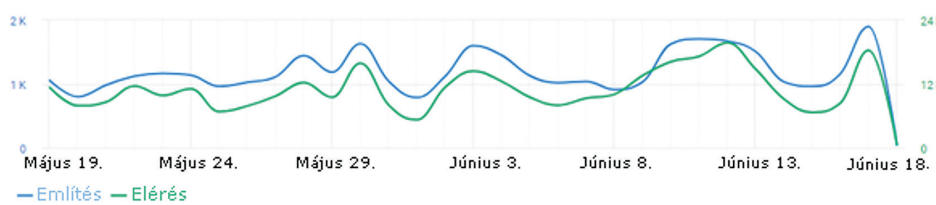
[10] Toth 2024.

Az adatgyűjtés arra irányult, hogy a kiválasztott közösségimédia-platformokon milyen elérést generált egy érintett téma/kulcsszó. A platformválasztás alapját itt az adatlekérdezés elérhetősége adta, sajnos több platform már nem ad lehetőséget arra, hogy automatizáltan adatot töltsünk le. Az elérésvizsgálat során a választás így a TikTokra, Quorára, YouTube-ra, X-re (Twitter), illetve kisebb blogokra és fórumokra esett.

A 2. számú ábra szemlélteti az „Electric Vehicle/EV" kifejezések említését kékkel, az elérés számát zölddel. Az elérés azt jelenti, hogy felhasználókhoz hányszor jutott el az adott tartalom (egy felhasználó akár többször is láthat azonos tartalmat), az említés pedig a konkrét felhasználói interakcióra irányul.

Klímaváltozás vonatkozásban az elérések és említések kapcsán teljesen azonos trendeket figyelhetünk meg, mindkét tengely együttesen mozog. Az említések csúcspontja 10 953 darab említés, míg az elérések esetében a csúcspont 69 628 933 darab felhasználó. Referenciaként azonos lekérdezési feltételekkel a „BMW" kifejezést is megvizsgáltuk. Rangos nemzetközi márkaként szintén kiemelkedő elérést generált: csúcsponton 598 említés és 26 121 805 felhasználói elérés. A kettőt összehasonlítva látható, hogy az autómárkáról folyamatosan beszélnek a felhasználók, de kirajzolódik, hogy ez közelében sincs a klímaváltozás körüli közösségimédia-jelenlétnek.

Fontos kiemelnünk, hogy az ábra végén lévő csökkenés nem jelent egyértelműen lappangást a felhasználók részéről, ez lehet akár .api lekérdezésből eredő anomália is. Az AI-eszközök népszerűsége miatt több közösségimédia-platform késlelteti, vagy akár le is tiltja az .api lekérdezést, ezért ilyen anomáliák az adatokban előfordulnak. Elektromos autók kapcsán jól látszik, hogy a felhasználóknál kifejezetten népszerű a téma. Csúcsponton a kifejezés 18 312 062 darab felhasználói elérést generált 2 283 említésből. A kulcsszóvizsgálat rávilágít némi hullámzásra, de összességében látható, hogy a felhasználók folyamatosan beszélnek a témáról. Az említésekben szintén az ábra végén mutatkozik egy jelentős bezuhanás, amelynek okául az .api[11] lekérdezések tiltását feltételezzük. A hullámzás mind említésekben, mind elérésekben együttesen mozog. Ez azt mutatja, hogy folyamatos az interakció, nincs „önálló influencer" akinek a kiesése a téma jelentős visszaeséséhez és érdektelenségéhez vezetne. A felhasználók között egészséges kommunikáció van a témában.



2. ábra: „Electric Vehicle/EV" kifejezés elérése és említésszáma választott közösségimédia-platformokon, május 19. és június 18. közötti időszakban
Forrás: a szerző fordítása a Brand24 szoftver általi lekérdezés alapján

[11] Alkalmazásprogramozási felület.

Választ adva az első kutatási kérdésre, hogy „milyen mértékben jelennek meg az elektromos autókkal kapcsolatos témák a közösségi médiában, különös tekintettel azok népszerűségére és elterjedtségére?", elmondhatjuk, hogy jelentős felhasználói interakció övezi az elektromos autók kérdéskörét. A felhasználók intenzív érdeklődése jól mutatja, hogy a téma széles körben foglalkoztatja a közönséget, ami jelentős társadalmi diskurzust vált ki.

Az Ipar 4.0 rendszerek szorosan kapcsolódnak ezekhez a kérdéskörökhöz, mivel a digitalizáció és az automatizáció egyre nagyobb szerepet játszik a fenntartható technológiák, például az elektromos autók fejlesztésében és gyártásában. Az intelligens gyártási rendszerek, a big data elemzés és a hálózatba kapcsolt eszközök lehetővé teszik az energiahatékonyság növelését és a környezetvédelmi szempontok figyelembevételét. Emellett az Ipar 4.0 megoldások hozzájárulnak a klímaváltozással kapcsolatos innovációk és megoldások gyorsabb terjedéséhez, támogatva az ipari szereplők fenntartható fejlődését.

Dezinformáció a digitális világunkban

Ebben a fejezetben a dezinformáció, álhírek *(fake news),* megtévesztő információ és kártékony információ fogalmát mutatjuk be. A fogalmi bemutatás után esettanulmány példáján kívánunk rávilágítani arra, hogy milyen következményekkel jár az, ha a dezinformáció kezeletlenül terjed a közösségi médiában.

Fogalmi meghatározás

Ebben a fejezetben elhelyezzük a dezinformációt fogalmilag az álhírek, illetve megtévesztő információk körében. A kutatási irányt szem előtt tartva általános jelleggel mutatjuk be a fogalmakat, hogy tisztázott legyen, miért tekintjük a dezinformációt súlyosabbnak, mint a megtévesztő tartalmakat.

A dezinformáció értelmezésénél szükséges egy lépéssel távolabbról vizsgálni a fogalmat, mivel az álhírek terminológiai meghatározása kapcsán komoly összemosódást tapasztalhatunk. A köznyelvben a megtévesztő információt gyakran álhírnek vagy *fake news*nak nevezik. Viszont a dezinformáció *(disinformation)* ennél tágabb fogalmi kategóriában értelmezhető:

„A […] dezinformáció a következőket foglalja magában: hamis, pontatlan vagy félrevezető információk minden olyan formája, amelyet a közvélemény szándékos megkárosítására vagy haszonszerzés céljából terveztek, mutattak be és népszerűsítettek."[12]

A dezinformáció egyik kulcseleme, hogy szándékosan kártékony legyen, míg az álhírek esetében ez nem mindig mondható el.

[12] European Commission 2018: 5.

Jelen fogalmi keretrendszer több megközelítést, kritériumrendszert is magában foglal, és értelmezése során új meghatározások feltüntetését is szükségessé teszi, amelyek adott esetben közvetlenül nem is tekinthetők álhírnek. A kritériumrendszer szempontjából és a pontos meghatározás érdekében két fő kérdést kell megválaszolnunk:

- Valós vagy valótlan információval állunk-e szemben?
- Az információ terjesztője tudatában van annak, hogy milyen következményei lehetnek az információ terjesztésének?

A kérdések megválaszolásával pedig három kategóriát határozhatunk meg:

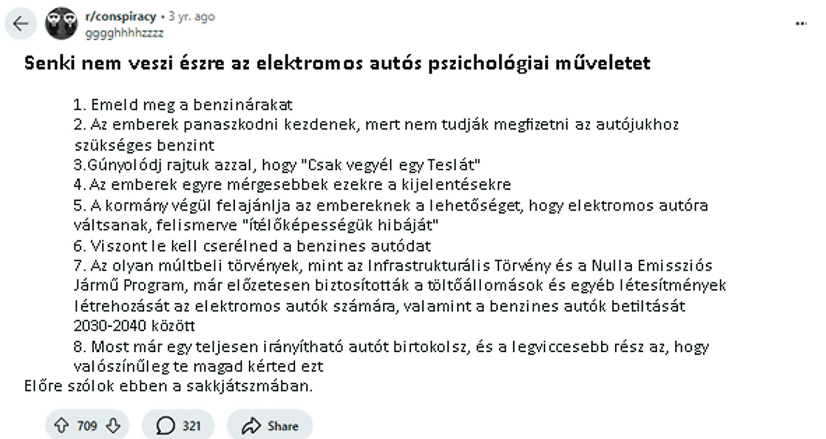
- Amennyiben hamis/valótlan információk tudatos, megtévesztő, rossz szándékú terjesztése a cél, abban az esetben a dezinformációt *(disinformation)* határozhatjuk meg. Ezen kategória az álhírek csoportjába tagolható.
- Amennyiben a hamis/valótlan információk terjesztésére oly módon kerül sor, amely szerint a terjesztő nincs tudatában annak, hogy az általa terjesztett információ valótlan, nincs megtévesztő célzat és rossz szándék, úgy a félretájékoztatást *(misinformation)* határozhatjuk meg. Ez a kategória szintén az álhírek csoportjába sorolható, hiszen az információ hamis, még akkor is, ha azzal annak terjesztője nincs tisztában.
- Amennyiben az információ igaz/valós, viszont annak terjesztése megtévesztő célzattal, rossz szándékkal történik, úgy az úgynevezett *malinformation*t határozhatjuk meg. (A magyar fordításban gyakran helytelen vagy rossz információként is hivatkoznak jelen fogalomra.) Ezen kategória az előzőkkel ellentétben nem sorolható az álhírek csoportjába, ugyanis, bár a megosztás szándékos és indíttatása rossz, az információ valós.

Mindezek mellett véleményünk, hogy az olyan információ is dezinformációnak minősül(het), amely valóságot tartalmaz vagy valós alapokon nyugszik, de a célja, hogy ártsanak vele. Az információszivárogtatás például olyan módja, amikor a másik fél érzékeny adatait szivárogtatják ki, és a körülötte lévő kontextusban a megtévesztő és valós információkat összemossák. A Reddit közösségimédia-platform Conspiracy (összeesküvés-) elméletekkel foglalkozó subredditjén gyakran ez utóbbi fordul elő dezinformáció esetében. A 3. számú ábrán látható, ahogy az elektromos autók térnyerését összemossák a növekvő üzemanyagárakkal. Tényszerűen elmondható, hogy az Egyesült Államokban 2021-ben az átlagos 2,1 dollár per gallonárról 2022 közepére átlagosan 5,107 gallonárra ugrott az üzemanyagár,[13] illetve az Egyesült Államok kormánya adókedvezmény formájában támogatja az elektromosautó-vásárlást.[14] De a kettő között nem jelenthetjük ki azt a kapcsolatot, amit a szerző fejteget. Az üzemanyagárakban a Colonial Pipeline-t ért kibertámadás[15] is szerepet játszott. Ahogy az ábrán is látható, a tartalomra érkezett felhasználói interakció (komment és felszavazás formájában).

Az ilyen jellegű hírt tekinthetjük dezinformációnak, hiszen megtévesztő tartalmat közöl, és az ártó szándék is felismerhető benne. Fontos kiemelnünk, hogy tényszerűen

[13] *US Retail Gas Price* [é. n.].
[14] *Electric Vehicles* [é. n.].
[15] Easterly 2023.

eldönteni valamiről, hogy dezinformáció, vagy sem, nagyon nehéz. Sokkal több befektetett energiát igényel a dezinformáció ellenőrzése, mint létrehozása. Ebből eredően létezik a folyamatos információs aszimmetria, a megtévesztő információt „létrehozni" és terjeszteni jelentősen kevesebb erőforrást vesz igénybe, mint azt ellenőrizni és cáfolni. Illetve mire az ellenőrzés lezajlik, és megjelenik a cáfolat, gyakran az adott téma már nem is releváns.



3. ábra: A Reddit Conspiracy subredditje: Összeesküvés-elmélet az elektromos autók és az üzemanyagárak kapcsolatáról

Forrás: a szerző fordítása [gggghhhhzzzz] 2022 alapján

Összefoglalva a gondolatmenetet, tehát a dezinformációnál „enyhébb" fogalmi kategória a megtévesztő/félrevezető információ *(misinformation),* vagyis a hamis/valótlan információk negatív szándék nélküli terjesztése. A megtévesztő információ kapcsán a tudománynak még olyan ismeretelméletet szükséges kialakítania, amely által maradéktalanul eldönthető egy információról, hogy az tárgyilagosan hamis-e.[16] A korábban említett alapvető különbség kapcsán – vagyis, hogy a megtévesztő információ hasonlóan a dezinformációhoz félrevezető, azonban megosztási szándéka nem ártó jellegű – következik, hogy nagy eséllyel a felhasználó a megosztott tartalmat igaznak gondolja, vagy hisz a valóságtartalmában, és ezért osztja meg. Ilyen jellegű hír volt a közösségi médiában a Covid–19-járvány alatt, hogy Budapestet le fogják zárni.[17]

A bevezetőhöz kapcsolódva a megtévesztő információ párja a kártékony információ *(malinformation).* Ez alatt értjük minden olyan valós információ/adat publikálását, amellyel az a cél, hogy a másik félnek ártson.[18] Az árnyalat a dezinformációhoz képest, hogy itt nincs megtévesztő körítés. A cél ilyen esetben hitelesen közölni azt, ami a másik félnek ártani fog. A közösségi médiában leggyakoribb példa erre a privát

[16] Uscinski–Littrell–Klofstad 2024.
[17] *Belügyminisztérium: Nem került szóba Budapest lezárása* 2020.
[18] *Misinformation, Disinformation and Mal-information* [é. n.].

beszélgetések képernyőmentése és publikálása. Súlyosabb esetben állami szinten a nem nyilvános vagy minősített adatok nyilvánosságra hozatala.

A dezinformációra így, ha el akarjuk helyezni a megtévesztő és kártékony információ skáláján, akkor azt mondhatjuk, egy kicsit mind a kettő érvényes rá.

1. táblázat: Megtévesztő információ, kártékony információ és dezinformáció elhelyezése

Fake news	
Megtévesztő információ *(misinformation)*	Kártékony információ *(malinformation)*
Dezinformáció *(desinformation)*	

Forrás: a szerző szerkesztése

A hatékony dezinformáció tartalmaz valóságalapot, ahogy ez a 3. ábrán is látható. Így tud a felhasználó kapcsolódni a felmerült hírhez. A párosuló hamis rész gyakran nagyon abszurd (például az 5G-tornyok és a Covid–19 összefüggése).

A fogalmi áttekintések, terminológiai elhatárolás kapcsán tehát véleményünk szerint a dezinformáció – jelentéstartalmának kettősségéből kiindulóan – adekvát módon alkalmazható a kutatásunk során megjelenő tevékenységek összefoglaló leírására.

Esettanulmány

A bevezetőben bemutatott 5G-tornyok kapcsán kialakult társadalmi bizonytalanság közismertnek mondható, esetében egy szélsőséges nézetű csoportra helyezzük a hangsúlyt. A fejezetben kapcsolódva a 2. ábrán bemutatott eléréselemzéshez, itt a szélsőséges csoport említéseit elemezzük kiválasztott szélsőséges közösségimédia-platformokon is. Illetve a 3. fejezet foglalkozik az elektromos autók eléréseivel, illetve bejegyzéseivel a kiválasztott szélsőséges platformokon. A fejezetben lévő eléréseket azért elemezzük, hogy legyen egy konkrét viszonyítási alap a szélsőséges csoport említéseihez.

Azt nem mondhatjuk, hogy a közösségi médiában jelen lévő „abszurd" témákat a felhasználók elvetik, és automatikusan szűrik, hogy épp miben bíznak meg. Az egyik legnépszerűbb dezinformációra nyitott közösség a QAnon-csoport, akik az amerikaikormányzat-ellenes hírekben hisznek, illetve abban, hogy az államot valójában egy hátsó hatalom, *deep state* irányítja. A csoport szinte minden népszerű közösségimédia-platformon jelen van (Facebook, Twitter/X), de fő színtere a 4chan és a Telegram.[19] A csoport esetében sajnos nem mondhatjuk azt, hogy ők „csupán" a nézeteiket terjesztik az interneten. Előfordul, hogy tettlegességig és jogsértésig fajul a nézetérvényesítés. Phillip Wright például páncélozott gépjárművével (amelyben két géppuska, két maroklőfegyver és 900 darab töltény volt) torlaszolta el a Hoover-gátat azért, hogy egy, a csoport által megkérdőjelezett kormányzati jelentést megtudjon.[20]

Phillip Wright esetének említése után most a QAnon-csoport közösségi médiás említésszámának vizsgálatára helyezzük a hangsúlyt. Ennek az elemzésnek az a célja,

[19] Hoseini et al. 2023.
[20] Holoyda 2022.

hogy összehasonlítási alapot biztosítson a későbbiekben bemutatandó elektromos autók témakörének vizsgálatához ugyanezeken a platformokon. A QAnon mint szélsőséges mozgalom jelenléte és említésszáma jelentős kontextust ad a társadalom érdeklődési és figyelmi fókuszainak feltárásához, és ennek mértékét hasznos lehet összevetni egy technológiai és fenntarthatósági szempontból fontos, de kevésbé polarizáló témával, mint az elektromos autók.

A csoport közösségimédia-trendjét (említéseit) az OpenMeasures szoftver segítségével referenciaként megvizsgáltuk a 2023. 06. 10. és 2023. 12. 09. közötti időszakban, amit az 5. ábra prezentál. A bevezetőben említett lekérdezési kihívás itt is felmerült, így a kiválasztott időszakot az elérhető adatok határozták meg. Ebben az esetben is, mivel harmadik platformról szereztük be az adatokat, nem ismert a gyűjtés laborkörnyezete, így nem tekinthetjük azokat reprezentatívnak.

A vizsgálat három platformra terjedt ki: Telegram, 4chan és Truth Social. A 3. fejezetben, amely a kutatás módszertanát tisztázza, részletezzük, hogy miért ezt a három platformot választottuk, és hogyan töltöttük le az adatokat.

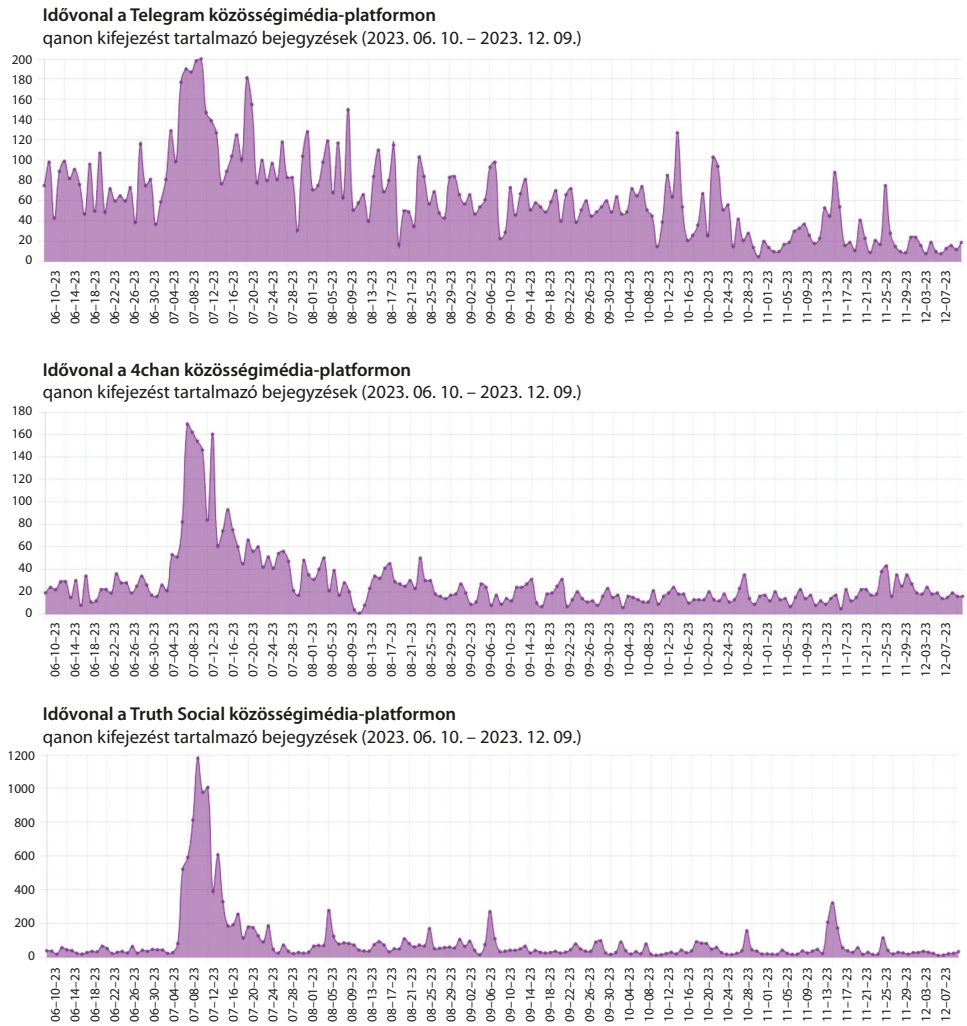
Az elemzés csak a „QAnon" kulcsszóra terjed ki, amelyet a 4. ábra mutat be. Feltételezzük, hogy a közösség által tárgyalt témák ennél tágabbak, és gyakran nem tartalmazza a QAnon szót a beszélgetés. A publikáció kutatási irányára tekintettel ezért ezt csak referenciajelleggel vizsgáltuk. Látható, hogy a közösség mindhárom platformon időszerű téma. A csoport kiinduló platformja a 4chan volt, amelyhez képest most már a Telegram és a Truth Social átvette említésekben a népszerűséget. A Telegram esetében a bejegyzések kezdeti kiugrása tapasztalható. A kiugrást követően júliusban tetőzött a bejegyzések száma, azt követően pedig lassú csökkenő tendencia volt jelen, időnkénti kiugrásokkal. A 4chan esetében egy jelentősebb kiugrást láthatunk, amit visszaesés követ. Kirajzolódik, hogy általánosságban alacsony a felhasználói interakció a téma körül, tehát a beszélgetés folyamatos csökkenő tendenciát mutat. A Truth Social platform követte a 4chan-hez hasonló tendenciát, egy sokkal magasabb kiugrással. A napi említési számok nagyban hasonulnak a Telegramhoz, viszont a július elején látható kiugrás sokkal számottevőbb volt.

Az ábra arra világít rá, hogy a szervezet körüli közösségi médiás említésszám nem magas. Mindössze havi pár száz bejegyzés kapcsolódik hozzájuk (a kevésbé moderált platformokon), viszont a gyakorlatban a szervezet kifejezetten aktív. A 2021-ben az Egyesült Államokban lezajló capitoliumi tüntetések során több kulcsfigura (például Sámán) is QAnon-tag volt.[21] A csoport jelenlétének mérése a közösségi médiában nehézkes, mert amit főleg mérni tudunk, az az, hogy irányukba milyen említések merülnek fel. Privát beszélgetéseket, végpontok között titkosított üzenetváltásokat elemezni nem tudunk. Ezzel a problémával a hatóságok is szembesültek. Határozottan az Egyesült Államok Capitol-tüntetései során, ugyanis a szélsőjobboldali csoportok végpontok között titkosított üzenetváltásokkal kommunikálnak.[22]

Viszont a lekérdezésből kirajzolódik, hogy mindhárom platformon 2023. július 08. és 2023. július 20. között magas kiugrás történt a kulcsszóra. Részletesen megvizsgáltuk az elérhető bejegyzéseket, és az állapítható meg, hogy a megugró említésszámot

[21] *Capitol Riot: »QAnon Shaman« Jacob Chansley Sentenced to 41 Months in Prison* 2021.
[22] Feldstein–Gordon 2024.

a 2023-as *Sound of Silence* című film okozta, és még a FoxNews is felkapta a hírt, miszerint az emberkereskedelemről szóló *Sound of Freedom* című filmet a liberális médiumok QAnon-közelinek minősítették.[23] Az elérhető bejegyzésekben is hasonló véleményeket láthatunk. Illetve még egy hír okozott kiugrást: QAnon Shaman börtönbüntetése is témává vált,[24] amelynek, úgy látjuk, mozgatórugója Tucker Carlson videója volt.



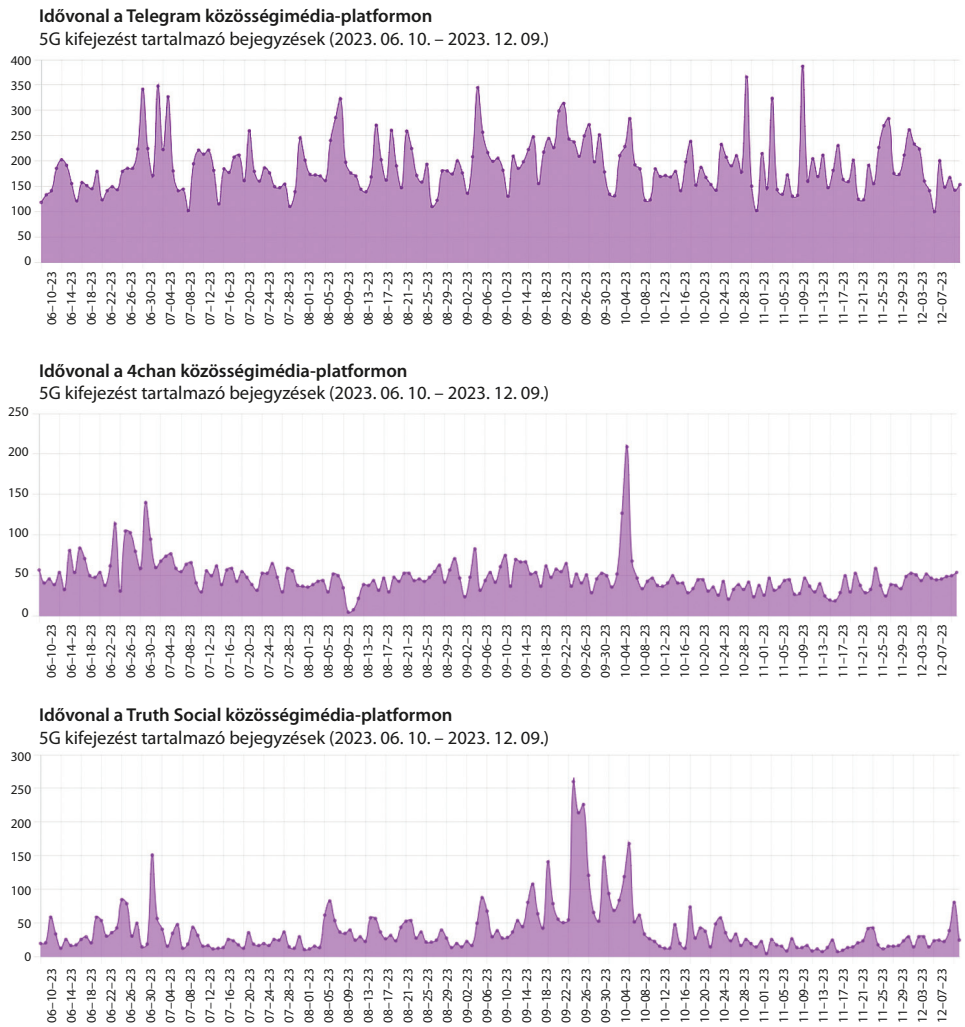
4. ábra: A QAnon-csoport említései a Telegram, a 4chan és a Truth Social közösségimédia-platformokon, idővonalon ábrázolva

Forrás: a szerző szerkesztése az OpenMeasures alapján

[23] Hays 2023.
[24] Truth Social. Post: Qanon shaman.

A hozott esetpéldákkal az elektromos autókhoz viszonyítás mellett, azt akarjuk szemléltetni, hogy a felhasználókban van nyitottság a dezinformáció irányába, függetlenül attól, hogy az adott információ mennyire reális. Nem szabad alábecsülnünk a veszélyeit, hiszen akár egy kormányzati épület ostromához is vezethet a kezeletlen álhír.

De ha az Ipar 4.0-hoz szűkebben nézzük a kérdéskört – bevezetőnkhöz kapcsolódva –, akkor sajnos az 5G-tornyok elleni támadások is egyfajta kitettséget mutatnak. A QAnonhoz viszonyítva a 5. ábrán látható az 5G kulcsszó említéseinek megoszlása.



5. ábra: Az 5G kulcsszó említése a Telegram, a 4chan és a Truth Social közösségimédia-platformokon, idővonalon ábrázolva

Forrás: a szerző szerkesztése az OpenMeasures alapján

Az ábra első része a Telegramon történő említéseket ábrázolja, ahol az aktivitás viszonylag egyenletes, de több kiugró csúcs figyelhető meg a vizsgált időszakban. Ezek a csúcsok egyes időszakokban 200-250 bejegyzést is elérnek, ami azt jelzi, hogy időnként megnövekszik az „5G" kifejezéshez kapcsolódó érdeklődés. Utána a 4chan következik, ahol az aktivitás általában alacsonyabb szinten mozog a Telegramhoz képest. Itt is látható egy jelentős kiugrás, amely valószínűleg valami specifikus eseményhez köthető, ami rövid ideig megnövelte az érdeklődést. Az utolsó grafikon a Truth Social platform említéseit ábrázolja. Itt az aktivitás változatosabb, több csúcs is látható, amelyek közül néhány eléri a 300 bejegyzést is. Az említések száma tehát időnként intenzívebben emelkedik ezen a platformon, ami azt jelezheti, hogy az „5G" kifejezés itt is egy-egy konkrét esemény kapcsán válik különösen népszerűvé.

A 4chan és a Truth Social kiugrása hasonló időszakban történt. A 4chan esetében konkrétan nem tudtuk meghatározni a kiugrás okát. A Truth Socialön teljesen értelmezhetetlen volt a kiugrás oka a felhasználók közötti csapongás miatt. Egy, már nem elérhető YouTube-videóra mutat több bejegyzés, illetve összefüggéstelenül 5G-dezinformációt osztanak meg. Jelen van az ukrán háború és az 5G kapcsolata, ukrán háború, 5G és biofegyverek, oltás és 5G, 5G és léghullámok, illetve biofegyverek és oltás.[25] Itt inkább egy furcsa felpörgést láthatunk, amit konkrétan nem tudunk eseményhez kötni, lehet kapcsolódási pont az ukrán biofegyverekkel kapcsolatos dezinformáció, de ez inkább említésként jelenik meg más témák mellett.

Összehasonlítva a két ábrát („QAnon-" és „5G-" említésszám) látható, hogy a kiugrások a két téma kapcsán nincsenek összefüggésben a három platformon. A Telegram esetében nincs is jelen kiugrás, hanem folyamatosan beszélnek az 5G-ről, míg a Truth Socialön egy kiugrást leszámítva minimális az 5G körüli interakció. A 4chan és a Truth Social esetében a felhasználói interakció elenyésző, de a mennyiséget nézve azonos a QAnon említéseivel. Az 5G-technológiáról feltételezzük, hogy már a terjedése után főleg a szakértők beszélnek róla. Ehhez képest a szélsőséges közösségimédia-platformokon látható, hogy jelen van egy folyamatos diskurzus. A kommenteket megvizsgálva viszont az volt látható, hogy dezinformáló tartalmat osztanak meg a felhasználók, például: „The jews used the 5g in the vaccines to turn all the burgers into impossible burgers. Woke vaccine impossibled our burgers."; „It is infussed with ESTROGEN delivering plastic and SIssys hypno 5G Rays. You still wante it little FAGGOT?". A kutatási témához kapcsolódóan fókuszunk az elektromos autók és a klímaváltozás, amire a következő fejezetben térünk ki. De kiemelendő, hogy az 5G körüli álhírek és dezinformáció továbbra is súlyos probléma.

Kutatási téma és módszertan

A bevezetőben bemutattuk egy szélsőséges csoport és az elektromos autók közösségimédia-trendjeit szélsőséges közösségimédia-platformokon. Látható, hogy ez egy nagyon aktuális téma és mindenképp meghatározó, hogy a felhasználók erről mit gondolnak. Ehhez kapcsolódóan elvégeztünk elemzést szélsőséges közösségimédia

[25] *Posts from Truth Social containing '5G'.*

platformokon is. A platformválasztás alapját az erősen moderálatlanság adta. Több ilyen platform is van, például 8kun, Telegram, Gab, 4chan, Truth Social, viszont a lekérdezésnél korlátozó tényező volt az elérhető adatmennyiség. Ahogy előzetesen említettük, a lekérdezések nehezebbé váltak a közösségimédia-platformokon, így harmadik platformot kell használnunk adatgyűjtéshez. Megbízhatóan a Telegramról, 4chanről és Truth Social-ről volt elérhető adat az OpenMeasures szoftverén keresztül. Itt is ki szeretnénk emelni, hogy az adatok így semmilyen módon nem tekinthetők reprezentatívnak. Harmadik platformon keresztül kérdeztünk le adatot, és a laborkörnyezet, illetve a gyűjtésmód részben ismeretlen. Az OpenMeasures automatizáltan gyűjt nyers adatot általuk szélsőségesnek tekintett közösségimédia-platformokról. Ezekben az adatokban lehetőség van nyíltan kifejezésekre keresni és elérést vizsgálni. Bizonyos mértékben nyers kommenteket is el tudunk érni. Az OpenMeasures arra szolgál, hogy segítse az újságírókat, kutatókat és társadalmi vállalkozásokat az olyan káros online tevékenységek, mint a szélsőségesség és a dezinformáció kivizsgálásában. Nyílt forráskódú és vállalati felhasználói közösségeink pedig funkció- és adatigényléseket tesznek, hogy segítsenek irányítani az eszközeinket.[26]

A lekérdezési időszak 2023. 06. 10-től 2023. 12. 09-ig tartott, szintén a lekérdezési időt az összefüggően elérhető adatmennyiség határozta meg.

Az elektromos autó kulcsszavakat ellenőriztük, az EV kulcsszó nem változtatott az eredményeken.

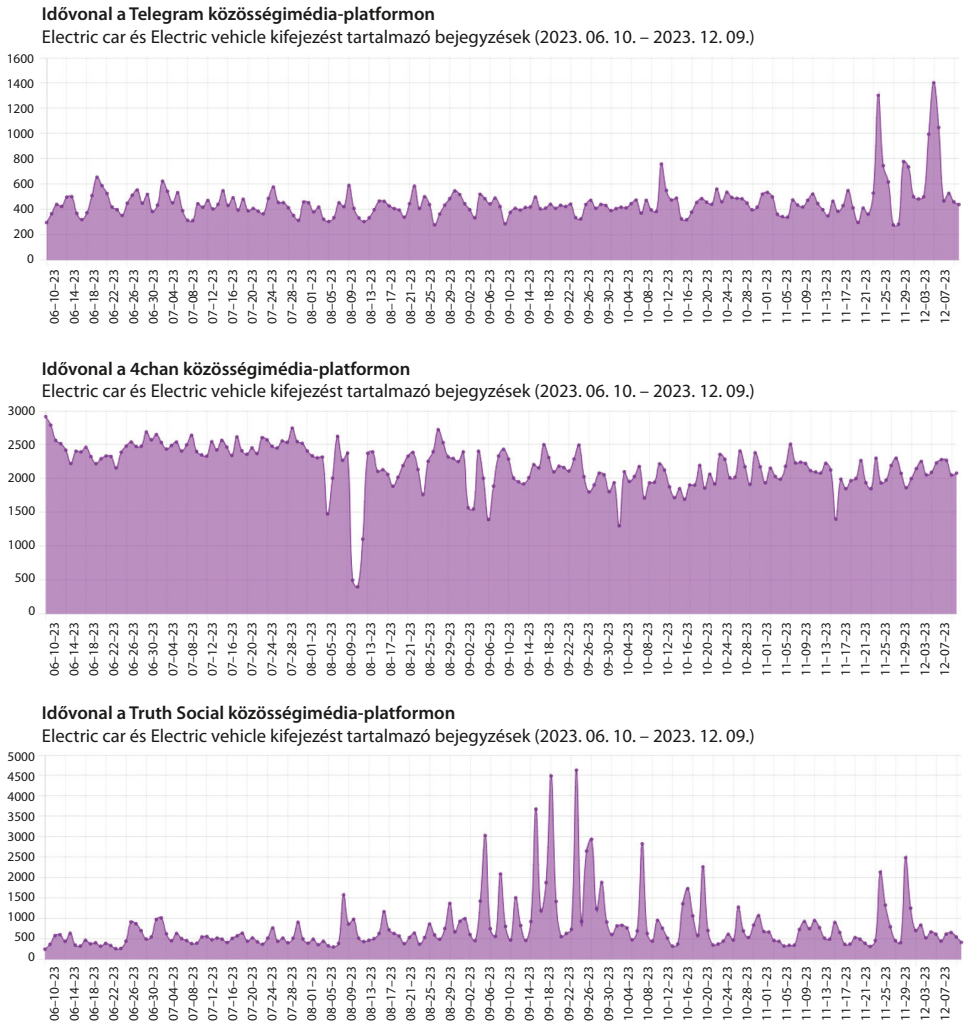
A 6. ábra két összevont kulcsszót tartalmaz *(electric car és electric vehicle)*. A Truth Socialnél azonos népszerűséget láthatunk, egy jelentős kiugrást leszámítva. A három platform közös jellemzője, hogy mindegyiken folyamatosan jelen van az *electric car* és *electric vehicle* kifejezések említése a vizsgált időszak alatt, ami arra utal, hogy az elektromos autók témája mindhárom közösségi térben releváns. Azonban az aktivitás dinamikájában különbségek figyelhetők meg: míg a 4chan említésszámai viszonylag stabilan, állandó szinten mozognak, addig a Truth Socialön nagyobb kilengések és kiugró csúcsok láthatók, ami intenzívebb, időszakos érdeklődést jelez. A Telegram szintén viszonylag állandó érdeklődést mutat, de kisebb kilengésekkel és néhány kiemelkedő nappal, ami arra utal, hogy ez a platform is mérsékeltebb aktivitást mutat a Truth Socialhöz képest.

A 4chan esetében láthatjuk a legnagyobb mennyiségű említésszámot a három platform közül. Az előzőleg a 4. és 5. ábrán bemutatott 5G és QAnon lekérdezésekhez viszonyítva az elektromos autókról folytatott diskurzus sokkal számottevőbb. A 4chanen és a Truth Socialön gyakoriak a jelentős hullámzások, amelyek azt jelzik, hogy a diskurzus változékony, és az elektromos autókhoz kapcsolódó témák iránti érdeklődés időszakosan csökken vagy nő. Ez arra utalhat, hogy az elektromos járművekkel kapcsolatos tartalmak néha heves vitákat generálhatnak a platformon, ami időszakos visszaesésekhez és fellendülésekhez vezet. A Truth Socialön a legeltérőbb az aktivitás a két másik platformhoz képest, körülbelül tíz esetben van kiemelkedő kiugrás az elektromos autók kapcsán. Ebből a két legjelentősebb 2023. szeptember 18-án és 2023. szeptember 22-én látható. Itt a kiugrásokban nagyon érdekes, hogy 2023. szeptember 29-én jelentette be Donald Trump elnökjelölt, hogy az elektromosautó-piacot támogató

[26] Forrás: OpenMeasures.io.

kormányzati döntéseket háttérbe fogja helyezni, és támogatja a fosszilis üzemanyagú járműipart.[27] A lekérdezésben viszont nem láthatunk semmilyen kiugrást egyik platformon sem a téma kapcsán. Az adatokból konkrétan nem tudtuk megfejteni, hogy a szeptember 18-i és 22-i kiugrást mi okozhatta. Megnéztük az adott időszak fő híreit, de nem találtunk számottevő bejelentést, ami okot adhat a kiugrásra. Az elérhető lekérdezett kommentek között vizsgálva azt állapíthatjuk meg, hogy a kiugrást Donald Trump elnökjelölt Truth Social-bejegyzése okozta,[28] amelyben teljes katasztrófának nevezte az elektromos autók gyártását.[29] Biztosan nem tudjuk kijelenteni, de úgy látjuk az elérhető bejegyzésekből, hogy ez a bejegyzés adott gyújtóerőt a felhasználók között, akik elkezdték saját véleményüket és nézeteiket posztolni az elektromos autókról. Catturd2 felhasználó például a Truth Socialön 8300 kedveléssel és 1740 újramegosztással szánalmasnak és értéktelennek nevezi az elektromos autókat és a hozzájuk kapcsolódó politikai döntéseket.[30] Ugyanennek a felhasználónak aznap szintén hasonlóan népszerű (8800 kedvelés és 2140 újramegosztás) bejegyzése volt arról, hogy a világot fosszilis üzemanyagok hajtják, és a napenergia, a szél és az elektromos autók államilag támogatott fantáziaországot működtetnek.[31] Ezek alapján azt állapíthatjuk meg, hogy a kiugrás oka nem egy tényleges esemény volt, hanem felhasználók közötti interakció, amelynek a központi eleme Trump elnökjelölt nézete az elektromos autókról, amit aznap osztott meg a platformon. A 4chanen 2023. augusztus 13-án látható kiugrást pontosan nem tudtuk meghatározni. A visszaesésre nem találtunk konkrét okot. A Telegramon 2023. december 3-án látható kiugrást a bejegyzések elemzésével a Tesla vállalat Cybertruck modelljének szállítási bejelentéséhez köthetjük. 2023. december 1-jén jelentette be a Tesla, hogy megkezdik a Cybertruck modellek szállítását a megrendelőknek; ez a felhasználók között nagyobb megosztást és interakciót okozott. A Truth Social-bejegyzéssel ellentétben itt elmondhatjuk, hogy a kiugrás egy pozitív érzelmű hírhez köthető, míg a Truth Socialön egy erősen negatív hangulatú hír okozta a kiugrást.

[27] Meyersohn 2023.
[28] Truth Social. Truth Social.
[29] Eredeti bejegyzés: The all Electric Car is a disaster for both the United Auto Workers and the American Consumer. They will all be built in China and, they are too expensive, don't go far enough, take too long to charge, and pose various dangers under certain atmospheric conditions. If this happens, the United Auto workers will be wiped out, along with all other auto workers in the United States. The all Electric Car policy is about as dumb as Open Borders and No Voter I.D. IT IS A COMPLETE AND TOTAL DISASTER! Magyarra fordítva: Az összes elektromos autó katasztrófa mind az Egyesült Autóipari Dolgozók Szakszervezete, mind az amerikai fogyasztók számára. Mindet Kínában fogják gyártani, túl drágák, nem mennek elég messzire, túl sokáig tart a feltöltésük, és bizonyos időjárási körülmények között különféle veszélyeket jelentenek. Ha ez bekövetkezik, az Egyesült Autóipari Dolgozók Szakszervezete, valamint az összes többi amerikai autóipari dolgozó el fog tűnni. Az elektromos autókra vonatkozó politika éppolyan ostobaság, mint a nyitott határok és a választói igazolvány nélküli szavazás. TELJES ÉS TÖKÉLETES KATASZTRÓFA!
[30] Truth Social. Post.
[31] Truth Social. Post: Wind and Solar.



6. ábra: Az Electric vehicle és Electric car kulcsszó említése a Telegram, a 4chan és a Truth Social közösségimédia-platformokon idővonallal ábrázolva

Forrás: a szerző szerkesztése az OpenMeasures alapján

A bemutatott három közösségimédia-platform közül a Truth Social és a 4chan erősen szélsőjobboldali platform, így előzetesen azt feltételezzük, hogy a felhasználói nézetek nem az elektromos autó pozitív aspektusai irányába húznak. Ezt a feltételezést ellenőrizve megvizsgáltuk, hogy a kommentek tartalmilag hogyan csoportosíthatók. A Truth Socialön három témakörre osztható a kommentek/bejegyzések jellege:

- elektromos autók bevezetésével/megjelenésével kapcsolatban hírt osztanak meg;
- elektromos autókkal kapcsolatban összeesküvés-elméletet fejtegetnek (például a Biden-adminisztráció Kína segítségével hogy szorítja ki az amerikai ipart);
- Trump elnök az elektromos autókat érintő irányelvet vissza fogja vonni.

A 4chan platformon sokkal szélsőségesebb bejegyzések születtek a vizsgált időszakban, itt megállapítható két jelleg a bejegyzésekről:

- az elektromos autók kapcsán Elon Musk üzleti sikereit vitatják;
- a „zöldeket"/környezetvédőket szidják, akik az emberi fajt akarják tönkretenni (ebbe beletartozik a bogárevés összeesküvés-elmélete is).

A negatív bejegyzési trend folytatódik a Telegramon is. A jelentősebb eltérés a 4chan és a Truth Social-platformhoz képest, hogy itt a felhasználók híreket osztanak meg az elektromos autók helyzetéről. Felmerülő vitakérdés a fenntarthatóság és az akkumulátorgyártás témaköre. A Telegramon vizsgált tartalmak esetében viszont nem volt érezhető erős dezinformációs jelenlét. Megtévesztő információ a vizsgált posztokban merült fel, de egyértelmű dezinformatív tartalom nem volt látható a bejegyzésekben. A 4chan és a Truth Social esetében viszont volt több olyan bejegyzés, amiről egyértelműen látható, hogy ártó szándékú megtévesztő tartalom. Feltételezésünk az, hogy a felhasználó a tartalommal egyetért, és hisz benne. Ezekben a kommentekben látható összefüggés az elektromos autók és a klímaváltozás-tagadás között. A 2. táblázatban (példálózó jelleggel) kiemeltünk pár ilyen kommentet. A kommenteket angolról magyarra fordítottuk, ahol a szleng relevanciával bír vagy nem igazán fordítható magyarra, ott zárójelben mögötte dőlten meghagytuk az eredeti kifejezést. Illetve a kommenteket fordítás során nem javítottuk, és nem finomítottuk a nyelvezetet, ezért a legtöbb erősen durva kifejezést használ egyes társadalmi csoportokra, illetve hovatartozásokra. A kommentek eredetiségének megőrzésével célunk szemléltetni azt, hogy ténylegesen milyen a kommunikáció ezeken a platformokon, és ezzel is prezentáljuk azt, hogy miért tekinthetők szélsőségesnek a platformok.

2. táblázat: Példaválogatás az elektromos autókkal kapcsolatos dezinformatív kommentekből

Szerző **Fórumrész**	**Komment**
Anonymous Üzenőfal: o	Úgy tűnik, ők a világ legnagyobb elektromos járműveket gyártó vállalata, és Kínából származnak. De nem sok autójukat láttam még az utakon. De mit jelent a nevük?
Anonymous Üzenőfal: sp	Saját magunkat basszuk meg azzal, hogy a faölelő retardáltakra hallgatunk, akiknek az a fő céljuk, hogy a természetkultuszukkal akadályozzák az emberi fajt. Úgy akarod megóvni a természetet, hogy túlárazott elektromos autót veszel? Rendben, csak tedd meg, leszarom. Veszek magamnak egy benzinüzemű autót. Olcsóbb, ugyanazt a munkát végzi, mint a te elektromos szarládád *(shitbox)* (és még jobb is), és könnyebb karbantartani. Ti faölelő komcsik csak annyit akartok, hogy minél több szabadságot vegyetek el az emberektől. Irányítani akarjátok az életünket, megmondjátok nekünk, hogy mit együnk a „neeee ne az én állatos:((((" *(itt eredetileg a „noooo not my animalinos" kifejezés szerepelt, amivel, feltételezzük, a szerző a spanyol anyanyelvű bevándorlók támogatóit próbálta kifigurázni)* baromságokkal, leállítjátok az orvosi vagy bármilyen más kutatást, hogy megóvjatok néhány kibaszott madárfajt a kihalástól, bármilyen okból kifolyólag, megállítjátok az emberiség elkerülhetetlen terjeszkedését ezen a bolygón.

Szerző Fórumrész	Komment
Anonymous Üzenőfal: sp	Ti vagytok itt a zsidók, csak nem veszitek észre. Több nukleáris, kevesebb olaj, gáz és szén. Naná, miért ne. Én mindezért vagyok és nem különösen mi, mivel mi kicsik vagyunk, hanem a feltörekvő országok, pl. Kína és India, amelyek sokat fogyasztanak. Még egyszer, miért ne. De a helyzet a következő: megbízható és hatékony atomerőművek építése kurva sok pénzt és főleg időt igényel. Ha ezek a nemzetek, amelyeknek minden kibaszott joguk megvan a fejlődéshez, növekedni akarnak, akkor szükségük van ezekre az erőforrásokra amilyen hamar csak lehet, ezért kell az olajra és a gázra támaszkodniuk.
Anonymous Üzenőfal: v	Meg fogod enni a bogarakat. Veszel egy elektromos autót. Kapsz egy rózsaszín hajú, BPD[32]-s barátnőt.
Anonymous Üzenőfal: pol	Mi lenne, ha egy kalapáccsal szétverném az önelégült köcsög fejedet. Paki[33] vadonatúj elektromos autóval megerőszakolja az essexi diáklányt, ez a szegénység kérdése. Remélem, kapsz egy jó adag AIDS-et a szaros lukadba.
Anonymous Üzenőfal: pol	Nincs semmi mondanivalód? Akkor a régi haraghoz és erőszakkal való fenyegetőzéshez folyamodsz? Klasszikus. A vadonatúj elektromos autóval essexi diáklányt megerőszakoló erőszaktevő a szegénység problémája…; A szegénység problémája, igen, az, igen, de az ilyen esetek gyakoriságát is túlbecsülöd… És köszi, hogy beleszuszakoltad az elektromos autók iránti gyűlöletedet, mi?
Anonymous Üzenőfal: pol	Évtizedek óta távvezérléssel zuhantatnak le repülőgépeket és helikoptereket, hogy politikusokat gyilkoljanak. Természetesen az önvezető autókat is arra fogják használni, hogy ellenőrizzék vagy megöljék a zavaró polgárokat. Ismerek olyan embereket, akik minden technikai újítást elfogadnak, olyannyira, hogy a pénzüket bank helyett Venmón tartják, szar elektromos autóval járnak, és állandóan töltőállomást keresnek hozzá (az itteni drogosok minden töltőkábelt elvágnak a rézért), és amikor jönnek az agyi implantátumok, ő lesz az első a sorban, ő mondta. Nem tudom, milyen trauma tette őt ennyire mazochistává, de attól tartok, hogy sokkal többen vannak, akik bevették a zsidó hollywoodi Star Trek-álmot.
Anonymous Üzenőfal: pol	Globális felmelegedés, haver. És amikor karácsony közeledtével hideg lesz, az dupla globális felmelegedés. Most vegyél egy elektromos autót, és élj egy 15 perces városban, és fogd be a szád!

Forrás: a szerző szerkesztése

Összességében láthatjuk, hogy rengeteg dezinformatív tartalom merül fel a példakommentek között. Van, ami kormányzati irányításról és kontrollról szól, van komment, amely a klímaváltozást parodizálja, illetve van a baloldal népszerű politikáit gúnyoló is (például: elektromos autók, kevesebb húsfogyasztás). Ezek jelenléte kifejezetten aggasztó, mert így a valós tartalom is bizalmatlanságot vet fel, ami a dezinformáció egyik kulcseleme.

[32] A BPD a *Bipolar Disorder* (bipoláris zavar) rövidítése, amely magyarul a bipoláris személyiségzavarnak felel meg. Szélsőséges platformokon gyakran szatirikusan ábrázolják a baloldali nézetű férfiakat, és ennek egyik módja, hogy barátnőjüket BPD-vel azonosítják.

[33] A *paki* kifejezés itt a pakisztáni származásra utal.

A dezinformáció metszéspontjai: Bejegyzéselemzés szélsőséges közösségimédia-platformokon

A három kiválasztott szélsőséges közösségimédia-platformról (4chan, Truth Social, Telegram) kommenteket gyűjtöttünk le. Célunk a kommentelemzésen keresztül bemutatni, hogy a kiválasztott platformon milyen a felhasználók véleménye, illetve vélekedése az elektromos autókról. A kommentek letöltése során rengeteg dezinformáló tartalommal találkoztunk, több összeesküvés-elmélet is felbukkant.

Az elemzést az elektromos autókra összpontosítva összesen 284 kommentet vagy bejegyzést vizsgálatunk. A letöltés során kirajzolódott, hogy a Truth Social platformon a legjelentősebb esemény a Rivian vállalat részvényeinek 90%-os értékvesztése volt.[34] Emellett a Telegram és Truth Social felületeken széles körben terjedt egy cikk Mr. Beanről, amely arról számolt be, hogy elektromos autóját belső égésű motoros járműre cserélte. Illetve jelentős Joe Biden-ellenes nézetek uralkodtak a bejegyzésekben.

3. táblázat: Az elektromos autókkal kapcsolatos kommentek megoszlása választott közösségimédia-platformokon

Közösségimédia-platform	Platformszámlálás (darab komment)	Sentimentszámítás (darab komment)
4chan	114,0	
Telegram	67,0	
Truth Social	103,0	
Negatív		74,0 (26%)
Semleges		56,0 (20%)
Pozitív		154,0 (54%)

Forrás: a szerző szerkesztése

Az elemzett bejegyzések 54%-a pozitív hangvételű, azonban fontos megjegyezni, hogy ez nem feltétlenül jelenti az elektromos autókkal szembeni pozitív érzelmeket. Inkább a megosztott hírek váltanak ki pozitív reakciókat. Az alábbi táblázat néhány példát mutat be erre a jelenségre. A bejegyzések között pozitív érzelműek sajátos módon azok voltak, amelyek arra reagáltak, hogy Trump elnök eltörli a Biden-adminisztráció EV-vel kapcsolatos közpolitikáját. Ha szigorúan nézzük, hogy a kommentek közül milyen mértékű ténylegesen az elektromos autókkal szembeni pozitív érzelmű, akkor csak a Tesla-töltők kiterjesztéséről szóló bejegyzés tekinthető annak.

[34] Partoll 2023.

4. táblázat: Példák az elektromos autókkal kapcsolatos pozitív érzelmű bejegyzésekre

1. bejegyzés: Kalifornia 20%-kal fog elmaradni a szükséges villamos energia előállításától, hogy teljesítse az államok 100%-os elektromos járművekre vonatkozó mandátumát a kaliforniai Pacific Research Institute szabadpiaci agytröszt által kiadott új jelentés szerint.
2. bejegyzés: A Tesla töltői egyre több támogatót nyernek, mivel a csatlakozója amerikai szabvány lesz. A Tesla Inc. töltési technológiája újabb támogatókat nyert, mivel az elektromos járműveket működtető iparág egy maroknyi szereplője közölte, hogy kompatibilis berendezéseket kínál, ami tovább erősíti, hogy az autógyártó rendszere amerikai szabvány legyen. A ChargePoint Holdings, Inc., a Blink Charging Co. és a Wallbox NV hétfőn közölte, hogy olyan töltőkkel fognak rendelkezni, amelyek képesek együttműködni a Tesla észak-amerikai töltési szabványával, ami gyorsan nyerésre áll az úgynevezett kombinált töltési rendszerrel folytatott versenyben. Az ausztrál Tritium DCFC Ltd. szintén közölte, hogy NACS-csatlakozó opciót kínál majd a töltőivel. A bejelentések gyors egymásutánja mindössze néhány nappal azután következik be, hogy az autóipari óriások, a General Motors Co. és a Ford Motor Co. megállapodtak abban, hogy csatlakoznak Elon Musk vállalatához, és szabványosított NACS-csatlakozókat vezetnek be a jövőbeli modellekbe. Bloomberg a TITVN-en keresztül.
3. bejegyzés: RT@epochtimes „Ez biztosan az első napon véget ér" – mondta Trump. A volt elnök@realDonaldTrump kijelentette, hogy ha újraválasztják, az első napon megszünteti a demokraták #ElectricVehicle (EV) politikáját. (Lásd: Lord 2023.)

Forrás: a szerző szerkesztése

A bejegyzések 20%-a semleges érzelmet mutatott (5. táblázat). Ide tartoznak azok a bejegyzések, amelyekben a felhasználók egymást tájékoztatták az elektromos autókkal kapcsolatos hírekről, és ezt semleges hangvétellel tették. Fontos megjegyezni, hogy ezek a bejegyzések sem mutattak pozitív érzelmeket az elektromos autókkal kapcsolatban; lényegében negatív híreket osztottak meg semleges vagy közönyös érzelmek kíséretében. A kommentek vizsgálatánál itt is látható volt, hogy több dezinformáló hír jelent meg.

5. táblázat: Példák az elektromos autókkal kapcsolatos semleges érzelmű kommentekre

Rowan Mr. Bean Atkinson beismeri, hogy becsapták a napsütötte állítások az elektromos járműről, visszatér a belső égésű autókhoz.
RT FoxNews: Több mint 150 republikánus fog össze, hogy elítélje Biden meggondolatlan, elektromos járművekre irányuló törekvéseit.
Shapiro: Látott már elektromos autó akkumulátortüzet, amit órákig tart eloltani?

Forrás: a szerző szerkesztése

A bejegyzések 26%-a kifejezetten negatív érzelmeket közvetített az elektromos autókkal kapcsolatban (6. táblázat). Ebben a csoportban jelentek meg leginkább az összeesküvés-elméletek, a Biden-kapcsolatok és a világ pusztulásáról szóló narratívák.

6. táblázat: Példák az elektromos autókkal kapcsolatos negatív érzelmű kommentekre

Az elektromos autó dolog, az a tény, hogy Biden dobott trilliókat az autógyáraknak, de nem kényszerítette őket, hogy használjanak egy szabványos akkumulátort, amit el lehet távolítani az autóból, és kicserélni egy teljesen feltöltöttre, ami azt jelenti, hogy nem igazán komolyak az elektromos autók, és ez csak egy átverés, hogy az adófizetők pénzét megszerezzék.
Utazz körbe a francia vidéken Eva kis elektromos autójának anyósülésén, miközben vegetáriánus éttermeket keresel, és tökön vág, amikor nem figyelsz oda az állatkínzásról szóló szónoklataira. Vége. Csak haljak már meg álmomban.
Trump egyértelműen be fogja bizonyítani, hogy politikailag motivált nyomozással néz szembe: volt munkatársak, informátorok stb. felfedik a politikai indítékokat, hivatalos dokumentumok igazolják az FBI együttműködését Trump ellenfeleivel. Elektromos járművek (EV) politikája, a Hunter Biden-laptop ügye és az orosz összejátszás hazugságai – 51 volt hírszerzési tiszt, köztük Clapper és Brennan állította, hogy ez egy orosz művelet volt bizonyíték nélkül. A volt CIA-helyettes Morell bevallotta, hogy Blinken, Biden vezető tanácsadója ösztönözte a levelet, független ellenőrzés nélkül. Durham különleges ügyész pedig feltárta az FBI hibás és elfogult, 'Crossfire Hurricane' nyomozását: thehill.com, judiciaryhouse.gov.

Forrás: a szerző szerkesztése

Összességében elmondható, hogy az elektromos autókat kifejezetten nagy interakció és negatív érzelem övezi a szélsőséges közösségimédia-platformokon. A vizsgált három platformon lényegében semmilyen pozitív érzelem nem övezi a kérdéskört. Pozitív érzelemmel viszonyultak a felhasználók bizonyos bejegyzésekhez, de ezek a bejegyzések az elektromos autókra nézve nem pozitív hírűek, hanem elektromos autókat negatívan érintő politikai döntések felé viszonyultak pozitívan. A legnépszerűbb és legtöbbet újraposztolt bejegyzéstípus ebben a kategóriában az volt, hogy Rowan Atkinson elektromos autóról belső égésű motorú autóra váltott. Ez a felhasználókból pozitív érzelmet váltott ki, de összességében az elektromos autókra nézve nem pozitív hír.

A kommentek elemzéséből levont következtetés az, hogy a szélsőjobboldali platformokon a felhasználók rendkívül bizalmatlanok az elektromos autókkal szemben. Ez aggasztó, mivel már láthattuk, hogyan kapcsolták össze az 5G-technológiát és a Covid–19-járványt, ami szélsőséges megnyilvánulásokhoz vezetett. Az 5G-tornyokkal kapcsolatos korábbi tapasztalatokhoz hasonlóan, az elektromos autók és töltőállomások ellen is egyre gyakrabban fordul elő vandalizmus. Feltételezzük, hogy ennek oka az egyes csoportokban erőteljesen polarizált, gyakran félretájékoztatáson alapuló vélemény és érzelmek. Az ilyen jellegű vandalizmus jelzi, hogy az elektromos járművek térnyerése nem csupán technológiai és infrastrukturális kihívásokat vet fel, hanem társadalmi és kulturális feszültségeket is, amelyek akadályozhatják az új, fenntartható megoldások széles körű elfogadását. Mivel a szélsőséges platformokon nincs pozitív szemlélet az elektromos autókkal kapcsolatban, különösen nagy kihívást jelent, hogy a felhasználók körében pozitív véleményt alakítsunk ki ezekről a járművekről.

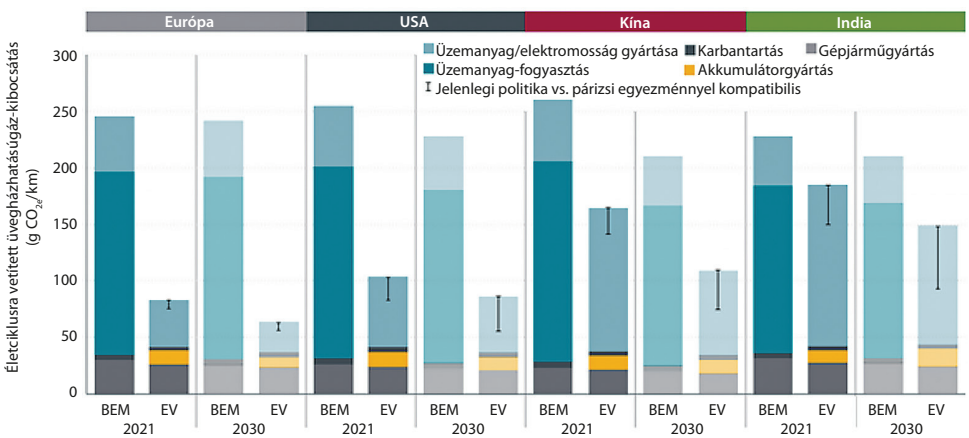
Fontos kiemelnünk a 2.2. esettanulmány fejezet, a 3. és 4. fejezet alapján, hogy a gyakorlatban úgy tűnik, a felhasználók nem szélsőséges csoportról beszélgetnek, azonban a diskurzus során keveredik a beszélgetésbe szélsőséges nézet a téma kapcsán. Hanem vannak témák, amelyek erős érzelmet váltanak ki a felhasználókból, és itt jelen esetben láthattuk, hogy erősen dezinformáló tartalmat foglal magába. Az a feltételezésünk, ami jövőbeli mélyebb kutatást igényel, hogy nem a közösség hozza

a szélsőséges csoportokat össze, hanem a dezinformáló témák. Ezekből a posztokból (elektromos autók témakörében) és a QAnon említésszámából ítélve azt javasoljuk, hogy nem a csoport ellen kell fellépni elsődlegesen, hanem a tartalmak moderációján keresztül kell fellépni. Ami a gyakorlatban nagyon nehéz, mert ezért az adott közösségimédia-platform a felelős, ami, ha szélsőséges és ilyen beállítottságú, akkor nem fogja moderálni ezt. Tehát a fellépésnek a platform ellen kell történnie, ha nem moderál dezinformáló tartalmakat.

Dezinformáció az Ipar 4.0 rendszerek ellen

Az előző fejezetekben megismertek alapján ebben a rövid összefoglaló fejezetben esetpéldákkal szemléltetjük, hogy miért probléma a gyakorlatban a dezinformáció az Ipar 4.0 ellen. A bevezetőben már szó volt az 5G-hálózatok elleni dezinformációs támadásokról, ami felhasználói bizonytalansághoz, félelemhez, illetve az eszközök megrongálásához vezetett.

Az elektromos autózás esetében is jelen van a felhasználói félelem. Ha nem a szélsőséges közösségimédia-platformok felől közelítjük meg, akkor enyhébb félelmet láthatunk. Ez úgy bontakozik ki a gyakorlatban, hogy terjed az a megtévesztő információ (nem dezinformáció), hogy az elektromos autók választása nem környezettudatosabb döntés.



7. ábra: Az elektromos és belső égésű járművek környezeti terhelése életkorukra vonatkozóan
Forrás: a szerző szerkesztése BIEKER *2021 alapján*

Ennek a változatát láthattuk szélsőséges oldalakon sokkal sarkalatosabban megjelenni. Ez azért nagyon aggasztó, mert ahogy előző esetekben (például 5G és Covid) begyűrűzött a köztudatba a dezinformatív tartalom, Bieker azt is feltárta tanulmányában, hogy az akkumulátorok környezeti hatása valójában nem nagyobb, mint a belső égésű autóké. Más források körülbelül 38 ezer megtett kilométerre teszik azt a pontot, amikor egy elektromos autó – gyártását is beleértve – környezetbarátabb lesz, mint egy

belső égésű jármű.[35] A példabejegyzésekben jól látható (2. és 6. táblázat), hogy az Ipar 4.0 és az elektromos autók kapcsán erős, sarkalatos nézetek alakultak ki. Gyakran találkozhatunk azzal a véleménnyel, hogy az automatizáció minden munkahelyet megszüntet, vagy hogy az elektromos autók környezetszennyezőbbek, mint a hagyományos járművek. Az elektromos autókhoz hasonló technológiák hiteltelenítése is gyakran része ezeknek a kampányoknak, amivel akadályozzák a fenntartható közlekedési és energiahatékonysági megoldások elfogadását. Az autógyártás esetében gyakran felmerül az automatizáció kérdése, amelynek az 5G-technológia alappillére tud lenni. Itt felmerülő társadalmi aggodalomként jelenik meg az a bizonytalanság, hogy az Ipar 4.0 eszközök és technológiák esetleg kiszoríthatják az embereket a munkaerőpiacról.[36]

Összegzés

Összességében elmondható, hogy a kutatás ezen részének célja az volt, hogy feltárja a dezinformáció szerepét és hatását az Ipar 4.0 rendszerek elleni támadásokban, különös tekintettel az elektromos autók témakörében. A kutatás során a *misinformation, malinformation* és *disinformation* fogalmak közötti különbségeket részletesen bemutattuk, hogy jobban megértsük ezen jelenségek mechanizmusait és következményeit. Vizsgálataink során szélsőséges közösségimédia-platformokat, mint a 4chan, a Truth Social és a Telegram, vettünk górcső alá. Célunk az volt, hogy feltérképezzük a dezinformációs tartalmak elérését és azok hatását a közösségre. Különös figyelmet fordítottunk a kommentek szentimentjének elemzésére, hogy megértsük a felhasználói reakciók érzelmi töltetét és polarizációját. A kutatásunk rávilágít arra, hogy a dezinformáció milyen mértékben befolyásolja az Ipar 4.0 rendszerek biztonságát és a társadalmi percepciót a klímaváltozás és az elektromos autók vonatkozásában.

A kutatás eredményei alapján megállapítható, hogy a dezinformáció hatással tud lenni az Ipar 4.0 rendszerek biztonságára és a társadalom elektromos autókról alkotott véleményére. A szélsőséges platformokon terjedő dezinformációs tartalmak nemcsak a közösségimédia-felhasználók véleményét polarizálják, hanem közvetlenül is veszélyeztetik az ipari rendszerek működését. Szeretnénk kiemelni, hogy a feltárt bejegyzések és nézetek alapján szükséges a közösségi média moderálása, mert aggasztóan szélsőséges nézeteket prezentáltak a posztolók. Az elemzett posztok és elérések alapján elmondható, hogy valójában nem a közösség (például QAnon) fogja össze a szélsőséges nézetű felhasználókat, hanem a nézetük alapján lépnek interakcióba egymással (például 5G vagy elektromos autók). Ezért azt javasoljuk, hogy a dezinformáció ellen nem a csoportokkal szemben érdemes fellépni, hanem a tartalommal szemben. A tartalom moderációjáért pedig maga az adott közösségimédia-platform a felelős: ha ők nem moderálják, akkor ténylegesen a platformmal szemben kell fellépni.

Összességében bízunk benne, hogy a kutatás hozzájárul a dezinformáció elleni küzdelemhez az Ipar 4.0 rendszerek védelme érdekében, és segít jobban megérteni az elektromos autók körüli társadalmi diskurzust befolyásoló tényezőket.

[35] P. A. R. 2024.
[36] *IPAR 4.0: Az elkerülhetetlen forradalom…* 2024.

Felhasznált irodalom

[gggghhhhzzzz] (2022): Nobody Is Noticing The Electric Car PsyOp. *Reddit,* 2022. március 26. Online: www.reddit.com/r/conspiracy/comments/tofc4b/nobody_is_noticing_the_electric_car_psyop/

Belügyminisztérium: Nem került szóba Budapest lezárása (2020). *Portfolio,* 2020. március 13. Online: www.portfolio.hu/gazdasag/20200313/belugyminiszterium-nem-kerult-szoba-budapest-lezarasa-419303

Bieker, Georg (2021): A Global Comparison of the Life-Cycle Greenhouse Gas Emissions of Combustion Engine and Electric Passenger Cars. *ICCT,* 2021. július 20. Online: https://bit.ly/4fYhdo3

Capitol Riot: „QAnon Shaman" Jacob Chansley Sentenced to 41 Months in Prison. *BBC,* 2021. november 17. Online: www.bbc.com/news/world-us-canada-59253090

Chan, Kelvin – Dupuy, Beatrice – Lajka, Arieta (2020): Conspiracy Theorists Burn 5G Towers Claiming Link to Virus. *AP News,* 2020. április 21. Online: https://apnews.com/article/health-ap-top-news-wireless-technology-international-news-virus-outbreak-4ac3679b6f39e8bd2561c1c8eeafd855

Chatterjee, Sheshadri – Chaudhuri, Ranjan – Vrontis, Demetris (2023): Role of Fake News and Misinformation in Supply Chain Disruption: Impact of Technology Competency as Moderator. *Annals of Operations Research,* 327, 659–682. Online: DOI: https://doi.org/10.1007/s10479-022-05001-x

Easterly, Jen (2023): The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. *CISA,* 2023. május 7. Online: www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Electric Vehicles [é. n.]. Online: https://www.energy.gov/save/electric-vehicles

European Commission (2018): *Final Report of the High Level Expert Group on Fake News and Online Disinformation. Shaping Europe's Digital Future.* 2018. március 12. Online: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation

Feldstein, Steven – Gordon, Sarah (2024): Are Telegram and Signal Havens for Right-Wing Extremists? *Foreign Policy,* 2024. június 20. Online: https://foreignpolicy.com/2021/03/13/telegram-signal-apps-right-wing-extremism-islamic-state-terrorism-violence-europol-encrypted/

Flō Networks (2023): *Revolutionizing Industry 4.0 with Private 5G Technology and Cloud Computing.* Online: https://flo.net/revolutionizing-industry-4-0-with-private-5g-technology-and-cloud-computing/

Hays, Gabriel (2023): Human-Trafficking Film 'Sound of Freedom' Trashed by Liberal Outlets as 'QAnon-Adjacent'. *Fox News,* 2023. július 7. Online: www.foxnews.com/media/media-outlets-trash-human-trafficking-film-sound-freedom-qanon-adjacent-mock-films-july-4-success

Holoyda, Brian J. (2022): The QAnon Conspiracy Theory and the Assessment of Its Believers. *Journal of the American Academy of Psychiatry and the Law Online,* 50(1), 124–135. Online: https://doi.org/10.29158/jaapl.210053-21

Hoseini, Mohamad et al. (2023): On the Globalization of the QAnon Conspiracy Theory Through Telegram. In *Proceedings of the 15th ACM Web Science Conference 2023*. 75–85. Austin TX USA: ACM. Online: https://doi.org/10.1145/3578503.3583603

IPAR 4.0: Az elkerülhetetlen forradalom – Minden, amit érdemes tudni róla. Online: www.tablazat.hu/cikkek/ipar-4-0/

Jakusné Harnos, Éva – Demeter, Márton – Bányász, Péter (2023): Social Media Issues and Fake News. In Molnár, Anna – Jakusné Harnos, Éva – Szente-Varga Mónika (szerk.): *Security, Resilience and Sustainability of the European Union*. Budapest: Ludovika, 131–147. Online: https://iris.unisalento.it/retrieve/3258a-af7-0cf7-4571-8008-b3eca8b7c899/1148_Security_Resilience_and_Sustaina-bility-muhdsk.pdf

Li, Lifang et al. (2020): Characterizing the Propagation of Situational Information in Social Media During COVID-19 Epidemic: A Case Study on Weibo. *IEEE Transactions on Computational Social Systems,* 7(2), 556–562. Online: https://doi.org/10.1109/TCSS.2020.2980007

Lord, Joseph (2023): Trump Says He'll End Democratics' Electric Vehicle Policies. *The Epoch Times,* 2023. június 10. Online: https://www.theepochtimes.com/us/trump-says-hell-end-democrats-electric-vehicle-policies-5325728?utm

Meyersohn, Nathaniel (2023): Trump Is Attacking Electric Vehicles. Automakers Already Bet Their Future on Them | CNN Business. *CNN,* 2023. szeptember 28. Online: www.cnn.com/2023/09/28/business/cars-trump-uaw-electric-ve-hicles/index.html

Misinformation, Disinformation and Mal-information [é. n.]. Online: https://bit.ly/3OjKpd

P. A. R. (2024): Tévhitek és tények az elektromos autózásról. *Világgazdaság,* 2024. június 7. Online: www.vg.hu/auto/2024/06/elektromos-auto-bosch

Partoll, Peter (2023): Struggling EV Company Gets Another Gut Punch as Flagship Vehicle Catches Fire with No Apparent Cause. *The Western Journal,* 2023. június 10. Online: www.westernjournal.com/things-just-got-worse-ev-company-brink-nasdaq-100-delisting/

Posts from Truth Social containing '5G'. Online: https://bit.ly/3UWwkWX

Reichert, Corinne (2020): 5G Coronavirus Conspiracy Theory Leads to 77 Mobile Towers Burned in UK, Report Says. *CNET,* 2020. május 22. Online: www.cnet.com/health/5g-coronavirus-conspiracy-theory-sees-77-mobile-towers-bur-ned-report-says/

Toth, Andras (2024): Industrial IoT and 5G in Critical Information Infrastructures. In Kovács, Tünde Anna et al. (szerk.): *Critical Infrastructure Protection in the Light of the Armed Conflicts*. Cham: Springer Nature Switzerland, 173–187. Online: https://doi.org/10.1007/978-3-031-47990-8_16

Truth Social. Post. Online: https://truthsocial.com/@juniorsfarm/posts/111077619393686491

Truth Social. Post: Qanon shaman. Online: https://truthsocial.com/@TruthSetsFree/posts/110675562684442864

Truth Social. Post: Wind and Solar. Online: https://truthsocial.com/@HenriAllen71/posts/111077661785167476

Truth Social. Truth Social. Online: https://truthsocial.com/@Alagar/111077586509206939
US Retail Gas Price [é. n.]. Online: https://ycharts.com/indicators/us_gas_price
Uscinski, Joseph – Littrell, Shane – Klofstad, Casey (2024): The Importance of Epistemology for the Study of Misinformation. *Current Opinion in Psychology,* 57. Online: https://doi.org/10.1016/j.copsyc.2024.101789
Yandell, Kate (2024): Viral Posts Misuse Rat Study to Make Unfounded Claims About COVID-19 Vaccines and Autism. *FactCheck.org* (blog), 2024. január 26. Online: www.factcheck.org/2024/01/scicheck-viral-posts-misuse-rat-study-to-make-unfounded-claims-about-covid-19-vaccines-and-autism/

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 3. szám 165–182.
DOI: 10.32567/hm.2024.3.10

Kis Márton[1] – Bódi Antal[2] – Számadó Róza[3]

A NIS2 hazai bevezetésének folyamata és kockázatai

The Process and Risks of Introducing NIS2 in Hungary

Absztrakt

Jelen tanulmány célja annak vizsgálata, hogy a NIS irányelv hatálya alá tartozó hazai vállalkozások és szervezetek megfeleléséhez a feltételek rendelkezésre állnak-e, illetve mi szükséges ahhoz, hogy az érintett szervezetek képesek legyenek megfelelni a NIS2 elvárásainak.

Kulcsszavak: kiberbiztonság, kockázat reziliencia, képességek, megfelelés, tudatosság, NIS2

Abstract

The purpose of this study is to investigate whether the conditions are available for the compliance of domestic enterprises and organizations covered by the NIS directive, and what is necessary for the relevant organizations to be able to meet the expectations of NIS2.

Keywords: cyber security, risk resilience, capabilities, compliance, awareness, NIS

[1] Semmelweis Egyetem Egészségügyi Közszolgálati Kar Egészségügyi Menedzserképző Központ; Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: mcihun@gmail.com
[2] Óbudai Egyetem Biztonságtudományi Doktori Iskola; Közlekedéstudományi Intézet, e-mail: bodi.antal@kti.hu
[3] Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Közigazgatás-tudományi Doktori Iskola; Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: szamado.rozaphd.uni-obuda.hu

Bevezetés

Nemzetközi trendek, hazai pillanatkép

A kibertérben zajló események, támadások száma, összetettsége az ezredfordulót követően jelentősen megnövekedett, és jelentős károkat okozott nemcsak a magánszektor, hanem a kormányzatok számára is. Ezen események egyértelművé tették, hogy szükség van átfogó kiberbiztonsági szabályozás létrehozására az EU-ban. Az unió 2016-ban elfogadta első uniós szintű kiberbiztonsági jogszabályát, a hálózat- és információbiztonsági (NIS) irányelvet, ami alapvető lépést jelentett az uniós szintű hálózati és információs rendszerek közös információbiztonsága felé. A végrehajtás során uniós és nemzeti szinten is több kihívással szembesültek az érintettek, továbbá a kiberfenyegetések gyors fejlődése, az új technológiák gyors terjedése miatt az irányelv – jellegéből következően – nehezen tudta lekövetni a folyamatos változásokat.

A felmerülő kihívások, a folyamatosan változó digitális környezet kikényszerítette az uniós keretrendszer felülvizsgálatát. Ennek eredményeként született meg a NIS2. A frissített irányelv az uniós kiberbiztonság területén átfogó stratégiát képvisel, deklarált célja, hogy megerősítse a végrehajtási mechanizmusokat, a terület alapvető jogi pillére. Egyúttal jelentős mértékben kiterjesztette – elődje, a NIS – alanyi és tárgyi hatályát, annak érdekében, hogy a kritikus infrastruktúrák és szolgáltatások ellenálló képességét megerősítse.

A NIS2 elfogadásával törvényi megfelelésben érintett szervezetek köre megsokszorozódott, a megfelelési követelmények is több jelentős pontban változtak, így mind a már gyakorlott, mind az újonnan kötelezettek részéről kérdések sokasága merül fel.

A Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) 2024 nyarán megrendezett konferenciáján ismertették egy 2022-es, a hazai cégek digitalizációjáról szóló kutatás néhány részeredményét. E felmérés szerint minden 5. cég kereskedik online is, a bevételük 25–28%-a származik elektronikus kereskedelemből, és a cégek 70%-ának van weboldala. E kutatás keretében felmérték, hogy hogyan állnak az információbiztonsági kompetenciákkal ezek a szervezetek. A felmérés eredményéből az derült ki, hogy a válaszadók 70%-a nem alkalmaz informatikai, biztonsági szakembert. A fennmaradó cégek 30%-a esetében minden, a területen felmerülő kérdést egy ember kezel, egy embert alkalmaznak.

A különböző szervezetek felkészültségének, kompetenciáinak a mértéke kiemelkedő kockázatot hordoz. Ezt támasztja alá a EU kiberbiztonsági ügynöksége, az ENISA 2030-as előrejelzése. A top 10 kiemelkedő kockázat esetében a hosszú távú, növekvő fenyegetési kilátások közé sorolta a mesterséges intelligenciával kapcsolatos kockázatokat és a felhasználók felkészültségéhez, kompetenciáihoz kapcsolódó kockázatokat. Erre erősít rá a World Economic Fórum 2024. januári kiadású, globális kockázatokat vizsgáló jelentése. A jelentés által megjelölt első öt kockázat között kettő is technológiai jellegű, így a mesterséges intelligenciához és a kibertámadások növekedéséhez kapcsolódó rizikófaktorok. Figyelmet érdemel még a globális kockázatok közül az összekapcsolt rendszerekhez fűződő rizikó is. A hazai kkv információbiztonsági helyzetéről megjelent tanulmány több jelentős problémára, hiányosságra hívja fel a figyelmet, amit a NIS2 hatálya alá tartozó szervezeteknek szintén kiemelten kell vizsgálniuk.

A fentiekből jól látszik, hogy a folyamatosan növekvő kitettségre csak komplex, holisztikus megközelítésű beavatkozás adhat kielégítő választ. Az SZTFH kidolgozott egy 4 faktoros megoldási javaslatot. A négy faktor: a cselekvő állam, a hatékony szabályozás, a felkészült szervezetek és a tudatosítás. Az első két faktor a kereteket határozza meg a cégek részére, míg a felkészülés és a tudatosság növelése érdekében jelentős erőfeszítések megtételére van szükség. Mindezek alapján a kutatási kérdések között az alábbiak merülnek fel: Mire van szüksége a hazai vállalkozásoknak és szervezeteknek, hogy a NIS2 elvárásainak meg tudjanak felelni? Melyek a kockázatos területek, amelyekre kiemelt figyelmet kell fordítani? Meghatározhatók-e ebben a feszített ütemtervben fokozatok, prioritások? A *complient* működés elérése érdekében milyen beavatkozásokra van szükség?

Az előzetes felmérések, a különböző vizsgálatok és jelentések alapján feltételezhető, hogy a NIS2 21. cikkében megfogalmazott elvárások teljesítéséhez az érintett szervezeteknek mind kapacitásban, mind kompetenciában, mind pedig a tudatosság területén jelentős hiányosságaik vannak.

A tanulmány célja

Jelen tanulmány célja, hogy megvizsgálja a NIS2 bevezetésére kötelezett hazai érintettek felkészültségét, és választ keressen arra a kérdésre, hogy milyen feltételek teljesülése mentén lehetséges a NIS2-megfelelés, a szervezetek napi gyakorlatába ültetése és fenntartható működtetése.

Alkalmazott módszerek

A szabályozási környezet áttekintése, a jogi dokumentumok elemzése után a kockázatelemzés módszertanával vizsgáljuk a kutatási kérdést. A választás indoka, hogy jelenleg a sikeres alkalmazkodás a cél, ezért szükséges elemezni a felmerülő tényezőket, hogy a megelőzéshez szükséges beavatkozások megalapozottak legyenek.

A célkitűzésben megfogalmazott kérdés megválaszolásához a következő 4 lépéses módszertanon keresztül tervezünk eljutni:

1) Kockázatok leltára

Számba kell venni azokat a lehetséges kockázatokat, amelyek a NIS2 bevezetése során a szervezeteknél külső vagy belső kockázatként felmerülhetnek.

2) Kockázati térkép

Az azonosított kockázatokat a bekövetkezésük hatása és valószínűsége alapján be kell sorolni.

3) Kockázati mátrix

A besorolt kockázatok súlyossága alapján beavatkozási protokoll hozzárendelése.

4) Skillmátrix

A NIS2 bevezetési folyamatában azonosított szervezeteknél a NIS2 bevezetéséhez szükséges skillek azonosítása és besorolása.

A módszertan logikai sorrendjét az 1-es ábra szemlélteti.

1. ábra: Módszerek logikai sorrendje
Forrás: a szerző szerkesztése

A módszertan mind a négy lépésének inputjait egyrészt a limitáltan rendelkezésre álló nemzetközi szakirodalom elemzésével igyekeztünk végrehajtani, másrészt nagy számú háttérbeszélgetést és strukturált interjút folytattunk kiemelt iparági és hatósági szereplők vezetőivel és kiberbiztonságért felelős szakembereivel.

Szabályozási környezet

EU-szintű szabályozás

A belga CERT vezetője találóan foglalta össze az eredeti 2016-os NIS és a 2023-ban elfogadott, 2024 során minden EU-tagállamban fokozatosan életbe lépő NIS2-szabályozás közötti különbséget:

„💪NIS2 = NIS 1 on Steroids👇”[4]

A 2010-es évek elején az uniós törvényhozók rengeteg olyan faktorral nem számolhattak – a digitalizáció rakétasebességű térnyerése, a világméretű pandémia katalizátorhatása, a kiberfenyegetettség ugrásszerű növekedése, a háborús konfliktusok kiberoldali hatása –, ami miatt a viszonylag friss EU-szintű szabályozás felülvizsgálata és a részletesebb, szigorúbb szabályozás bevezetése elkerülhetetlenné vált.

Az EU azt várja a módosított előírásoktól, hogy a jelentősen szélesebb körben bevont szervezetek és vállalkozások összehangolt megfelelése mentén nemcsak az egyedi szervezetek, hanem az egész EU védettsége és rezilienciája lényegesen megemelkedik a korábbi szinthez képest, és a megnövekedett felhasználói tömegek alapvető kibertudatossága is hozzájárul a nagyobb EU-digitális biztonsághoz.[5]

Az eredeti NIS-irányelv – az első uniós kiberbiztonsági jogszabály – volt az első olyan szabályozó eszköz, amelynek célja az EU IT-rendszereinek kiberbiztonsági kockázatokkal szembeni ellenálló képességének javítása. A bizottság felismerte, hogy jelentős eredményei ellenére a NIS-irányelv bizonyos korlátokat mutatott. A társadalom digitális átalakulása, amelyet a Covid–19-válság felerősített, kiterjesztette a fenyegetettséget. Új kihívások jelentek meg, amelyek adaptált és innovatív válaszokat igényeltek.

Mindezek orvoslására a Bizottság a korábbi NIS-irányelv (amire ma már leggyakrabban a szakirodalomban NIS1-ként hivatkoznak) kiterjesztését javasolta: több ágazat és entitás bevonása a hatályba; harmonizálni az ezen entitások azonosítására

[4] Jean-Luc Peeters, head of CERT.be at Centre for Cybersecurity Belgium.
[5] Európai Bizottság 2023a.

vonatkozó szabályokat (a méretkorlát automatikus és egységes kritériumként történő alkalmazásával); a biztonsági követelmények kiterjesztése; a vezetők és igazgatóságok fokozottabb bevonása és felelősségvállalása; a szankciók, valamint az illetékes hatóságok felügyeleti jogkörének harmonizálása és megerősítése; az incidensek bejelentési kötelezettségeinek tisztázása (például ütemterv, feltüntetendő információ); valamint az ellátási lánc biztonságának megerősítése mind az egyes entitásokon belül, mind pedig európai szinten.

A Bizottság azt is javasolta, hogy erősítsék meg az európai együttműködést a NIS Együttműködési Csoport és a CSIRT-hálózat megbízatásának megerősítésével, valamint a nagyszabású, határokon átnyúló kiberbiztonsági válságok kezelésére szolgáló új platform hivatalos elismerésével. Javasolt továbbá egy európai keret létrehozása a sérülékenység koordinált közzétételére.[6]

A NIS-irányelv hatásának elemzése és hiányosságainak azonosítása érdekében a Bizottság kiterjedt konzultációt folytatott az érdekelt felekkel. A következő főbb problémákat azonosították:

- az EU-ban működő vállalkozások kiberellenállásának elégtelen szintje;
- a tagállamok és az ágazatok közötti nem megfelelő együttműködés;
- a fő fenyegetések és kihívások nem kielégítő közös értelmezése a tagállamok között;
- a közös válasz és válságreakció hiánya, a büntető szankciók elégtelen volta.

A megállapítások eredményeként, valamint a felgyorsult digitalizáció és a külső és belső növekvő fenyegetésekre való reagálás érdekében a Bizottság 2020 decemberében egy felülvizsgált, komplexebb szabályrendszert javasolt, amelynek célja a kiberreziliencia szintjének erősítése az unióban. A jogalkotók 2022. május 13-án politikai megállapodásra jutottak, és 2022. november végén hivatalosan is elfogadták az új irányelvet.[7]

A NIS és a NIS2 közötti változást a 2. ábra részletesen szemlélteti.

A NIS2 irányelv jogi intézkedéseket ír elő a kiberbiztonság általános szintjének növelésére az EU-ban, annak érdekében, hogy hozzájáruljon a belső piac általános működéséhez. A NIS1 irányelv három fő pillérre épült:

1. A hálózati és információs rendszerek biztonságára vonatkozó NIS1 stratégiára építve a tagállamok magas szintű felkészültségének elérése érdekében a NIS2 irányelv előírta a tagállamok számára, hogy fogadjanak el nemzeti kiberbiztonsági stratégiát. A tagállamoknak ki kellett jelölniük a kockázatok és incidensek kezeléséért felelős nemzeti számítógépes biztonsági eseményekre reagáló csoportokat (CSIRT), egy illetékes nemzeti kiberbiztonsági hatóságot és egyetlen kapcsolattartó pontot (SPOC). Az SPOC-nak kapcsolattartó funkciót kell ellátnia, hogy biztosítsa a határokon átnyúló együttműködést a tagállami hatóságok és a többi tagállam illetékes hatóságai között, és adott esetben a Bizottsággal és az ENISA-val, valamint biztosítsa az ágazatokon átnyúló együttműködést a többi illetékes hatósággal.

2. A NIS2 irányelv folytatja a NIS1-keretet is, amely létrehozza a NIS-együttműködési csoportot a tagállamok közötti stratégiai együttműködés és információcsere

[6] Byttebier 2022.
[7] Európai Bizottság 2023b.

támogatására és elősegítésére, valamint a CSIRT-hálózatot, amely elősegíti a nemzeti CSIRT-ek közötti gyors és hatékony operatív együttműködést.

3. A NIS1 irányelv biztosította, hogy a kiberbiztonsági intézkedéseket hét olyan ágazatban hozzák meg, amelyek létfontosságúak gazdaságunk és társadalmunk számára, és amelyek nagymértékben támaszkodnak az IKT-ra, mint a közigazgatás, az energia, a közlekedés, a bankszektor, a pénzügyi piaci infrastruktúra, az ivóvíz, az egészségügy és a digitális infrastruktúra.

2. ábra: NIS2 Adatlap – #DigitalEU
Forrás: a szerző fordítása és szerkesztése az Európai Bizottság 2023a, 2023b alapján

A tagállamok által ezekben az ágazatokban alapvető szolgáltatások üzemeltetőiként azonosított állami és magánjogi szervezeteknek kiberbiztonsági kockázatértékelést kell végezniük, és megfelelő és arányos biztonsági intézkedéseket kell bevezetniük. A súlyos következménnyel járó eseményekről értesíteniük kell az illetékes hatóságokat.

A NIS2 irányelv jelentősen kibővíti az ágazatok körét (például államigazgatás, gyártási tevékenységek, szennyvíz- és hulladékkezelés), és méretküszöböt vezet be annak meghatározására, hogy mely jogalanyok tartoznak az irányelv hatálya alá, és melyek kötelesek jelenteni a jelentős kiberbiztonsági incidenseket az illetékes nemzeti hatóságoknak.[8]

[8] Európai Bizottság 2023b.

A kiberbiztonsági szabályozást az EU-ban régóta részlegesen hajtják végre, ami széttagolt szabályozási környezetet eredményez. A közelmúltbeli fejlemények arra késztették az EU-t, hogy felülvizsgálja megközelítését, mert az eredeti szabályozás nem eredményezte uniószerte a tervezett magas szintű kiber-ellenállóképességet. E tekintetben a NIS 2.0 irányelvre vonatkozó közelmúltban elfogadott szabályozás és a kiberrezisztenciáról szóló törvényjavaslat rávilágít arra, hogy az EU miként igyekszik összehangolni a jogszabályokat, és csökkenteni a különböző, gyakran ágazati szabályozási megközelítéseket a kiberbiztonság terén, ugyanakkor kiterjesztik a szabályozást a magas szintű kiberbiztonság elérése érdekében az egész EU-ban. A kiberrezisztenciáról szóló törvény további kiegészítést nyújt a NIS 2.0 irányelvhez a meglévő szabályozási hiányosságok megszüntetése érdekében, amire ebben a dokumentumban nem térünk ki.[9]

A NIS2 magyar vonatkozásai

Rendszerszintű szereplők

A hazai NIS2 hatósági környezetét alapvetően a *2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről* határozza meg, illetve a tanúsításról szóló kiegészítő SZTFH rendelet, *10/2023. (V. 15.) SZTFH rendelet az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról.*

Ennek értelmében a hazai NIS2 szabályozás központi kijelölt hatósági szereplője a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH), és fő feladata a NIS2 hatálya alá tartozó szervezetek kiberbiztonsági tanúsításának nyilvántartása és ellenőrzése, és hogy a hazai kiberbiztonsági megfelelésről rendszeresen tájékoztassa a Bizottságot.

A cikk írásának időpontjában a törvény végrehajtási rendeletét még nem hirdették ki, de a társadalmi egyeztetésre bocsátott változata ismert: „A Miniszterelnöki Kabinetirodát vezető miniszter MK rendelete a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről (TERVEZET)". Ezen végrehajtási rendelet végleges, kihirdetett verzióját az összes érintett szervezet várja, hogy az elvárt törvényi megfelelés pontos hatósági részletei megismerhetők legyenek, és a felkészülés, illetve annak auditálása és megfelelési értékelése elfogadható legyen.

A szabályozás alá vont szervezetek köre két lépésben meghatározott. A következő fejezetben felsorolt mérföldkövek és határidők mentén a törvény hatálya alá tartozást a szervezeteknek önazonosítás után kell meghatározniuk a törvényben szereplő kritériumrendszer figyelembevételével. Az elsődleges kötelezettség az érintett szervezeteknek az SZTFH-nál történő elektronikus regisztrációja 2024. 06. 30-ig.

A végrehajtási rendelet hiányában a szabályozás alá vont szereplők többféle stratégia mentén végzik a felkészülésüket. Van, aki kivár a pontos részletszabályok megérkezéséig, mások proaktívan a jelenlegi ismeretek alapján igyekeznek előre dolgozni és a megfelelésre felkészülni.

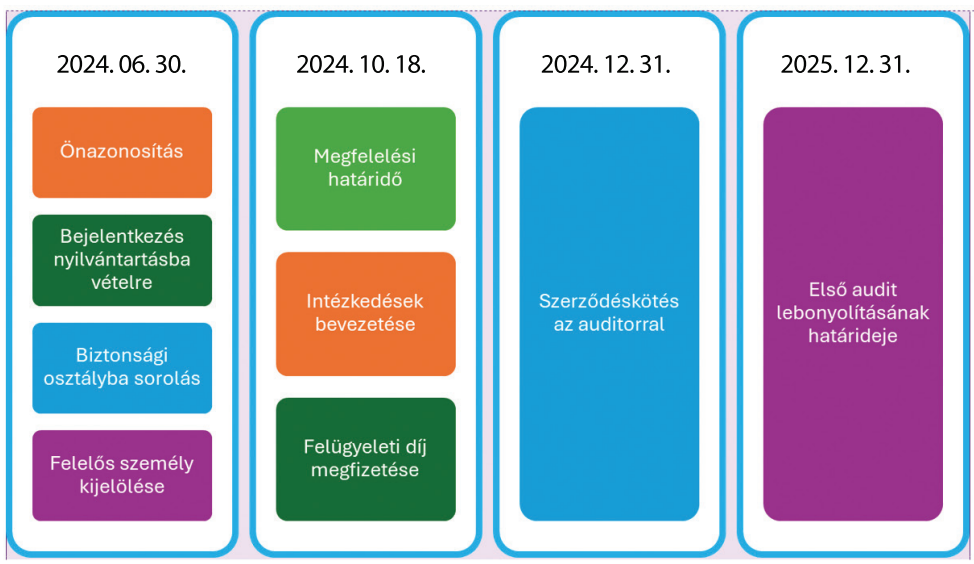
[9] Schmitz-Berndt–Cole 2023.

A felkészítő szereplőkre vonatkozóan nincs törvényi kijelölés, a szervezetek akár saját hatáskörben is felkészülhetnek a NIS2-megfelelésre. Mivel az érintett szereplők nagy részének nincs megfelelő saját belső szaktudása, illetve HR-kapacitása, piaci alapon igény keletkezett a felkészítő tanácsadó tevékenységre. A versenyszféra cégei különböző szolgáltatáscsomagokat kínálnak az érintett cégek részére (komplex felkészítés, biztonsági osztályba sorolás, szabályzatok elkészítése, gap-analízis, előaudit stb.). Kiemelt kockázatként jelentkezik, hogy a felkészítő szervezet munkatársai nagyon szenzitív belső információkhoz férhetnek hozzá, így a kiválasztásnál a megfelelő személyi garanciákat be kell építeni a folyamatba.

A kötelező audit lebonyolítására alkalmas cégek köre valószínűleg nagyon limitált lesz a szigorú megfelelőségi kritériumok mentén, azonban a cikk írásának idején még sem a végleges pontos kritériumrendszer, sem az audit lebonyolítására képes cégek teljes körű hivatalos jegyzéke nem elérhető. A felkészítő szervezeteknél jelentkező személyi garancia kockázata itt sem zárható ki, így kiemelten fontos a megfelelő személyi garanciák beépítése a folyamatba.

NIS2-megfelelés kötelező lépései szervezeti oldalon

Az érintett szervezetek NIS2-megfeleléshez szükséges tevékenységeinek köre meglehetősen komplex. A lépések és határidők a *2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről* 30. §-a alapján a következők:



3. ábra: NIS2-megfelelés törvényi határidői
Forrás: a szerző szerkesztése

A szervezetek oldalán jelentkező kockázatok körét a következő pontban részletesen is feldolgozzuk, azonban általánosságban is megállapítható, hogy az alábbi lehetséges általános problémák, kockázatok merülhetnek fel a 4 kiemelt határidő teljesítése körül:

- Végrehajtási rendelet meglehetősen későn jött ki a határidők teljesítéséhez.
- 2013. évi L. törvény vs. NIS2-előírások megfeleltetése (szabályzatok, kockázatértékelés, biztonsági osztályba sorolás) időt és szakértelmet igényel, amelyek korlátozottan állnak rendelkezésre.
- Kritikusnak minősített kockázatokhoz kapcsolódó korrekciós tevékenységek erőforrás-szükségletének rendelkezésre állása (HR és pénzügyi egyaránt).
- A korrekciós tényezők miatti szükséges fejlesztések és eszközbeszerzések fedezete és közbeszerzési folyamatainak időigénye.
- Az előírt – teljes munkavállalói létszámot érintő – biztonságtudatossági oktatások megszervezése és lebonyolítása (a napi üzletmenetet nem akadályozva).
- Olyan szervezetekre is kiterjed a NIS2-kötelezettség, ahol korábban ez a feladat még nem merült fel, ezért nagyon alacsony a szervezet kibertudatossága, a menedzsment nem készült fel a feladatra, nincs tapasztalat a valós kockázatokról.

Szervezeti érintettek a bevezetés során

A megfelelésre kötelezett intézmények szervezeti struktúrájának megfelelően – függetlenül attól, hogy a szervezet mely ágazatban tevékenykedik – a NIS2-megfeleléshez szükséges feladatok több szervezeti egységnél és a hierarchia több szintjén jelentkeznek. Mivel a megfelelés komplex intézkedéseket igényel, ami a teljes szervezet tekintetében tartalmaz feladatokat, elsődleges fontosságú kérdés, hogy a menedzsment értse a kérdés jelentőségét, támogassa a végrehajtásból fakadó feladatokat, és biztosítsa a szükséges (HR- és pénzügyi) erőforrásokat. Jó megoldás lehet a NIS2-bevezetést projektformában, előre lefektetett feltételek mentén végrehajtani, de amennyiben ez nem lehetséges, akkor is egyértelmű felelősöket és erőforrást kell kijelölni a 3-as ábrában felsorolt törvényi határidőkhöz kapcsolódó feladatok végrehajtásához. Az 1-es táblázat a legfontosabb szereplőket és azok kulcscélfüggvényét veszi számba a NIS2-bevezetés problémakörére koncentrálva.

1. táblázat: Az érintettek érdekei, megoldási irányok

Érintettek	**Érdekek, motiváció, kooperáció**
IT-szervezeti egység, IT-biztonsági felelős	A rendszerek gazdájaként a végrehajtás ide koncentrálódik, a fő motiváció a hibamentes végrehajtás. Sokszor kooperációs, kommunikációs problémák vannak a többi szervezeti egységgel. Gyakori az általános, illetve a specifikus információbiztonsági tudással rendelkező HR-kapacitás hiánya. Gyakori hiba, hogy az IT-biztonsági felelős az IT-üzemeltetés alá kerül szervezeti beosztásra, így gyakran nem jut el a menedzsmenthez az információ a kötelezettségből adódó feladatok méretéről és a nem megfelelés esetén felmerülő valós kockázatról.
Üzemeltetés	A fő motiváció a zökkenőmentes működés biztosítása. Szükséges annak a tudatosítása, hogy a NIS2-megfelelés része ennek. Konfliktus van a napi üzemeltetési gyakorlat és a kapcsolódó üzleti elvárás, illetve a NIS2-előírások betartása, betartatása, betarthatósága és ellenőrizhetősége között. A konfliktus feloldása szükséges, aminek a fentieken túl a kooperáció lehet az eszköze.
Adminisztráció	Az adminisztráció célja a NIS2-megfelelés lehető legkisebb költség (HR-többletigény, lehetséges többlet-infrastrukturális beruházások, felkészítés, audit tanácsadói költsége, munkavállalók oktatásának költsége, oktatás miatti munkaidő-kiesés költsége) melletti megvalósítása. Jellemző a legkisebb árajánlat kiválasztása a külső tanácsadóknál, amely komoly szakmai kockázattal jár együtt, mivel nincs a felkészítő tanácsadókra egységes szakmai elvárás, végzettség vagy szakmai tapasztalat.
Menedzsment	Sok esetben gyakorlatilag feloldhatatlan konfliktust eredményez a költséggazdálkodás miatti nyomás és a törvényi megfelelési kényszer közötti ellentmondás feloldása. A NIS2-bevezetést kiváltó valós megnövekedett kiberkitettség kockázatának felismerése és az *ownership* felvállalása. A szigorúbb szabályok miatti szervezeti ellenállás csak a menedzsment teljes elkötelezettsége mellett kezelhető, amihez szükséges a kockázatokból adódó hátrány, veszély, veszteség megismerése, felismerése.
Munkavállalók	Digitális higiénia és tudatosság alacsony, a napi gyakorlat megváltoztatása szükséges, az új, szigorúbb szabályok óhatatlanul kényelmetlenebbé és bonyolultabbá teszik a napi megszokott munkát, ami feszültséget okoz. A kikényszerítés sem egyszerű, a hosszú távú szemléletváltás és – a képzéssel, szervezetfejlesztéssel támogatott – vállalati kultúrába épülés a megoldás.

Forrás: a szerző szerkesztése

Eredmények

Probléma-/kockázati térkép

A 2-es táblázat alapján jól követhető, hogy még az egy szervezetben, alapvetően közös célok érdekében dolgozó érintetteknek is gyakran erősen eltérnek az érdekeik és motivációjuk; természetesen igaz lesz ez az állítás a kiberbiztonsági megfeleléshez szükséges feladatok végrehajtására is.

A következőkben számba vesszük az ebből az eltérő nézőpontból és érdekeltségből fakadó kockázatok listáját. A lista a dinamikusan változó környezet hatására nyilvánvalóan dinamikusan változik, de igyekeztünk a fő kockázatokat teljeskörűen számba venni.

2. táblázat: Kockázatok listája

#	Kockázat
A	Alacsony szintű kibertudatosság
B	Felhasználók szabálykövetése alacsony
C	Egységes NIS2-bevezetési módszertan hiánya
D	Nem megfelelő IT-szabályozottság
E	Hiányzó IT-kockázatmenedzsment
F	Az üzemeltetés kockázatos
G	Nincs vagy nem megfelelő a DRP
H	Nincs vagy nem megfelelő a BCP
I	A NIS2-megfelelés bevezetésére és fenntartására nincs tapasztalat és egységes módszertan
J	Késik a Kibertan. tv. végrehajtási rendelete
K	A szervezet IT-rendszerének extrém kitettségei
L	A menedzsment elköteleződésének hiánya
M	Felkészületlen vagy csalárd „felkészítők” – NIS2-bűnözők megjelenhetnek

Forrás: a szerző szerkesztése

A felsorolt kockázatok áttekintésével felismerhető, hogy bár van néhány, a szervezet hatáskörén kívül eső kockázat (C, J, M), mégis a kockázatok többsége vagy a szervezet menedzsmentjéhez kötődik (D, E, G, H, K, L), vagy az egyedi felhasználók magatartásából következik (B, F).

Az 1-es számú mellékletben a felsorolt kockázatok értelmezését követően a bekövetkezés valószínűségét és annak szervezetre gyakorolt hatását értékeltük.

A 3-as táblázatban kockázati mátrixba rendezve látható ezeknek a lehetséges eseményeknek a vizuális megjelenítése. A táblázat színkódjai megmutatják a szervezet incidenshez kapcsolódó attitűdjét és az ebből következő beavatkozás szintjét és időtávját.

Az ábrázolás egyértelműen megmutatja, hogy a lehetséges kockázatok túlnyomó többsége azonnali beavatkozást igényel a szervezetek részéről.

3. táblázat: Kockázati mátrix

Valószínűség (1–5)	Következmény (1–5)				
	Jelentéktelen	Mérsékelt	Közepes	Súlyos	Kritikus
Elhanyagolható					
Alacsony					
Közepes			C	J	H, L, M
Valószínű				D	B, F, G, K
Nagyon valószínű			I		A, E

Kockázati szintek	Tolerancia	Akció
Elhanyagolható	**elfogadható**	**Nincs, elegendő kontroll**
Alacsony	**elfogadható**	**Nincs, elegendő kontroll**
Normál	**elfogadható**	**További szorosabb kontroll**
Magas	**nem elfogadható**	**Kockázatkezelési beavatkozás monitorozott határidővel**
Kritikus	**nem elfogadható**	**Azonnali kockázati beavatkozás**

Forrás: a szerző szerkesztése

Skillmátrix

Kiemelt figyelmet érdemel, hogy a sikeres NIS2-bevezetéshez, és a megfelelés folyamatos fenntartásához minimum két fő tényező együttes bekövetkezésére van szükség:

- Az előző pontban részletezett kockázatok kezeléséhez szükséges erőforrások (HR-kapacitás és pénzügyi fedezet) gyakorlatilag azonnali és párhuzamos rendelkezésre állása.
- A törvényi előírások és kötelezettségek pontos ismerete és a végrehajtáshoz szükséges skillek szervezeti jelenléte a NIS2-ökoszisztéma minden érintett szervezetét figyelembe véve.

A NIS2-megfelelés érdekében szükséges fejlesztések, beavatkozások megítélésének érdekében alkottunk meg egy többdimenziós mátrixot a rendszer szereplőivel, a szükséges készségekkel, képességekkel, szakismeretekkel, a meglévő tudásszintekkel és a hozzájuk tartozó tevékenységgel a megfelelés fenntartásához.

A rendszer szereplői: szabályozó, törvényhozó; ágazati irányító minisztérium; ellenőrző szervezet; ágazati középirányító szervezet; felkészítő szervezet; auditor; oktató szervezet; szabályozás alá vont szervezet.

Az azonosított, a NIS2-bevezetés lebonyolításához szükséges készségek, szakismeretek az alábbiak:

- NIS2-előírások ismerete;
- vonatkozó hazai szabályzók ismerete;
- szükséges szabályzatok struktúrája és elemei;
- IT-infrastruktúra rendszerelemeinek ismerete;
- IT-alkalmazási szint ismerete;
- ágazati specifikumok ismerete;
- jelenlegi rendszer állapotismerete;
- jelenlegi rendszerkorlátok ismerete (forrás, HR stb.);
- rendszerszereplők oktatásának képessége;
- rendszerszereplők ellenőrzésének képessége;
- szervezeti szintű IT-biztonsági tudatosság;
- támogató szervezeti kultúra;
- felelős egyéni szintű viselkedés, szabálykövetés.

Az is fontos információ, hogy az adott készség mely szereplőnél milyen tudásismereti mélységben, illetve milyen gyakorlati felhasználási képességgel párosulva kell hogy megjelenjen. A skillmátrixban ezt a dimenziót színekkel azonosítottuk a beavatkozási irányok megjelölésével.

A 4. táblázatot áttekintve könnyen felismerhető, hogy az elvárások, törvényi kötelezettségek oktatására minimum 3 szinten van szükség:

- A kötelezett szervezetek munkavállalóinak érzékenyítő oktatásokat kell tartani, amelyhez a megfelelő tananyagot is létre kell hozni.
- A majdani oktatásokat végző szervezetek, csakúgy, mint a felkészítő tanácsadók és auditorcégek részére is központi, egységes képzéseket kell tartani.
- A végrehajtásban és a kötelezettek felügyeletében, irányításában érintett szervezetek részére is oktatást kell szervezni az irányelv részletes megismerése és feladataik gyakorlati részleteit érintően.

Ez a 3 szintű feladat teljeskörűen felkészült oktató szervezetet, gárdát és a 3 szintnek megfelelően kifejlesztett oktatási anyagokat és számonkérési keretrendszert feltételez.

A skillmátrix áttekintésével vizuálisan is gyorsan átlátható, hogy az egyik azonnali feladat annak biztosítása, hogy a szabályozásban és a végrehajtásban érintett (felkészítő, oktató és auditor-) intézmények és cégek minél hamarabb rendelkezzenek a különböző ágazati specifikumokkal (például egészségügy esetén a 7/24 működés és a folyamatos ellátási kötelezettségből fakadó eltérő napi gyakorlat) és az ehhez kapcsolódó IT-infrastruktúra és HR-támogató személyzet egyedi vonásaival.

A mátrix vizsgálata – a későbbiek során – segítséget nyújthat egy komplex, rugalmas és szinergikusan működő többszintű képzési rendszer kialakításához.

4. táblázat: Skillmátrix

	Szükséges skillek és rendelkezésre állásuk												
Érintettek/ rendszer-szereplők	NIS2-előírások ismerete	Vonatkozó hazai szabályzók ismerete	Szükséges szabályzatok struktúrája és elemei	IT-infrastruktúra rendszerelemeinek ismerete	IT-alkalmazási szint ismerete	Ágazati specifikumok ismerete	Jelenlegi rendszerállapot ismerete	Jelenlegi rendszerkorlátok ismerete (forrás, HR stb.)	Rendszerszereplők oktatásának képessége	Rendszerszereplők ellenőrzésének képessége	Szervezeti szintű IT-biztonsági tudatosság	Támogató szervezeti kultúra	Felelős egyéni szintű viselkedés, szabálykövetés
Szabályozó, törvényhozó													
Ágazati irányító minisztérium													
Ellenőrző szervezet													
Ágazati közép-irányító szervezet													
Felkészítő szervezet													
Auditor													
Oktató szervezet													
Szabályozás alá vont szervezet													

Tudásszint	**Szükséges tevékenység, kompetencia állapota**
Hiányos ismeretek	oktatás szükséges
Felhasználói/végrehajtó szintű ismeret	képes a szabályozási utasítást végrehajtani
Rendszerszintű ismeret	képes a végrehajtás szakszerűségét ellenőrizni
Mester-/oktatói szintű ismeret	képes a rendszer többi szereplőjét oktatni, instruálni

Forrás: a szerző szerkesztése

Értékelés, további vizsgálandó területek

A kockázatok és a szükséges és hiányzó skillek vizsgálatát követően számos lehetséges és szükséges feltétel megfogalmazható, amelyek ahhoz kellenek, hogy a NIS2-megfelelés ne csak egyszeri, kampányszerű tevékenység legyen, hanem fenntartható, a szervezetek napi gyakorlatába és szervezeti kultúrájába szervesen beépülő, napirutin-szerű tevékenységek sorozatává váljon.

Amíg az EU és a hazai törvényhozói szándék egyértelmű – a megnövekedett kiberkockázatok megelőzésére és kezelésére hozott magasabb szintű intézkedések

bevezetése –, addig a kötelezett szervezetek szintjén ez a szándék elsődlegesen megnövekedett költségeket, komplexebb folyamatokat és a jelenlegi HR-kapacitás további terhelése mellett még extra HR szükségletet is teremt. Összességében a NIS2-megfelelés mindenképpen jelentős anyagi és HR-terhet ró a szervezetekre, amelyek fedezetét a piaci cégek kénytelenek kigazdálkodni, azonban az állami fenntartású szervezetek esetében a szükséges kiadások fedezetéről az államnak kell gondoskodni.

A részletszabályok hivatalos ismeretének hiányában jelen pillanatban a kötelezettek nagyrészt önállóan és különböző intenzitással foglalkoznak a feladattal. A részszabályokon túl szükség lenne az ágazati középirányítók részéről olyan egységes módszertanok kidolgozására és közzétételére, amelyek mentén a hasonló tevékenységet folytató szervezetek egységes keretek között tudhatnak felkészülni a megfelelésre, és ezáltal a fenntartható megfelelés is könnyebben elérhető lehet.

Mindezek figyelembevételével a specifikus ajánlások megtételéhez még sok változó ismerete és feldolgozása lenne szükséges, azonban már most látható néhány általánosan levonható következtetés:

- szervezeti kultúraváltás kell majdnem minden érintett szintjén és jelentős edukáció szükséges:
  - a hazai digitális éberség és tudatosság egyéni és szervezeti szinten is komoly fejlesztésre szorul. Minden szereplőnek el kell fogadnia, hogy a digitalizáció nem visszafordítható folyamat, és a digitális, online világban más típusú és nagyobb odafigyelést igénylő veszélyek leselkednek a napi használat során. Ennek a tudásnak a megszerzése csakis szervezett oktatás mentén valósítható meg, és utána nap mint nap szükséges az új folyamatok kikényszerítése, amíg az a megszokott rutin részévé nem válik;
- a tudatosság és egyéni felelősségvállalás kérdése kritikus:
  - az előző pont kiterjesztéseként szükséges a szemléletváltás a szervezeti és egyéni felelősség kérdésében is. Tudatosulnia kell annak a ténynek, hogy a legkisebb felhasználói figyelmetlenség is (például adathalász-e-mailre kattintás) nagyon komoly károkat okozhat a szervezet számára. Az oktatás ezen a szinten is kritikus, az egyénnek tisztában kell lennie cselekedetei hatásával és felelősségével a nem várt incidensek hatására vonatkozóan;
- vezetői/fenntartói/szabályozói támogatás mellett lehetséges csak a fenntartható NIS2-bevezetés:
  - az egyénektől elvárt éberség és felelősségvállalás folyamatos fenntartása nem képzelhető el a szervezet közvetlen vezetői és menedzsmenttámogatása nélkül, de szükséges a folyamatos visszacsatolás és kommunikáció a szabályozói szinten is (a tájékoztatásnak, oktatások tematikájának reagálnia kell a várhatóan fejlődő felhasználói tudásszintre, és annak megfelelő további magasabb szintű információk rendelkezésre bocsátása válik majd szükségessé;
- standard módszertanok kellenek, jógyakorlatok bemutatása, érzékenyítő események (például HunEx, hackathonok stb.):
  - az oktatásokon túl szükség lesz olyan egyéb platformok bevonására, ahol a szervezetek a hétköznapokban tudnak adott felmerülő probléma esetén tájékozódni, információt szerezni. A jógyakorlatokat, módszertanokat közzétevő online felületek mellett érdemes lehet olyan személyes

eseményeket is szervezni, ahol a napi problémákat, tapasztalatokat tudják a szervezetek képviselői megosztani és megbeszélni. A valós problémákra reflektáló szimulációs és problémamegoldó események szintén jobb hatásfokú eredményeket hoznak a közös alkotás és az eltérő skillek együttes felhasználása miatt;

- a digitalizációt finomhangolni kell:
  - az elvárt szabálykövetés napi fenntartásában a felhasználói élmény kritikus. A digitális megoldás nem lehet bonyolultabb, időigényesebb, mint a régi analóg, mert akkor a felhasználó kiskapukat fog keresni, a szabályszegés kockázata meg fog nőni;
- automatizmusokat kell keresni, ami mentesíti, de legalább támogatja a felhasználókat, IT-üzemeltetőket a kockázatok elkerülésében:
  - az előző pont folyományaként szükséges lehet olyan lokális vagy központi egységes NIS2-megfeleléshez kapcsolódó támogató intézkedéseket hozni, ami egyszerűbbé teszi a szervezetek és az egyéni felhasználók számára a napi munkavégzés során a digitális szabályok észszerű betartását.

Összefoglalásként kijelenthető, hogy a NIS2 megszületése és több dimenziójában is kiterjesztett hatálya a megnövekedett kiberkockázatok miatt szükséges és elkerülhetetlen volt.

A jelen helyzet hazai vizsgálata több limitáló tényező miatt is csak részleges következtetések levonását tette lehetővé.

A megvalósítás tapasztalatainak ismerete nélkül a jelenleg látható kockázatok és a bevezetéshez szükséges készségek elemzését követően csak általános, de mégis alapvetően releváns következtetések levonása volt lehetséges.

A hipotéziseket igazoltuk, és tézisként kijelenthető, hogy a NIS2 hatálya alá tartozó szervezeteknek mind kapacitás-, mind kompetenciafejlesztésre szükségük van.

Kimondható, hogy a NIS2 fenntartható megfelelés napi gyakorlatba való rögzülésének alapvető kritériuma a rendszer több szintjén minél hamarabb megtervezett és megvalósított oktatások rendszere. Ennek hiányában sem a kötelezett szervezetek és azok felhasználói, sem a felkészítésüket és ellenőrzésüket a jövőben ellátni hivatott szereplők nem lesznek képesek a feladatukat megfelelően elvégezni.

Egyúttal az is leszögezhető, hogy a NIS2 hatálya alá tartozó szervezetek egy proaktív, stratégiai szinten megfogalmazott cselekvési tervvel eleget tudnak tenni az irányelv elvárásainak, és egyúttal kialakíthatják a saját maguk biztonságos és rugalmas működési kereteit.

A kutatás következő fázisában tovább lehet és kell majd vizsgálni, hogy a NIS2 kötelező megfelelése lehetőség az érdemi változásra, vagy csak egy következő kipipálandó feladat (mint az ISO vagy a GDPR sok szervezetnél). Létrejön-e a valós szervezeti felismerés, hogy a kiberkockázatok jelentősen növekedtek az elmúlt években, és ezek új megoldásokat, válaszokat igényelnek? Léteznek-e olyan módszertanok, amik támogathatják ezt a felismerési, tudatosságnövelési folyamatot?

Felhasznált irodalom

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

10/2023. (V. 15.) SZTFH rendelet az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról

Bor Olivér – Bencsik Balázs (2024): Ki és hogyan készüljön fel a NIS2-re? *SZTFH konferencia.* Online: www.youtube.com/watch?v=IAsXC_qFNNc

Byttebier, Pieter (2022): NIS-2: Where are you? *Centre for Cybersecurity Belgium,* 2022. április 30. Online: https://ccb.belgium.be/en/news/nis-2-where-are-you

ENISA (2024): *Foresight Cybersecurity Threats For 2030. Executive Summary.* Online: www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary

Európai Bizottság (2023a): *NIS2 Directive*. Online: https://digital-strategy.ec.europa.eu/hu/policies/nis2-directive

Európai Bizottság (2023b): *NIS2 FAQS*. Online: https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

Megyeri Lajos – Farkas Tibor (2017): Kockázatkezelés, tudomány vagy kuruzslás. *Hadmérnök,* 12(3), 198–209. Online: https://real.mtak.hu/64731/1/1.Farkas_Hadm%C3%A9rn%C3%B6k2017.pdf

Mike Nimród – Krén Enikő – Kecskeméti Tamás (2023): Farkasbiztos téglaház? A KKV-k információbiztonsága Magyarországon. *Vezetéstudomány,* 54(9), 44–57. Online: https://doi.org/10.14267/VEZTUD.2023.09.04

Schmitz-Berndt, Sandra – Cole, Mark (2023): Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act. *Applied Cybersecurity and Internet Governance,* 1(1), 1–17. Online: https://doi.org/10.5604/01.3001.0016.1323

Vandezande, Niels (2024): Cybersecurity in the EU: How the NIS2-directive Stacks up Against Its Predecessor. *Computer Law and Security Review*. Online: https://doi.org/10.2139/ssrn.4383118

World Economic Forum (2024): *Global Risks Report 2024*. 19th Edition: Online: www.weforum.org/publications/global-risks-report-2024/

Zágon Csaba – Gecsei Márton (2021): Kockázatelemzés a gyakorlatban: cigaretta a repülőtéren. In *Tradíció, tudomány, minőség. 30 éves a Vám- és Pénzügyőri Tanszék.* Tanulmánykötet. Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozata, 129–142. Online: http://doi.org/10.37372/mrttvpt.2021.2.7

1.sz. melléklet – kockázati térkép

Azonosító	Kockázat	Kockázat leírása	Esemény bekövetkezésének valószínűsége (1–5)	Esemény hatása (1–5)	Kockázati érték
A	Alacsony szintű kibertudatosság	A felhasználók kiberhigiénia-szintje alacsony. A hétköznapi gyakorlatban sok NIS2-ben elfogadhatatlan elem rögzült.	5	5	25
B	Felhasználók szabálykövetése alacsony	Az ellátás érdekét előtérbe helyezve kockázatos tevékenységet folytatnak (pl. jelszómegosztás, nincs MFA kikényszerítve vagy megkerülhető).	4	5	20
C	Egységes módszertan hiánya	A szervezetek különböző szabályzatokat hoznak létre és eltérő gyakorlatok alakulnak ki az incidensek kezelésére.	3	3	9
D	Nem jó az IT-szabályozottság	Hiányos, elavult szabályzatok, hibás vagy kockázatos gyakorlatok.	4	4	16
E	Nincs IT-kockázatmenedzsment	Nem azonosított, fel nem ismert kockázatok és forgatókönyvek.	5	5	25
F	Az üzemeltetés kockázatos	Nincs elegendő tudás vagy személyzet az események megelőzésére, a kitettségek és a kockázatok felismerésére.	4	5	20
G	Nincs vagy nem megfelelő a DRP	Esemény bekövetkezése esetén nincs megfelelő követendő protokoll a normál szolgáltatási szint mielőbbi helyreállítására.	4	5	20
H	Nincs vagy nem megfelelő a BCP	Esemény bekövetkezését követően nincs megfelelő eljárás az üzletmenet fenntartására.	3	5	15
I	A NIS2-megfelelés bevezetésére és fenntartására nincs tapasztalat és egységes módszertan	Nincs központi (ágazati) követendő módszertan, keretrendszer, irányelv a NIS2-megfelelés bevezetésére és fenntartására.	5	3	15
J	Késik a Kibertan. tv. végrehajtási rendelete	Nem ismertek a megfeleléshez kapcsolódó pontos részfeladatok, a folyamatban részt vevő hivatalos szereplők (pl. felkészítők, auditorok).	3	4	12
K	A szervezet IT-rendszerének extrém kitettségei	Nincs fedezet orvosolni az elavult gépparkot, a nem támogatott vagy nem frissített szoftvereket és a nem naprakész alkalmazásokat.	4	5	20
L	A menedzsment elköteleződésének hiánya	A menedzsment nem kezeli kiemelt prioritásként a kiberbiztonságot, a NIS2 esetében a teljesítés elkerülésére helyez nagyobb hangsúlyt.	3	5	15
M	Felkészületlen vagy csalárd „felkészítők" – NIS2-bűnözők megjelenhetnek	Az időzavarban vagy az elodázott döntések következtében a nem megfelelően kiválasztott felkészítést végző szervezet hamis biztonságot ad, közben kiszolgáltathat a belső rendszerekről sok bizalmas információt, amelynek ismeretében kihasználhatók lesznek a cégek IT-rendszereinek gyengeségei vagy akár zsarolhatókká tehetők. A „GDPR-bűnözés"-hez hasonlóan.	3	5	15

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 3. szám 183–200.
DOI: 10.32567/hm.2024.3.11

Kiss Adrienn[1]

Az orosz–ukrán háború hatása a kritikus infrastruktúrákra – fókuszban az energiaszektor[2]

The Impact of the Russian–Ukranian War on Critical Infrastructure – Focus on the Energy Sector

Absztrakt

Az orosz–ukrán háború során is megjelent a kibertér mint hadszíntér, ez pedig jelentősen hozzájárul a modern konfliktusok természetének folyamatos átalakulásához. A tanulmány célja az orosz–ukrán háború során végrehajtott kibertámadások empirikus elemzése, kitekintéssel az energiaszektorra. A kutatás a 2022-es és a 2023-as adatokat vizsgálja, feldolgozva az ismert kibertámadások időbeli trendjeit, földrajzi eloszlását és típusait. A tanulmány rámutat a kibervédelem felépítésének, fejlesztésének és fenntartásának, valamint a támadások elemzésének és a megfelelő tanulságok levonásának fontosságára. A kutatásban idősorelemzést, trendelemzést és hőtérképes megjelenítést alkalmaztam. Az eredmények rámutatnak arra, hogy mely szektor vált különösen kiemelt célponttá a kibertámadások során. Ezen felül bemutatja a kritikusinfrastruktúra-szektorok támadottságának mértékét a háború kapcsán, illetve a kibertámadások során alkalmazott technikákat.

Kulcsszavak: kritikus infrastruktúra, orosz–ukrán háború, kibertámadás

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: adriennk73@gmail.com
[2] Az Innovációs és Technológiai Minisztérium ÚNKP-23-3-I-NKE-114 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Abstract

During the Russia-Ukraine war, cyberspace also emerged as a theatre of war, contributing significantly to transforming the nature of modern conflicts. This study aims to provide an empirical analysis of cyber-attacks during the Russian-Ukrainian war, focusing on the energy sector. The research examines data from 2022 to 2023, analyzing the temporal trends, geographical distribution, and types of attacks. The study highlights the importance of building, developing, and maintaining cyber defenses, analyzing attacks, and drawing lessons learned. The research used time series analysis, trend analysis, and heat map visualization as scientific methods. The results show which sector has become a particular target of cyber-attacks. In addition, it shows how critical infrastructure sectors have been attacked in the context of the war and the techniques used in the attacks.

Keywords: critical infrastructure, Russian-Ukranian war, cyber attack

Bevezetés

Napjaink egyik meghatározó kihívásainak tekintendők a kibertérben zajló konfliktusok, illetve ezen konfliktusoknak a globális hatásai. Az információs technológia fejlődése és a digitális infrastruktúra térhódítása alapjaiban változtatta meg a hadviselés fogalmát, így ki kell emelni az államok közötti fegyveres konfliktusokra vonatkozó aspektusát is. A 2022-ben kirobbant orosz–ukrán háború példátlan mértékű kibertámadások sorozatát indította el, amelyek célpontjai között szerepelnek többek között a kritikus infrastruktúrák, valamint magán- és közszolgáltatók is. Ezen támadások hatása messze túlmutat a harcmezőkön, hiszen ezek képesek a gazdasági, társadalmi és politikai stabilitás megingatására is.

A 2022-ben kezdődött orosz–ukrán háború idején végrehajtott kibertámadások rávilágítottak arra, hogy az államok közötti konfliktusok során a kibertérben zajló műveletek szerves részévé váltak a hadviselésnek. A háború jelentős mértékben érintette Ukrajna kritikus infrastruktúráit, jelentős károkat okozva a különféle kommunikációs rendszerekben, energiarendszerekben és egyéb technológiai rendszerekben is.[3] Az energiaszektort célzó támadások különösen nagy veszélyt jelentenek, hiszen ezek az ellátás megszakításával vagy a rendszerek megbénításával akár egész régiók működését is veszélyeztethetik. Az ilyen támadások hatásainak vizsgálata elengedhetetlen ahhoz, hogy megértsük, milyen kockázatokkal és kihívásokkal kell szembenézni a jövőben. A kritikus infrastruktúrák – kiemelendő az energiaszektor – rendkívül sebezhetővé váltak a kibertámadásokkal szemben. Ezek a támadások nem csupán a célpontként szolgáló államok működését zavarhatják meg, hanem közvetetten más-más országokat is érintve világszintű fenyegetéseket hordoznak magukban.[4] Számos támadó csoport célzott kibertámadásokkal próbálta megbénítani Ukrajna egyes kritikus infrastruktúráit,

[3] Singla et al. 2023: 18.
[4] Aviv–Ferri 2023.

ezzel is gyengítve az ország védekezőképességét és társadalmi stabilitását.[5] Már 2013 óta Oroszország számos alkalommal hajtott végre különböző kiberműveleteket Ukrajna ellen,[6] a háborút illetően pedig a kibertámadások nemcsak a katonai célpontokat, hanem a civil infrastruktúrákat is sújtották, ami a lakossági ellátást tekintve súlyosbította a háborúban felmerülő kockázatokat és a háború következményeit.[7] Mivel az ipari technológiák alkalmazása során egyre inkább az összekapcsolt és egymásra ható rendszerekről beszélhetünk, így ez a tény is újfajta biztonsági kihívásokkal – például a kibertámadásokkal szembeni védelmi megoldások alkalmazásának nehézségével – erősíti a kritikus infrastruktúrák védelmének akadályait.[8] A digitális térben zajló hadviselés új kihívásokat hoz a nemzetközi jog és kapcsolatok számára, mivel a kibertámadások hatásai nemzetközi szinten is érezhetők.[9] Az orosz–ukrán háború során végrehajtott kibertámadások nemcsak Ukrajnát, hanem a háborúban érintett más országokat is sújtották, amelyek jelenleg is a gazdasági, politikai és társadalmi stabilitást veszélyeztetik.[10]

A kutatás céljai kettősek voltak. Egyrészről, az érintett szektorokat – kitekintéssel az energiaszektorra – érintő kibertámadások részletes feltérképezése és elemzése volt, az orosz–ukrán háború során. A célkitűzés lényege, hogy átfogó képet nyújtson a kritikus infrastruktúrák körébe tartozó szektorokat – kitekintéssel az energiaszektorra – érintő kibertámadásokról, feltárva azok gyakoriságát. Másrészről a kutatás célja volt a támadók leginkább alkalmazott stratégiáinak és módszereinek azonosítása. Ez alapján a kutatás során célom, hogy azonosítsam a leggyakrabban alkalmazott támadási technikákat.

A kutatás során, a következő kutatási kérdéseket határoztam meg:

- Milyen mértékben és milyen típusú kibertámadások érték az energiaszektort az orosz–ukrán háború során?
- Milyen stratégiákat és módszereket alkalmaztak a támadók, az egyes szektorok elleni kibertámadások folyamán?

Ezek alapján a kutatás során a következő hipotéziseket állítottam fel:

H1: A kibertámadások mértékét tekintve az energia mint ágazat a leginkább támadott kritikusinfrastruktúra-szektor.

H2: A DDoS-t mint támadási technikát alkalmazták a támadók a leggyakrabban a kritikusinfrastruktúra-szektorok ellen.

[5] Chukhua 2023.
[6] Lunn 2023.
[7] Cyberpeace Institute 2022.
[8] Bhaiyat–Sithungu 2022: 48.
[9] Feledy–Virág 2022.
[10] Givens–Gorbachevsky–Biernat 2023: 12.

Tudományos módszer

Jelen cikkben szereplő adatok alapját az úgynevezett CyberPeace Institute (szervezet) nyújtotta. A szervezet jelenleg elsősorban, de nem kizárólagosan, az orosz–ukrán háború során történt kibertámadások felmérésére koncentrál. Tehát, bár a feljegyzett támadások száma bővülhet a jövőben, a cikk jelen formájában a hiteles információkra törekszik, így csak a szervezet által közölt és feljegyzett kibertámadásokkal foglalkozik. Érdemes tisztázni, hogy a szervezetnek saját metódusa van arra vonatkozóan, hogy mikor tekint incidensnek egy eseményt, így fontos, hogy adott feltételek valamelyike teljesüljön az incidensnek való minősítéshez.

Az adatgyűjtés során jelentős nehézségeket jelentett volna a dezinformáció, amely az orosz–ukrán háború információáramlására is jellemző. A hírfogyasztók és kutatók a háborúval kapcsolatos információkat számos esetben dezinformációként kezelik addig, amíg meg nem győződnek annak teljes hitelességéről. A háborúban előforduló információs torzítások általánosan megnehezítik, hogy a háború során bekövetkezett kibertámadásokat felmérjük és azonosítsuk és a hitelességüket ellenőrizzük.[11] Az elemzett adatok teljes mértékben ettől a szervezettől származnak, ugyanis hiteles módszerük van az események minősítésére. Az incidensek megerősítése, különösen Oroszországban és Fehéroroszországban, jelentős kihívást jelent. Az intézet az adatgyűjtést nyilvánosan elérhető információkra alapozza, beleértve médiaközleményeket, kormányzati és az egyes kiberbiztonsági jelentéseket. Minden azonosított incidenst legalább két belső elemző vizsgál meg, és ahol lehetséges, több forrással is megerősítik azt. A kibertámadások dokumentálása során az incidenseket az információforrások megbízhatósága alapján három kategóriába sorolják: megerősített, valószínű és lehetséges.

A kutatás három darab tudományos módszertant alkalmaz: idősorelemzést, trendelemzést és hőtérképes vizualizációt.

Eredmények

A kibertámadások gyakoriságának és módszereinek vizsgálata fontos, hogy megértsük a támadói oldal szemszögét, indíttatásait és azt, hogy összességében milyen képességek rejlenek a támadások alkalmazásai mögött. Azt azért érdemes megemlíteni, hogy az egyes kibertámadások nem pusztán az infrastruktúrák megzavarását célozzák meg, hanem előfordul, hogy összehangolt módon különféle dezinformációs kampányokkal is párosulnak. Olyan célok társulnak ezekhez a kampányokhoz, mint a saját narratívák népszerűsítése, az ellenség demoralizálása, bizalmatlanság keltése, konfliktusok provokálása stb.[12]

[11] Hameleers et al. 2024: 1642–1645.
[12] Ináncsi et al. 2023: 120–121.

Az orosz–ukrán háború rendkívüli mértékben tematizálta az online platformokat, és a támadók célja, a belpolitika szempontjából a szemben álló ország lakosságát, külpolitikai szempontból pedig a világot és a világ közvéleményét befolyásolni a saját preferenciák alapján.[13] Bár a jelen cikk a dezinformáció témáját kapcsolatba hozza a kibertámadások lebonyolításának mikéntjével, mélyebben nem vizsgálatam, ugyanis a kutatás célja a fő támadási technikák feltérképezése és a gyakoriságának vizsgálata volt, a dezinformációs tevékenységek alkalmazása pusztán kiegészítő információként jelentős.

Az idősorelemzés során a kibertámadások havi gyakoriságát vizsgáltam 2022. január 1. és 2023. december 31. között. A támadások számának elemzésekor érdemes elválasztani az egyes hónapokat, hogy részletesebb képet kaphassunk a támadások intenzitásának alakulásáról. A támadások nem pusztán az orosz és ukrán erőkre vonatkoznak, azonban a különféle országokban működő támadási célpontok valamilyen formában köthetőek a háborúhoz és a két szemben álló fél valamelyikéhez. Az 1. ábrán látható, hogy miként alakultak a trendek a támadási események bekövetkezése kapcsán. Fontos az egyes kiemelkedőbb hónapokat megemlíteni, hiszen a támadások számának kiugrásait feltételezhetően előidézhette a háború eseményeinek alakulása:

- 2022. február, az invázió kezdete, az ismert kibertámadások száma: 42 darab volt.

Az orosz–ukrán háború 2022. február 24-én robbant ki, amikor Oroszország katonai inváziót indított Ukrajna ellen. Már 2022 januárjában is voltak kibertámadások, februárban a kibertámadások száma megnőtt, nagy valószínűséggel az inváziához köthetően.

- 2022. március, az invázió intenzitásának növekedése, az ismert kibertámadások száma: 82 darab volt.

Az orosz erők folytatták a nagyobb ukrán városok ostromát. A kibertámadások száma az előző hónaphoz képest jelentősen megugrott, a háború intenzitásának növekedésével egyidejűleg.

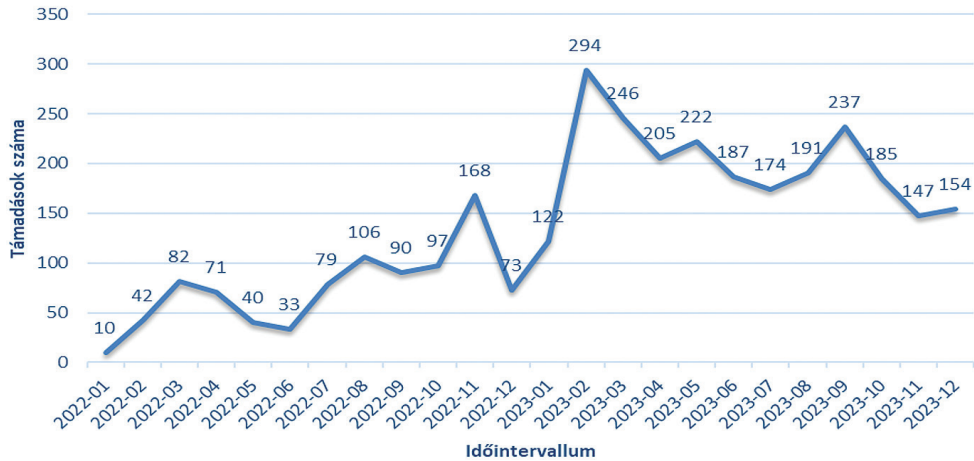
- 2022. november, a herszoni visszavonulás, az ismert kibertámadások száma: 168 darab volt.

2022 novemberében az orosz csapatok visszavonultak Herszonból, ami egyfajta katonai és stratégiai visszalépésnek minősült Oroszország szempontjából. A kibertámadások száma ebben a hónapban érte el a 2022-es év csúcsát. Ebből arra következtethetünk, hogy a visszavonulás hatására váltak intenzívebbé a kibertámadások.

- 2023. február, az egyéves évforduló, az ismert kibertámadások száma: 294 darab volt.

2023 februárjában volt a háború kezdetének egyéves évfordulója. A hónapban a kibertámadások száma jelentősen megugrott, ami feltételezhetően összefüggésbe hozható az évfordulóval kapcsolatos fokozott politikai és katonai feszültségekkel.

[13] Bányász et al. 2024: 56–57.



1. ábra: A kibertámadások számának alakulása a vizsgált időszakban
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

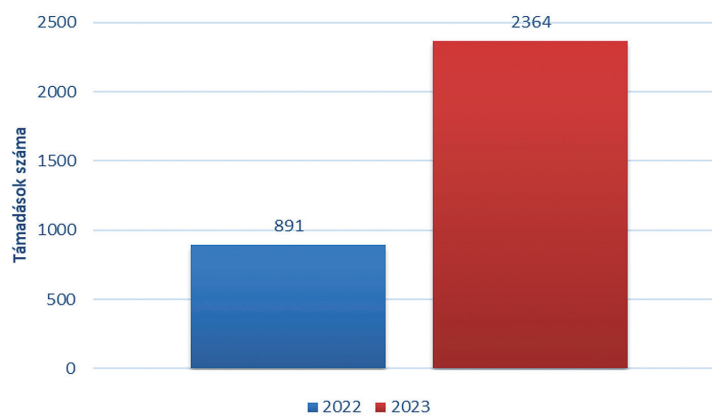
- 2023. szeptember, az őszi hadjáratok és ukrán ellentámadások, az ismert kibertámadások száma: 237 darab volt.

2023 szeptemberében az ukrán erők folytatták az ellentámadásokat Dél-Ukrajna és Kelet-Ukrajna területén. A kibertámadások száma ebben a hónapban ismét kiugróan magas volt, ami valószínűleg összeköthető az ellentámadások intenzitásával.

- 2023. december – év vége, az ismert kibertámadások száma: 154 darab volt.

Decemberben a támadások száma kismértékű növekedést mutat novemberhez képest, ami arra utalhat, hogy a felek az ünnepi időszakot is kihasználták a támadások számának fokozására. Azonban jelentős változást az év végének ténye sem okozott a kibertámadások számában.

A 2. ábrán látható a 2022-es és 2023-as kibertámadások száma, amely jelentős növekedést mutatott a 2023-as évben, a 2022-es évhez képest.



2. ábra: A kibertámadások évenkénti megoszlása az orosz–ukrán háborúban
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

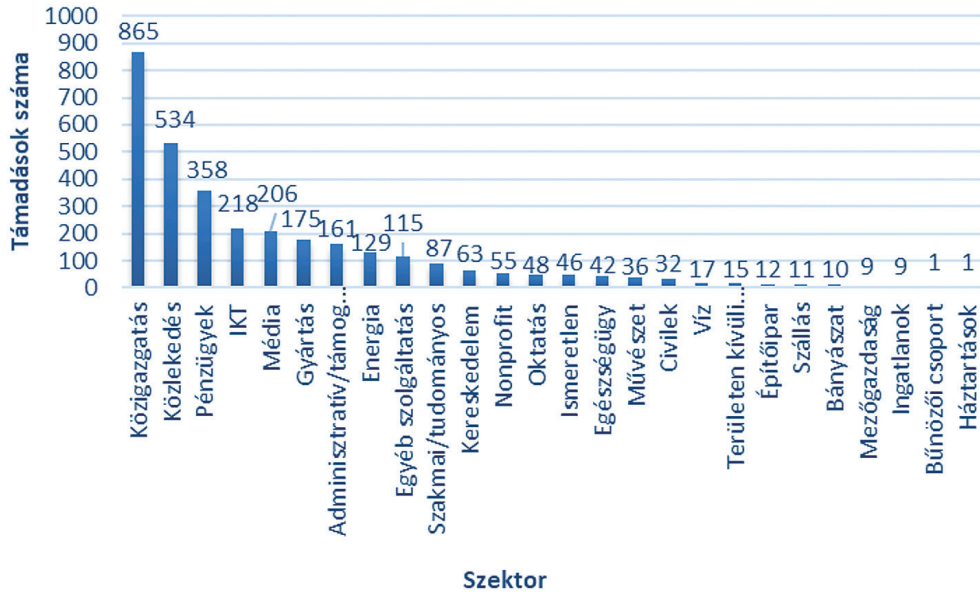
Az ismert támadások száma alapján 2022-ben 891 darab rögzített támadás volt, míg 2023-ra ez a szám 2364 darabra emelkedett. A növekedést, a támadók tapasztalatszerzésén túl az is okozhatja, hogy egyre többen csatlakoznak a különböző támadó csoportokhoz. Továbbá, a növekvő támadások száma nagy valószínűséggel összefüggésben áll a háború eszkalálódásával.

A támadások mennyiségének növekedése mellett a támadási módszerek és a célpontok is diverzifikálódtak 2023-ban. A háború során folyamatosan, egyre több szektor vált célponttá és a támadók újabb technikákat alkalmaztak. A támadások számának ilyen fokú növekedése azt is jelezheti, hogy a kibertámadások egy-egy konfliktusban vagy háborúban való alkalmazásának komplexitása nőtt, a kibertámadások lebonyolításához egyre több erőforrást lehet felhasználni mind a támadói, mind a védelmi oldalon. A számadatok arra is utalhatnak, hogy a jövőben a kibertámadások száma még tovább növekedhet, különösen akkor, ha a politikai feszültségek fennmaradnak vagy tovább fokozódnak.

A támadások számának növekedésével együtt érdemes megemlíteni azt a tényezőt is, hogy a 2022-ben kirobbant háború során nem ment végbe olyan kiberművelet, amely kiterjedt módon megbénította volna Ukrajna kritikus nemzeti infrastruktúráját. A háború előrehaladtával számos, eltérő nézőpont alakult ki arról, hogy a háború kiberműveleti oldala mennyire jelentős. Oroszország már évek óta fejleszti és alkalmazza a kiberműveleti képességeit, és ahogyan a későbbi ábrákon is meg lehet figyelni, a különféle műveletek nem pusztán az infrastruktúrák megzavarását célozzák, hanem a propaganda és a dezinformáció célzatával is alkalmazzák őket.[14] Továbbá Oroszország – a Geraszimov-doktrína értelmében – a közösségi médiát is egy szélesebb hadszíntér részének tekinti. A háború közösségimédia-megjelenését és a két szemben álló fél egymáshoz való viszonyát vizsgáló tanulmány alapján, a háború kitörése után, a másik ország iránt az ukránok 2%-a és az oroszok 23%-a mutatott pozitív hozzáállást. Ugyanezek a számok a tanulmány alapján 83% és 74%-os mutatók voltak 2012-ben.[15] Ez a példa a jelen cikk szempontjából azért is lényeges, mert a közösségi média potenciálisan hozzájárulhat ahhoz, hogy egy amúgy is ellenséges hangulatot felerősítsen, és feltételezhetően ahhoz is hozzájárulhat, hogy ösztönözze a támadói egyének és csoportok tevékenykedéseit.

Összességében a kibertámadások évenkénti megoszlása rávilágít a kibertér kihasználásának egyre növekvő jelentőségére napjaink modern konfliktusaiban. A kibertámadások intenzitásának növekedése égetővé teszi a kiberbiztonsági intézkedések megtételének fokozását, valamint a nemzetközi együttműködések erősítését ezen a téren.

[14] Willet 2022: 7–8.
[15] Kyrychenko et al. 2024: 1–3.



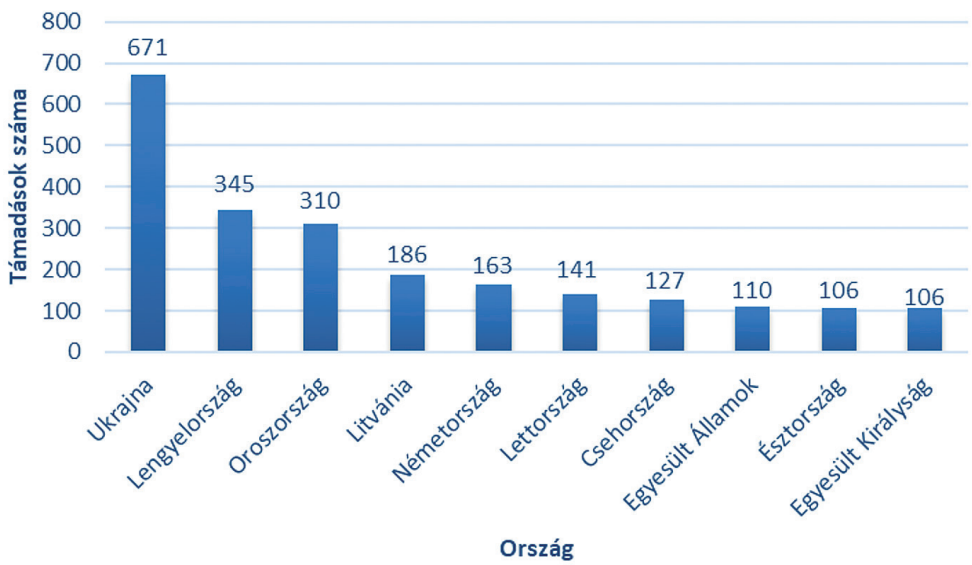
3. ábra: A kibertámadások számának megoszlása a célpontszektorok alapján
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

Megvizsgáltam a támadások ágazatspecifikus megoszlását, amely a 3. ábrán látható: az elemzett időszakban a közigazgatás, a közlekedés (amelybe a szállítmányozás, ellátási láncok is beletartoznak), a pénzügyi, az infokommunikációs technológiák (IKT), valamint a média ágazatot érte a legtöbb támadás. Az energiaszektor a kibertámadások számának tekintetében a 8. helyet foglalja el, az ismert kibertámadások száma 129 darab. Ez alapján elmondható, hogy a feldolgozott adatok szerint a kibertámadások mennyiségének szempontjából az energiaszektor – a többi kritikus szektorhoz viszonyítva – korántsem volt annyira érintett, mint például a közigazgatás, a közlekedés vagy a pénzügyi szektor.

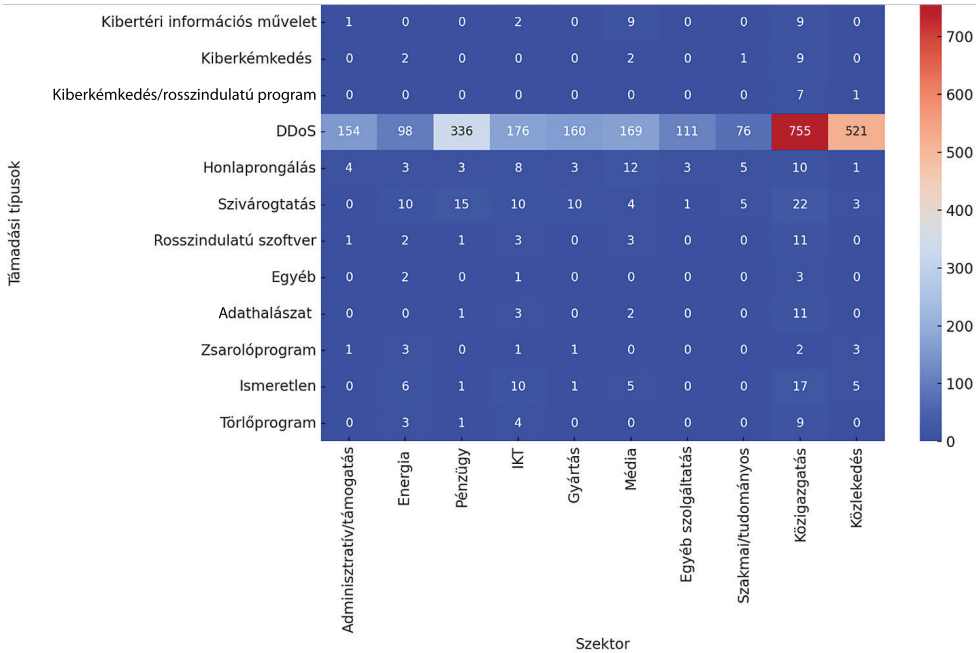
Az 4. ábra alapján elmondható, hogy a 2022-es és 2023-as évben a kibertámadásokban leginkább érintett ország Ukrajna, Lengyelország, Oroszország, Litvánia és Németország. Az ábrákon már nem látható, de a listán még számos más ország is szerepel, mint például Olaszország, Svédország, Spanyolország vagy éppen Szlovákia, Fehéroroszország vagy Horvátország. Az országonkénti kibertámadások számának megoszlása a vizsgált időszakban jelentős eltéréseket mutat, ami rávilágít a geopolitikai és a kibertérben fellelhető feszültségek összefüggéseire. Ukrajna messze a legtöbb kibertámadási incidenst szenvedte el, összesen 671 darab dokumentált támadással. Ukrajnának nagy valószínűséggel a háború alatt, illetve már az azt megelőző években is jelentős erőforrásokat kellett mozgósítania a kibervédelmi képességeinek a megerősítésére.

Ukrajnát a sorban Lengyelország követi 345 darab támadással, majd – Oroszországot, Németországot, Csehországot és az Egyesült Államokat leszámítva – a balti államok, különösen Litvánia (186 darab támadás), Lettország (141 darab támadás)

és Észtország (106 darab támadás), amely országoknál szintén viszonylag magas számú kibertámadási eseményt regisztráltak. Ezek az országok feltételezhetően stratégiai helyzetük miatt váltak célponttá, különösen az Oroszországgal való közelségük és NATO-tagságuk miatt. Az ilyen országokban megjelenő kibertámadások akár geopolitikai célokat is szolgálhatnak, például a NATO és az Európai Unió destabilizálását. Oroszországban 310 darab kibertámadást dokumentáltak, ami azt jelzi, hogy nemcsak támadóként, hanem célpontként is érintett az ország. A támadások egy része valószínűleg válaszlépésként érkezhetett a háborús tevékenységekre, illetve olyan célok is szolgálhattak a támadások hátterében, mint az orosz állam destabilizálása. Nyugat-európai országok, mint Németország (163 darab támadás) és az Egyesült Királyság (106 darab támadás) szintén gyakorta megjelenő célpontok voltak. Ezek az országok fontos gazdasági és politikai szereplők, így a támadások célja feltételezhetően lehetett a gazdasági zavarok okozása vagy politikai nyomásgyakorlás is. Az Egyesült Államok (110 darab támadás) szintén a 10 leggyakrabban támadott ország közé tartozik, különösen mint a globális hatalom egyik központja. Számos kisebb országban is dokumentáltak kibertámadásokat, bár ezek száma jelentősen alacsonyabb. Ezen országok, előfordul, hogy közvetett célpontokként jelennek meg, vagy más országokkal kapcsolatos konfliktusok miatt válnak célponttá.



4. ábra: A 10 legtöbb kibertámadást elszenvedő ország a vizsgált időszakban
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján



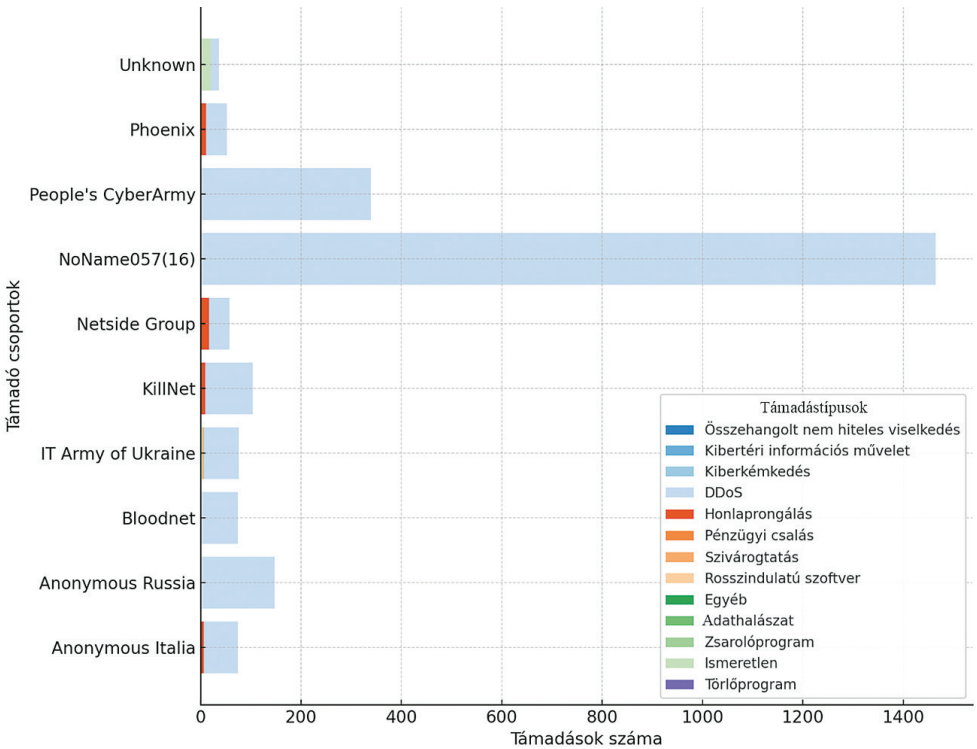
5. ábra: A 10 leginkább támadott ágazat hőtérképes mátrixa a támadástípusok szerint
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

Az 5. ábrán látható a tíz leginkább támadott szektorban előforduló különböző támadási típusok eloszlása összesítetten a vizsgált időszakban és az összes, vizsgált országra vonatkozóan. A rendelkezésre álló információk alapján – ahogy a 3. ábrán is megjelent – a közigazgatás, a közlekedés és a pénzügyi szektor voltak a legtöbbször érintett célpontok, különösen az elosztott túlterheléses (DDoS) támadások szempontjából. A 2022-es és 2023-as évet összesítve, a közigazgatási szektort érte a legtöbb DDoS-támadás, míg a közlekedési és pénzügyi szektort szintén jelentős mennyiségű DDoS-támadás érte, de látható, hogy más típusú kibertámadásokat is alkalmaztak a támadók, mint például a szivárogtatást *(hack and leak)*. Az energiaszektort is többfajta támadás érte, gyakori eset a szivárogtatás vagy a törlőprogramok alkalmazása, azonban itt is kiemelkedik ezek közül a DDoS mint támadási forma. Az ábra rávilágít arra, hogy a különböző szektorok számos, akár eltérő támadási módszerekkel néznek szembe. A DDoS-támadások a legtöbb szektorban dominálnak, különösen a közigazgatásban, közlekedésben és a pénzügyi szektorban, míg például a szivárogtatás a közigazgatás és pénzügyi szektoron kívül az energia- vagy az IKT-szektorban is megjelenik.

Az egyes rubrikákon belüli színtelítettség a támadások számának nagyságát jelzi, átlátható mátrixát nyújtva az érintett támadási technikáknak és szektoroknak. Az ábra alapján vélelmezhetően a közigazgatás, a közlekedés és a pénzügyi szektorban – az adatok alapján – adott mértékben magasabb szintű védelmi funkciókat szükséges kiépíteni, mint a többi szektorban a kiberbiztonsági kockázatok mérséklésének céljából. Azonban nem elhanyagolható a többi szektor, mint például az energiaszektor védelmének fejlesztése és fenntartása sem, bár vélelmezhetően az energiaszektor esetében magasabb

fizikai károkozásról lehet beszélni, mint kibertéri károkozásról. A közigazgatási szektor esetében feltételezhető, hogy a kibertérben zajló támadások nagyobb károkat tudnak okozni, mint a fizikai térben lévők.

A 6. ábra bemutatja a tíz legaktívabb támadó csoport által alkalmazott támadási típusok megoszlását. Látható, hogy a NoName057(16) csoport volt a legaktívabb, főként DDoS-támadások végrehajtásával. Ezt követi a People's CyberArmy, amely csoport szintén jelentős számú DDoS-támadást hajtott végre. A honlaprongálás mint támadási formában a Netside Group és a Phoenix, illetve a KillNet csoportok voltak a legaktívabbak, míg a szivárogtatás típusú támadásokban az IT Army of Ukraine 6 darab rögzített támadási eseménnyel és az Anonymous Russia 1 darab rögzített támadási eseménnyel voltak a legkiemelkedőbbek.



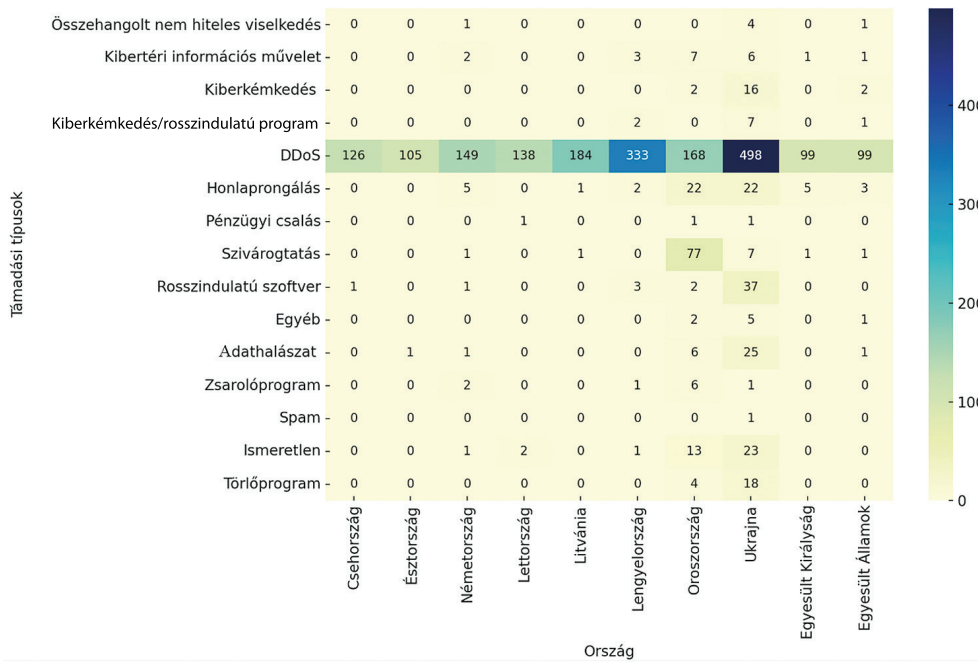
6. ábra: A különböző támadástípusok megoszlása a 10 legaktívabb támadó csoporthoz köthetően
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

A be nem azonosítható *(unknown)* kategóriába sorolt támadók számos különböző támadási módszert alkalmaztak, de leginkább az adathalászatot vetették be a célpontok ellen.

Ahogyan a korábbiakban is látható volt, a DDoS-támadások dominálják a legtöbb támadó csoport tevékenységét, különösen a NoName057(16) csoport és a People's CyberArmy esetében. Ezek a csoportok a támadások számában és intenzitásában is kiemelkednek a DDoS-támadás elkövetésének szempontjából. Összességében, bár

a támadó csoportok többféle támadási módszert alkalmaztak, azokat a DDoS-támadásokhoz képest csak elvétve alkalmazták, így az ábrán is alig-alig jelennek meg. Ezen felül – további kutatási szempontokból – még további elemzést érdemel azoknak a támadó csoportoknak a vizsgálata, amelyek a 6. ábrán nem jelennek meg, mert kevésbé minősültek aktív szereplőknek. Azonban ezek a csoportok változatosabb támadási formákat alkalmaztak.

A 7. ábrán látható a vizsgált időszakban a 10 leginkább támadott ország és az ellenük alkalmazott különböző támadástípusok hőtérképes mátrixa. A DDoS támadási forma számosságát tekintve az összes ország esetében kiemelkedik. Ez különösen Ukrajna, Lengyelország és Litvánia esetében számottevő. A honlaprongálás, a rosszindulatú szoftver alkalmazása és a szivárogtatás legfőképpen Oroszország és Ukrajna esetében jelentős.



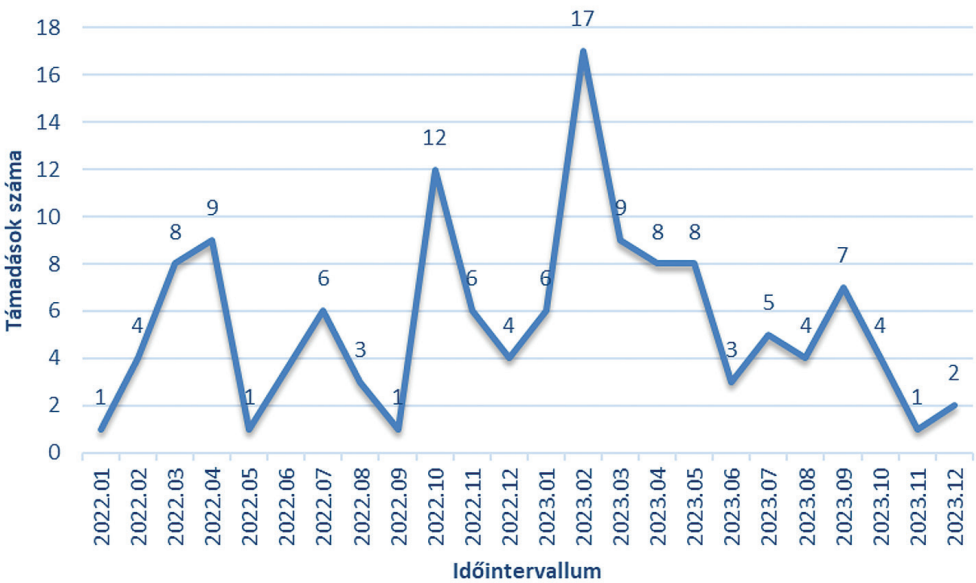
7. ábra: A 10 leginkább támadott ország és az őket ért támadási fajták hőtérképes mátrixa
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

A 6. ábrához hasonlóan a 7. ábrán is a támadások gyakoriságának nagysága látható, jelen esetben a támadási technikák és célpontországok mátrixaként. Látható, hogy az orosz–ukrán háborút illetően, bár Ukrajna a fő célpont, nem tekinthetünk el attól, hogy a háborús felek mellett más-más országok is célpontként szolgálnak. A feldolgozott adatok, ezzel együtt a támadások összessége az orosz–ukrán háborúhoz köthető valamilyen szempontból, tehát nem pusztán a szemben álló feleknek kell a kibervédelmükre – és annak a fejlesztésére – koncentrálni, hanem ez az érintett és egyébként minden más ország számára is fontos cél kell hogy legyen.

Energiaszektor

Az energiaszektor az egyik legkritikusabb iparág, így sokkal könnyebben válhat a kibertámadások célpontjává, mint más – ehhez az ágazathoz viszonyított – kritikus szektor, különösen olyan rendkívüli helyzetekben, mint az orosz–ukrán háború. Az energiaellátás megszakadása súlyos következményekkel járhat többek között a gazdaságra és a társadalom működésére is. Az alábbiakban több szempontból is vizsgálom az energiaszektort, beleértve az időbeli trendeket, a támadástípusok megoszlását, a támadó csoportok kapcsolatát a szektorral és az energiaszektort érintő kibertámadások földrajzi megoszlását.

Először azt vizsgálom, hogyan változott az energiaszektor elleni támadások száma a vizsgált időszakban:



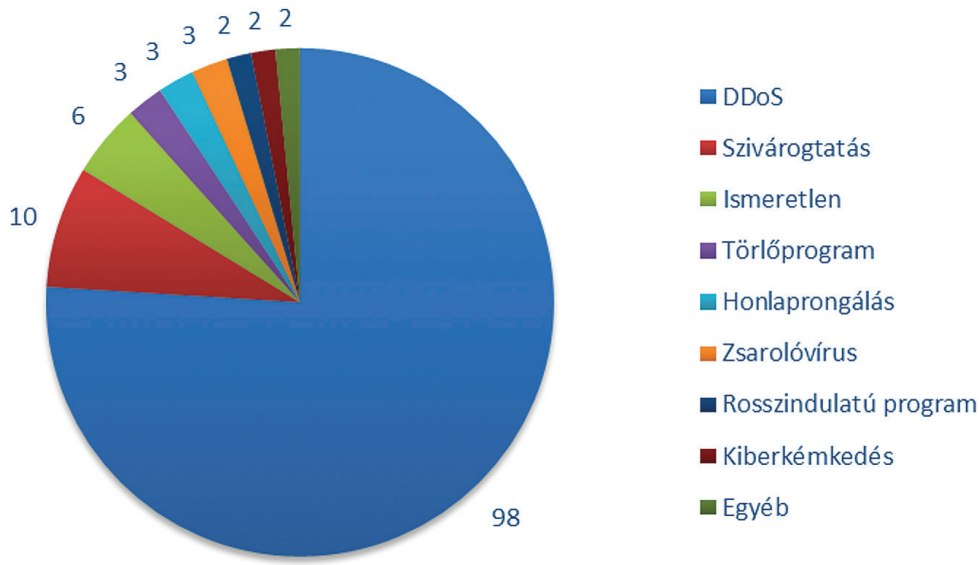
8. ábra: Energiaszektor elleni kibertámadások száma a vizsgált időszakban
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

A 8. ábrán az energiaszektor elleni kibertámadások (összesen: 129 darab) időbeli elemzése alapján megfigyelhető, hogy a támadások száma jelentős ingadozásokat mutatott a vizsgált időszakban. 2022 elején az energiaszektor elleni támadások száma fokozatosan növekedett, különösen a háború első hónapjaiban. Márciusban és áprilisban megvalósult az első csúcsosodás. Ez az időszak jelentős volt ebből a szempontból a háború kezdeti szakaszában, a támadók feltételezhetően arra törekedtek, hogy destabilizálják az energiaellátást.

A vizsgált időszak távlatában a támadások száma 2023 februárjában érte el a csúcsot, ekkor 17 darab kibertámadást regisztráltak. Ez valószínűleg összefügg a háború egyéves évfordulójával és az energiaellátás megbénítására irányuló törekvésekkel. A támadások száma az év hátralévő részében viszonylag ingadozó volt, és többet már

nem érte el a februári csúcsot. Feltételezhetően azért, mert a támadók stratégiája folyamatosan változó volt, és a támadások intenzitása a háború menetétől, a politikai történésektől függően alakult.

A támadási technikák elemzése során azt vizsgálom, hogy az energiaszektorban mely típusú kibertámadások voltak a leggyakoribbak. Ez segít megérteni, hogy milyen típusú fenyegetésekkel szembesül ez a szektor.

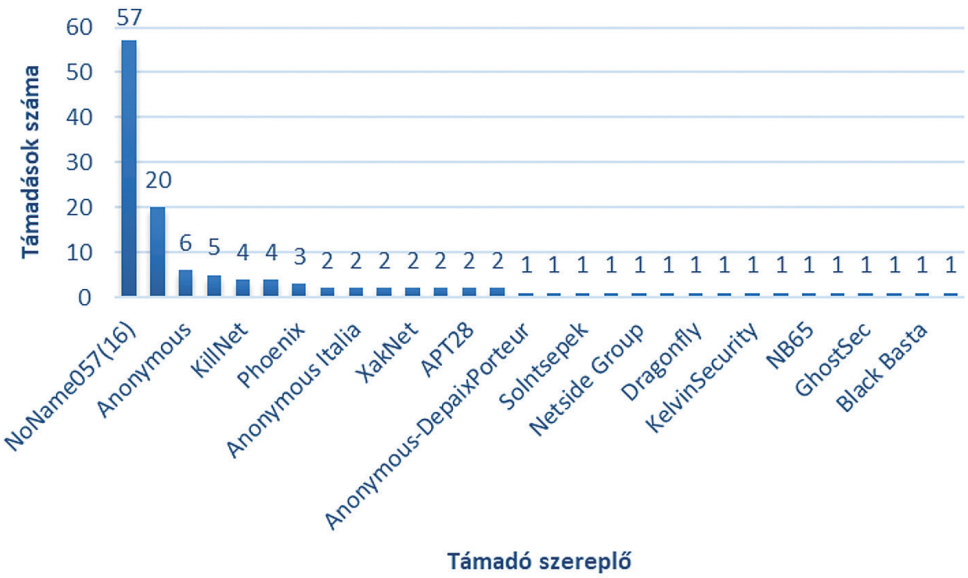


9. ábra: Energiaszektor elleni kibertámadások típusa
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

Ahogyan a 9. ábrán is látható, az energiaszektor elleni kibertámadások típusainak elemzése során a következő, főbb megállapításokat tehetjük: A DDoS-támadások voltak messze a leggyakoribbak az energiaszektorban is, összesen 98 darab ismert támadással. A támadások célja nagy valószínűséggel az volt, hogy túlterheljék az infrastruktúrát, ezzel megszakítva a szolgáltatások működését. A DDoS-támadások gyakorta minősülnek elsődleges választásnak a kritikus infrastruktúrák elleni támadások esetén, mivel gyorsan és viszonylag egyszerűen képesek jelentős zavarokat okozni.

A második leggyakoribb támadástípus a szivárogtatás volt, ahol a támadók olyan információkat szereztek meg, amelyeket a megszerzés után kiszivárogtatnak. Ez a fajta támadás 10 alkalommal fordult elő, potenciális célja a bizalom megrendítése vagy politikai célok elérése lehetett. A támadók ekkor érzékeny adatok kiszivárogtatásával próbálnak nyomást gyakorolni a támadásban érintett szervezetekre vagy országokra. Kismértékben ugyan, de jellemzők voltak még azok a támadási fajták is, amelyeket konkrétan nem lehetett behatárolni, hogy hova tartoznak, pusztán a kibertámadás tényét lehetett sejteni.

A következő elemzésben feltárom, hogy mely támadó csoportok voltak a legaktívabbak az energiaszektort érintő támadások okozása során. Az energiaszektor elleni támadásokat elemezve a következő főbb támadó csoportok emelkedtek ki:

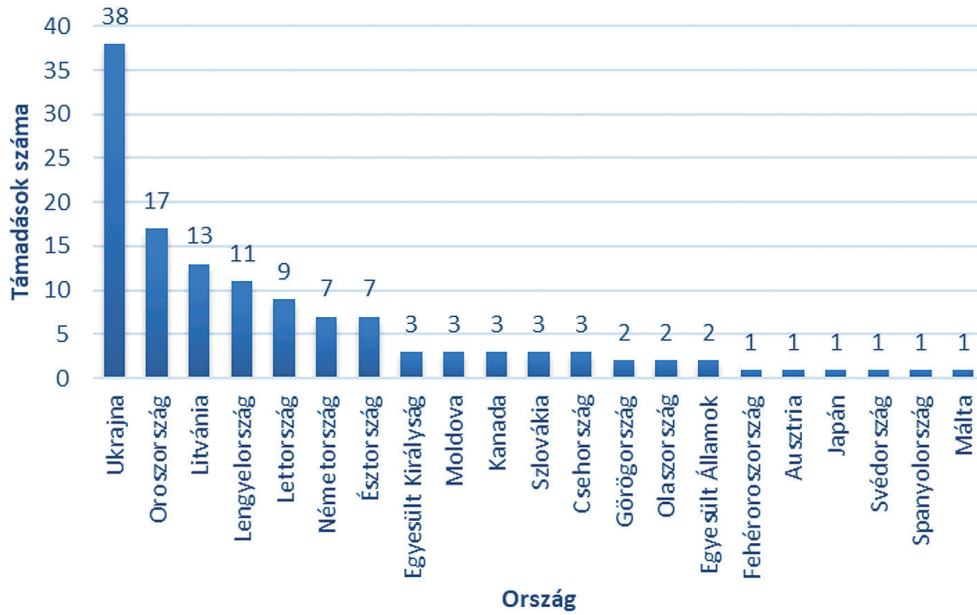


10. ábra: Az energiaszektort támadó csoportok és az általuk indított támadások számának megoszlása
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

A 10. ábrán látható, hogy a NoName057(16) volt a legaktívabb támadó csoport az energiaszektorban, összesen 57 darab támadással. Ez a csoport elsősorban DDoS-támadásokat hajtott végre, amely támadások célja az energiaellátás biztosításának akadályoztatása volt. Szintén az energiaszektor tekintetében a People's CyberArmy a második legaktívabb csoport, 20 darab támadás indításával. Ez a csoport szintén a DDoS-támadások alkalmazására fókuszált. Az energiaszektort érő támadások tekintetében az Anonymous és más hacktivista csoportok, mint például az Anonymous Italia és Anonymous-DepaixPorteur, szintén aktívak voltak, bár jóval kisebb mértékben, mint az első két helyen említett csoport. A Sandworm, az APT28 és az IT Army of Ukraine az energiaszektort kevésbé támadták más szektorokhoz képest.

Érdemes megemlíteni, hogy a különféle támadó csoportok tevékenysége gyakran része a szélesebb körű katonai stratégiáknak, ahol a kibertámadások a fizikai támadások kiegészítéseként szolgálnak.

Az energiaszektorra vonatkozó utolsó elemzési szempont során azt vizsgálom, hogy az energiaszektor mely országokban volt a leginkább érintett a kibertámadások által.



11. ábra: Az energiaszektort érő támadások földrajzi eloszlása
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

A 11. ábrán megfigyelhető az energiaszektor elleni kibertámadások földrajzi eloszlása, ami fontos információkat nyújt arról, hogy mely országok voltak a leginkább érintettek célpontként a vizsgált időszakban. Az energiaszektor elleni támadások többsége Ukrajna ellen irányult, ahol összesen 38 darab kibertámadást regisztráltak. Ez összhangban áll a háborús körülményekkel, ahol az energiaellátás megszakítása közvetlen hatással lehet a háborús erőfeszítésekre és a lakosság életére.

Ahogyan a 3. ábra kapcsán is említettük, Oroszország is célpont volt ebben a tekintetben, 17 darab támadás érte az országot. Ezen felül a balti államok, mint Litvánia (13 darab támadás), Lettország (9 darab támadás) és Észtország (7 darab támadás), szintén célpontoknak minősültek nemcsak összességében, de az energiaszektor tekintetében is. Az Egyesült Államokban és Kanadában is jelentek meg kibertámadási incidensek az energiaszektor ellen (2 és 3 darab támadás), ami arra utal, hogy a támadók globálisan is figyelembe veszik a stratégiai energiaforrásokat. Így az ezen országokat érintő támadások célja feltételezhetően az, hogy zavart keltsenek a nemzetközi energiaellátásban.

Összegzés

Az orosz–ukrán háború kibertámadásai eddig kismértékben tapasztalt, újszerű kihívásokat hoztak magukkal a modern, technológián nyugvó kritikus infrastruktúrák számára. A kutatás célja az volt, hogy átfogóan elemezze az ismert kibertámadásokat, kitekintéssel az energiaszektorra. Az elmúlt években tapasztalt jelentős digitális fejlődés,

valamint a globális hálózati infrastruktúra növekvő függősége miatt a kibertámadások egyre komolyabb fenyegetést jelentenek. Ezen támadások nem csupán a katonai célpontokat érintik, hanem széles körben hatnak a civil infrastruktúrára, a pénzügyi rendszerekre és a kritikus ellátási láncokra is. Az energiaszektor különösen sebezhető, mivel a modern társadalmak energiafüggősége központi szerepet játszik a mindennapi élet fenntartásában és a gazdasági stabilitás megőrzésében. A kibertérben zajló harcok nemcsak a konfliktus közvetlen résztvevőire, hanem a globális közösségre is kihatnak, hiszen a digitális világ határok nélküli természetéből fakadóan a támadások könnyen érinthetnek más államokat is, illetve világszintű gazdasági és politikai következményekkel járhatnak. Az orosz–ukrán háború során alkalmazott kibertámadások nem pusztán az energiaszektorra irányuló támadások révén váltak jelentőssé, bár az energiaellátás zavarai közvetlen hatással vannak a lakosság életminőségére, az ipari termelésre és a nemzetbiztonságra. Az országonkénti megoszlás rávilágított arra, hogy a kibertámadások eloszlása szorosan összefügghet a geopolitikai helyzettel is. Azok az országok, amelyek közvetlenül érintettek háborúban – mint például Ukrajna – és a helyzet adta további konfliktusokban, vagy éppen stratégiai jelentőségűek, mint Lengyelország és a balti államok, vannak a legnagyobb fenyegetésnek kitéve.

Az energiaszektor nem a legnagyobb mértékben, de ugyanúgy célpont volt a 2022-es év és 2023-as év között vizsgált kibertámadások során, különösen a háborúban közvetlenül érintett régiókban. Az elemzés rámutatott, hogy az energiaellátás megszakítása a kibertámadások szempontjából nem a legfontosabb, de fókuszban lévő eleme volt a támadók stratégiájának. Továbbra is igaznak bizonyult, hogy az energiaszektor védelme fontos, különösen a jelenlegi, rendkívül feszült, globális helyzetben.

A kutatás célja egyrészről a kritikusinfrastruktúra-szektorokat érintő, az orosz–ukrán háború első két évében lezajlott kibertámadások elemzése volt, kitekintéssel az energiaszektorra, valamint a támadók stratégiáinak, leggyakrabban használt támadási technikáinak azonosítása.

A kutatás során a kutatási célkitűzések és kérdések megfogalmazása után két darab hipotézist állítottam fel. Ezeket három darab tudományos módszertannal vizsgáltam: végeztem trendelemzést, idősorelemzést és hőtérképes megjelenítést. A kutatás során a hipotézisekhez kapcsolódóan két darab megállapítás született:

T1: A kibertámadások mértékét tekintve nem az energiaágazat a leginkább támadott kritikusinfrastruktúra-szektor, hanem a közigazgatási szektor.

T2: A DDoS-t mint támadási technikát alkalmazták a támadók a leggyakrabban a kritikusinfrastruktúra-szektorok ellen.

A kibertámadások számának és a támadási technikáknak a fajtája változó volt, de általánosságban elmondható, hogy a DDoS-támadások és a zsarolóvírus-támadások voltak a leggyakrabban előforduló technikák. Ezek a támadások súlyos működési zavarokat tudnak okozni a szolgáltatások ideiglenes megállását, a rendszerek megbénulását eredményezve.

A jelen cikkben feldolgozott adatokat a jövőben szükséges lesz további szempontok alapján is feldolgozni és elemezni ahhoz, hogy a jövőben megfelelő következtetéseket lehessen levonni. A kutatási eredmények hasznosíthatók a jövőben az orosz–ukrán háború kibertámadásainak további elemzésére és a védelmi megoldások kialakításának megalapozásához.

Felhasznált irodalom

Aviv, Itzhak – Ferri, Uri (2023): Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem. *International Journal of Critical Infrastructure Protection,* 43, 1–31. Online: https://doi.org/10.1016/j.ijcip.2023.100637

Bányász, Péter et al. (2024): Empirical Studies of Russian–Ukrainian War Related Fake News – Part 2. *Hadmérnök,* 19(1), 55–83. Online: https://doi.org/10.32567/hm.2024.1.4

Bhaiyat, Humairaa – Sithungu, Siphesihle (2022): The Emergence of IIoT and its Cyber Security Issues in Critical Information Infrastructure. *European Conference on Cyber Warfare and Security,* (21)1, 46–51. Online: https://doi.org/10.34190/eccws.21.1.248

Chukhua, Ilona (2023): Russian Aggressive Cyber-Policy During Russia-Ukraine War. In Chitadze, Nika (szerk.): *Cyber Security Policies and Strategies of the World's Leading States.* Hershey, PA: IGI Global, 224–238. Online: https://doi.org/10.4018/978-1-6684-8846-1.ch014

CyberPeace Institute (2022): Cyber Attacks in Times of Conflict. Online: https://cyberconflicts.cyberpeaceinstitute.org/threats

Feledy, Botond – Csaba, Virág (2022): An Assessment of Cyber Volunteer Groups in Interstate Conflicts and Their Impact on Public Policies. *Scientia et Securitas,* 3(1), 1–7. Online: https://doi.org/10.1556/112.2022.00091

Givens, Austen – Gorbachevsky, Max – Biernat, Anita (2023): How Putin's Cyber-war Failed in Ukraine. *Journal of Strategic Security,* 16(2). Online: https://doi.org/10.5038/1944-0472.16.2.2099

Hameleers, Michael et al. (2024): Mistakenly Misinformed or Intentionally Deceived? Mis- and Disinformation Perceptions on the Russian War in Ukraine Among Citizens in 19 Countries. *European Journal of Political Research,* 63(4), 1642–1654. Online: https://doi.org/10.1111/1475-6765.12646

Ináncsi, Mátyás et al. (2023): Empirical Studies of Russian–Ukrainian War Related Fake News, Part 1. *Hadmérnök,* 18(4), 109–128. Online: https://doi.org/10.32567/hm.2023.4.8

Kyrychenko, Yara et al. (2024): Social Identity Correlates of Social Media Engagement Before and After the 2022 Russian Invasion of Ukraine. *Nature Communications,* 15(8127). Online: https://doi.org/10.1038/s41467-024-52179-8

Lunn, Stephen (2023): Human Security and the Digital Threat: Russia and Ukraine. In Reimer, L. E. – Standish, K. (szerk.): *Perspectives on Justice, Indigeneity, Gender, and Security in Human Rights Research.* Singapore: Palgrave Macmillan, 263–283. Online: https://doi.org/10.1007/978-981-99-1930-7_13

Singla, Rishabh et al. (2023): An Analysis of War Impact on Ukrainian Critical Infrastructure Through Network Measurements. In *Proceedings of the 2023 7th Network Traffic Measurement and Analysis Conference (TMA).* Naples, 1–10. Online: https://doi.org/10.23919/TMA58422.2023.10199005

Willett, Marcus (2022): The Cyber Dimension of the Russia–Ukraine War. *Survival: Global Politics and Strategy,* 64(5), 7–26. Online: https://doi.org/10.1080/00396338.2022.2126193

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 3. szám 201–212.
DOI: 10.32567/hm.2024.3.12

Nagy Sándor[1]

Szubjektivitás a kockázatmenedzsmentben

Subjectivity in the Riskmanagement

Absztrakt

Hérakleitosz ókori görög gondolkodó mondta, hogy „az egyetlen állandó a változás maga". Változó világban élünk és a túlnépesedés, az erőforrások kihasználása, az éghajlatváltozás és még nagyon sok tényező gyorsítja ezeket a folyamatokat, amelyek nemzeti, szervezeti, de egyéni szinten is hatással vannak mindennapjainkra. A változás nem feltétlenül hordoz negatív jelentéstartalmat, ugyanakkor a negatív hatások azok, amelyeket el akarunk kerülni, miközben a pozitív kimenetelekkel szemben bizalommal lépünk fel. A változásokra való felkészülés, illetve a lehetséges kimenetek értékelésének egyik elterjedt és talán leghatékonyabb módja a kockázatmenedzsment, amelynek alapja a kockázatok értékelésével meghatározni, hogy mely kimenet elvárt, elfogadható, illetve melyek azok a folyamatok, amelyeket kezelni kell. Ugyanakkor a kockázatértékelés mindig függ az értékelőtől, akinek objektivitása nagymértékben befolyásolja a végeredményt.

Kulcsszavak: kockázatmenedzsment, kockázatelemzés, kockázatértékelés, kockázatkezelés

Abstract

Heraclitus, the ancient Greek philosopher, said that „change is the only constant." We live in a dynamic world where factors such as overpopulation, resource exploitation, climate change, and many others accelerate these processes, impacting our daily lives on national, organizational, and individual levels. Change does not necessarily carry a negative connotation; however, we seek to avoid the negative impacts while approaching positive

[1] Oktató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: nagysandor.phd@gmail.com

outcomes with confidence. One prevalent and perhaps most effective way of preparing for and evaluating possible outcomes of change is through risk management. The foundation of risk management lies in assessing risks to determine which outcomes are expected, acceptable, and which processes need to be addressed. Nevertheless, risk assessment always depends on the evaluator, and the objectivity of the evaluator significantly influences the end result.

Keywords: risk management, risk analysis, risk evaulation, risk treatment

A kockázatmenedzsment terminológiai problémái hazánkban

A kockázatmenedzsment az életünk szinte minden területén meghatározó szerepet játszik, a nemzetközi standardokhoz való alkalmazkodás és a hazai szabályozások betartása pedig különösen nagy figyelmet igényel. Ugyanakkor a kockázatelemzési és -kezelési folyamatok objektivitását gyakran veszélyezteti a szubjektivitás. Érzelmi és érdekalapú befolyásoló tényezők jelenhetnek meg, amelyek torzíthatják az értékelések eredményét és befolyásolhatják a döntéshozatalt. Ebben a cikkben bemutatom, hogyan jelenik meg a szubjektivitás a kockázatmenedzsmentben, és milyen módszerekkel lehet ennek hatásait minimalizálni. Emellett ismertetem a magyar és a nemzetközi terminológia közötti különbségeket, amelyek nehézségeket okozhatnak a szabályozás egységes értelmezésében.

Kockázatmenedzsment, kockázatelemzés, kockázatértékelés és a kockázatkezelés a magyar köznapi szóhasználatban hasonló jelentéssel rendelkező fogalmak, miközben szakmai tartalmukban elkülönülnek. A köznapi gyakorlatban a mai napig nem sikerült tisztázni a jelentésbeli különbségeket, holott például az *MSZ ISO 31000:2018 Kockázatmenedzsment. Irányelvek* szabvány[2] (szabvány) közérthetően fogalmazva írja le a következőképpen: „*Kockázatmenedzsment*: Egy szervezetnek a kockázatokkal kapcsolatos összehangolt irányítási és felügyeleti tevékenységei."[3] A szabvány ezen meghatározásával nem feltétlenül érthetünk egyet, mivel az kizárólag a szervezeti szinten értelmezi, szűkíti a kockázatértékelést, pedig az lehet akár globális, nemzeti vagy akár egyéni is. Látni kell, hogy a kockázatmenedzsment kialakulása az angolszász területeken költséghatékonysági okokra vezethető vissza.[4] Ez az oka annak, hogy az angol irányelvek fordításával készült szabvány nem tudott a szervezeti megközelítéstől elszakadni, illetve, hogy az ötletgazda országok is elsődlegesen erre értelmezik. Ugyanakkor már hazánkban is kialakult, jogszabályi alapja van a katasztrófavédelmi rendszer részeként tekintett kockázatmenedzsmentnek,[5] vagyis nemzeti szinten is megjelent, igaz, elsődlegesen az elemzés és értékelés tekintetében. Az Európai Unió törekvése is az, hogy a tagállamok kockázatkezelési stratégiákat is alakítsanak ki.[6] Mivel a kockázatmenedzsment olyan folyamat, amelyet az ember az élete

[2] MSZ ISO 31000:2018.
[3] MSZ ISO 31000:2018. 3.2.
[4] Nagy 2013.
[5] 234/2011. (XI. 10.) Kormányrendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtására.
[6] EU 2019/420.

alakulásának folyamán jórészt ösztönösen végez, a ma ismert formalizált eljárások csak ennek a tevékenységnek racionalizált lenyomatai. Elég, ha csak belegondolunk, hogy a gondolkodó ember mindig is mérlegelte, hogy egy adott cselekvésbe belevág-e, vagy sem. Alapvetően ez az ösztönös tevékenység vált tudatossá és szabályozottá, majd terjedt ki az élet különböző területeire. Az egyéni gondolatkör, a lehetőségek latolgatása a maga szorongásaival, reményeivel, optimizmusával és pesszimizmusával, valamint reakcióival már önmagában is egyfajta kockázatmenedzsment, még ha nem is annak nevezzük, vagy nem is tudunk róla, hogy az.

Blaise Pascal (1623–1662) francia matematikus, fizikus, vallásfilozófus és teológus írta le az Isten létére való szerencsejátékos-fogadás elemzését,[7] amely a halála után fennmaradt, de nem publikált írásaival együtt jelent meg az 1670-ben posztumuszként kiadott, *Gondolatok* című műben.

A fogadás lényege Pascal nézőpontjából az, hogy pusztán az értelmünkkel nem juthatunk el Isten létezésének ismeretére. Ezért a legbölcsebb az, ha úgy éljük az életünket, mintha lenne Isten, hiszen az ilyen életvitellel mindent megnyerhetünk, viszont semmit sem veszíthetünk. Ha úgy élünk, mintha lenne Isten, és tényleg van, akkor elnyertük a mennyet. Ha nem létezik, semmit sem vesztettünk. Ha viszont úgy élünk, mintha nem lenne Isten, de mégis létezik, akkor pokol és büntetés lesz az osztályrészünk, és elveszítjük a mennyet és az örömöt. Ha mérlegeljük a lehetőségeket, akkor a racionális döntés nyilván az lenne, hogy úgy élünk, mintha Isten létezne. Ez a gondolatmenet sem volt más, mint egyfajta kockázatmenedzsment, hiszen a bekövetkezési valószínűség (előbb-utóbb mindenki meghal), valamint a várható hatás (mennyország vagy pokol) próbált a döntést segítő elemzést adni.

A *kockázatelemzés* fogalmát illetően a szabvány nem nyújt adekvát meghatározást, ugyanakkor leírja annak célját mint a kockázat jellegének és jellemzőjének megértése, beleértve, ahol ez értelmezhető, a kockázati szint meghatározását is.[8] Az elemzési technika lehet kvantitatív vagy kvalitatív, az előbbi módszernél elegendő mennyiségű információ, ismeret áll rendelkezésre, hogy az elemzést matematikai alapon lehessen végrehajtani, míg az utóbbinál a bekövetkezési valószínűség és a prognosztizált hatás szempontjából egy úgynevezett *fuzzy* logikai mátrix használatával, formalizált logikai döntést hozunk a kimenetel szempontjából. Minden kockázatmenedzsment az elemzés időszakában van leginkább kitéve a szubjektivizmus hatásainak, ahogy ezt a későbbiekben látni fogjuk.

Kockázatértékelés: a szabvány szerint a kockázatértékelés célja a döntések támogatása, magában foglalja a kockázatelemzés eredményeinek az előzetesen meghatározott kockázati kritériumokkal való összehasonlítását. Ezután négyfajta döntés születhet:[9]

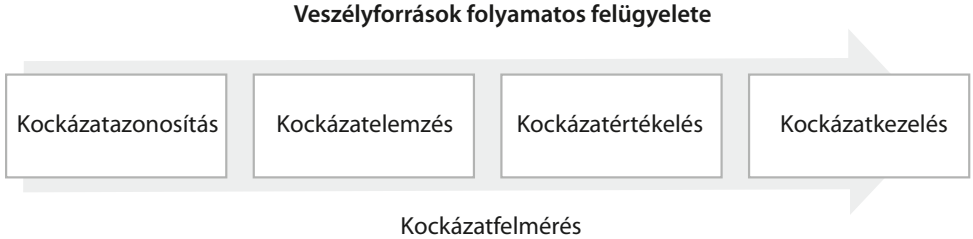
1. nincs szükség további intézkedésre;
2. a kockázatkezelési lehetőségek vizsgálata;
3. a további elemzés a kockázat jobb megértése céljából;
4. a meglévő felügyelet (monitoring) tovább folytatása;
5. a célok újragondolása.

[7] Pascal 1670.
[8] MSZ ISO 31000: 2018 6.4.3.
[9] MSZ ISO 31000:2018. 6.4.4.

A *kockázatkezelés* célja a szabvány értelmezésében, hogy a rendelkezésre álló lehetőségek közül választva a kockázatot mérsékelhessük. A szabvány rögzíti ezért a lehetőségeket is:[10]

1. a kockázat elkerülése;
2. a kockázat vállalása;
3. a kockázati forrás eltávolítása;
4. a bekövetkezési valószínűség megváltoztatása;
5. a következmények megváltoztatása;
6. a kockázat megosztása;
7. a kockázat megtartása.

Látható tehát, hogy a különböző kifejezések más-más jelentéstartalmat jelölnek, amelyek egymásra épülve fedik le a kockázatmenedzsment folyamatát, amelyet a fentiek alapján az alábbiak szerint ábrázolhatunk:



1. ábra: A kockázatmenedzsment folyamata
Forrás: a szabvány alapján a szerző szerkesztése

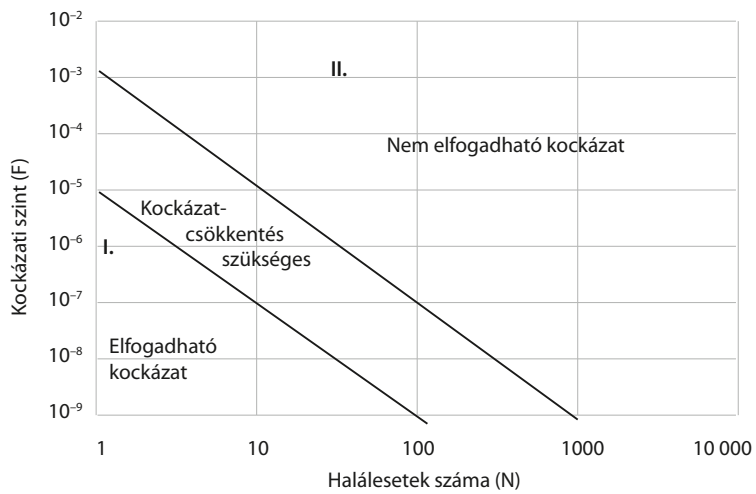
A kockázatmenedzsment strukturált folyamat, amelynek célja a kockázatok azonosítása, elemzése, értékelése, és azoknak a lehető legjobb módokon való kezelése a célok és az értékek védelme érdekében. A terminológiai problémák a szabályozásban számos esetben pontatlansághoz vezethetnek. A települések katasztrófavédelmi osztályba sorolását leíró jogi szabályozás[11] például használja a kockázatbecslés fogalmát, amelyet a kockázatazonosítás, a kockázatelemzés és a kockázatértékelés átfogó folyamataként ír le. Ugyanerre a szabvány a kockázatfelmérést használja. Egy objektivitásra törekvő eljárásban a „becslés" szó használata egyébként sem feltétlenül szerencsés, egyértelműbb lenne a „kockázatfelmérés" kifejezés alkalmazása a szabályozás minden területén.

[10] MSZ ISO 31000:2018. 6.5.2.
[11] 234/2011. (XI. 10.) Korm. rendelet.

Objektivitás kontra szubjektivitás

A magyar nyelv értelmező szótára[12] az *objektív* szóra 4 jelentést is hoz. A kockázatértékelés terén a „személyi szempontokból nem befolyásolt" jelentését lehet értelmezni, vagyis az objektivitás tárgyilagosságot jelent. A szubjektivitás az objektivitással ellentétes fogalmat jelöl, vagyis a személyes szempontból való befolyásoltságra utal. Felvetődik a kérdés, melyek azok a körülmények, amelyek befolyásolhatják tárgyilagosságunkat. Felsorolható lenne számos tényezőcsoport a neveltetéstől a kultúrkörnyezetig, amelyben szocializálódik és fejlődik személyiségünk, de a döntési helyzetekben két elemi hatás meghatározó: az egyik az *érzelem,* a másik pedig az *érdek*. Ezek küzdelme átjárja a mindennapi életünket, vagyis addig, amíg a kockázatértékelést emberek végzik, a teljes objektivitás nehezen érhető el.

Mennyiségi kockázatértékelésnél viszonylag objektív eljárást lehet elérni, viszont mindig van egy döntés, hogy az elfogadható kockázatot hol húzzuk meg.



2. ábra: A társadalmi kockázat elfogadhatósági ábrázolása
Forrás: 219/2011. Korm. rendelet

A 2. ábrán a jelenlegi iparbiztonsági szabályozás[13] szerinti társadalmi kockázat elfogadhatósági ábrázolása látható. A halálozás egyéni kockázatának számítási eredményeit összehasonlítják az engedélyezési kritériumokkal. Elfogadhatónak számít a veszélyeztetés, ha a kockázat a 10^{-6} esemény/évértéket nem éri el; ha 10^{-5} és 10^{-6} között helyezkedik el, a kockázatot különböző kockázatcsökkentő intézkedéssel elfogadhatóvá lehet tenni; ha azonban a kockázat 10^{-5} esemény/év, akkor elfogadhatatlannak számít a veszélyeztetés.[14]

[12] Bárczi–Országh 1962.
[13] 219/2011. Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről.
[14] Ronyecz – Vass – Kátai-Urbán 2015.

Habár a balesetben részt vevő anyagmennyiségeket lehetséges modellező szoftverekkel jól megbecsülni, a kibocsátási időtartamok becslése szubjektív. Azt, hogy hol húzódik a vonal, amely alatt elfogadható egy kockázat, az érzelem és érdek által is orientálható döntés eredménye.

A minőségi kockázatértékelések esetében az objektivitás és szubjektivitás viszonylatában erősebben jelentkezik az érzelmek és érdekek menti szakadás, amely elhomályosíthatja az értékelő tisztánlátását. Az ember hajlamos egy általa kívánt cél elérése érdekében bizonyos kockázatok szintjét alá- vagy felülbecsülni, vagy ha az adott kockázatot megfelelő szinten is látja, akkor az azzal kapcsolatos elfogadhatósági hajlandósága lesz alacsonyabb vagy magasabb az érzelmi vagy érdekalapú befolyásoltsága függvényében.

Nézzük ezt meg egy példán keresztül: hogyan mutatható mindez be a minőségi kockázatértékeléseknél használt *fuzzy* logikai mátrix segítségével. A *fuzzy* mátrixok számos típusa létezik, hiszen a logika lényege, hogy a bekövetkezési valószínűséget a várható hatás tekintetében ábrázolja. A példánkban egy 5 x 5-ös mátrixot használunk a jobb szemléltethetőség érdekében.

		Bekövetkezési valószínűség				
		Nem valószínű	Ritka	Lehetséges	Valószínű	Gyakori
Várható hatás		A	B	C	D	E
Végzetes	I					
Kritikus	II					
Súlyos	III					
Jelentős	IV					
Csekély	V					

3. ábra: Kockázatértékelési mátrix, alapverzió
Forrás: a szerző szerkesztése

A kockázatértékelés eredménye színkódokkal jelölt. Minden veszélyforrás esetében ez a színkód fogja meghatározni, hogy az adott veszélyforrást extrém kockázatúnak (piros), magas kockázatúnak (narancs), átlagos kockázatúnak (citromsárga) vagy alacsony kockázatúnak (zöld) értékeljük.

A bekövetkezési valószínűség statisztikai adatokkal viszonylag jól meghatározható, de azt, hogy a meghatározott statisztikai adatok alapján mit tekintünk gyakorinak, valószínűnek, lehetségesnek, ritkának vagy nem valószínűnek, hacsak nem vagyunk statisztikusok, azt szubjektíven értelmezzük. Ugyanígy szubjektív az is, hogy mit

tekintünk a hatás tekintetében végzetesnek, vagy teszem azt, kritikusnak, súlyosnak, jelentősnek vagy csekélynek.

Az elfogadási hajlandóság szempontjából az összegzett értékelés a példa szerinti négy szintű (négy színkóddal jelölt) kimenetelének változását kell érteni (a piros és narancssárga színkódú kimenetelek drasztikus csökkenése látható).

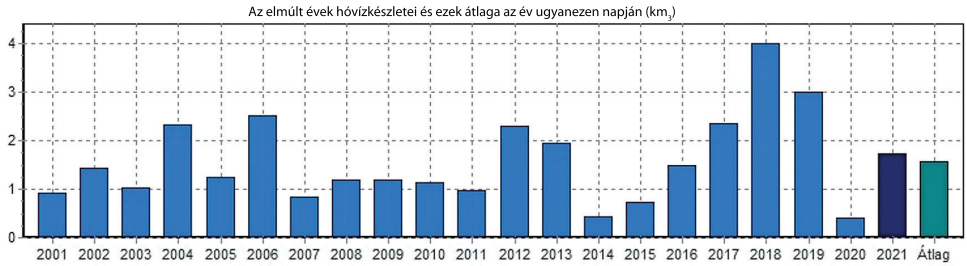
		Bekövetkezési valószínűség				
		Nem valószínű	Ritka	Lehetséges	Valószínű	Gyakori
Várható hatás		A	B	C	D	E
Végzetes	I					
Kritikus	II					
Súlyos	III					
Jelentős	IV					
Csekély	V					

4. ábra: Kockázatértékelési mátrix, magasabb elfogadhatósági hajlandóság
Forrás: a szerző szerkesztése

Egy kívánt cél elérése érdekében az ember hajlamos a racionálisnál magasabb vagy alacsonyabb kockázatot is elfogadhatónak látni. Ugyanígy, ha érdekünkben áll valamit kerülni, annak kockázatát magasabbnak fogjuk becsülni.

A kockázatértékelések terén a szubjektivitás teljes mértékben sosem zárható ki, azonban léteznek olyan rendszabályok, amelyekkel minimalizálhatjuk, csökkenthetjük a szubjektivitás befolyását az értékelési folyamatra. Ilyen lehet a függetlenített kockázatértékelési szervezet alkalmazása, az integritás folyamatos felügyelete, a kockázatértékelést végzők érzelmi és érdekalapú befolyásoltságának ellenőrzése, valamint az elfogadhatósági határok, illetve a hatás és bekövetkezési valószínűségek meghatározására szolgáló irányelvek keretei egységes értelmezésének meghatározása, illetve a Magyar Szabvány kiegészítése és nyilvánosan elérhetővé tétele.

Az érzelmi alapú behatások közé sorolhatjuk be azt a speciális helyzetet is, amikor az értékelést végző saját tapasztalatainak hatása befolyásolja a kockázatértékelés eredményét. Például egy gyakorlatorientált szakember is elvetheti az árvízi kockázat súlyosságát egy katasztrófaosztályba sorolással kapcsolatos kockázatértékelésnél, ha azt látja, hogy évek óta nem volt árvíz, és a hóban lévő vízkészletek mennyisége ezt nem támasztja alá. Csakhogy az árvízi veszélyt nem csupán a vízgyűjtő területeken hóban tárolt vízkészlet mennyisége határozza meg, hanem annak kiolvadási sebessége is, ami viszont a várható hőmérséklettel mutat korrelációt.



5. ábra: A hóban tárolt vízkészletek alakulása a Duna vízgyűjtőjén
Forrás: www.hydroinfo.hu/graf/ho/DunaazInnfelett.jpg

Látható, hogy a nagy dunai árvizekhez (2006. és 2013. évi árvizek) kapcsolódóan a hóban tárolt vízkészletek meg se közelítették a 2018. és 2019. években mért értékeket, utóbbiak mégsem okoztak árvizeket. Ez azért történt, mert a jelzett években nappali enyhe olvadás és esti visszafagyás volt tapasztalható a vízgyűjtőn, illetve egy-két nap 0 °C hőmérséklet feletti időszak után rendszerint pár napos fagypont alatti hőmérséklet következett be, ezáltal a víztömeg szakaszosan olvadt ki az adott területen, így került a Dunába is, nem okozva hirtelen vízszintnövekedést. Hasonló volt ez ahhoz, mint amikor a víztározókat feltöltjük, majd szakaszosan leürítjük.

Profitorientált és nonprofit kockázatértékelések

F. H. Knight, amikor PhD-értekezésére alapozva megírta *Risk, Uncertainty and Profit*[15] című művét 1921-ben, talán maga se gondolta, hogy alig 100 év múlva szerte a világban elterjedt eljárásrend alapjait rakja le. Knight közgazdász volt, így a hivatkozott műve is gazdasági alapú szemléletet tükröz. Egy közgazdasági kockázatértékelés általában nyereségorientált. A pénzügyi kockázatértékeléseknél tehát jól megbecsülhető a veszteség pénzben kifejezett értéke, ami az objektivitást támogatja. Egy nonprofit célzatú kockázatértékelésnél a veszteség értéke széles skálán mozoghat. Ki mondja meg előre például, hogy egy belvízi elöntés milyen közvetlen és járulékos veszteséggel fog járni? Egyfajta kimeneti bizonytalanság mindig létezik, amelynek következtében az értékelés a szubjektivitás irányába mozdul el, hiszen alul- vagy felülértékelhetjük a várható hatást, megváltoztatva ezzel az értékelés kimenetelét.

Ugyanakkor a nonprofit kockázatértékelések valódi értéke elsődlegesen nem a kimeneteli eredményhez kötődik, hanem magához az értékelési folyamathoz. Egy *fuzzy* logikai mátrixot használó minőségi értékelésnél elsődlegesen nem a kimenetel számít, hanem maga az út, amelyet az eredményért bejárunk, nevezetesen, hogy valamennyi létező veszélyforrást, az ISO szabvány szerinti elnevezés szerinti kockázatforrást számításba vegyünk, ezáltal teljes képünk legyen az összes lehetséges kockázatpotenciálról. Természetesen az sem másodlagos, hogy az értékelés kapcsán azok egymáshoz való viszonya is kimutatható legyen.

[15] Knight 1964.

A nonprofit értékelések során gyakran nagyobb hangsúlyt kap az érintettek véleménye, a közösségi igények és a társadalmi hasznosság figyelembevétele. Ezért az ilyen kockázatelemzési folyamatok több szempontból is szubjektív elemekkel gazdagodhatnak, például a szakértők személyes tapasztalatainak, kulturális különbségeknek és a közösségi prioritásoknak köszönhetően. Az objektivitás fenntartása érdekében fontos, hogy az elemzés átlátható maradjon, és különböző nézőpontokat vonjon be, hogy az eredmények sokoldalúak és megalapozottak legyenek.

Végső soron a nonprofit kockázatértékelés folyamata segít a döntéshozóknak az erőforrások hatékony elosztásában, és támogatja a közösségek biztonságának és jólétének előmozdítását. Ez a megközelítés lehetővé teszi a rugalmas, adaptív stratégiák kialakítását, amelyek jobban illeszkednek a változó környezethez és a váratlan kihívásokhoz.

Veszélyforrás kontra kockázatforrás

A szabvány a kockázatforrást olyan elemnek írja le, amely önmagában vagy kombinálva kockázat bekövetkezését idézheti elő.

A magyar nyelv értelmező szótára[16] a veszélyt olyan helyzetnek, állapotnak vagy lehetőségnek írja le, amely kárral, bajjal, romlással vagy elveszéssel fenyeget valakit vagy valamit. A kockázat nem más, mint a veszély, baj, kár lehetősége.

Ebből adódóan minden kockázatforrás veszélyforrás is, de nem minden veszélyforrás kockázatforrás, míg a szabvány szerinti megközelítésben mindent kockázatforrásnak vesz, ami kockázat bekövetkezését idézheti elő. Itt tetten érhető az angolszász és a magyar nyelvhasználat közötti diszharmónia, amely félreviheti az egységes értelmezést.

Wilhelm von Humboldt (1767–1835) porosz államférfi, korszakalkotó nyelvész és esztéta szerint a nyelvben a nemzeti jelleg, ezen belül a nemzeti gondolkodásmód (a nemzet minden egyes tagjának gondolkodása, szubjektív alkotótevékenysége) testesül meg, s amikor az egyes beszélő az elsajátítás során a nyelvvel mint gondolkodását óhatatlanul kívülről strukturáló, objektív erővel találkozik, a nyelvnek a gondolkodásra való hatása – össznemzeti szinten – visszahatásként érvényesül.[17]

Az emberek különböző értelemben használják a szavakat és kifejezéseket, és a kulturális, társadalmi vagy egyéni különbségek miatt más és más jelentéseket társíthatnak hozzájuk. Ez a nyelvi relativitás elve[18] szerint azt jelenti, hogy a nyelv és a jelentés viszonylagos, és az értelmezésünk a kulturális és szociális kontextusoktól függ.[19]

Ez az eltérő értelmezési mód nemcsak a kommunikációt nehezítheti meg, hanem a gondolkodást is befolyásolhatja. Amikor az emberek eltérően értelmezik ugyanazt a kifejezést vagy fogalmat, könnyen előfordulhatnak félreértések és kommunikációs nehézségek.

Ezenkívül a szubjektivitás, vagyis az egyéni tapasztalatok és nézetek szerepe tovább bonyolítja a helyzetet. Mivel az emberek eltérő élményekkel és perspektívákkal

[16] Bárczi–Országh 1962.
[17] Havas 1997.
[18] Sapir–Whorf-hipotézis.
[19] Benczes–Kövecses 2016.

rendelkeznek, az azonos szavak vagy kifejezések más és más érzelmi és kognitív tartalmat hordozhatnak számukra.

Az ilyen kihívások megértése azonban fontos a kommunikáció és a kultúrák közötti párbeszéd hatékonyabbá tétele érdekében. A nyelvfilozófiai és kommunikációelméleti szempontok segíthetnek jobban megérteni, hogyan épül fel a jelentés, és hogyan értelmezik az emberek a nyelvet a saját környezetükben. Az eltérő nyelvi értelmezés tehát nehezíti a megértést, így szubjektivitást okozhat.

Nem feltétlenül kell tehát egyetértenünk azzal, hogy a nemzetközi standard „kockázatforrás" megnevezést használ, hiszen a veszélyforrások azonosítását objektívan el lehet végezni, míg azt eldönteni, hogy mely veszélyforrás kockázatforrás is, az már szubjektív megítélés eredménye. A veszélyforrások helyett a kockázatforrás-szempontú megközelítés másik hátránya, hogy a veszélyforrások egymással való viszonyát és ráhatását egyszerűbb elemezni, mint a lehetőségek egymásra hatását, ami a szubjektivitás szinte gordiuszi csomóját tárhatja elénk.

Fentiek alapján az objektivitás érdekében a nemzetközi irányelv kockázatforrás-centrikus megközelítése helyett a veszélyforrás-alapú megközelítés alkalmazása a hazai gyakorlati használatban előnyösebb lehetne.

A kockázatkezelés szubjektivitása

A korábbiakban már szó volt a szabványban azonosított kockázatkezelési módszerekről, amely felsorolásból különösen a kockázatvállalás és a kockázat megtartása szorul magyarázatra. Az alapvető különbséget úgy lehet a legérthetőbben megfogalmazni, hogy a kockázat vállalásakor intézkedések készülnek azok mérséklésére, míg a kockázat megtartásakor a várható előny miatt, a szervezet kockázattűrő képessége figyelembevételével nem tesznek intézkedést. A kockázat megosztására a legegyszerűbb példa a biztosítás, amely némileg egybecseng a következmények megváltoztatásával, de eltér abban, hogy nem közvetlenül, hanem közvetetten enyhíti a várható hatást.

Ezt követően a szubjektivitás az alábbi részfolyamatoknál lehet hatással az elemzés végeredményére, így a kockázatkezelésre tekintettel:

1. Kockázatok azonosítása: az érintettek személyes tapasztalatai és megérzései befolyásolhatják, hogy mely kockázatokat azonosítják és tartják fontosnak.
2. Kockázatok értékelése és priorizálása: a kockázatok súlyosságának és valószínűségének értékelése gyakran szubjektív elemzéseken alapul. Különböző személyek eltérően ítélhetik meg ugyanazokat a kockázatokat, attól függően, hogy milyen információik vannak és hogyan értékelik azokat.
3. Kockázattűrés: a szervezetek vagy egyének kockázattűrési szintje szintén szubjektív, és a korábbi tapasztalatokon, a jelenlegi helyzeten, valamint a jövőbeli célokra és stratégiákra vonatkozó elvárásokon alapulhat.
4. Kockázatkezelési stratégiák kiválasztása: a különböző kockázatkezelési lehetőségek közötti választás során a döntéshozók személyes preferenciái és prioritásai szintén szerepet játszhatnak.
5. Kommunikáció és jelentéstétel: a kockázatokról való kommunikáció és jelentéstétel módja is tükrözheti a készítők szubjektív nézeteit és értékeléseit.

A kockázatkezelés során az objektivitás és szubjektivitás egyensúlya meghatározó szerepet játszik az értékelési és döntéshozatali folyamatokban. Mivel a kockázatelemzést emberek végzik, a teljes objektivitás elérése szinte lehetetlen, hiszen a személyes tapasztalatok, érzelmek és a döntéshozók érdekei befolyásolják a folyamatot. Az értékelők eltérő háttérismerete, szakmai tapasztalata és akár kulturális befolyásoltsága mind hozzájárulhatnak a szubjektivitás különböző formáinak megjelenéséhez. Ez különösen igaz akkor, amikor az elemzési folyamat során a döntések nem csupán szigorúan meghatározott adatokon és statisztikai modelleken, hanem értelmezésen, elemzésen és előrejelzéseken alapulnak. A kockázatértékelési folyamat szubjektivitását a döntési helyzetek komplexitása is növelheti, hiszen a beérkező információk és a lehetséges hatások értelmezése, priorizálása és a kapcsolódó döntési folyamatok gyakran személyes véleményekkel és preferenciákkal egészülnek ki.

A szubjektivitás nem feltétlenül negatív; valójában hozzáadhat értéket a kockázatmenedzsment folyamatához azáltal, hogy szélesíti a perspektívákat és elősegíti az adaptív döntéshozatalt. Azonban fontos felismerni és kezelni a szubjektivitásból adódó potenciális torzulásokat, például a konfirmációs torzítást (amikor az emberek csak azokat az információkat keresik, fogadják el vagy azokról emlékeznek meg, amelyek megerősítik előzetes meggyőződéseiket) vagy a túlzott optimizmust. Ezt objektív adatok és analízis, valamint a döntéshozatali folyamatok diverzifikálása és átláthatósága révén lehet elérni.

A kockázatkezelés objektivitása a kockázatfelmérés (kockázat azonosítása, elemzése és értékelése) objektivitásán alapul. Minél objektívabb volt a folyamat, amíg a kockázatkezelési stratégiai meghatározásához eljutottunk, annál objektívabb és hatékonyabb kezelési stratégiát tudunk célul kitűzni. Ezt a munkát azonban a közös terminológia beágyazásával kell megkezdeni, mert az adja meg az egységes alapot a hazai kockázatmenedzsment-eljárások fejlesztéséhez.

Összegzés

A kockázatmenedzsment szubjektivitása összetett problémákat vet fel, mivel bár az objektivitás elérése alapvető cél, a szubjektivitás hatása elkerülhetetlen. A kockázatok azonosítása, értékelése és a stratégiák kiválasztása során az értékelők személyes tapasztalatai és érzelmei befolyásolhatják az eredményeket. Ahogy a cikkben is rámutattam, az érdekalapú hatások és érzelmek torzíthatják az elemzési folyamatokat, ugyanakkor a szubjektivitás megfelelő kezelés mellett hozzájárulhat az adaptív döntéshozatalhoz. Az objektivitás fenntartása érdekében az egységes irányelvek és a függetlenített elemzési struktúrák alkalmazása javasolt, mivel ezek segíthetnek a torzítások minimalizálásában.

Megállapítottam továbbá, hogy a magyar és nemzetközi kockázatmenedzsment terminológiája közötti eltérések nehézségeket okozhatnak az egységes értelmezésben. Az olyan fogalmak, mint a „veszélyforrás" és „kockázatforrás" eltérő értelmezése gátolhatja a hatékony kockázatkezelést. A közös terminológia és az objektivitást támogató módszerek bevezetése hozzájárulhat a hazai kockázatkezelési gyakorlat

fejlődéséhez, amellyel elősegíthetik a megalapozottabb és eredményesebb kockázatkezelési döntéshozatalt.

Felhasznált irodalom

219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

234/2011. (XI. 10.) Kormányrendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtására

Az Európai Parlament és a Tanács 2019/420 határozata

Bárczi Géza – Országh László (1959–1962): *A magyar nyelv értelmező szótára*. Budapest: Akadémiai.

Benczes Réka – Kövecses Zoltán (2016): *Kognitív nyelvészet.* Budapest: Akadémiai. Online: https://doi.org/10.1556/9789630597340

Havas Ferenc (1997): Nyelv és gondolkodás. In *Pannon Enciklopédia. Magyar nyelv és irodalom.* Budapest: Dunakanyar 2000.

Knight, Frank H. (1964): *Risk, Uncertainty and Profit. Reprints Old Economic Classic.* New York: Augustus M. Kelley.

Magyar Szabvány MSZ ISO 31000:2018. Kockázatmenedzsment. Irányelvek (2019).

Nagy Sándor (2013): A hazai lakosságvédelmi kockázatértékelés összehasonlítása a nyugati kockázatelemzési eljárásokkal. *Bolyai Szemle,* 22(1), 159–176. Online: https://real.mtak.hu/19637/1/11.pdf

Pascal, Blaise (1978): *Gondolatok.* Budapest: Gondolat.

Ronyecz Lilla – Vass Gyula – Kátai-Urbán Lajos (2015): Veszélyes üzemi kockázat és következményelemző eszközök alkalmazhatósága. *Bolyai Szemle,* 24(1), 111–123. Online: https://real.mtak.hu/192662/1/2015_I_10_ronyecz_vass_katai-urban.pdf

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 3. szám 213–224.
DOI: 10.32567/hm.2024.3.13

Pozderka Gábor[1]

A Magyar Honvédség kiberképzési rendszerének evolúciója

The Evolution of the Hungarian Defence Forces's Cyber Training System

Absztrakt

A katonai képességek kialakítása során a kibertér mint külön műveleti tér jelenik meg, azonban hatását kifejti minden haderőnem vonatkozásában. A kibervédelmi és kiberműveleti oktatási tematikák esetében ezen keresztfunkció megjelenése elengedhetetlen az összhaderőnemi gondolkodás és művelettervezés megteremtése érdekében. Az elmúlt években a Magyar Honvédség működésében is egyre hangsúlyosabb szerepet kaptak az infokommunikációs szolgáltatások, valamint az ezek védelmét biztosító elektronikus információvédelmi, ebből továbbfejlődve kibervédelmi képességek és a felhasználói tudatosság növelésére irányuló képzések, gyakorlatok. A Magyar Honvédség 2019-ben megalakította a Kiberakadémiát, amely platformot biztosít ezen feladatok végrehajtására mind az ügyintézői, mind a vezetői, mind az üzemeltető állomány részére. A kialakított oktatási tematikát a felmerült igények figyelembevételével rendszeresen aktualizálják, az oktatói állomány folyamatosan nyomon követi a kiberbiztonsági trendek alakulását.

Kulcsszavak: kiber, kiberakadémia, tudatosítás, oktatás, kiképzés

Abstract

During the development of military capabilities, cyberspace appears as a separate domain of war, however, it impacts all other domains. In the case of cyber defence and cyber operations education topics, the emergence of this cross-function (between domains) is

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: pozderka.gabor@hm.gov.hu

essential to joint military thinking and operations planning. In recent years, communications and information systems (CIS) as well as CIS protection services have played an increasingly prominent role in Hungarian Defence Forces operations, further developing cyber defence capabilities, training and exercises aimed at raising user awareness. In 2019, the Hungarian Defence Forces established the Military Cyber Academy, which provides an appropriate platform for the implementation of these tasks for the administrator, management and operating staff. Cyber education topics are regularly updated considering emerging needs and the teaching staff continuously monitors (ever-evolving) cybersecurity trends.

Keywords: cyber, cyber academy, awareness, education, training

Bevezetés

A NATO 2016-os varsói csúcstalálkozóján az országok vezetői egyetértettek abban, hogy a kibertér önálló hadszíntér *(domain),* és a védelme részét képezi a NATO kollektív védelmi feladatainak, és ebben a tekintetben a Szövetségnek ugyanúgy képesnek kell lennie megvédeni a tagállamokat, mint a hagyományos hadszíntereken vívott harcok során.[2]

Magyarország Kormánya és a Magyar Honvédség vezetése érzékelve és megértve az új hadszíntérben rejlő veszélyeket, kihívásokat és lehetőségeket, 2019-ben elrendelte a Kibervédelmi Haderőnemi Szemlélőség (KIBSZ) mint stratégiai szintű vezetési és képességfejlesztési szervezeti elem megalakítását. 2022-ben a KIBSZ feladatrendszere kiegészült a nem kinetikus képességi elemekkel, ennek eredményeként megalakult az MH Kiberműveleti Parancsnokság (KIBP). A KIBSZ a kezdeti képességfelmérést követően, az azonosított hiányosságok mihamarabbi felszámolása érdekében javasolta és kezdeményezte a honvédelmi miniszter részére olyan kibervédelmi képző- és oktatóhely létrehozását, amely a kiberbiztonság, a kibervédelem, valamint az elektronikus információbiztonsági és az elektronikus eseménykezelő beosztásokban feladatot ellátók képzését és továbbképzését biztosítani képes a Magyar Honvédség számára. Ezen javaslat eredményeként a Magyar Honvédség 2019-ben megalakította Szentendre székhellyel a Kiber Képzési Központot, ismertebb nevén a Kiberakadémiát.[3] A Kiberakadémia megalakulásával a Magyar Honvédség képességkatalógusa egy szervezetszerű képzéseket nyújtani képes, korszerű infrastruktúrával rendelkező, az MH egész állományát kiszolgálni hivatott képzőhellyel bővült, amely megfelelő alapot teremtett a kibervédelmi és kiberműveleti képességek kialakításához szükséges képzések folyamatos nyomon követéséhez, továbbfejlesztéséhez. Már a kezdeti célok között szerepelt a honvédtiszti, valamint honvédaltiszti képzésben részt vevők általános, illetve a speciálisan kibervédelmi beosztásokba tervezett állomány tanfolyami rendszerű, illetve képzési tervükbe illesztett felkészítése.

Az oktatási portfolió evolúciójának vizsgálata logikai kapcsolatot teremt a képességfejlesztési célok megvalósulása és kiberműveleti feladatok végrehajtása között. Célom olyan képzési javaslatcsomag megfogalmazása, amely az evolúció következő

[2] NATO 2016.
[3] Draveczki-Ury 2019.

szakaszában elősegíti majd ezen folyamatok sikerességét. A kitűzött cél eléréséhez a korábban kialakított oktatási tematika többütemű vizsgálatán keresztül kívánok eljutni, megértve annak logikáját a továbblépéshez szükséges javaslatok megfogalmazásával. Hipotézisem szerint a Magyar Honvédség feladatrendszeréhez kapcsolódó kiberszakterületi képzéseket a kibervédelmi és kiberműveleti feladatok végrehajtásának érdekében, az arra történő felkészülés jegyében alakították ki, összhangban az érvényben lévő jogszabályi hátérrel, felhasználva a civil szektor tapasztalatait. A hipotézisnek való megfelelést az alábbi feltételek teljesülésén keresztül kívánom vizsgálni és igazolni, valamint szükség esetén kiegészítő javaslatokat megfogalmazni:

- Tudatosság növelése: a kibervédelmi oktatások célja, hogy növeljék a felhasználók tudatosságát a kiberfenyegetésekkel szemben.
- Gyakorlati ismeretek: az elméleti tudás mellett fontos, hogy a résztvevők gyakorlati tapasztalatokat is szerezzenek.
- Biztonsági protokollok: a képzések során bemutatják a legjobb biztonsági protokollokat és gyakorlatokat.
- Rendszeres frissítés: a kibervédelmi oktatásoknak folyamatosan frissülniük kell az új fenyegetések és technológiák ismeretében.
- Szabályozási ismeretek: fontos, hogy a résztvevők tisztában legyenek a vonatkozó jogszabályokkal és szabályozásokkal.

Az evolúció kezdeti szakasza

A Magyar Honvédség feladatrendszere törvényi szinten szabályozott, amelyben a kor követelményeinek megfelelően értelemszerűen megjelennek a kibervédelmi és kiberműveleti hadszintérrel kapcsolatos feladatok is.[4] Magyarország Nemzeti Katonai Stratégiája szintén megerősíti ezen feladatok szükségességét, kiemeli, hogy a kiberfenyegetésnek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát és adott esetben módosítását, a kiberhadviselés anyagi kár okozásában és a közrend megzavarásában potenciálját tekintve egyre kevésbé marad el a hagyományos fegyverektől.[5] Ez a hatás folyamatosan gyorsuló tendenciát mutat a kibertér sajátosságából adódóan, az adott eseményekre adható válaszidők pedig folyamatosan rövidülnek, a siker érdekében olyan kidolgozott eljárásrendekkel kell rendelkezni a vezető és üzemeltető állománynak is, amelyet készségszinten már a felkészülési időszakban elsajátítanak.

Mivel az oktatás és képzés minden esetben hosszú távú „befektetés", az oktatás megkezdése előtt az oktatói állományt kellett kiválasztani, akik megfelelő szakmai háttér birtokában, a szükséges kiegészítő felkészítéseket követően alkalmasnak bizonyultak a speciális képzési tematika kialakítására, a tanfolyami rendszer elindítására. A Kiberakadémia működésének kezdeti fázisában az első körös tanfolyamok tematikájának részleteit alakítottuk ki, figyelembe véve a nemzeti és nemzetközi trendeket,[6]

[4] 2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről.
[5] A Kormány 1393/2021 (VI. 24.) határozata Magyarország Nemzeti Katonai Stratégiájáról.
[6] *Cybersecurity Education… 2022.*

valamint a Magyar Honvédség működéséből adódó sajátosságokat. A tervezés során egyértelművé vált, hogy azon eljárások, amelyek egy civil környezetben működőképesek, nem minden esetben elégítik ki a sajátos feladatrendszerből adódó igényeket, azok biztosítására elkülönült eljárásrendet kell kidolgozni és alkalmazni.

A hiteles, teljes spektrumot átölelő és széles körű oktatási tematika kialakításának céljából, a Magyar Honvédség által üzemeltetett hálózaton és hálózati elemeken azonosított biztonsági események összegzése és megfelelő kiértékelése érdekében a Kiberakadémia oktatói állománya mellett a tervezésbe már a kezdeti szakaszban bekapcsolódtak az MH Elektronikus Eseménykezelő Főközpont (EEFK) szakemberei, akik a hálózatvédelem szempontjából nélkülözhetetlen feladatukat a nap 24 órájában látják el. Ennek a sikeres együttműködésnek folytatásaként 2022-ben megalakult az MH Kiber- és Információs Műveleti Központ (KIMK), amely már egységes képességként integrálta a korábban külön szervezeteknél kialakított információs műveleti elemeket (Kiber Képzési Központ, EEFK, Civil-Katonai Együttműködési és Lélektani Műveleti Központ).

Figyelembe véve és priorizálva a rendelkezésre álló erőforrásokat és igényeket, kezdeti képességként az alábbi képzési portfólió alakult ki:

- Kiberbiztonsági tudatosság tanfolyam (Cyber Security Awareness Course): 1 hét
  - Tartalom: a mindennapi munkavégzés során jelentkező kiberbiztonsági kihívások és a védelem komplex ismeretei.
  - Célközönség: MH teljes állománya.
- Kiberbiztonság – katonai döntéshozók számára tanfolyam (Cyber Security for Military Decision Makers): 2 nap
  - Tartalom: általános kiberbiztonsággal kapcsolatos ismeretek átadása, amely tartalmazza a kibertér meghatározását, a kibertéri kihívásokat, a kibertér védelmével kapcsolatos tervezési eljárások ismereteit.
  - Célközönség: katonai/honvédelmi alkalmazott közép- és felső vezetők.
- Kiberbiztonsági szervezés tanfolyam (Cyber Management Course): 3 hónap
  - Tartalom: magasabb szintű kiberbiztonsági stratégiai, technikai és szervezési ismeretek a kiberbiztonság és az információbiztonság területeken.
  - Célközönség: a kiberbiztonság, az információbiztonság és az elektronikus információbiztonság területén középvezetői feladatokat ellátók.
- Kiberbiztonsági üzemeltetés tanfolyam (Advanced Operators Course): 3,5 hónap
  - Tartalom: magasabb szintű kiberbiztonsági szervezői és tervezői ismeretek átadása, amely kiegészül a CISSP (Certified Information Systems Security Professional, azaz minősített információs rendszer biztonsági szakértő) képzéssel.
  - Célközönség: informatikai üzemeltetésben dolgozó szakemberek.
- Digitális helyszínelő és eseménykezelő tanfolyam (Advanced Analyst Course): 6 hónap
  - Tartalom: kiberbiztonsági incidensek kivizsgálásának technikai ismeretei.
  - Célközönség: informatikai üzemeltetésben és incidenskezelésben dolgozó szakemberek.

A portfolió kialakításakor fontos szempont volt a hatékonyság mellett, hogy melyek lehetnek azok a képzések, amelyek már a kezdeti fázisban megvalósíthatók saját erőforrásokból, és melyek azok, amelyek nemzetközi vagy szövetségesi képzéseken megszerzett tapasztalatokból integrálhatók sikeresen az elkövetkező években a fokozatosság elvét követve. A hatékony jövőbeni feladat-végrehajtás érdekében a KIBSZ állandó szakértőt delegált a tallinni székhelyű Cooperative Cyber Defence Centre of Excellence kutatási és képzési központba (CCD COE), így az ott kialakított új megoldásokat már párhuzamosan alkalmazták a Kiberakadémia portfóliójában is, ennek egyik látványos példája a katonai döntéshozók felkészítése a *kiberdomain* vonatkozásában. A NATO és EU oktatási intézményei is folyamatosan fejlesztik saját specifikált képzéseiket, ennek részeként megjelentek többek között a kiberműveleti tervezői, kommunikációs és jogi szakértői állomány felkészítésére szolgáló tanfolyamok. A kiber- és elektronikus információvédelmi szakterület vonatkozásában meghatározónak tekinthető az NCI Academy Oeiras, valamint a NATO School Oberammergau képzési rendszere, a képességfejlesztés érdekében ezek a tanfolyamok *train-the-trainer* rendszerben működtek. A NATO oktatási rendszerébe visszacsatolásként kerültek a Kiberakadémia oktatói állományának tapasztalatai is a kölcsönös információmegosztás részeként. Nemzetközi téren fontos elemét képezik a képzési tematika kialakításának a hardver- és szoftvergyártó cégek specifikált kurzusai, ennek a tudásnak a bevonzása kezdetben vendégelőadókon keresztül valósult meg, később részben integrálódtak a tanfolyamokba.

A kezdeti szakaszban a képzések elindításával párhuzamosan, a KIBSZ végrehajtotta azon nemzetközi gyakorlatok feltérképezését, amelyek a Magyar Honvédség feladatrendszeréhez kapcsolódóan (beleértve nemcsak a saját hálózatok védelmét, hanem az országvédelmi feladatokat is) valós képességnövekedést eredményezhettek, amelyek tapasztalatai hatékonyan felhasználhatók voltak a hasonló jellegű nemzeti gyakorlatok és képzések kialakítása során. Az MH szervezeti elemei már korábban is részt vettek szakterületi gyakorlatokon, amelyek közül a kiberterület vonatkozásában kiemelkedtek a Cyber Coalition,[7] Locked Shield[8] és CMX[9] gyakorlatok, ezeket beillesztették a kiberszakterület stratégiai tervezési folyamatába. Ebben az időszakban kijelenthető volt a fenti gyakorlatok esetében, hogy bár azok hasonló területhez kapcsolódtak, a végrehajtás során megjelenő feladatok fókuszterületei eltértek egymástól, míg az LS alapvetően a technikai megoldásokra, addig a CC inkább a folyamatokra fókuszált, a CMX pedig egy komplex krízismenedzsmentet modellezni hivatott gyakorlatként jelent meg. A gyakorlatok profilja az évek során kiegészült, átalakult, ma már inkább az intenzitás, kompetitivitás és az együttműködési feladatrendszer mélysége, ami megkülönbözteti őket.

[7] Cyber Coalition – a NATO egyik legnagyobb és legösszetettebb kibervédelmi gyakorlata.
[8] Locked Shields – a NATO Cooperative Cyber Defence Centre of Excellence által rendezett kibervédelmi gyakorlat.
[9] Crisis Management Exercise – a NATO válságkezelési gyakorlata.

Az evolúció jelenlegi szakasza

A tanfolyami tematika hatékonyságának vizsgálatára a KIBSZ és Kiberakadémia szakállománya olyan eljárásrendet dolgozott ki, amely egyszerre biztosítja a tanfolyamok finomhangolását, valamint az újonnan meghatározott követelmények képzésekbe történő beépítését. A 2020–2024 közötti időszakban az alábbi főbb tényezők azok, amelyek jelentős befolyást gyakoroltak a képzések tematikájának átalakítására:

A Kiberbiztonsági tudatosság tanfolyamok esetében kiemelt feladat azok felkészítése, akik jelentős mértékben találkoznak érzékeny adatokkal, vagy munkakörükből adódóan nagy és koncentrált adatmennyiséggel dolgoznak. A felkészítési sorrend priorizálásánál kiemelt figyelmet kapott az ügyviteli pontok üzemeltetéséért felelős, valamint a szervezetek és felső vezetők adminisztratív állománya. Feladatrendszerükből adódóan hosszabb időre kiszakítani őket a napi munkavégzésből igen körülményes, így esetükben egyedi tematika kidolgozása vált szükségessé.

Tartós nemzetközi beosztásokat megelőzően a beosztás függvényében szükségessé válhat az adott helyőrségben, szervezetnél alkalmazott eljárásrendek kibervédelemmel kapcsolatos kiegészítése, aktualizálása oktatás keretében. Egyes speciális célcsoportok számára a jövőbeni feladatrendszerük miatt speciális célképzések szükségesek.

A nemzeti és nemzetközi kiber- és hibrid gyakorlatokra történő felkészüléshez a Kiberakadémia megfelelő platformot képes biztosítani mind elméleti, mind technikai vonatkozású feladatok esetén. Az információs műveletek különböző elemei nem függetleníthetők egymástól,[10] azok folyamatos hatást gyakorolnak egymásra, ahogyan az a KIMK megalakulásakor is alapvetés volt.

A képzéseknek minden esetben az aktuális információkat kell tartalmazni, ennek érdekében az oktatói állomány folyamatos továbbképzése, civil környezetben történő felkészítése is szükséges. Az erőforrás-menedzsment szempontjából számolni kell azzal a ténnyel, hogy nem minden erőforrás használható azonos időintervallumban.

Az online képzések kialakítása erősíti az információbiztonságot, ezzel a módszerrel gyorsabban és nagyobb tömegek megszólíthatók egy időben, azonban a személyes képzések, konzultációk hatékonysága túlmutat ezeken a képzéseken. A képzések megindítását megelőzően minden esetben ki kell alakítani a szükséges technikai hátteret, létre kell hozni a kiértékeléshez szükséges platformot, és minden esetben megfelelően kell méretezni a rendszer keresztmetszetét.

A mélyebb technikai tudást igénylő tanfolyamok esetében fontos a szükséges bemeneteli feltételek megléte, ennek érdekében egymásra épülő tanfolyamok kialakítása.

Figyelembe véve a fent megfogalmazott és csoportosított igényeket, a korábbi portfóliót az alábbi képzésekkel kell kiegészíteni:

- Kiberbiztonsági tudatosság tanfolyam (Cyber Security Awareness Course): 2 nap
  - Tartalom: a mindennapi munkavégzés során jelentkező kiberbiztonsági kihívások és a védelem komplex ismeretei, kiemelt figyelemmel a szervezet feladatrendszerére.
  - Célközönség: szervezetek és felső vezetők adminisztratív-ügyviteli állománya.

[10] Kovács 2023.

- Kiberbiztonsági tudatosság zászlósállomány számára tanfolyam (Cyber Security Awareness): Modulelem
  - Tartalom: a mindennapi munkavégzés során jelentkező kiberbiztonsági kihívások és a védelem komplex ismeretei.
  - Célközönség: zászlós, tanfolyamon részt vevő állomány.
- Kiberbiztonsági tudatosság ÖVAT-[11] állomány számára tanfolyam (Cyber Security Awareness): Modulelem
  - Tartalom: a mindennapi munkavégzés során jelentkező kiberbiztonsági kihívások és a védelem komplex ismeretei altiszti vezető feladatok viszonylatában.
  - Célközönség: ÖVAT tanfolyamon részt vevő állomány.
- Biztonsági tesztelő tanfolyam (Etikus hacker/Ethical Hacker Course): 10 nap
  - Tartalom: a mindennapi munkavégzés során jelentkező kiberbiztonsági kihívások és a védelem komplex ismeretei, tesztelői alapok megszerzése.
  - Célközönség: kibervédelmi beosztásban és incidenskezelésben dolgozó szakemberek.
- Python programozás alapjai tanfolyam: 10 nap
  - Tartalom: programozás alapjainak ismertetése.
  - Célközönség: kibervédelmi beosztásban és incidenskezelésben dolgozó szakemberek.
- Kiberművelet-tervezői képzés (Cyber Operational Planer Training): Online
  - Tartalom: kiberművelet-tervezés alapjai.
  - Célközönség: műveletttervező állomány.
- Forgatókönyvszerű kiképzések (szituációs felkészítések, technikai gyakorlatok):
  - Cyber Range alkalmazása;
  - felkészülés nemzetközi gyakorlatokra (Locked Shields, Cyber Coalition, CMX, MIC);
  - nemzeti és saját szervezésű gyakorlatok (Digitális Csapás, Adaptive Hussars);
  - Kiberműveleti Parancsnokság és KIMK állományának felkészítése, megszerzett tudás szinten tartása;
  - nemzetközi beosztásokat megelőző felkészítések.

Jövőbeni igények és lehetőségek

A Kiberakadémia megalakulásától 5 év telt el, amely elégséges időintervallum ahhoz, hogy értékelni tudjuk az eddig végrehajtott feladatokat, és azonosítani tudjuk a jövőbenieket. Fontos megjegyezni, hogy a kibertérben, így a kiberműveletekben, valamint az azokat végrehajtó állomány tevékenységének esetében is az elsődleges tényező az időfaktor. A 21. század biztonsági kihívásai között első helyen szerepel a hibrid tevékenységekkel és műveletekkel szembeni fellépés, amelynek elemei között megtalálhatók többek között a kibertérben vagy azon keresztül megvalósított információs

[11] Az Acélkocka Altisztképzési Rendszer legmagasabb szintű tanfolyama – Összhaderőnemi Vezető Altiszti Tanfolyam (ÖVAT).

műveletek. A nem katonai környezetben sikeresen alkalmazott technikai eljárások nem minden esetben elégítik ki maradéktalanul a speciális katonai igényeket, azokat megfelelően kialakított katonai biztonsági környezetben a kiberműveleti tervező állomány részére speciális tematika alapján szükséges oktatni. A kiberhaderőnem, ahogyan a fenti összegzésből is tisztán látszik, nem csak technikai szakemberekre épül, a feladatok végrehajtása során bekapcsolódnak a műveleti tervező, kommunikációs, jogi és más szakterületek képviselői is, értelemszerűen ezen feladatoknak az oktatásban is meg kell jelenniük.[12]

A kibertér a számítógépes eszközök világméretű információcsere-hálózatával kapcsolódik össze. A digitális forradalom és az adatfeldolgozó eszközök fejlődése kétségkívül megváltoztatta életmódunkat, a korábban különálló eszközök rendszerbe integrálása fokozatosan történt, ma már a rendszerek más rendszerekkel történő folyamatos adatcsere-lehetőségének megteremtése alapkövetelmény. A dolgok internete (*internet of things,* IoT)[13] lényegében olyan különböző, egyértelműen azonosítható elektronikai eszközöket jelent, amelyek képesek felismerni valamilyen lényegi információt, és azt egy internetalapú hálózaton egy másik eszközzel kommunikálni. A fogalom más szavakkal hálózatba kötött „intelligens" eszközöket takar, amelyek a beépített érzékelőknek és szenzoroknak köszönhetően képesek adatokat gyűjteni. Ez a technológia és az 5G gyorsuló ütemben fejlődik, illetve terjed. A mesterséges intelligencia *(Artificial Intelligence)* jelenleg kiszámíthatatlan fejlődése szintén új távlatokat nyit meg és egyszerre veszélyeket is jelent a szakterületek számára, ennek az oktatásban is meg kell jelennie.[14]

A fegyverrendszerek teljes mértében nem függetleníthetők a fenti folyamatoktól, bár a hardver- és szoftvereszközök specifikáltak, azok alap kommunikációs folyamatai nem térnek el jelentősen. A rendszereket kezelő állomány kibervédelmi felkészítését kiemelt figyelemmel kell végrehajtani, az oktatási tematikák folyamatos felülvizsgálata elengedhetetlen. A komplex gyakorlatok megfelelő platformot teremtenek a kritikusinfrastruktúra-védelmi képességek védelméhez szükséges folyamatok begyakorlásához, a honvédelmi és más ágazatok együttműködésének modellezéséhez. A feladatok sikeres végrehajtása érdekében a kapcsolati és együttműködési rendszer kialakításának már korábban meg kell történnie mind a képzések, mind valós időben történő feladat-végrehajtás érdekében.[15]

Mivel a kibertérben végrehajtott feladatok részben más logikai felépítést követnek, mint a fizikai tér műveleti feladatai,[16] ezért azok megjelenése a katonai oktatási tematikákban kiemelt fontosságú, ennek érdekében a KIBP szoros kapcsolati rendszert alakított ki a Nemzeti Közszolgálati Egyetemmel, az Óbudai Egyetemmel és más oktatási intézményekkel. A szövetségi rendszerekben (NATO, EU, V4, bilaterális) végrehajtott feladatok érdekében rendkívül fontos a nemzetközi kapcsolati rendszer

[12] CCD COE 2017.
[13] *Internet of Things* [é. n.].
[14] Németh–Virágh 2022.
[15] NATO 2020.
[16] Clapson 2023.

kiépítése[17] és folyamatos aktualizálása, ennek megvalósításához kiváló platformot biztosítanak a nemzetközi gyakorlatok és konferenciák.

A Covid–19 a kiberszakterület vonatkozásában is sok változást hozott, a személyes érintkezések számának csökkenésével exponenciálisan nőt a kibertérben történő kapcsolatfelvételek száma, így az alkalmazott rendszerek kitettsége is. Bár a honvédségi rendszerek túlnyomó többségben zártak, az otthonról dolgozás lehetősége ebben a szektorban is megjelent. Ennek a változásnak is betudható, hogy a kibertámadások számában drámai növekedés mutatkozott ezen időszakban, jellemzően a támadók e-mailes adathalászati módszerekre és az ellátási láncot érintő támadásokra helyezték a hangsúlyt. Az oktatási tematikák kialakítása során ezen tapasztalatok felhasználása elengedhetetlen, folyamatos továbbfejlesztésük szükséges.[18]

Figyelembe véve a nemzeti-nemzetközi trendeket és felmerült igényeket, a jelenlegi portfóliót tervezetten az alábbi irányokkal szükséges kiegészíteni (folyamatos utánkövetéssel):

- Online képzési katalógus bővítése, hatékonyságának vizsgálata: folyamatos feladat, amely jelentősen elősegíti a felhasználói tudatosság erősítését a részt vevő állomány létszámának növelésével. A folyamatnak szerves részét kell hogy képezze a visszacsatolások kiértékelése, ellenkező esetben a színvonal szinten tartása nem garantálható.
- Lehetőség biztosítása a részvételre más közigazgatási szervezetek számára a kiberbiztonsági képzéseken: a megszerzett tapasztalatok átadása más közigazgatási szervezetek részére – figyelembe véve az erőforrások rendelkezésre állását – fontos részét kell hogy képezze az egységes országvédelem és az együttműködési rendszer kialakításának. Természetesen ez a folyamat, ahogyan a NATO esetében is láttuk, nem szükségszerűen egyirányú, a más szervezetek által kialakított képzések modulelemként, vendégoktatókon keresztül is megvalósulhatnak.
- Mobil oktatási képességek erősítése, műveleti területen történő képzések technikai hátterének megteremtése: amennyiben csak a jelenlegi oktatási képességekre és infrastrukturális lehetőségekre összpontosítunk, elveszítjük a fejlődés lehetőségét, ütemét és dinamikáját. Olyan megoldásokban szükséges gondolkozni, amelyek biztosítják a mobilitást az oktatói állomány részére, így gyorsabban, nagyobb létszámú felhasználó felkészítése válik lehetségessé, akár műveleti területen is. Fontos a haderőnemek közötti együttműködés az igények meghatározásakor.
- Felhőszolgáltatások és mobilalkalmazások használatának vizsgálata: összhangban a vezető nemzetközi trendekkel a jövőbeni feladat-végrehajtás hatékonyságnövelése érdekében fókuszpontban kell szerepelni ezen alkalmazások használati lehetőségeinek, így erősítve a katonai és nem katonai szolgáltatások közötti interoperabilitás megvalósulását.

[17] Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

[18] Magas 2022.

- Nemzetközi kiajánlású (ki)képzések (NATO, EU, V4, bilaterális): Magyarország és a Magyar Honvédség nemzetközi pozíciójának, reputációjának, tapasztalatszerzésének, feladat-végrehajtásának erősítése érdekében a nemzetközi képzések kialakítása kiemelt célként kezelendő mind rövid, mind hosszú távon.
- Nemzetközi kibergyakorlatok helyszínének biztosítása (NATO, EU, V4, bilaterális): a kibertér jellegéből adódóan a nemzeti és nemzetközi szolgáltatások és az azokat biztosító infrastruktúra nem minden esteben szegmentálható teljes mértékben, ennek megfelelően a felkészüléseknek, gyakorlatoknak is ezt a logikát kell követniük. A sikeres gyakorlati feladat-végrehajtás egyik alapfeltétele a szükséges platformok kialakítása, ezek a valós műveleti feladatok során is kiemelt szerepet fognak kapni.
- A kiberfizikai rendszerekre való hatásainak vizsgálata: a valós folyamatok oktatása, üzemeltetett rendszerek sérülékenységeinek felderítése (fegyverrendszerek, vezérlőszoftverek, irányítás)[19] olyan kiemelt feladat, amely elemi részét kell hogy képezze a katonai kibertérműveleti erők felkészítésének.
- Más nem kinetikus képzések erősítése, egységes rendszerbe integrálása: az információs műveleti elemek egymásra kifejtett hatásai nagymértékben befolyásolják a kibertérben a feladat-végrehajtás hatékonyságát, a korábban kialakított, nem kinetikus tematikák és képzések (PSYOPS, CIMIC) hangsúlyosabb megjelenése a Kiberakadémia portfóliójában erősítik és gyorsítják a valós műveleti feladatvégrehajtást.
- StratCom-[20] együttműködés erősítése: a gyakorlatokra és valós műveleti feladat-végrehajtásra történő felkészülés érdekében, az információs műveletek teljes életciklusának modellezésében és a hatások elemzésében, szükséges az információs műveleti platform elemei hatékony együttműködésének megteremtése. Ezen modellek kialakításához a Kiberakadémia ideális helyszínt képes biztosítani.

Összegzés

Megállapítható, hogy a Magyar Honvédség megfelelő ütemben alakította ki hiánypótló kiberoktatási központját, ez a szervezeti elem kiváló alapot teremtett a kibervédelmi és információbiztonsági képzések megkezdéséhez.[21] A szervezet és szakterület jelenlegi fejlődési állapota garantálja a továbblépést és a folyamatos fejlődést.

A bevezetésben megfogalmazott hipotézis valósnak bizonyult, a meghatározott feltételek alapján az oktatási tematikák megfelelők, felülvizsgálatuk folyamatosan megtörténik. A jövőbeni képességeket az alábbi irányok figyelembevételével javasolt kialakítani:

[19] Kovács 2021.
[20] Stratégiai kommunikáció: a StratCom kifejezés a stratégiai kommunikációval kapcsolatos tevékenységeket takarja. Magában foglalja a kommunikációs tervek kidolgozását, az üzenetek célzott terjesztését és a hatékony kommunikációs stratégiák kidolgozását.
[21] Országgyűlés Hivatala 2019.

- Kockázatelemzés: a képzések során a kockázatelemzés módszertanát is bemutatják, hogy a résztvevők képesek legyenek azonosítani és kezelni a kockázatokat.
- Interaktív tanulás: az interaktív előadások és szimulációk hatékonyabbá teszik a tanulási folyamatot.
- Kritikus ágazatok védelme: kiemelten fontos a kritikus ágazatokban és rendszerekkel dolgozók képzése, mivel ezek a területek különösen érzékenyek a kiberfenyegetésekre.[22]
- Kiberpszichológia: a kiberpszichológia ismerete segít megérteni a támadók motivációit és módszereit.

A Magyar Honvédség állománya nemcsak elfogadta a kiberképzések rendszerbe illesztését, hanem igényli is azokat, a tanfolyamokra jelentkezők száma minden esetben meghaladja a kiajánlott létszámkeretet. A sikeres evolúciós folyamat következményeként az oktatások mennyisége, színvonala és az oktatók száma folyamatosan növekvő tendenciát mutat, ezzel összhangban hajtja végre az MH Kiberműveleti Parancsnokság a Kiberakadémia jövőképének kialakítását és fejlesztését.

A felmerült igények kielégítése érdekében az oktatáson részt vett állomány visszajelzései alapján az MH kijelölt állománya folyamatosan felülvizsgálja az oktatási tematikák időszerűségét és tartalmát. Az új tanfolyamok véglegesítését megelőzően azokat tesztelik a KIBP- és KIMK-állomány részvételével (speciális tanfolyamok a jövőbeni célközönség bevonásával), azokat a finomhangolást követően ajánlják ki az MH-állomány részére. Az így kialakuló szervezeti ellenálló képesség *(reziliencia)* megfelelő alapot teremt a nemzeti ellenálló képesség erősítéséhez, a megszerzett tapasztalatok átadásához.

A kibertér sajátosságából adódóan a nemzetközi és civil szervezetekkel történő kapcsolattartás nagyon fontos, a kritikus infrastruktúrákat üzemeltető civil szolgáltatókkal közös feladatok végrehajtását a gyakorlatok felhasználásával készségszintre kell fejleszteni.

Felhasznált irodalom

CCD COE (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched.* Online: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

Clapson, Colin (2023): Microsoft Belgian Scrutinises International Digital Battlefield for Western Governments. *VRT NWS,* 2023. február 18. Online: www.vrt.be/vrtnws/en/2023/02/13/microsoft-belgian-scrutinises-international-digital-battlefield/

Cybersecurity Education Initiatives In The EU Member States (2022). [h. n.]: ENISA. Online: www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states

[22] European Union 2016.

Draveczki-Ury Ádám (2019): Átadták a Magyar Honvédség Kiber Képzési Központját. *Honvédelem.hu,* 2019. június 13. Online: https://honvedelem.hu/media/aktualis-videok/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat.html

European Union (2016): *Protecting critical infrastructure.* Online: https://eur-lex.europa.eu/EN/legal-content/summary/protecting-critical-infrastructure.html

Internet of Things [é. n.]. Online: https://www.britannica.com/science/Internet-of-Things

Kovács László (2021): Offenzív kiberműveletek II. Kibererők és képességeik. *Hadmérnök,* 16(3), 119–137. Online: https://doi.org/10.32567/hm.2021.3.7

Kovács László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika.

Magas Bianka (2022): Kiberhigiéniai kisokos – 1. rész. *Ludovika.hu,* 2022. június 30. Online: www.ludovika.hu/blogok/cyberblog/2022/06/30/kiberhigieniai-kisokos-1-resz/

NATO (2016): *Warsaw Summit Communiqué. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8–9 July 2016.* Online: www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO (2020): *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations.* Online. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

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

Országgyűlés Hivatala (2019): *Kiberhadviselés és katonai kibervédelem.* Online: www.parlament.hu/documents/10181/1789217/Infojegyzet_2019_49_Kiberhadviseles.pdf

Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration Text with EEA relevance. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011R0580

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 3. szám 225–239.
DOI: 10.32567/hm.2024.3.14

Tekla Varró[1]

The Effects of Storing Electric Scooters and Bicycles in Office Buildings on Fire Safety

Abstract

In recent years, we have seen more and more electric vehicles on the streets, and the author looks at electric bicycles and electric scooters, which are considered as "personal transport". With the increase in the number of office buildings, it has become topical to study the storage of these vehicles in office environments. The study covers the fire safety hazards of electric scooters and electric bicycles, the lithium-ion batteries that pose a risk and their safe storage for fire safety. This will be followed by a summary of the hazards and rules of storage in office buildings, with the aim of informing and alerting the general public to the storage rules to be observed and the rules of conduct to follow in the event of a fire. The author suggests extending the rules on storage and informing the owners of electric scooters and electric bicycles about the dangers of their vehicles.

Keywords: e-scooter, e-bicycle, office building storage, fire protection

Introduction

In recent years, more and more electrically powered vehicles have appeared on the streets, with electric bicycles (hereinafter: e-bikes) and electric scooters (hereinafter: e-scooters) becoming increasingly popular and appearing in increasing numbers on public roads. More and more people are also choosing this form of transport for commuting, as they are relatively fast, can travel longer distances and can be stored in a small space. As the number of these means of transport has increased, so has the number of office buildings. Thanks to the increasing use of e-scooters and bicycles, it has become relevant to study the storage of these vehicles in office environments. In this article, the investigation covers the fire safety hazards of e-scooters and e-bikes,

[1] Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: tekla.varro@yahoo.com

the lithium-ion (Li-ion battery) batteries that pose the hazard, and their safe storage for fire safety. The author's aim is to raise awareness of the dangers and rules for storing e-scooters and bicycles in office buildings and to inform the general public about the storage and charging rules to be followed in Hungary. The author proposes to extend the rules on storage, to inform the owners of e-scooters and e-bikes on a wide range of measures to avoid the dangers hidden in their vehicles, and to develop the relevant legislation to protect both the operators of the building and the workers in the office buildings.

The author identifies as a scientific problem related to the topic that despite the recent widespread social use of electric scooters, few publications of scientific value have been written on the problems of operation, technical service and fires generated by the devices, and therefore the availability of the Hungarian and international literature is limited.

The legal regulation of the storage of electric scooters has not been elaborated, the methods and technologies of preventing and fighting electric scooter and bicycle fires in residential buildings and office buildings, the aspects of the mandatory design of safe storage rooms for the safety of residential buildings have not been conclusively proven.

The author assumes that the storage of e-scooters and bicycles will require fire safety investments due to enhanced fire safety measures that may require extra infrastructure to the existing ones. These extra investments include smoke detection systems and fireproof storage areas.

Furthermore, the author assumes that inadequately and inappropriately located storage facilities for e-scooters and e-bikes may obstruct traffic routes, increasing the fire risk. In many cases, transport routes are also escape routes, the restriction of which is critical for fire safety.

The author assumes that storing and charging e-scooters and e-bikes in office buildings increases the risk of fires, as Li-ion batteries are prone to overheating and explosion, especially if not properly stored and maintained.

The research methods include research and processing of the relevant national and international literature, legislation, representation of numerical data and statistical analysis. The research method primarily used by the author is the empirical method, based on experience in the field under study.

Charging, storage and hazards of electric scooters and e-bikes

First, it is important to clarify what we mean by e-scooter and e-bike. E-scooters are two-wheeled means of transport that are powered by an electric motor, so they do not require human effort to operate. E-scooters are generally lightweight and portable due to their small size. They usually require only a small control panel to control the speed, and in most cases the electric drive is provided by a Li-ion battery. They are ideal for urban commuting or short trips. The European Commission's Road Traffic (Electric Scooters) Regulations 2023 defines electric scooters as "a type of electric passenger transport vehicle with a bodywork, two axles and at least one electric motor,

mainly powered by electricity, designed to carry one person in a standing position, without a seat". E-bikes are powered by an electric motor that helps you pedal or even move the bike autonomously. These motors usually assist the pedals or provide full electric propulsion for the e-bike, allowing the user to move more easily, faster, with less or no effort. Additional requirements for e-bikes are laid down in Regulation (EU) No. 168/2013 of the European Parliament and of the Council.

The use, storage and charging of e-scooters and e-bikes is not without risk, and their batteries can in some cases catch fire posing a serious safety risk. Particular attention must be paid to extinguishing these fires, as Li-ion batteries require special care. It is not enough to extinguish the flames from the battery, because the Li-ion will feed the flames until the chain reaction is over. The process can be stopped by cooling, for which water is an excellent solution.[2]

Legal regulations

The storage of e-scooters and e-bikes must comply primarily with Decree 54/2014 (XII. 5.) of the Ministry of the Interior (in Hungarian: Országos Tűzvédelmi Szabályzat, hereinafter used its Hungarian abbrevation: OTSZ) in Hungary. Chapter III of the OTSZ defines the objectives of the protection of life, community and property, which everyone is obliged to comply with. Chapter VI provides for protection against the spread of fire, setting out requirements for the design of fireproof storage areas. Section 39 of the OTSZ provides for regulations for office buildings. The author proposes to amend this section if large quantities of e-scooters and e-bikes are stored and charged in the designated area of the office building. Chapter VIII provides for the evacuation of the building and Chapter X for the protection against heat and smoke, which sets out general requirements for the design of the office building.

For special fire protection solutions related to the charging and storage of electric passenger vehicles, the Technical Guidelines for Fire Safety (in Hungarian: Tűzvédelmi Műszaki Irányelvek, hereinafter used its Hungarian abbrevation: TvMI) are applicable, for special installation solutions related to the design of protection against fire spreading, the TvMI 1.6:2024.02.01. Annex P of the TvMI, which covers the protection of electric passenger car charging points against fire spread, the safety equipment of vehicle storage facilities including electric passenger car charging points and the design of passenger car charging points in existing buildings. The protection against heat and smoke shall be in accordance with the TvMI, TvMI, paragraph 16.2, Heat and Smoke Protection, TvMI 3.5:2024.02.01, which covers the design of vehicle storage areas for electric passenger car charging points. The design and installation of fixed fire extinguishing systems is covered by point 7.5 of the TvMI, Design and Installation of Fixed Fire Extinguishing Systems, TvMI 6.5:2024.02.01, which covers the design of vehicle storage facilities including charging points for electric passenger vehicles. The above listed Fire Safety and Technical Directives apply to electric passenger vehicles,

[2] Magyar Tűzoltó Szövetség 2023c.

but can provide a basis for the development of fire safety legislation for the storage of e-scooters and bicycles in office environments.

In Hungary, fire brigade intervention, the issue of the electric drive battery, is regulated by the Fire Tactics Code. The Code contains provisions for hybrid vehicles, which are defined as "a vehicle in which, in addition to the conventional internal combustion engine, there is also an electric engine and a battery pack which is essential for propulsion". The regulation specifies water as the extinguishing agent for batteries, which can also be used for e-scooters and e-bikes.

Danger during charging electric scooters and e-bikes, preventive measures against fires caused by them

The most dangerous parts of e-scooters and e-bikes from a fire safety point of view are the batteries that make them work. The most advanced, mass available, high-energy-density, and long-life Li-ion batteries currently available power most of these vehicles. These batteries are less sensitive to operating temperatures but can be extremely flammable. Their flammability is based on a phenomenon called thermal runaway,[3] which only occurs under certain conditions.[4] An important thing to know about thermal runaway is that it is an unstoppable chain reaction that occurs as a result of the sudden release of energy stored in the battery, at temperatures of around 400 degrees Celsius. It cannot be extinguished by conventional means; it can burn back out after extinguishing while the battery is still charged. Its danger starts at 60 degrees Celsius and reaches critical levels at 100 degrees Celsius. The biggest problem is that it is not known when it will actually ignite. Ignition can be caused by an internal short circuit due to internal mechanical damage, an external short circuit due to deformation, excessive current consumption during overcharging or fast charging, or a discharge. If one cell of the battery is damaged, it will almost certainly spread to the other cells.[5]

"The fire suppression method should suppress any Li-ion batteries fire and control any rise in battery temperature. If not sufficiently cooled, thermal runaway reactions may continue and the battery re-ignite. […] It is more important to cool the cells in a large battery pack, to prevent heat propagation, than to extinguish fires from a single cell. Li-ion battery firefighting strategies should be based on not only extinguishing the burning cell, but include cooling the burning cell as well as its adjacent cells."[6]

[3] "A severe failure of li-ion batteries can lead to heat generation at a rate that causes what is known as a heat runaway. This can result in extremely intense combustion in one or more cells, causing damage through sputtering from the battery, toxic and flammable gas emissions and intense self-sustained combustion that is very difficult to control." See: https://katasztrofavedelem.hu/37082/li-ion-akkumulatorok-veszelyei

[4] Magyar Tűzoltó Szövetség 2023a.

[5] Veresné Rauscher 2022.

[6] Ghiji et al. 2020.

Water is the most suitable extinguishing agent to control a chain reaction involving a violent flame, smoke, shell rupture or even an explosion.[7]

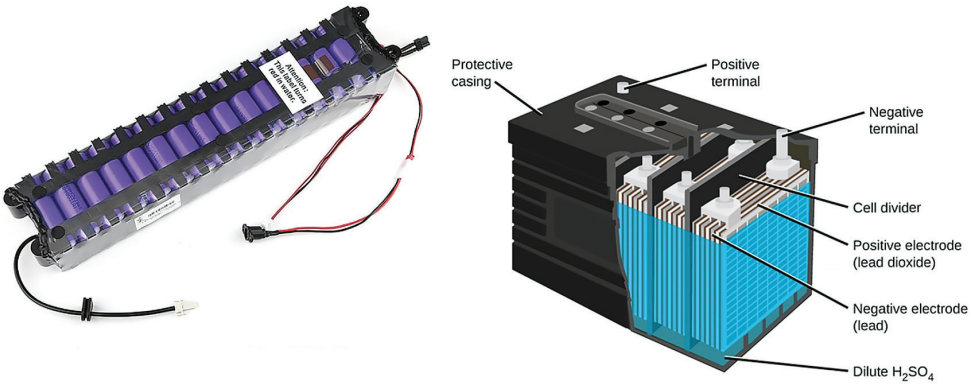


Figure 1: Xiaomi Mijia M365 e-roller battery and an electric bike battery
Source: Gayathri *2023; www.li-ion.hu/Elektromos-bicikli-roller-funyiro-akkucsere-akkufelujitas*

Figure 2: Electric bicycle and electric scooter
Source: www.li-ion.hu/Elektromos-bicikli-roller-funyiro-akkucsere-akkufelujitas

The first and most important basic rule is to always follow the manufacturer's instructions for charging and storage. The instructions may contain specific information that is unique to the product in question, so that the vehicle can be charged more safely. Always use a suitable, undamaged and manufacturer-issued cable for charging. Using

[7] Magyar Tűzoltó Szövetség 2023b.

a damaged cable is dangerous, and a cable not manufactured for the specific device will not provide proper charging and will overload the charging head.

It is very important to create a charging point (hereinafter: e-charging point) in the covered lobbies of office buildings, in storage areas and garages for e-scooters and e-bikes, where only and exclusively e-scooters and bicycles are charged, in order to avoid overloading the electricity network by employees charging their e-scooters and e-bikes individually. It is also proposed to install an external disconnection system to cut the power supply to the storage or charging facility in the event of an emergency. A fire can easily occur during 'home charging' and an e-charging point should be provided to prevent this and to prevent fires.

Charging should preferably be carried out in dry conditions, indoors, ideally at room temperature, but charging these devices is prohibited below 0 °C and above 40 °C. The device/accumulator under charging should never be exposed to direct sunlight, heat, rain or moisture, and must not be covered. A covered battery or charger may overheat or catch fire.

It is very important to regulate the times when devices can be charged: never leave the battery on the charger overnight. If the office building has a permanent porter service, a security guard can rush to the scene immediately when the fire alarm and smoke alarm are triggered and alert the fire brigade instantly. If the premises has a sprinkler or mist extinguishing system, it can be activated and start extinguishing any vehicle on fire until the fire brigade arrives. It is therefore extremely important that employees in office buildings do not leave a vehicle/battery charging overnight. Although modern batteries and chargers have electronics designed to prevent overcharging, if these electronics fail, it is unlikely that anyone in the office building will immediately notice if they start smoking. It is therefore advisable to provide smoke detectors in enclosed rooms where e-scooters and bicycles are stored. Another important criterion is that the vehicle/battery to be charged should be charged on a solid, flat surface, away from flammable objects.[8]

Should any of the following occur to the attention of the vehicle owner – or anyone else in the building – charging must stop immediately:

- strange burnt smell around the charger
- the battery is leaking fluid
- the battery is humped, deformed, discoloured
- the battery area is unusually hot
- smoke is spreading from the battery[9]

Rules on the design of storage facilities for electric scooters and e-bikes

The owner, operator or occupier of the building shall designate an appropriate storage space for e-scooters and e-bikes, taking into account the following:

[8] See: https://nfcc.org.uk/our-services/position-statements/e-bikes-and-e-scooters-fire-safety-guidance/
[9] Magyar Tűzoltó Szövetség 2023a.

- For enhanced fire safety, it is recommended that existing e-bikes storage facilities are upgraded or modified, where possible, so that they are easily accessible, easy to use and secure for employees and they do not feel the need to store their vehicles inside the building.
- The manager responsible for the operation of the building must take into account the risks of enclosed spaces for charging e-scooters and e-bikes, bicycle storage, escape corridors and common areas, and the provision of fire and smoke protection.
- It is forbidden to load or store e-scooters and e-bikes on the escape route, as this significantly impairs the ability of the occupants to escape.[10]
- If e-scooters and e-bikes pose a risk to the fire safety of the building, they must necessarily be included in the building risk assessment and the building fire safety plan.
- E-scooters, e-bikes and their batteries should be stored in a cool place out of the sun, if possible. Avoid storage and charging in places that are too hot or too cold.[11]
- The number of charging sockets should be set so that even at maximum capacity, no one needs to use an extension lead or adapter.
- No flammable material may be stored in the affected area.
- Where possible, battery charging stations should be located outdoors, in a secure area, on the ground floor, in a safe place where the owner does not have to worry about theft or damage to the device.

Ágoston Restás and his co-authors in their paper[12] also state that fire prevention measures for electric car charging stations include "People acting in case of fire must be trained in the safe charging process and they should be familiar with the location of the charging equipment. They have to know how to deenergise and the measures to be taken in case of an emergency." This clause may also apply to persons acting in the event of a fire at charging points for e-scooters and e-bikes.

If the storage and charging is still to be carried out indoors, the author recommends the installation of a fire alarm system in accordance with Annex 14 of the OTSZ. In addition to the fire alarm system, a gas concentration detection system can accelerate the early detection of a Li-ion fire, as it is capable of detecting the content of evolving gas, smoke, hydrogen, carbon monoxide and carbon dioxide before the fire starts. Heat build-up can be detected at an early stage using an infrared camera. Furthermore, in accordance with Annex 14 of the OTSZ, it is recommended that the premises be equipped with fire extinguishing equipment, which may be a sprinkler or a water mist extinguishing system.

Point 3.2 of the TvMI[13] on protection against heat and smoke states that open motor vehicle storage facilities do not need to be equipped with heat and smoke

[10] See: https://nfcc.org.uk/our-services/position-statements/e-bikes-and-e-scooters-fire-safety-guidance/
[11] Pinnington 2024.
[12] Terjék et al. 2021.
[13] National Directorate General for Disaster Management of Hungary: Technical Directive on fire safety, Protection against heat and smoke 2024.

ventilation, which means that open storage facilities for e-scooters and e-bikes do not need to be equipped with it. Where a large area of e-scooters and e-bikes is stored in covered storage, heat and smoke ventilation may be appropriate. In this case, air supply may be provided by natural ventilation, mechanical heat and smoke ventilation or a combination of these.[14]

"One of the most important means of prevention is to comply with the fire safety requirements set out in the OTSZ:
(a) the design, construction, alteration, extension, modernisation, restoration, renovation, use and change of use of the installation, building or part of a building,
(b) the installation, maintenance, alteration, removal or use of a fixed fire protection system prescribed by law or by a decision of a public authority,
(c) the use of other means to ensure the fire protection of the building,
(d) other uses and activities affecting fire protection.
Where the Regulation does not provide for the cases referred to in the preceding points, the application of the fire safety provisions of the relevant technical requirements or equivalent solutions or designs shall comply with the level of safety laid down in the Regulation."[15]

In Hungary, official statistics on the number of fires involving e-scooters and e-bikes are currently not available, and there is also a lack of aggregated statistics on fires involving e-scooters and e-bikes in the European Union. Most of the statistics published by the authorities on this subject have been collected in the United Kingdom, and the author wishes to draw attention to the fact that Li-ion powered e-scooters and e-bikes are not without danger, that their charging and storage requires great care, and that their storage may require changes in legislation. Figure 3 shows the cumulative data on fires involving e-scooters and e-bikes in the UK from 2017 to 2023.

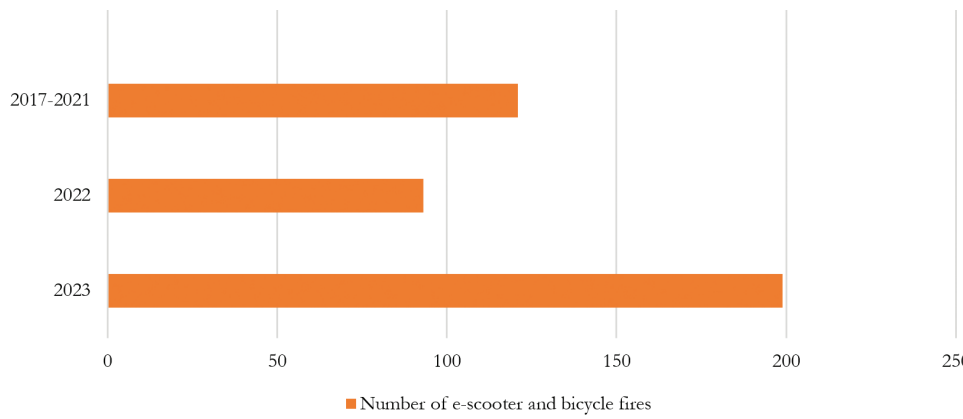


Figure 3: Number of fires involving electric scooters and bicycles in the UK
Source: Government of the United Kingdom 2024

[14] Farkas et al. 2022.
[15] Muhoray 2016: 19.

The data in Figure 3 shows that between 2017 and 2021, a total of 121 e-scooter and e-bike fires were reported to the UK's Product Safety and Standards Agency. The number of fires caused by e-scooters and e-bikes rose to 93 in a single year in 2022, rising to 199 in 2023.

The author proposes to compile statistics on the data on fires caused by e-scooters and e-bikes in Hungary for all fires caused by e-scooters and e-bikes received by the professional emergency services. A further proposal of the author is to extend the document entitled "Special fire safety installation solutions for charging and storage of electric passenger cars in a single structure",[16] issued by the National Directorate General for Disaster Management of the Ministry of the Interior, to include the parts on the storage of e-scooters and e-bicycles. In view of the statistics for Hungary, it may be necessary to extend the relevant TvMI to cover e-scooters and e-bicycles.

Extinguishing fires from electric scooters and e-bikes in an office building environment

Li-ion batteries burn at extremely high temperatures, emitting toxic gas. Depending on the capacity of the battery, very serious fires can develop, which can only be extinguished by using large quantities of water. With smaller capacity batteries – under appropriate storage conditions – there is a chance that the flames will be extinguished quickly, but even in this case it is not worth taking the risk, call 112 for help and wait for the fire brigade to arrive.[17]

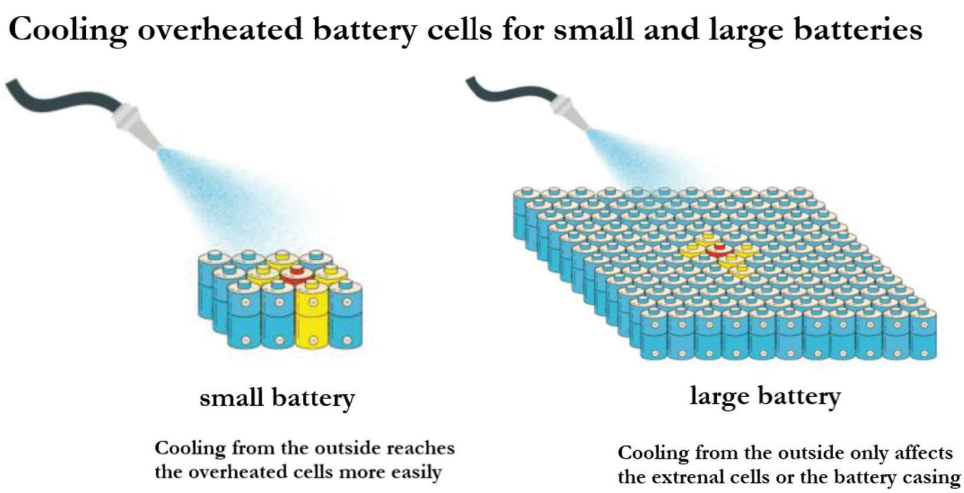


Figure 4: Cooling overheated battery cells for small and large batteries
Source: Magyar Tűzoltó Szövetség 2023c

[16] Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság 2024a.
[17] Magyar Tűzoltó Szövetség 2023c.

If the battery starts to burn or smoke, the device must be disconnected from the power supply. If possible, the damaged equipment should be removed from the room and away from combustible materials. If it is safe to do so, small appliances that have been disconnected can be cooled in a bucket of water.

It is extremely important to pay attention to prevent the inhalation of smoke and fumes. All occupants should leave the room and close the door after leaving to slow down the spread of fire and smoke. Gases, vapours and fumes emitted from a damaged battery are extremely toxic and flammable, so it is especially important to prevent their inhalation.

Paragraph 5(11) of Article 5 of Act XXXI of 1996 on Fire Prevention, Technical Rescue and Fire Brigades states that "anyone who detects a fire or an imminent threat thereof shall immediately report it to the call centre, the operations control centre of the disaster management directorate or the fire brigade, or, if this is not possible, to the police or the ambulance service, or to the mayor's office of the municipality". In the light of this and in accordance with the before mentioned information, the person detecting the fire should call 112 for help and wait for the fire brigade to arrive. If the battery has not been properly cooled, there is a good chance that it will re-ignite.[18] A series of images shows the progression from ignition to explosion of an electric scooter under charge in Figure 5. The scooter's battery started to heat up at 9:00:38, reaching the ignition point at 9:00:51. The increase in activity energy continued until 9:00:52, at which point the flashover occurred. Burning of the mature fire lasted until 9:01:06, after which the fire started to decay.[19]

Figure 5: Electric scooter being charged catches fire before exploding
Source: London Fire Brigade 2023

Restás and his co-authors set out the measures to be taken in case of fire for electric cars, which are also used for e-scooters and e-bikes:

- "The manual call point must be operated. This starts the fire alarm and the fire protection equipment.
- De-energisation shall be performed by using on-site fire protection switches.

[18] Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság 2024c.
[19] Érces 2015: 19.

- The switching devices used for disconnection must be secured against reconnection.
- People should start the firefighting with the available fire extinguishers, if it can be started safely.
- The professional firefighters must be informed of the measures taken so far, the condition of the charging equipment and to give them the Fire Alert Plan and its annexes.
- If necessary, the evacuation of the building shall be carried out in accordance with the provisions of the Fire Alert Plan.
- After the successful firefighting, the condition of the reconnection of the equipment is a joint permission from the maintenance company and the Disaster Management
- All fires must be reported to the appropriate Disaster Management Branch Office."[20]

Based on current research, the available literature classifies fire extinguishing agents into different categories. The first and most important extinguishing agent is water, which appears to be the most cost-effective and most commonly used extinguishing agent. In addition to its good extinguishing and cooling properties, it can reduce or even stop the phenomenon of heat build-up, but its use also carries risks. The extinguishing water can react chemically or conduct electricity, causing a short circuit. This can cause further heat build-up in other parts of the burning battery. The next method of extinguishing is the use of a water jet, which has the advantage of being able to be used over long distances, depending on the jet pattern, and can be accurately directed. Compared to a bound water jet, a sprinkler system can be used over shorter distances, with the advantage of better flame cooling and less secondary damage during extinguishing, but with the disadvantage of not being effective in confined spaces of vehicles and other equipment stored in protected areas. Added materials can be used to reduce the surface tension of the extinguishing water, thus achieving a more direct extinguishing effect on different surfaces, but this method of extinguishing also requires the use of a foaming agent. Water mist extinguishing, compared to sprinkler extinguishing, is capable of producing smaller droplet sizes, thus allowing more economical use of water and even better cooling effect.[21]

There are some studies in the international literature using other types of extinguishing agents for Li-ion battery fires. These extinguishing agents include foam, which cools and seals the surface of the material to be extinguished, forms a barrier between the burning material and the surrounding air – combustible gases – but can also have a corrosive effect.[22] In case of powder extinguishing, effective extinguishing can be achieved in the airspace, but it does not cool the battery and has a more limited blanketing effect. Extinguishing with carbon dioxide chokes the combustion and with it the breathing, which can pose a danger to bystanders, rescuers and the

[20] Terjék et al. 2021.
[21] Pántya 2023: 23–24.
[22] See: https://scottyfire.com/product/foam-fast-foam-systems/

intervention forces. No extinguishing agent remains after application, but the cooling capacity required for Li-ion batteries is low. Halon is an extinguishing agent with similar effects to carbon dioxide, but their use was banned in 1994. Liquid nitrogen has a good cooling capacity and is non-toxic, but is difficult to transport and store, and fire brigades do not stock this type of extinguishing agent.[23]

Summary

The research has shown that storing and charging e-scooters and e-bikes in office buildings increases the risk of fires, as Li-ion batteries are prone to overheating and explosion, especially if not properly stored and maintained. Failure of batteries and charging with batteries other than their own chargers can cause fires, which can spread dramatically quickly in confined spaces. Figure 4 shows that it only takes a few seconds for a failed battery to ignite and burst into flames.

The storage and charging of e-scooters and e-bikes inside buildings requires increased attention, and a safe charging and storage unit with minimal fire risk can be created by properly designing the storage and charging room, installing fire alarms, providing heat and smoke protection and fire extinguishers. Inadequately designed and inappropriately located storage areas can obstruct traffic routes, increasing the fire risk. In many cases, transport routes are also escape routes, the restriction of which is critical for escape, therefore these must always be left clear and storage facilities must not be provided.

The author's first assumption, that the storage of e-scooters and e-bikes requires fire safety investments, can be considered valid. Enhanced fire safety measures may require extra infrastructure, investments that include smoke and gas detection systems and the construction of fireproof storage areas. It is also recommended to install a hand-held fire extinguisher capable of extinguishing electrical fires in the storage facilities, if no sprinkler or mist extinguishing system is installed. Hand-held fire extinguishers specially designed for Li-ion battery fires (Lith-Ex) are specifically designed for use in an office environment, so their use may also be necessary in the part of the building used for storing e-scooters and e-bikes. The author feels it is particularly important to draw the attention of the owner of the electric vehicle to the fact that damaged vehicles must not be stored and charged inside the building, and that charging with a damaged charger or with a charger not belonging to the device is prohibited. If possible, charging points should be located at the entrance to the vehicle storage area to facilitate access by firefighters in the event of a fire.

The author identifies as a problem the fact that no summary statistical data on e-scooter and e-bike fires in all countries of the EU and Hungary have been published, and no representative data can be obtained to support the need for legal regulation of e-scooters and e-bikes. As part of the legal regulation to be established, the author proposes to extend Annex 14 of the OTSZ with rules on the construction of premises for the storage and charging of a larger number of e-scooters and bicycles and

[23] Pántya 2023: 25–26.

to limit the number of e-scooters and e-bikes stored at the same time in the same place. The author also proposes to make it compulsory to affix a short, graphically illustrated storage and charging code on the walls of the premises where e-scooters and e-bikes are stored, and to include instructions for staff using the storage facilities, including what to do in the event of a fire and the rules of conduct to be followed, and to incorporate them into legislation.

References

Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (2024a): *Egységes szerkezetben az elektromos személygépjárművek töltésével és tárolásával kapcsolatos speciális tűzvédelmi létesítési megoldások.* Online: www.katasztrofavedelem.hu//application/uploads/documents/2023-12/82919.pdf

Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (2024b): *Li-ion akkumulátorok veszélyei.* Online: https://katasztrofavedelem.hu/37082/li-ion-akkumulatorok-veszelyei

Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (2024c): *Mit tegyünk, ha készülékünk vagy akkumulátorunk füstöl, illetve ég.* Online: https://katasztrofavedelem.hu/37087/mit-tegyunk-ha-keszulekunk-vagy-akkumulatorunk-fustol-illetve-eg

Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (2024d): *Tűzvédelmi Műszaki Irányelvek.* Online: www.katasztrofavedelem.hu/213/tuzvedelmi-muszaki-iranyelvek

Booth, Robert (2023): E-bike and E-Scooter Fires have Injured at Least 190 People in UK, Data Shows. *The Guardian,* 2 May 2013. Online: www.theguardian.com/news/2023/may/02/e-bike-e-scooter-battery-fires-uk-data

Érces, Gergő (2015): *A komplex tűzvédelem vizsgálata mérnöki módszerekkel történő vizsgálat alkalmazásával.* Online: https://vedelem.hu/letoltes/anyagok/-a-komplex-tuzvedelem-vizsgalata-mernoki-modszerekkel-torteno.pdf

Farkas, Flóra – Szikra, Csaba – Takács, Lajos Gábor (2022): *Elektromos járművek tárolásának és töltésének védelme.* Online: https://doi.org/10.33268/Met.2022.6.8

Gayathri, N. S. (2023): Lead Acid Battery. *LinkedIn,* 24 August 2023. Online: www.linkedin.com/pulse/lead-acid-battery-dr-gayathri-n-s/

Ghiji, Mohammadmahdi – Novozhilov, Vasily – Moinuddin, Khalid – Joseph, Paul – Burch, Ian – Suendermann, Brigitta – Gamble, Grant (2020): A Review of Lithium-ion Battery Fire Suppression. *Energies,* 13(19). Online: https://doi.org/10.3390/en13195117

Government of the United Kingdom (2024): Fires in E-Bikes and Scooters. *Gov.uk,* 27 August 2024. Online: www.gov.uk/government/publications/fires-in-e-bikes-and-e-scooters

London Fire Brigade (2023): *Brigade Shares Frightening Footage of E-Scooter Battery Explosion with #ChargeSafe Plea.* 18 May 2023. Online: www.london-fire.gov.uk/news/2023/may/brigade-shares-frightening-footage-of-e-scooter-battery-explosion-with-chargesafe-plea/

Magyar Tűzoltó Szövetség (2023a): *Akkumulátor kisokos, Li-ion akkumulátorok. 04 December 2023.* Online: https://tuzoltoszovetseg.hu/hirek/1757

Magyar Tűzoltó Szövetség (2023b): *Elektromos kerékpárok: tűzvédelmi útmutató, Töltés, használat. 11 December 2023.* Online: https://tuzoltoszovetseg.hu/print_page.php?pageid=hirek&hirid=1760

Magyar Tűzoltó Szövetség (2023c): *Miért vízzel oltjuk a lítium-ionos akkumulátorokat?, Oltóanyag: a víz. 27 November 2023.* Online: https://tuzoltoszovetseg.hu/hirek/1749-miert-vizzel-oltjuk-a-litiumion-akkumulatorokat

Muhoray, Árpád (2016): *Katasztrófamegelőzés I.* Budapest: NKE, Szolgáltató Nonprofit Kft.

National Fire Chiefs Council (2024): *E-bikes and E-scooters Fire Safety Guidance.* Online: https://nfcc.org.uk/our-services/position-statements/e-bikes-and-e-scooters-fire-safety-guidance/

Pántya, Péter (2023): A Li-ion akkumulátorok tűzoltásával kapcsolatos kutatási tapasztalatok, a tűzoltói beavatkozás lehetőségei. *Védelem Tudomány,* 8(2), 19–29. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13493

Pinnington, Phil (2024): E-scooters and Lithium Batteries: The New Fire Risk for the Workplace? *British Safety Council,* 19 February 2024. Online: www.britsafe.org/safety-management/2024/e-scooters-and-lithium-batteries-the-new-fire-risk-for-the-workplace#:~:text=There%20should%20be%20no%20storing,affect%20people's%20ability%20to%20escape

Terjék, Ágnes – Kerekes, Zsuzsanna – Restás, Ágoston (2021): Comparison of the Hungarian and International Standards for Electric Car Charging Stations. *Védelem Tudomány,* 6(3), 615–616. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/download/13755/11182/

Veresné Rauscher, Judit (2022): Li ion akkumulátorok tűzvédelmi kérdéseivel kapcsolatos nemzetközi kitekintés. In *Konferencia kiadvány VI. Tűzesetek vizsgálata, tapasztalatai konferencia.* Kecskemét: Bács-Kiskun Megyei Katasztrófavédelmi Igazgatóság, 23–32. Online: https://vedelem.hu/letoltes/document/567-20220908-rauscher.pdf

Xiaomi szerviz (2024): *Xiaomi Mijia M365 Akkumulátor.* Online: https://xiaomiszerviz.com/xiaomi-mijia-m365-szerviz/mijia-m365-akkumulator-csere/

Legal sources

6/2016 (VI. 24.) BM OKF Instruction on the issuance of the Firefighting Tactical Code and the Technical Rescue Code [6/2016 (VI. 24.) BM OKF utasítás, a Tűzoltás-taktikai Szabályzat és a Műszaki Mentési Szabályzat kiadásáról]

Act XXXI of 1996 on Fire Prevention, Technical Rescue and Fire Brigades [1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról]

Decree 54/2014 (XII. 5.) of a the Ministry of the Interior [54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról]

Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles. Online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013R0168

Tartalom