



HADMÉRNÖK

Kiemelt közlemények

PAPP ISTVÁN: *Rakétairányítási és célbefogási folyamatok a modern kor hadviselésében*

SZAJKÓ GYULA: *Az Összhaderőnemi Logisztikai Felderítő Csoport lehetséges összetételének meghatározása és alkalmazása az MH szervezeti struktúrájában*

VARRÓ TEKLA: *A katasztrófavédelmi oktatás és tájékoztatás fejlesztési lehetőségei a magyar felnőtt lakosság körében*

20. évf. (2025)
3. szám

ISSN 1788-1919 (elektronikus)



LUDOVIKA
EGYETEMI KIADÓ

Hadmérnök

Katonai műszaki tudományok online folyóirata

ISSN 1788-1919 (elektronikus)

A szerkesztőbizottság elnöke

Kovács László vezérőrnagy, egyetemi tanár

A szerkesztőbizottság elnökhelyettese

Munk Sándor ny. ezredes, professor emeritus

A szerkesztőbizottság tagjai

Alexandru Babos alezredes, egyetemi docens

Berek Tamás ezredes, egyetemi tanár

Eleki Zoltán ezredes

Földi László ezredes, egyetemi tanár

Haig Zsolt ezredes, egyetemi tanár

Horváth Attila ny. ezredes

Kállai Attila alezredes, egyetemi docens

Lukács László ny. alezredes, professor emeritus

Pohl Árpád ny. dandártábornok

Bryson Payne egyetemi docens

Josef Procházka ny. alezredes, egyetemi docens

Szászi Gábor ezredes

Taksás Balázs őrnagy, egyetemi docens

Turcsányi Károly ny. ezredes, egyetemi tanár

Ujházy László ezredes, egyetemi docens

Szerkesztőség

Főszerkesztő

Farkas Tibor egyetemi docens

Szerkesztőségi tagok

Biró Gabriella, tanársegéd

Kovács László vezérőrnagy, egyetemi tanár

Németh József Lajos egyetemi docens

Nemzeti Közzolgálati 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 Közzolgálati 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, Gergely Zsuzsánna, Resofszi Ágnes



Tartalom

Haditechnika

PAPP ISTVÁN: <i>Rakétairányítási és célbefogási folyamatok a modern kor hadviselésében</i>	5
--	---

Védelem-informatika

BENKE BÁLINT PÉTER: <i>A kriptovaluták kettős arca</i>	25
BOTTYÁN SÁNDOR: <i>Nagy nyelvi modellek az internetes nyílt forrású információgyűjtésben</i>	49
ATTILA HAMMAS: <i>More Data, More Problems?</i>	71
SZABOLCS JOBBÁGY: <i>The Convergence of the Digital Virtual World and Artificial Intelligence – Or What the Future Symbiosis Brings in the Synergy of the Metaverse and AI</i>	85
PÁL KÁROLY LASKA: <i>Empirical Analysis of the Impact of Personality Traits on Cybersecurity Awareness</i>	101
PATAKI JÁNOS IMRE, SULÁNYI PÉTER: <i>Az autópári vállalatok és beszállítók integrált biztonsági és védelmi stratégiája</i>	113
SZABÓ GERGŐ: <i>A generatív mesterséges intelligencia használata a kibertudatosítási képzésekben, 2. rész</i>	135

Fórum

SOMOGYI JÁNOS JÓZSEF, NAGY SÁNDOR: <i>A geopolitika és a lakosságvédelem kapcsolata</i>	157
---	-----

Környezetbiztonság

ISTVÁN MIHÁLY: *Estimating the Air Leakage Rate of Smoke Control Doors for Calculations Procedures, Part 2*175

VARRÓ TEKLA: *A katasztrófavédelmi oktatás és tájékoztatás fejlesztési lehetőségei a magyar felnőtt lakosság körében* 189

Katonai logisztika és közlekedés

SZAJKÓ GYULA: *Az Összhaderőnemi Logisztikai Felderítő Csoport lehetséges összetételének meghatározása és alkalmazása az MH szervezeti struktúrájában.*213

Papp István¹

Rakétairányítási és célbefogási folyamatok a modern kor hadviselésében

Missile Guidance and Targeting Processes in Modern Warfare

Absztrakt

A rakétairányítási és célbefogási folyamatok szakterület a korszerű technológia és a komplex matematikai modellek alkalmazására koncentrál. Az irányítási folyamat közben figyelembe kell venni a dinamikai faktorokat, mint például a sebesség, az időjárási körülmények és a cél mozgásának jellemzői. A célbefogás során a rakéták képesek valós időben adaptálódni a cél mozgásához, optimalizálva a pályát és a manőverezést. A folyamatok magukban foglalják a prediktív algoritmusok és a gépi tanulás alkalmazását is, amelyek javítják a rakéták precizitását és hatékonyságát. Az ipari és tudományos közösség számára a rakétairányítási rendszerek folyamatos fejlesztése létfontosságú a globális biztonság és a technológiai versenyképesség megtartásához. A drónok használata a rakétairányítási és célbefogási folyamatokban forradalmi új perspektívákat kínál, amelyek jelentősen javíthatják a pontosságot.

Kulcsszavak: rakéta, célbefogás, irányítás, drón

¹ Gyakorlati oktató, Nemzeti Közsolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Repülő Sárkányhajtómű Tanszék, e-mail: papp.istvan@uni-nke.hu

Abstract

The missile guidance and targeting focuses on the application of advanced technology and complex mathematical models. During the guidance process, dynamic factors such as velocity, weather conditions and target movement characteristics must be taken into account. During target engagement, missiles are able to adapt in real time to the target's motion, optimising trajectory and manoeuvring. The processes also include the use of predictive algorithms and machine learning to improve the precision and efficiency of the missiles. For the industrial and scientific community, the continued development of missile guidance systems is vital to maintain global security and technological competitiveness. The use of drones in missile guidance and targeting processes offers revolutionary new perspectives that can significantly improve accuracy.

Keywords: missile, targeting, guidance, drone

Bevezetés

A pilóta nélküli légi járművek megjelenése gyökeresen átalakította a modern hadviselést, rámutatott arra, hogy elkezdődött egy új korszak, és az ezzel járó változások nemcsak a katonai harcászatot, hanem a társadalmi látásmódot is befolyásolják.

A drónok képesek nagy magasságból és távolról megfigyelni a célterületeket, lehetővé téve a precíz célmeghatározást. Felszerelhetők különböző érzékelőkkel, mint például kamerákkal, hőkamerákkal és radarokkal, amelyek segítenek a célok azonosításában és nyomon követésében. A gyűjtött adatok valós időben elemezhetők, ezáltal a döntéshozók gyorsan reagálhatnak a változó helyzetekre. Az információk feldolgozása segíthet a jövőbeli támadások megtervezésében és a rakéták irányításának tökéletesítésében. Korszerű navigációs rendszereik lehetővé teszik a precíz és pontos mozgásukat. Ezek a rendszerek integrálhatók a rakéták irányító rendszereibe, így a rakéták a drónok által gyűjtött adatokat felhasználva gyorsabban és pontosabban képesek elérni a célt.

A drónok nemcsak a célzási folyamatban játszanak szerepet, hanem önmaguk is képesek fegyverek szállítására és célzott támadások kivitelezésére. Ez lehetővé teszi a precíziós csapásokat, csökkentve a polgári áldozatok számát és minimalizálva a környezeti károkat. A drónok távolról irányíthatók, így csökkenthető a személyi sérülések valószínűsége.

A pilóta nélküli légi járművek könnyen integrálhatók más katonai rendszerekbe, például információs hálózatokba, ami lehetővé teszi a különböző egységek közötti hatékony kommunikációt és együttműködést, alkalmazásuk a rakétairányítási és célbefogási folyamatokban jelentős előnyöket kínál. A cikk célja, hogy bemutassa az irányítási folyamat két fő szintjét, a vezérlést és az irányítást, ügyelve arra, hogy ne „merüljünk el” a rakétatest szabályozási témakörébe. Ennek két oka van:

- Léteznek a szakirodalomban hozzáférhető hasznos könyvek és publikációk, amelyek a repülőgépek és rakéták irányításával foglalkoznak;

- a rakétatest szabályozási köre gyorsabb, mint az irányítási hurkok. Az irányítástechnikai terminológiákban a rakétatest irányító körei nagy sáv-szélességű belső szabályozási köröket foglalnak magukba, az alacsonyabb sáv-szélességű irányítási hurkokon belül (1. ábra). Elemzések azt támasztják alá, hogy a belső hurok olyannyira gyors, hogy az előzetes külsőhurok-analízis figyelmen kívül hagyható.

Amikor az irányítási törvényszerűségeket tanulmányozzuk, nem hagyhatjuk figyelmen kívül azt a tényt, hogy a rakétatest-szabályozási körnek megvan a saját dinamikája, és ezek nemlineáris hatásait bizonyos esetekben meg is kell vizsgálni.

Terminológia és definíciók

Az irányítási folyamat megértéséhez elengedhetetlen több fogalom és kifejezés meghatározása. Néhány ezek közül nem egységes, másképpen használják mind a brit, mind az amerikai szakirodalomban, továbbá az egyes szerzők munkáiban is. Ebben a részben olyan terminológiát alkalmazok, amelyik a leginkább elfogadott, adott esetben alternatívaként is felhasználható.

Az irányítási folyamat három szintje

Az „irányítás” az a folyamat, amely során a rakéta (jelen esetben) egy adott pont felé halad, amely általában mozog. Ha a pont fix, és az irányítható objektum kezelőszemélyzettel ellátott (kézi irányítású), akkor a folyamatot navigációnak² hívjuk. Így kimondhatjuk, hogy a navigáció az irányítás egyik változata. Ebben a részben szűkebb értelemben elemzem az irányítást, kizárva a navigációt, a konkrét jelentését fogom ismertetni.

Definíciók

Az irányítás hierarchikus folyamat, három szintből áll.

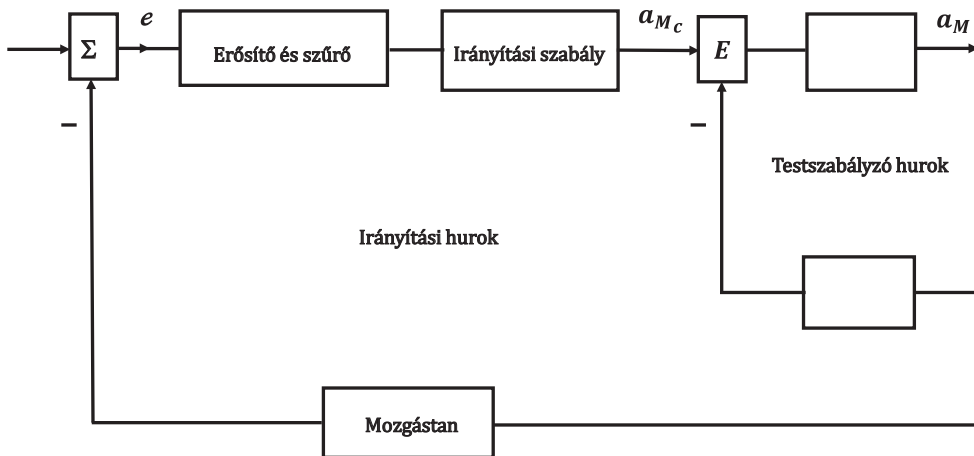
Az első helyen a geometriai szabály áll, amely meghatározza a látótávolságot (irányzóvonalat, LOS³), katonai értelemben célpontot, ezen belül az irányítás célját (feladatát). A továbbiakban, a jelölések egyszerűsítése érdekében, a következőket vezetem be:

- a cél: T (target);
- az irányított tárgy (esetünkben egy rakéta): M.⁴

² Egy szűkebb, ám mégis használatos definíciója a navigációnak, például megtalálni egy repülő (mozgó) tárgy pontos helyét a földhöz képest.

³ LOS: *line of sight* – célzóvonal, vizuális.

⁴ M az irányítási hurokban nullarendű dinamikával képviselteti magát, az $a_M \equiv a_{M_c}$ definíció szerint.



1. ábra: Rakétatest-szabályzó kör az irányítási hurkon belül

Forrás: a szerző szerkesztése SHNEYDOR 1998: 23 alapján

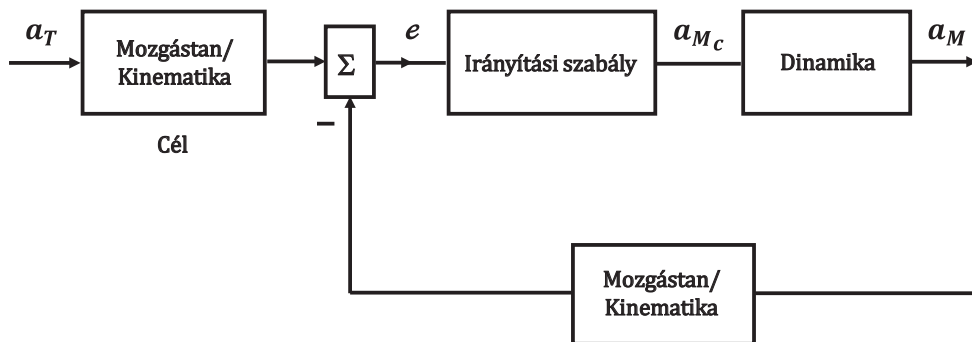
Amikor a rakéta becsapódását tanulmányozzuk a célobjektummal, néhány problémát figyelembe kell venni, mint például a repülési pálya formája, görbülete és a szükséges oldalirányú gyorsulások elemzése. Az irányítási folyamat teljes idejét $t = 0$ időpillanattól, amikor elkezd a cél elfogását, $t = t_f$ időpillanatig vizsgáljuk, mert ebben a szakaszban van jelentősége. Ezt az időt repülési időnek (t_f) hívjuk.⁵

A folyamat második fázisa az irányítási elv. Ez nem más, mint az az algoritmus, amellyel a kívánt geometriai szabály megvalósul. Ez az irányítási hurok lezárásával történik meg (2. ábra). Az e „eltérés” ebben a visszacsatolásban egyenesen arányos az M állapotvektor által mért eltéréssel. Arra használják, hogy létrehozzanak egy kormánymozgási parancsot adott M irányítási elv alapján.

Leginkább a keresztirányú gyorsulási parancs (az ábrán az A_{M_c}), a „c” jelöli a „irányítást”. A rakéta oldalirányú gyorsulása M -ből lett képezve, és az ábrán a_{M_c} -ként jelöltem, hasonlóképpen, a cél oldalirányú gyorsulásához, ahol T -ből lett származtatva, és jelzése a_T . A rakéta (M) elmozdulásának eredményeképp csökken az e („eltérés”) visszacsatolás, végül eléri a nullát.

A folyamat harmadik szintje a felügyelet (kontroll/ellenőrzés). Itt M nem egyéb, mint egy pont. Sokkal inkább egy merev test, amelynek tömege és tehetetlenségi nyomatéka van, valamint mozgása a térben x, y, z koordináták szerint definiálható. Nyilvánvaló, hogy ezen a pályán, hogy tanulmányozzuk az adott test stabilitását és a teljesítményt, szükségünk van egy úgynevezett testszabályozóra, zárt hurokra az irányítási körön belül. Néhány esetben azonban nem létezik önmagában ilyen szabályozó kör. Ekkor a felügyelet „nyílt hurkú”.

⁵ SHNEYDOR 1998: 24.



2. ábra: Az irányítási hurok

Forrás: a szerző szerkesztése SHNEYDOR 1998: 21 alapján

Példa

Vegyük egy hárompontos irányítási mechanizmust, amely a célzóvonal (LOS) geometriai szabályai szerint funkcionál. Ezen szabály szerint az M -nek egy OT sugarú körben kell maradni, az O referenciaponttól a T célíg. Ne felejtsük azt, hogy a használt szimbólumaink, T és M , a tér adott pontjain elhelyezkedő objektumok. T nem szükség-szerűen mozdulatlan. Tegyük fel, hogy a rakéta tudja mérni a céltól való távolságát, ekkor erre a távolságra e „eltérésként” lehet tekinteni, így az irányítási szabályból $a_{Mc} = f(e)$, ahol $f(\cdot)$ lineáris, telítődő, vagy valami egészen más nemlineáris, általában páratlan szimmetrikus karakterisztika definiálja. Egy kifinomultabb szabály lehet az $a_{Mc}(t) = k \left(1 + T(d) \frac{d}{dt} \right) e(t)$, $T_d = konstans$, ahol egy derivált kifejezéssel bővült a lineáris függvény.

Ha M egy rakéta, a testkontrollra (szabályzásra) azért van szükség, hogy az felügyelhető maradjon repülés közben, és meg kell bizonyosodni arról, hogy a_M tudja követni a_{Mc} parancsait. Például úgy, hogy egy „fel” utasításra a válasz tényleg „fel” és nem „lefelé” vagy „balra” legyen.⁶

A terminológiához kapcsolódó végrehajtás (kivitelezés)

Az irányítható rendszerek lehetnek önállóak vagy nem önállóak, attól függően, hogy az M kér-e az irányítási folyamat közben külső segítséget. Ilyen lehet például:

- egy referenciapont, LOS-irányítás esetén;
- a cél kiemelése, elektromágneses sugárzás alkalmazásával, félaktív rendszerek esetén;
- lézer célmegjelölés létrehozása.

Amennyiben a fent említett támogatások kellenek, akkor a rendszer nem önálló.

⁶ BRYSON 1985: 417.

Definíciók

Parancsadó rendszerek tekintetében azok a jelek, amelyeket a rakétára juttatnak (például rádióon vagy vezetékes vonalon), értelemszerűen nem függetlenek. Ezen folyamat során igen gyakran a geometriai szabályt alkalmazzák, vagyis a vizuális irányítást, ahol M egy OT sugarú körben tevékenykedik. Ekkor már parancsirányításról (CLOS⁷) beszélünk. Vannak ugyanakkor olyan parancsirányítási rendszerek, amelyek nem tartoznak a CLOS-kategóriába, példákat a következő fejezetben mutatok be. Ezzel ellentétben néhány LOS-irányítórendszer nem a parancsirányítási elven működik, mint például a félaktív lézerrányítás.

Az irányítási rendszerek, amelyekbe csupán M és T tartozik bele, prezentálják az M és T pontokat. Ezek az úgynevezett kétpontos rendszerek. Amikor egy harmadik pont elengedhetetlen, mint a LOS-irányítás esetén, a rendszer hárompontosá válik.⁸

A rendszer önirányítható, amennyiben M észleli a T célt, utóbbi kibocsátott energiájának köszönhetően. Ha a T energiaforrás kellően befogható, azaz keletkezik a rakéta célkoordinátorán valamilyen hasznos jel, mint például rádióadás, akusztikus zaj, hő, ekkor passzív önirányításról beszélünk. Az infravörös önirányítás a legelterjedtebb verzió, itt ugyanis a repülőgép-hajtómű kiáramló gázainak, a sárkányszerkezet felmelegedett elemeinek hősugárzását érzékeli a célkoordinátor. Ezeknek a rendszereknek több előnyös tulajdonsága is van, ilyen például a viszonylag egyszerű, olcsó felépítés, a nagy pontosság, valamint az a tény, hogy a rakéta indítása után a hordozó repülőgép azonnal kiválhat a manőverből, és elkezdheti egy másik, új cél támadását, vagy visszatérhet a bázisra. Ezt nevezzük a „Tűzelj és felejtsd el!” elvnek. Alkalmazásuknak csak a rossz időjárási viszonyok szabnak határt.

Ha a T-ről visszavert energia M-re sugárzik, akkor pedig aktív vagy félaktív önirányításról beszélünk. Közelebbről, a célról visszaverődött jeleket a rakéta célkoordinátora érzékeli, és a szükséges jelfeldolgozás után kiszűri belőle a szükséges információt a cél pozíciójáról és mozgásáról. A hasznos információk alapján kidolgozza az önirányító rendszerben az irányító jeleket, ami a kormánygépek segítségével módosítja a rakéta pályáját. Azokat a rendszereket, ahol a sugárzó berendezés is a rakéta fedélzetén található, aktív önirányításnak, ahol csupán a vevő berendezés van a rakéta fedélzetén, félaktív önirányításnak nevezzük (3. ábra).



3. ábra: (bal) aktív, (jobb) félaktív

Forrás: a szerző szerkesztése

⁷ CLOS: *command to line of sight* – parancsirányítású.

⁸ BRYSON 1985: 4120.

Példák

- a) Amikor a sólymok megkaparintják a prédát, passzív önirányítással irányítják magukat. Sokféle denevér használja az aktív önirányítást, ultrahangimpulzusokat kibocsátva.
- b) A félaktív önirányító rendszerek (mint például az Egyesült Államok által fejlesztett Sparrow légi harc rakétarendszer) nem önálló, nem sorolható a parancs-irányítási osztályba.
- c) A német második világháborús levegő-tenger bomba, a HS-293D (ami végül nem lett használható), TV-kamerával, illetve ennek megfelelő rádiókapcsolat létesítésére alkalmas eszközzel volt felszerelve. Mindezt úgy, hogy a bombát üzemeltető személy látta a repülőgép fedélzetén a bomba által megjelenített képet, ahogy az közeledett a cél felé. Az üzemeltető továbbította a cél pontos helyének paramétereit a bomba irányítórendszerére. Emiatt a berendezés parancsvezérlésű volt, de nem CLOS.
- d) A közép-hatótávolságú rakéta/bomba a repülés elején lehet parancsirányítású, és önirányítású a repülés második felében. Az izraeli Gabriel tenger-tenger rakéta irányítása repülés elején CLOS-irányítással történik, a második felében pedig félaktív önirányítással, arányos megközelítéssel (PN⁹) valósul meg. Egy föld-levegő rakétarendszer esetében, amely azonos irányítási szabályt használ, azaz a PN-t, a repülés mindkét szakaszára kiterjed, bár a repülés második felében itt is csupán az önirányítás érvényesül.
- e) Vannak légvédelmi rendszerek, ahol M befogja a T célt, és követi azt, majd továbbítja a paramétereit a földi irányítóállomásra. Ott elvégzik a szükséges kalkulációkat és átküldik azokat a rakétára (M), ahol az irányítórekeszben létrejött kormányelmozdulás-parancsokat az aktuátorok végrehajtják. Az efféle rendszerek mind a parancsirányítású, mind pedig az önirányítható kategóriákba egyaránt besorolhatók, mert a cél követése a rakéta révén valósul meg.

Geometria és kinematika

Ebben a részben több olyan fogalmat tisztázok, amelyeket a következő fejezetekben gyakran fogok alkalmazni.

Alapvető definíciók és jelölések

Legyen O a kiindulópontja egy inerciális referencia vonatkoztatási koordináta-rendszernek (FOC¹⁰). Az M és T helyzete ebben a FOC-ban az $\mathbf{r}_M$ és az $\mathbf{r}_T$ vektorok által megadottak, és a következő kapcsolatok írhatók fel:

⁹ PN: *proportional navigation* – arányos megközelítés.

¹⁰ FOC: *frame of coordinates* – vonatkoztatási koordináta-rendszer.

$$\mathbf{r}_M \triangleq OM \text{ és } \mathbf{r}_T \triangleq OT. \quad (1)$$

A kétpontos irányítási rendszerben a vektorok:

$$\mathbf{r} \triangleq \mathbf{r}_T - \mathbf{r}_M. \quad (2)$$

Ez szokványosan az úgynevezett hatótávolság. Amennyiben deriváljuk, a következőt kapjuk:

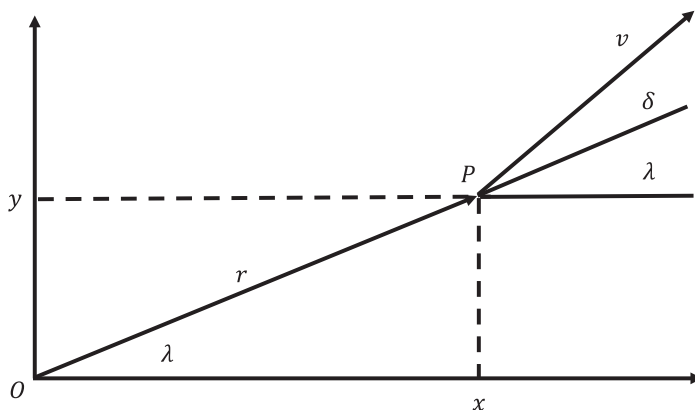
$$\dot{\mathbf{r}} = \dot{\mathbf{r}}_T - \dot{\mathbf{r}}_M \triangleq \mathbf{v}_T - \mathbf{v}_M. \quad (3)$$

Ez a relatív sebesség a két test között $\mathbf{v}_T$ és $\mathbf{v}_M$ a T és M sebességei. A zárósebesség kifejezést gyakran alkalmazzák irányítási folyamatokban, ennek képlete egyszerűen felírható:

$$\mathbf{v}_C \triangleq -\dot{\mathbf{r}}. \quad (4)$$

Általában az irányítási folyamat háromdimenziós (3D-) térben zajlik. Az *irányítás háromdimenziós kinematikájának jellegzetességei* című rész egy rövid emlékeztetőt tartalmaz a vektormozgás-egyenletekről 3D-ben.

A korábbiakban említettem, hogy a síkbeli viszonyoknál használt koordináta-rendszerben (x, y) vagy (x, z) helyen lévő szögek fogják kijelölni (pozitív, az óramutató járásával ellentétes irányban), hogy a harmadik tengely (azaz ami hiányzik) z vagy y lesz.¹¹



4. ábra: A síkbeli mozgás kinematikája

Forrás: a szerző szerkesztése SHNEYDOR 1998: 27 alapján

Legyen P a tengely egy adott helyén (x, y) és bírjon valamilyen v sebességgel. Meghatározzuk, hogy $\mathbf{r} \triangleq OP$, habár specifikus irányítási problémák esetében OP jelentheti $\mathbf{r}_T$ -t, vagy $\mathbf{r}_M$ -et. A 4. ábra alapján a következőket írhatjuk fel:

¹¹ BRYSON 1985: 425.

$$\mathbf{r} = x\mathbf{1}_x + y\mathbf{1}_y = (r \cos \lambda)\mathbf{1}_x + (r \sin \lambda)\mathbf{1}_y \quad (5)$$

és

$$\mathbf{v} = \dot{\mathbf{r}} = v_z\mathbf{1}_z + v_y\mathbf{1}_y, \quad (6)$$

ahol $\mathbf{1}_x$ és $\mathbf{1}_y$ az egységvektorok (r, λ) P polár koordinátái, és $v_x = \dot{x}$, $v_y = \dot{y}$.

A v sebesség két komponensre bontható r mentén. Az egyik a *radiális sebesség* (v_{rad}), $v_{||}$, a másik a *tangenciális sebesség* (v_{tan}), amelynek jele $v_{\perp}$. Ezek az értékek megadhatók a következő egyenletekkel

$$\begin{aligned} v_{||} &= \dot{r} = v \cos \delta \\ v_{\perp} &= \dot{r} = v \sin \delta, \end{aligned} \quad (7)$$

ahol δ az r és v közötti szög (4. ábra).

A $\gamma = \lambda + \delta$ szög, ami az x tengelyen keletkezik, P pályaszögének nevezzük. Emlékeznünk kell arra, hogy P pályadőlési szöge az (x, y) tengely mentén $\tan \gamma$.

Állandó v esetében, a jól ismert elemi mechanikából az a gyorsulás egy szorzatot eredményez

$$\mathbf{a} = v\dot{\gamma}. \quad (8)$$

Gyakran hasznos lehet a vektoros formulák alkalmazása síkbeli, valamint a 3D-s helyzetekben is.

Az a kifejezhető két vektor összegeként [lásd (22) egyenletet] r mentén, illetve

$$\mathbf{a} = \mathbf{a}_{||} + \mathbf{a}_{\perp} = (\ddot{r} - r\omega^2)\mathbf{1}_r + (r\dot{\omega} + 2\omega\dot{r})\mathbf{1}_t, \quad (9)$$

ahol $\omega = \dot{\lambda}$, $\mathbf{1}_r$ és $\mathbf{1}_t$ az egységvektorok r mentén. A (16) összefüggést követve

$$\omega = \frac{\|r \times v\|}{r^2} = \frac{xv_y - yv_x}{r^2}, \quad (10)$$

(28)-ből

$$\omega = \frac{v \sin \delta}{r} = \frac{v_{\perp}}{r}, \quad (11)$$

végül (19)-ből:

$$\dot{\mathbf{r}} = \frac{r \cdot v}{r} = \frac{xv_x + yv_y}{r} \quad (12)$$

Az irányítás háromdimenziós kinematikájának jellegzetességei

Ebben a fejezetben az irányítás háromdimenziós kinematikájának néhány jellegzetességét és általános képleteit vázolom fel röviden.

Az M irányított test, a T cél, és az inerciális vonatkoztatási koordináta-rendszer kiindulási pontjai az M , T és O . A OM és a OT jelölővektorok $\mathbf{r}_M$ és az $\mathbf{r}_T$, valamint az idő szerinti deriváltjuk, $\mathbf{v}_M$ és a $\mathbf{v}_T$ sebességek (5. ábra). Egy további differenciálás biztosítja a gyorsulásokat, amelyek jelölése $\mathbf{a}_M$ és $\mathbf{a}_T$. Az $\mathbf{r} \triangleq \mathbf{MT}$ hatótávolság megegyezik az $\mathbf{r}_T$ és az $\mathbf{r}_M$ vektorok különbségével, tehát

$$\begin{aligned}\mathbf{r} &= \mathbf{r}_T - \mathbf{r}_M \\ \dot{\mathbf{r}} &= \mathbf{v}_T - \mathbf{v}_M \\ \ddot{\mathbf{r}} &= \mathbf{a}_T - \mathbf{a}_M.\end{aligned}\tag{13}$$

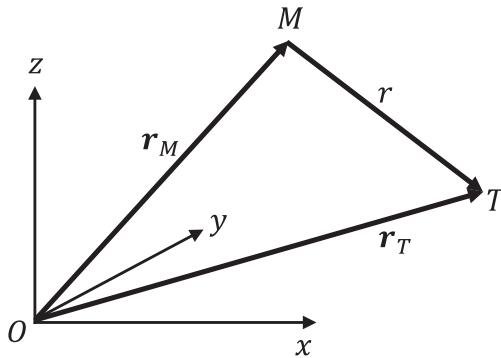
Meghatározás szerint az „ r ” a célzóvonal (LOS) látóterében helyezkedik el, amelynek sugara M -ből indul ki (kezdődik) és áthalad T -n. $\dot{\mathbf{r}}$ a relatív (viszonylagos) sebesség. Ezt két alkotóelemre lehet bontani a következőképpen:

$$\dot{\mathbf{r}} = \dot{r}\mathbf{1}_r + r\dot{\mathbf{1}}_r = \dot{r}\mathbf{1}_r + \mathbf{w} \times \mathbf{r},\tag{14}$$

ahol $\mathbf{1}_r$ az egységvektor „ r ” irányában, vagyis $\mathbf{1}_r = \mathbf{r}/r$. A „ $\mathbf{w}$ ” az „ $\mathbf{r}$ ” gyorsulási sebessége és „ $\times$ ” jelöli a vektori szorzatot. Ne feledjük, hogy $\dot{r}\mathbf{1}_r$ az $\dot{\mathbf{r}}$ összetevője párhuzamos $\mathbf{r}$ -rel, és a $\mathbf{w} \times \mathbf{r}$ komponense merőleges $\mathbf{r}$ -re.

Amennyiben megszorozzuk a (14) egyenletet $\mathbf{r}$ -rel (vektoros szorzat), az egyenlet a következőképp formálódik:

$$\mathbf{r} \times \dot{\mathbf{r}} = \dot{r}\mathbf{r} \times \mathbf{1}_r + \mathbf{r} \times (\mathbf{w} \times \mathbf{r}).$$



5. ábra: Találati geometria

Forrás: a szerző szerkesztése SHNEYDOR 1998: 218 alapján

Az egyenlet jobb oldalán lévő első formula nyilvánvalóan nullával egyenlő, a második része pedig $r^2 \mathbf{w}$ lesz, mivel $\mathbf{w}$ merőleges $\mathbf{r}$ -re.

Megjegyzem, hogy bármely $\mathbf{c}$ vektor és minden $\mathbf{1}_r$ egységvektor a vektor vegyes szorzata $\mathbf{1}_r \times (\mathbf{c} \times \mathbf{1}_r)$ megegyezik $\mathbf{c}$ merőleges összetevőjével, keresztezve $\mathbf{1}_r$ -t. Ezt $c_\perp$ -gal jelöltem. Az $\mathbf{1}_r$ mentén lévő összetevőt pedig $c_\parallel$ -gyel. Az ezek által adott szorzat $\mathbf{1}_r (\mathbf{c} \cdot \mathbf{1}_r)$, ahol a „ $\cdot$ ” skaláris szorzatot jelöl.¹² A könnyebb érthetőség érdekében:

$$\mathbf{c} = c_\perp + c_\parallel = \mathbf{1}_r \times (\mathbf{c} \times \mathbf{1}_r) + \mathbf{1}_r (\mathbf{c} \cdot \mathbf{1}_r). \quad (15)$$

Visszatérve az előzőekben felírt algebrai egyenletekhez, láthatjuk, hogy

$$\mathbf{w} = \frac{\mathbf{r} \times \dot{\mathbf{r}}}{r^2} = \frac{\mathbf{r} \times (\mathbf{v}_T - \mathbf{v}_M)}{r^2}. \quad (16)$$

A v_c zárósebesség kifejezésére a szakirodalomban rendszeresen alkalmazott forma a következő

$$v_c \triangleq -\dot{r} = v_M - v_T. \quad (17)$$

A (14) egyenletet szorozva $\mathbf{1}_r$ -rel (skaláris szorzattal) a következőt kapjuk:

$$\dot{\mathbf{r}} \cdot \mathbf{1}_r = (\dot{r} \mathbf{1}_r + \mathbf{w} \times \mathbf{r}) \cdot \mathbf{1}_r = \dot{r} \quad (18)$$

Köztudott, hogy $\mathbf{1}_r \cdot \mathbf{1}_r = 1$ és $(\mathbf{w} \times \mathbf{r}) \cdot \mathbf{1}_r = 0$. Ezért

$$\dot{r} = \frac{\mathbf{r} \cdot \dot{\mathbf{r}}}{r} = \frac{\mathbf{r} \cdot (\mathbf{v}_T - \mathbf{v}_M)}{r}. \quad (19)^{13}$$

Például ha $\mathbf{v}_T = [100 \ 200 \ 0]^T$, $\mathbf{v}_M = [0 \ 400 \ 600]^T$ és $\mathbf{r} = [2000 \ 0 \ 0]^T$ (m/s-ban és m-ben), akkor segítségül a (16) egyenletet hívjuk:

$$\mathbf{w} = \frac{1}{2000^2} \begin{vmatrix} 1_x & 2000 & 100 - 0 \\ 1_y & 0 & 200 - 400 \\ 1_z & 0 & 0 - 600 \end{vmatrix} = \begin{vmatrix} 0 \\ 0,3 \\ -0,1 \end{vmatrix} \text{ rad/sec}.$$

A (19) összefüggésből pedig:

$$\dot{r} = \frac{1}{2000} [2000 \ 0 \ 0] \begin{bmatrix} 100 - 0 \\ 200 - 400 \\ 0 - 600 \end{bmatrix} = 100 \text{ m/s}.$$

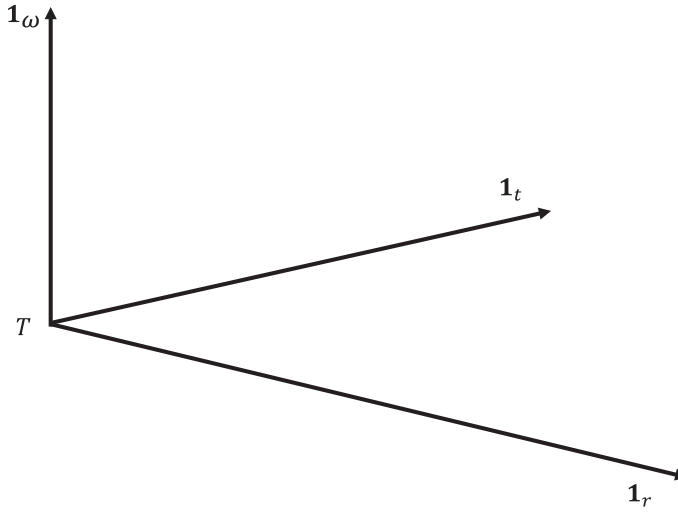
¹² ETKIN 1982: 34.

¹³ Megjegyzés: $\dot{\mathbf{r}} \neq \|\dot{\mathbf{r}}\|$ kivéve, ha $\dot{\mathbf{r}}$ és $\mathbf{r}$ kollineárisak.

Forgó vonatkoztatási koordináta-rendszer

Elemzések alapján, egy forgó FOC, amelynek tengelye mentén az egységvektorok $\mathbf{1}_\omega$, $\mathbf{1}_r$ és $\mathbf{1}_t$, ahol $\mathbf{1}_\omega = \mathbf{w}/\omega$, $\omega = \|\mathbf{w}\|$ és $\mathbf{1}_t = \mathbf{1}_\omega \times \mathbf{1}_r$ (6. ábra). Legyen a forgási tengely vektor-szögsebessége $\mathbf{w}_{tri}$ és $v_\parallel$ jelezze a $\mathbf{w}_{tri}$ komponenst r mentén, oly módon, hogy

$$\mathbf{w}_{tri} = \omega \mathbf{1}_\omega + \omega_\parallel \mathbf{1}_r \quad (20)$$



6. ábra: T középpontú FOC

Forrás: a szerző szerkesztése SHNEYDOR 1998: 219 alapján

Ahol $\omega_\parallel = \|\mathbf{w}_\parallel\|$. Ebből ered a vektorszorzatok kijelölése és a jellemzői, hogy

$$\begin{aligned} \dot{\mathbf{1}}_r &= \mathbf{w}_{tri} \times \mathbf{1}_r = \omega \mathbf{1}_t \\ \dot{\mathbf{1}}_r &= \mathbf{w}_{tri} \times \mathbf{1}_t = -\omega \mathbf{1}_r + \omega_\parallel \mathbf{1}_\omega \\ \dot{\mathbf{1}}_\omega &= \mathbf{w}_{tri} \times \mathbf{1}_\omega = -\omega_\parallel \mathbf{1}_t. \end{aligned} \quad (21)$$

Ezeket az egyenleteket alkalmazva a (14) és (20) révén a következő eredményeket érjük el

$$\dot{\mathbf{r}} = \dot{r} \mathbf{1}_r + r \omega \mathbf{1}_t \quad (22)$$

$$\ddot{\mathbf{r}} = (\ddot{r} - r\omega^2) \mathbf{1}_r + (r\dot{\omega} + 2\dot{r}\omega) \mathbf{1}_t + r\omega\omega_\parallel \mathbf{1}_\omega. \quad (23)$$

Az első kifejezést (22) v_{rad} (radiális vagy sugárirányú), a másodikat (23) v_{tan} pedig tangenciális (érintőleges) sebességnek nevezik.¹⁴

Síkbeli vektorok

Elmondhatjuk, hogy v_T , v_M és r azonos síkban helyezkednek el. Ennek a szükséges és elégséges feltétele az, hogy bármelyik három skaláris szorzata nullával egyenlő. Részletesebben:

$$\begin{cases} v_T \cdot (r \times v_M), \\ r \cdot (v_M \times v_T), \\ \text{vagy} \\ v_M \cdot (v_T \times r) \end{cases} \quad (24)$$

Tehát a három szorzat azonos egymással.

A vektorok összetevőit kifejezve a következő feltételeket fogalmazhatjuk meg:

$$D \triangleq \begin{vmatrix} v_{Tx} & v_{Ty} & v_{Tz} \\ r_x & r_y & r_z \\ v_{Mx} & v_{My} & v_{Mz} \end{vmatrix} = 0. \quad (25)$$

Észrevehető, hogy ha bármelyik két vektor a háromból egy síkbeli (kolineáris), akkor $D = 0$.

Tegyük fel, hogy v_T , v_M és r egy síkban vannak. Így a következőt állíthatjuk:

$$v_T \cdot w = v_T \cdot \frac{r \times (v_T - v_M)}{r^2} = \frac{v_T \cdot (r \times v_T) - v_T \cdot (r \times v_M)}{r^2} \quad (26)$$

Az egyenlet első felében a számláló nullával egyenlő, a skalár- és vektorszorzatok jellegzetességei miatt. Az egyenlet második fele szintén zérus a síkbeli ütközés okán (24). Így az egész egyszerűsítve:

$$v_T \cdot w = 0 \quad (27)$$

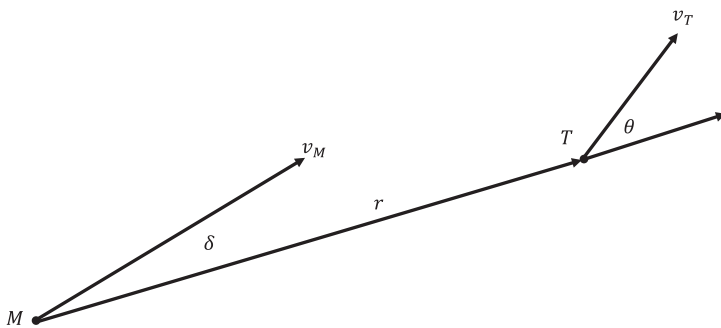
Hasonlóképpen $v_M \cdot w = 0$, és már tudjuk, hogy az $r \cdot w = 0$ meghatározás szerint. Vagyis a síkbeli egyezések (ütközések) okán, w merőleges mind a v_T , v_M és az r vektorokra és kolineáris mind $r \times v_T$ és $r \times v_M$ skalárszorzataikkal.

Az r és a v_T közti, valamint az r és v_M közti szögeket θ vonatkozási és δ metszési szöggel jelöljük. A síkbeli helyzetben mindkettő meghatározott, a tengelyek körül párhuzamosan w -vel (7. ábra). Ebből a (16) egyenlet és a vektorszorzat definíciójából

$$w = \frac{v_T \sin \theta - v_M \sin \delta}{r} \quad (28)$$

$$\dot{r} = v_T \cos \theta - v_M \cos \delta \quad (29)$$

¹⁴ MCLEAN 1990: 17.



7. ábra: θ vonatkozási, és δ metszési szögek

Forrás: a szerző szerkesztése SHNEYDOR 1998: 221 alapján

A (28) és (29) egyenletekből nyilvánvaló, hogy

$$\cos \theta = \frac{r \cdot v_T}{r v_T} \quad (30)$$

A meghatározás lehet pozitív vagy negatív (nem általában, azt vételezve, hogy $0 \leq \theta \leq \pi$), aszerint, hogy $r \times v_T$ -t érzékeli-e w , vagy azzal ellentétes. Más szavakkal

$$\text{sgn } \theta = \text{sgn}\{(r \times v_T) \cdot w\} \quad (31)$$

Megemlítem, hogy (31) és (16), amely $v_M = 0 \rightarrow \theta > 0$. Hasonlóképpen, $v_T = 0 \rightarrow \delta < 0$.

Ha r kolineáris v_T -vel, a kapcsolat kétségtelenül síkbeli, amiképp a $D = 0$, és θ is 0, vagy 180° , hasonlóan r , v_M és δ is. Ugyanebből a megfontolásból a kapcsolat szintén síkbeli, ha a v_T és a v_M egyaránt kolineáris. Ekkor $\delta = \theta$ vagy $\delta = \theta \pm \pi$

Abban az esetben, ha mind a három vektor egyvonalú, triviális.

Példák

Az irányítás háromdimenziós mozgástanának egyszerűbb megértését két példán keresztül mutatom be.

1. példa

Az első példában állandó vektorokkal számolok. Legyen v_T , v_M és r megadott értékekkel.¹⁵ Ezek $v_T = [-200 \ -100 \ 100]^T$, $v_M = [-100 \ 400 \ 500]^T$, $r = [-3000 \ 6000 \ 9000]^T$ (m/s-ban és méterben, adott esetben). Ez egy síkbeli ütközés (kapcsolat), mivel

¹⁵ JENKINS 1984: 43.

$$D = \begin{vmatrix} -200 & -100 & 100 \\ -3000 & 6000 & 9000 \\ -100 & 400 & 500 \end{vmatrix} = 0.$$

Mivel $\dot{r} = [-100 \quad -500 \quad -400]^T$, a következő eredményt nyerjük a (16) és (19) egyenletekből

$$w = \frac{1}{r^2} \begin{vmatrix} 1_x & -3000 & -100 \\ 1_y & 6000 & -500 \\ 1_z & 9000 & -400 \end{vmatrix} = \frac{1}{60} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} \text{ rad/s}$$

és

$$\dot{r} = \frac{10^2 \times 10^3}{r} [-3 \quad 6 \quad 9] \begin{bmatrix} -1 \\ -5 \\ -4 \end{bmatrix} = -561 \text{ m/s},$$

ahol $r = \|r\| = \sqrt{(-3000)^2 + 6000^2 + 9000^2} = 1000\sqrt{126}$.

A (30) relációt alkalmazva

$$\cos \theta = \frac{1}{rv_T} [-200 \quad -100 \quad 100] \begin{bmatrix} -3000 \\ 6000 \\ 9000 \end{bmatrix}$$

$$\cos \delta = \frac{1}{rv_M} [-100 \quad 400 \quad 500] \begin{bmatrix} -3000 \\ 6000 \\ 9000 \end{bmatrix},$$

ahol $v_T = \|v_T\| = 100\sqrt{6}$ és $v_M = \|v_M\| = 100\sqrt{42}$.
Ezért $|\theta| = 70,9^\circ$, $|\delta| = 8,2^\circ$.

Annak érdekében, hogy a fenti jelek a helyes szögben legyenek, figyelembe kell vennünk, hogy

$$r \times v_T = \begin{vmatrix} 1_x & -3000 & -200 \\ 1_y & 6000 & -100 \\ 1_z & 9000 & 100 \end{vmatrix} = 10^5 \begin{bmatrix} 15 \\ -15 \\ 15 \end{bmatrix}$$

$$r \times v_M = \begin{vmatrix} 1_x & -3000 & -100 \\ 1_y & 6000 & 400 \\ 1_z & 9000 & 500 \end{vmatrix} = 10^5 \begin{bmatrix} -6 \\ 6 \\ -6 \end{bmatrix}.$$

Mivel $w = (1/60)[1 \quad -1 \quad 1]^T$, így végül a (30)-ból következik, hogy θ pozitív, miközben δ negatív előjelű lesz, azaz

$$\theta = 70,9^\circ, \delta = -8,2^\circ.$$

Ellenőrzésül újra tudjuk számítani w -t és $\dot{r}$ -t, a (27) és (28) egyenleteket felhasználva.

$$w = \frac{100\sqrt{6} \sin 70,9^\circ + 100\sqrt{42} \sin 8,2^\circ}{1000\sqrt{126}} = 0,0289 \frac{\text{rad}}{\text{s}},$$

ami megegyezik $(1/60)\sqrt{3}$, amelyet fentebb felírtam, és

$$\dot{r} = 100\sqrt{6} \cos 70,9^\circ - 100\sqrt{42} \cos 8,2^\circ = -561 \text{ m/s}.$$

2. példa

A második feltevésben a vektorok időben változók lesznek. Tegyük fel, hogy M mozdulatlan a vonatkoztatási koordináta-rendszerben, míg a T egy egyenes henger mentén halad a z tengely mentén. Más szavakkal, mozgása kör alakú spirált rajzol. Az r hatótávolság és a v sebesség adottak, az egyenletek alapján:

$$r(t) = \begin{bmatrix} x(t) \\ y(t) \\ z(t) \end{bmatrix} = \begin{bmatrix} c \cos \Omega t \\ c \sin \Omega t \\ vt \sin \gamma \end{bmatrix}, \quad v(t) = \begin{bmatrix} -c\Omega \sin \Omega t \\ c\Omega \cos \Omega t \\ v \sin \gamma \end{bmatrix}, \quad (32)$$

ahol c a henger sugara, Ω a körfrekvencia, v a T sebessége és γ a repülési pálya szöge. Az (32) egyenletekből

$$c\Omega = v \cos \gamma \quad (33)$$

és

$$c = r \cos \theta, \quad z = r \sin \theta, \quad (34)$$

ahol θ a T emelkedési szöge. $z = 0$.

(16) és (32)–(34) képletekből a következő összefüggést kapjuk w -re

$$w = \frac{v}{r} \begin{bmatrix} \cos \theta(t) \sin \gamma \sin(\Omega t) - \sin \theta(t) \cos \gamma \cos(\Omega t) \\ -\cos \theta(t) \sin \gamma \cos(\Omega t) - \sin \theta(t) \cos \gamma \sin(\Omega t) \\ \cos \theta(t) \cos \gamma \end{bmatrix}. \quad (35)$$

Emlékezzünk arra, hogy az r -t az idő függvényében szemléljük.¹⁶ Az a (vagy $\dot{v}$) gyorsulás egyértelmű

$$a = \begin{bmatrix} -\Omega^2 c \cos(\Omega t) \\ -\Omega^2 c \sin(\Omega t) \\ 0 \end{bmatrix}. \quad (36)$$

Megjegyzem, hogy az $a = \Omega^2 c$ a nagyságára (mértére, terjedelmére) vonatkozik, továbbá állandó és független γ -tól.

A (19) egyenletet alkalmazva (32)-höz a következőt nyerjük:

$$\dot{r} = \frac{1}{r} (v \sin \gamma)^2 t, \quad (37)$$

$\ddot{r}$ a (37) differenciálásából adódik.

Annak érdekében, hogy minél több rálátást nyerjünk a pillanatnyi geometriai helyzetre, „befagyasztjuk” a mozgásokat egy időpontban, így $\cos(\Omega t) = 1$ és $\sin(\Omega t) = 0$. A vektorok

$$r(t) = \begin{bmatrix} c \\ 0 \\ z \end{bmatrix} = r \begin{bmatrix} \cos \theta \\ 0 \\ \sin \theta \end{bmatrix}, \quad v(t) = v \begin{bmatrix} 0 \\ \cos \gamma \\ \sin \gamma \end{bmatrix} \quad (38)$$

és

$$w = \frac{v}{r} \begin{bmatrix} -\sin \theta \cos \gamma \\ -\cos \theta \sin \gamma \\ \cos \theta \cos \gamma \end{bmatrix}. \quad (39)$$

Mivel a forgási sebességvektor a koordináta-rendszerben

$$w_{tri} = v \begin{bmatrix} 0 \\ -(c \sin \gamma)/r^2 \\ (\cos \gamma)/c \end{bmatrix} = \frac{v}{r} \begin{bmatrix} 0 \\ -\cos \theta \sin \gamma \\ (\cos \gamma)/\cos \theta \end{bmatrix}, \quad (40)$$

$w_{\parallel}$ így már könnyen meghatározható, $w_{tri} - w$ különbségeiből. Ez a következő egyenletet adja:

$$w_{\parallel} = \frac{v \cos \gamma \tan \theta}{r} \begin{bmatrix} \cos \theta \\ 0 \\ \sin \theta \end{bmatrix}. \quad (41)$$

Miután meghatároztuk r és w -t, ezáltal $\mathbf{1}_r$ és $\mathbf{1}_w$ -t, megkapjuk $\mathbf{1}_t$ -t az $\mathbf{1}_t = \mathbf{1}_w \times \mathbf{1}_r$ relációból.

¹⁶ REGAN 1993: 27.

Összefoglalás

A rakétairányítási és célbefogási folyamatok rendkívül összetett és bonyolult rendszerek, amelyek a modern katonai és űrtechnológiai felhasználások alapkövei. Ezen folyamatok magukban foglalják a rakéták pályájának megtervezését, a célok követését és a precíziós találatok végrehajtását, figyelembe véve a dinamikai és statikai tényezőket.

Ezen rendszerek alapvetően két fő fázisból állnak: a tervezésből és a végrehajtásból. A tervezési fázis során a rendszerek különféle algoritmusokat és matematikai modelleket használnak a rakéta optimális pályájának meghatározására. Ez a folyamat figyelembe veszi a rakéta sebességét, a cél mozgásának dinamikáját, valamint a környezeti feltételeket, mint például a légköri ellenállást.¹⁷

A végrehajtási fázisban a rakéta irányításáért felelős rendszerek valós időben elemzik a kapott adatokat, és szükség esetén módosítják a pályát. A célbefogás során a rakéta képes reagálni a cél mozgásának változásaira, alkalmazkodva a helyzethez, így emelve a találat valószínűségét. A bonyolultságot fokozza, hogy a modern rakéták nemcsak passzív szenzorokat használnak, hanem aktív irányítórendszereket is, amelyek lehetővé teszik a célok dinamikus követését.

A folyamatok komplexitása abban is rejlik, hogy a rakéták irányítása gyakran többszintű rendszereket igényel, amelyek integrálják a műholdas navigációt, a radartechnológiát és a számítógépes szimulációkat. Az ilyen rendszerek fejlesztése és működtetése komoly technológiai kihívásokkal jár.¹⁸

Összességében a rakétairányítási és célbefogási folyamatok egy olyan multidiszciplináris területet képviselnek, amely a matematikai modellezés, az informatikai rendszerek, a fizika- és a mérnöki tudományok egyesítésével működik, és folyamatos innovációt kíván, a hatékonyság és a biztonság növelése érdekében.

Felhasznált irodalom

- BLAKELOCK, John H. (1991): *Automatic Control of Aircraft and Missiles, Second Edition*. New Jersey: Wiley.
- BRYSON, Arthur E. (1985): New Concepts in Control Theory, 1959–1984. *Journal of Guidance, Control and Dynamics*, 8(4), 417–425. Online: <https://doi.org/10.2514/3.20000>
- ETKIN, Bernard (1982): *Dynamics of Flight – Stability and Control, Second Edition*. New York: John Wiley.
- JENKINS, Philip N. (1984): *Missile Dynamic Equations for Guidance and Control Modeling and Analysis*. Redstone Arsenal, Alabama: U.S. Army Missile Command.
- KORN, Granino A. – KORN, Theresa M. (1968): *Mathematical Handbook for Scientists and Engineers*. London: McGraw-Hill.
- MCLEAN, Donald (1990): *Automatic Flight Control Systems*. New York: Prentice Hall.

¹⁷ SHNEYDOR 1998: 29.

¹⁸ KORN–KORN 1968: 41.

- REGAN, Frank J. – ANANDAKRISHNAN, Satya M. (1993): *Dynamics of Atmospheric Re-Entry*. Washington, D.C.: American Institute of Aeronautics and Astronautics. Online: <https://doi.org/10.2514/4.861741>
- SHNEYDOR, N. A. (1998): *Missile Guidance and Pursuit Kinematics, Dynamics and Control*. Chichester: Horwood Publishing. Online: <https://doi.org/10.1533/9781782420590>

Benke Bálint Péter¹

A kriptovaluták kettős arca

A kriptovaluták által nyújtott technológiai
innovációk szerepe a kiberbűncselekményekben,
1. rész

The Dual Nature of Cryptocurrencies

The Impact of Technological Innovations behind Cryptocurrencies on Cybercrime, Part 1

Absztrakt

A digitális világ dinamikus fejlődése alapjaiban alakította át a pénzügyi tranzakciók működését, amelyben a kriptovaluták megjelenése új korszakot nyitott. Az olyan decentralizált eszközök, mint a Monero, Zcash és Dash lehetővé teszik az anonim és gyors pénzmozgásokat, komoly kihívások elé állítva a hagyományos ellenőrzési mechanizmusokat. Bár e technológiák számos előnyt hordoznak, jelentős biztonsági kockázatokat is rejtnek. Anonimitásuk és szabályozatlanságuk különösen vonzóvá teszi őket a bűnözők számára pénzmosás, csalás, zsarolóvírus-támadások és terrorizmusfinanszírozás céljára. A dark web piacterei tovább erősítik ezen eszközök illegális felhasználását azáltal, hogy anonim hozzáférést biztosítanak illegális szolgáltatásokhoz, jelentősen megnehezítve a bűnüldöző szervek munkáját. A tanulmány sorozat első része a releváns tudományos és szakirodalom feldolgozásán, valamint esettanulmányok elemzésén keresztül ad áttekintést a témáról. A második rész empirikus kutatásra támaszkodva vizsgálja a rendvédelmi szervek gyakorlati tapasztalatait a kriptovalutákhoz kötődő bűncselekményekkel kapcsolatban.

Kulcsszavak: kiberbűnözés, kriptovaluta, privacy coin, bűnüldözés, anonimitás

¹ Okleveles kiberbiztonsági és nemzetközi biztonság- és védelempolitikai szakértő, e-mail: benke.balint@proton-mail.com

Abstract

The dynamic evolution of the digital world has fundamentally transformed the nature of financial transactions, ushering in a new era with the emergence of cryptocurrencies. Decentralised assets such as Monero, Zcash, and Dash enable fast and anonymous transfers, posing significant challenges to traditional regulatory mechanisms. While these technologies offer several benefits, they also entail serious security risks. Their anonymity and lack of oversight make them particularly attractive to criminals for activities such as money laundering, fraud, ransomware attacks, and terrorism financing. Dark web marketplaces further amplify their illicit use by facilitating anonymous access to illegal services, significantly complicating the work of law enforcement agencies. The first part of the study series provides an overview of the topic through the analysis of relevant scientific and professional literature, as well as case studies. The second part builds on empirical research to examine the practical experiences of law enforcement agencies regarding crimes related to cryptocurrencies.

Keywords: cybercrime, cryptocurrency, privacy coin, law enforcement, anonymity

Bevezetés

A pénz fogalmának értelmezése a 21. századra jelentős átalakuláson ment keresztül, amelynek egyik legmarkánsabb megnyilvánulása a blokkláncalapú, digitális fizetőeszközök – azaz kriptovaluták – elterjedése. Ezen eszközök közül külön figyelmet érdemelnek az úgynevezett privacy coin²-ként kategorizált valuták (például monero, zcash, dash), amelyek működésükből fakadóan fokozott anonimitást biztosítanak a tranzakciók során. Ezek a technológiai megoldások megnehezítik a pénzügyi felügyeleti szervek számára a tranzakciók ellenőrzését és visszakövetését.

Az Európai Unió több jogalkotási megoldással igyekszik reagálni a kriptoeszközök által támasztott pénzügyi és bűnüldözési kihívásokra. A legfrissebb 2024-es szabályozás, a 6. pénzmosás elleni irányelv (AMLD6) már kifejezetten nevesíti a kriptoeszközöket mint pénzmosásra alkalmas vagyonformát, és kötelező regisztrációs, valamint ügyfél-azonosítási kötelezettséget ír elő a kriptotőzsdék és tárcaszolgáltatók számára. Az irányelv egyúttal külön büntetőjogi státuszt biztosít a pénzmosásnak mint önálló bűncselekménynek, kiterjesztve a büntethetőséget a segítő személyekre, a pénzmosásból származó javak átruházóira, valamint a jogi személyek felelősségére is.³

A 2023-ban elfogadott Markets in Crypto-Assets Regulation (MiCA), valamint a vele párhuzamosan bevezetett Anti-Money Laundering Regulation (AMLR) célja a kriptoeszközök piacának átláthatóvá tétele, a fogyasztóvédelem erősítése, továbbá

² A *privacy coin*ok olyan kriptovaluták, amelyeket kifejezetten a tranzakciók anonimitására és a felhasználók adatainak védelmére terveztek. Ezek a kriptovaluták, mint például a monero vagy a zcash speciális kriptográfiai technikákat alkalmaznak (mint a *ring signature* vagy zk-SNARK), hogy elrejtsek a tranzakciós felek címét, az összegeket és a tranzakciók láncolatát.

³ Az Európai Unió és a Tanács (EU) 2024/1640 irányelve.

a pénzmosás megelőzése.⁴ A szabályozási törekvések azonban nemcsak európai szinten jelennek meg. A nemzetközi szervezetként működő Pénzügyi Akciócsoport (FATF) a kriptoeszközökkel kapcsolatos pénzmosás és terrorizmusfinanszírozás-ellenes szabályok kialakításában is szerepet vállal. Az FATF 2019-es ajánlásai értelmében a kriptoeszköz-szolgáltatókra ügyfélazonosítási és tranzakciókövetési kötelezettségek vonatkoznak. Ezek közül kiemelkedik a Travel rule elnevezésű előírás, amely szerint a kriptoeszközök továbbításakor a tranzakcióban részt vevő felek adatait is rögzíteni kell. Az ilyen ajánlások világszerte alapul szolgálnak a nemzeti szabályozások kialakításához.⁵

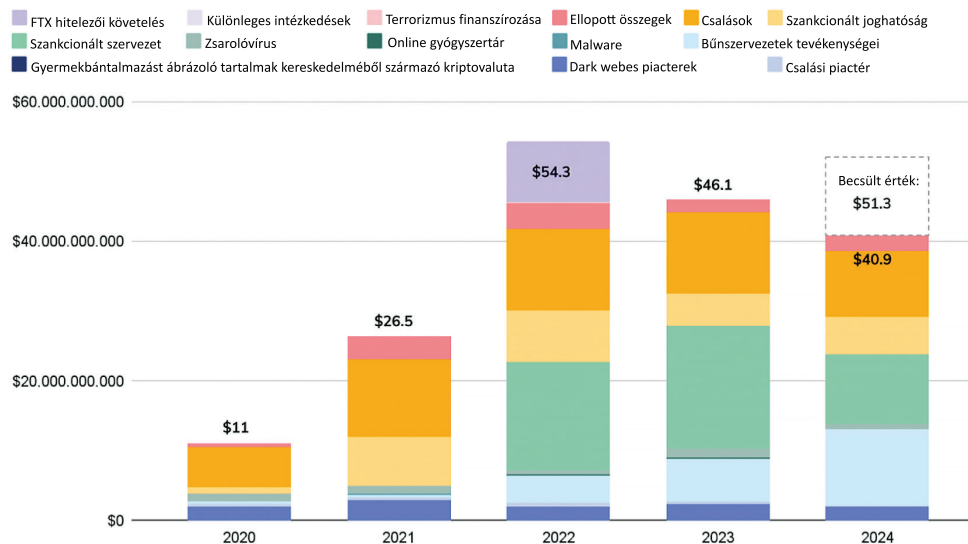
A felsorolt jogszabályi normák hatálya ugyanakkor elsősorban a centralizált, illetve a hagyományos webes felületeken működő kriptotőzsdékre és szolgáltatókra terjed ki. Az olyan decentralizált vagy anonimitásra épülő megoldások, mint a privacy coinokat támogató rendszerek vagy a dark weben működő escrow (letéti) platformok technológiai sajátosságaik révén kívül esnek az intézményesített felügyelet hatókörén, így ezek ellenőrizhetősége továbbra is korlátozott. Ahogy a kriptovaluták egyre szélesebb körben ismertté és hozzáférhetővé válnak, a felhasználók körében egyre erősebben megjelenik a kimaradástól való félelem (FOMO⁶) érzése is, ami jelentősen hozzájárul a felhasználói bázis gyors bővüléséhez. Ez a növekedés azonban nemcsak a pénzügyi és technológiai fejlődést támogatja, hanem sok laikus felhasználója is lesz az ilyesfajta vagyonelemeknek, ami párhuzamosan együtt jár azzal is, hogy a kriptovaluták bűncselekményekhez való felhasználása is fokozódik, kiemelten a csalások terén.

A kriptovaluták előnyei – mint a pénzügyi szabadság, az adatvédelem vagy a globális hozzáférés – vitathatatlanok, ugyanakkor fennáll a veszélye, hogy ugyanezek az eszközök visszaélésekre, csalásokra, pénzmosásra és kiberbűncselekmények támogatására is felhasználhatók. Az elmúlt években drasztikusan nőtt azoknak a kriptovaluta-összegeknek a mennyisége, amelyeket jogellenes tevékenységekhez kötöttek. A Chainalysis 2025-ös Crypto Crime Reportja szerint például 2022 óta jelentős mértékben emelkedett az illegális célokra felhasznált digitális eszközök aránya, amint az az 1. ábrán látható. Az illegális tranzakciók azonosítása és visszakövetése rendkívül komplex, idő- és erőforrás-igényes feladat a bűnüldöző hatóságok számára. A helyzet súlyosságát fokozza, hogy ezeknek a szervezeteknek nemcsak a gyorsan változó technológiai környezettel, hanem az egyre felkészültebb bűnelkövetőkkel is versenyt kell futniuk.

⁴ Az Európai Unió és a Tanács (EU) 2023/1114 rendelete; Az Európai Unió és a Tanács (EU) 2024/1624 rendelete.

⁵ FATF 2021.

⁶ A FOMO (*fear of missing out*), vagyis a kimaradástól való félelem egy pszichológiai jelenség, amely során az egyén szorongást él át attól tartva, hogy lemarad valamilyen számára előnyös vagy népszerű eseményről, lehetőségéről. A kriptovaluták világában ez gyakran ösztönöz impulzív befektetési döntéseket a hirtelen árfolyam-emelkedések vagy piaci trendek hatására.



1. ábra: A bűncselekményekhez köthető kriptovaluta-tranzakciók becsült éves összértékének alakulása 2020 és 2024 között, milliárd dollárban

Megjegyzés: Az adatok a vizsgált időszakban folyamatos növekedést mutatnak, 2022-ben érve el a csúcst (54,3 milliárd USD), majd 2023-ban kisebb visszaesés következett be (46,1 milliárd USD). A 2024-es becslés (51,3 milliárd USD) arra utal, hogy a piac részben visszanyerte korábbi szintjét. A változások hátterében jelentős események – például a Hydra Market 2022-es bezárása – álltak, amelyek szerkezeti átrendeződést és új szereplők megjelenését eredményezték.

Forrás: a szerző szerkesztése Chainalysis 2025 alapján

A fentiek alapján megállapítható, hogy a kriptovaluták köztudatban és gazdaságban való elterjedése, valamint azok anonimitást biztosító technológiai sajátosságai komoly kihívás elé állítják a jogalkalmazó szerveket, különösen a bűncselekmények nyomozásának és a pénzügyi visszaélések felderítésének területén. Az anonim tranzakciók térnyerése elősegíti, hogy a kriptovaluták a kiberbűnözés, pénzmosás, csalás vagy éppen zsarolóvírusos támadások eszközeivé váljanak. Ennek hátterében olyan technikai megoldások állnak, mint a coin mixerek, a decentralizált tőzsdék vagy az úgynevezett privacy coinok, amelyek jelentősen megnehezítik a tranzakciók visszakövethetőségét és a bűnelkövetők azonosítását.

Ebből fakadóan e tanulmány kutatási célkitűzései az alábbiak szerint foglalhatók össze:

1. Feltérképezni, hogy mely kriptovalutákat használják leggyakrabban bűnelkövetések során.
2. Bemutatni és elemezni azokat a technikákat és módszereket, amelyeket a bűnözők a kriptovaluta-tranzakciók elrejtésére és a visszakövetés megnehezítésére alkalmaznak.
3. Azonosítani a kriptovalutákhoz kapcsolódó leggyakoribb bűncselekménytípusokat és azok jellemzőit.

A kutatás során az alábbi kérdésekre kerestem választ:

1. Mely kriptovaluták a leggyakoribb eszközei a különböző típusú bűncselekményeknek?
2. Milyen technológiai eszközökkel és módszerekkel igyekeznek a bűnelkövetők eltüntetni vagy elrejtetni a kriptovaluta-tranzakciók nyomait?

A fenti szempontok alapján a kutatáshoz az alábbi hipotéziseket fogalmaztam meg:

H1: A bitcoin továbbra is a leggyakrabban alkalmazott kriptovaluta a kiberbűnözésben, azonban a privacy coinok és az ethereum szerepe növekszik, ami új bűnügyi trendek és kihívások megjelenéséhez vezet.

H2: A kriptovalutákkal kapcsolatos bűncselekmények elkövetői folyamatosan alkalmazzák az anonimizálást és a visszakövethetőség akadályozását szolgáló technológiákat – például coin mixereket, privacy coinokat és decentralizált tőzsdéket –, ami változó és összetett kihívást jelent a bűnüldöző hatóságok számára.

Módszertan

A tanulmány kvalitatív módszertani elemeket alkalmaz, kombinálva az elméleti és az esettanulmány-alapú megközelítéseket. A kutatás első szakaszában szisztematikus szakirodalmi áttekintést végzek, amelynek célja a kriptovalutákhoz köthető bűncselekménytípusok, a kapcsolódó technológiai eszközök, valamint azok bűnügyi relevanciájának feltérképezése volt.

A szakirodalmi keresés során a Scopus és IEEE Xplore adatbázisok szolgáltak elsődleges forrásként. A keresések során alkalmazott kulcsszó-kombinációk a következők voltak: „cryptocurrency AND cybercrime”, „privacy coin AND money laundering”, „cryptocurrency AND ransomware”, „cryptocurrency AND dark web”. A találatok szűrése relevancia, szakmai elismertség (Scimago Journal Rank Q1 – Q2 besorolás), valamint publikációs aktualitás alapján történt. Az elméleti keret kiegészítéseként bevontam olyan szakmailag elismert, nem lektorált, de megbízható forrásokból származó jelentéseket, elemzéseket és hírközléseket is, különösen a Chainalysis és TRM Labs publikációit, amelyek az aktuális fejleményekről gyakran a tudományos közléseket megelőzően számolnak be.

A kvalitatív módszertani részben célzott mintavétellel kiválasztott esettanulmányokat elemeztem. A válogatás szempontját az adott fejezetek tematikus fókuszához való illeszkedés, valamint az a cél jelentette, hogy az esetek a szakirodalomban leírt elméleti kategóriákat szemléletesen illusztrálják, és hozzájáruljanak a kriptovaluta-alapú bűncselekmények gyakorlati kontextusának jobb megértéséhez. A kiválasztás további meghatározó szempontja az volt, hogy az esettanulmányok hazai jelentőségűek legyenek, mint például az UNIX Autó Kft.-t ért zsarolóvírus-támadás, vagy a nemzetközi szinten a legjelentősebb ügyek közé sorolhatók legyenek, mint a Bitconnect csalási eset vagy Colonial Pipeline elleni zsarolóvírus-támadás.

A kvantitatív adatok a *Chainalysis Crypto Crime Report* 2024-es és 2025-ös kiadásain alapulnak, amelyek megbízható és naprakész statisztikai információkat szolgáltatnak a kriptovalutákhoz köthető bűncselekmények volumenére, típusaira és dinamikájára vonatkozóan.

A tanulmány felépítése az IMRAD módszert követi, amely magában foglalja a bevezetést, a kutatási módszertant, az eredmények fejezetet és a diszkussziót. A bevezetés ismerteti a kutatás hátterét és célkitűzéseit, a módszertan fejezet részletezi az alkalmazott kutatási eljárásokat, míg az eredmények rész bemutatja a kriptovalutákkal kapcsolatos bűncselekménytípusok főbb fajtáit és jellemzőit. A diszkusszió fejezet a hipotézisek vizsgálatának eredményeit tézisszerűen összegzi, majd ezek értelmezésével és kifejtésével betölti a záró következtetések fejezet funkcióját.

A módszertani kialakítás célja nem pusztán a kriptovalutákhoz köthető bűncselekménytípusok katalogizálása volt, hanem a mögöttes mintázatok azonosítása és értelmezése is, különös tekintettel a szabályozási és bűnüldözési kihívások gyakorlati vetületeire. A tanulmány egy két részből álló cikksorozat első része. A folytatás olyan interjúalapú kvalitatív és kvantitatív elemzéseket mutat be, amelyek kifejezetten a rendvédelmi szervek gyakorlatára és tapasztalataira összpontosítanak.

Alapfogalmak

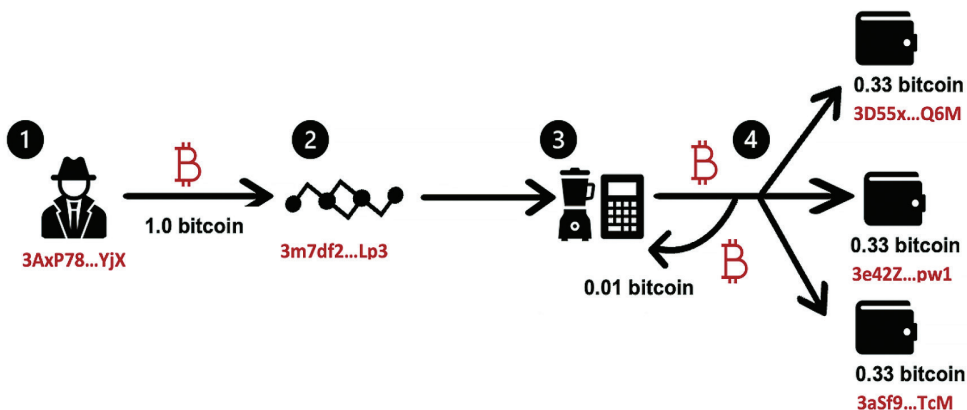
A kriptovaluta olyan digitális fizetőeszköz, amely nem rendelkezik fizikai megjelenési formával, így eltér a hagyományos valutáktól, mint például az érmék vagy a bankjegyek. Működése kriptográfiai módszereken alapul, és decentralizált technológiai infrastruktúrára, elsősorban blokkláncalapú hálózatokra épül. A hálózatok lehetővé teszik a biztonságos, ellenőrizhető és transzparens tranzakciók lebonyolítását anélkül, hogy központi hatóság vagy pénzügyi közvetítő beavatkozására lenne szükség.⁷ A blokklánc-technológia alapegysége a blokk, amely strukturált formában tartalmazza a tranzakciós adatokat. Minden blokk egy adott időintervallumban végrehajtott tranzakciók összesítését reprezentálja, továbbá tartalmazza az előző blokk kriptográfiai hasítóértékét (hash), amely biztosítja a láncolat folytonosságát és integritását. Ez a megoldás lehetővé teszi, hogy a blokkok időrendi sorrendben kapcsolódjanak egymáshoz, és így egy visszamenőlegesen nem módosítható, elosztott főkönyv jöjjön létre. A blokklánc mint technológiai rendszer decentralizált környezetben működik, ahol minden résztvevő (node) másolatot tárol a teljes tranzakciós előzményről. A rendszer alapvető jellemzője, hogy a rögzített információk transzparenssek, nyilvánosan hozzáférhetők és utólagos módosításra gyakorlatilag nem alkalmasak, mivel bármely változtatás érvénytelenné tenné az utána következő blokkok hasítóértékeit. Ez a struktúra egy olyan biztonságos és megbízható adatbázist eredményez, amelyben a tranzakciók hitelesítése konszenzusalapú mechanizmusok révén történik, központi ellenőrzés nélkül.⁸

⁷ NAKAMOTO 2008.

⁸ MUKHOPADHYAY et al. 2016.

A kriptovaluták tranzakcióinak nyomon követhetőségét jelentősen megnehezíti a különféle anonimizáló technológiák alkalmazása. Az egyik legelterjedtebb eszköz ebben a körben a coin mixer (más néven coin tumbler) szolgáltatás, amely a blokkláncon végzett pénzmozgások forrásának és céljának összekapcsolását hivatott obfuszkálni. Jelen tanulmányban a coin mixer terminust használjuk. A coin mixer szolgáltatások működési elve azon alapul, hogy a felhasználók kriptovalutát juttatnak el a keverési platformra, ahol az adott összegeket más felhasználók tranzakcióival együttesen dolgozzák fel. Az így kialakuló kriptovaluta halmazából újbóli szétosztása során a rendszer a címzettek részére olyan új tranzakciókat hoz létre, amelyek nem tartalmaznak közvetlen kapcsolatot az eredeti forráshoz. Ezzel a módszerrel a küldő és a végső címzett közötti összefüggés megszakad vagy jelentősen obfuszkálódik, így a tranzakciók visszafejtése és nyomon követése blokkláncelemzéssel nagyban megnehezül.⁹ Egyik legismertebb platform a Samourai Wallet nevű Bitcoin mixer volt, amelyet 2015-ben hoztak létre azzal a céllal, hogy pénzügyi anonimitást biztosítson felhasználóinak. A szolgáltatás működése azonban 2024-ben jelentős figyelmet kapott, amikor az alapítókat pénzmossással kapcsolatos összeesküvés vádjával letartóztatták.¹⁰

A kiberbűnözés elleni fellépés során jelentős strukturális kihívást jelent az erőforrásbeli aszimmetria a bűnözői szereplők és a bűnüldöző hatóságok között. A rendelkezésre álló eszközök és technológiák költséghatékonysága gyakran a bűnelkövetők oldalán jelent előnyt, mivel az általuk használt szolgáltatások olcsóbbak és rugalmasabbak, mint azok a komplex megoldások, amelyeket a hatóságok kénytelenek alkalmazni. Emellett egyes szervezett bűnözői hálózatok olyan mértékű anyagi forrásokkal rendelkeznek, amelyek lehetővé teszik számukra fejlett technikai infrastruktúrák kiépítését és működtetését, időnként meghaladva az állami szereplők technológiai lehetőségeit.



2. ábra: A kriptovaluta-keverés folyamata lépésről lépésre

Forrás: a szerző szerkesztése Intel 471 2021 alapján

⁹ MARIANI–HOMOLIAK 2025.

¹⁰ Southern District of New York 2025.

A 2. ábra vizuálisan szemlélteti, hogyan működik egy tipikus kriptovalutamixer-szolgáltatás:

1. lépés: A kiberbűnöző kriptovalutát küld egy mixerszolgáltatás által megadott kriptovaluta-tárca¹¹ címre.

2. lépés: Az utalt összeg bekerül a mixerszolgáltatás platformjára, ahol más felhasználóktól származó kriptovalutákkal, valamint a szolgáltató saját tartalékaival keveredik össze.

3. lépés: A rendszer egy kriptográfiai keverő algoritmust alkalmaz, amelynek célja a tranzakciós nyomvonal obfuszkálása. Ebben a fázisban továbbá a szolgáltatás levonja a működtetéséért járó jutalékot is.

4. lépés: A „megtisztított” összeget visszautalják a kiberbűnöző által megadott, többnyire újonnan létrehozott tárcacímekre, ezzel megnehezítve az eredeti forrás azonosítását.¹²

Nem minden kriptovaluta esetében szükséges külső keverési szolgáltatás igénybevétele, mivel egyes kriptovaluták, például a monero, zcash vagy dash natívan beépített anonimizációs megoldásokat alkalmaznak. A Monero működésének alapját a Crypto-Note protokoll képezi, amelyet kifejezetten a tranzakciók visszakövethetetlenségének és a felhasználói anonimitásnak a biztosítására fejlesztettek. A protokoll három anonimitást biztosító technológiát integrál:

- Stealth addresses (védett címek): minden tranzakcióhoz egyedi, egyszer használatos cím generálódik, így a címzett személye nem köthető össze a publikus címmel.
- Ring signatures (gyűrűalíráások): az aláíró nyilvános kulcsát egy véletlenszerűen kiválasztott csoport kulcsai közé „rejtje el”, megnehezítve a küldő egyértelmű azonosítását.
- Ring Confidential Transactions (RingCT): a tranzakciók összegeit titkosítja, így sem az összeg, sem a küldő és fogadó fél kiléte nem rekonstruálható.¹³

A felsorolt technológiai megoldások révén a Monero jelenleg az egyik legfejlettebb anonimitást biztosító kriptovalutának tekinthető.¹⁴

Érdemes kiemelni, hogy ezzel szemben a Bitcoin egy pseudoanonim fizetési rendszernek tekintendő, mivel a tranzakciók során a felhasználók valós személyazonossága helyett kriptográfiai címeket használnak. Ezek a Bitcoin-címek álvéletlenszerűen generálódnak egy adott matematikai algoritmus alapján, így minden cím egyedi és látszólag véletlenszerű. Ez a megoldás bizonyos fokú anonimitást kínál, ugyanakkor nem teszi lehetővé a teljes rejtettséget. Mégis, a felhasználóknak lehetőségük van arra, hogy minden egyes tranzakcióhoz új címet hozzanak létre. Ezzel a gyakorlattal csökkenthető annak az esélye, hogy egyetlen cím alapján átfogó képet lehessen alkotni az adott felhasználó pénzügyi tevékenységéről. Bár a címek kriptográfiai alapokon nyugszanak, és visszafejtésük

¹¹ A kriptovaluta-tárca olyan digitális fizikai eszköz vagy szoftver, amely lehetővé teszi a felhasználók számára, hogy privát és nyilvános kulcsokat hozzanak létre, tároljanak, és ezek segítségével biztonságosan kezeljék kriptovalutáikat, valamint lebonyolítsák blokláncalapú tranzakcióikat. A kriptovaluta-tárcák fő típusai a szoftveres (asztali, online, mobil), valamint a hardveres tárcák, amelyeken belül megkülönböztetünk forró (internetes) és hideg (offline) tárolási megoldásokat.

¹² Intel 471 2021.

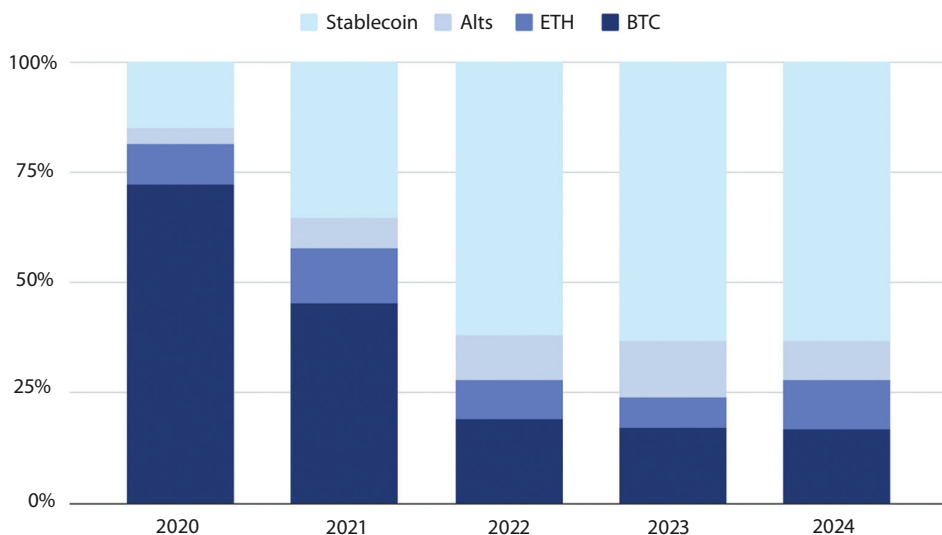
¹³ Monero 2024.

¹⁴ NOETHER 2015; LI et al. 2021.

jelentős technikai kihívást jelent, megfelelő elemzőeszközök és metaadatok segítségével bizonyos esetekben mégis azonosíthatók a felhasználók.¹⁵

A Chainalysis 2025-ös Crypto Crime Reportja megállapításai szerint továbbra is a bitcoin a leggyakrabban használt kriptovaluta bűncselekmények elkövetése során. Ennek oka elsősorban a bitcoin széles körű ismertsége, elterjedtsége, valamint az, hogy a legtöbb kriptovalutát elfogadó platform alapértelmezés szerint ezt tekinti elsődleges fizetőeszköznek. A 3. ábra alapján ugyanakkor megfigyelhető, hogy a tranzakciók bűnözéshez kapcsolható összértékének jelentős hányadát már az úgynevezett stablecoinok¹⁶ teszik ki, mint például az USDC, USDT vagy EUROC. Míg a Bitcoin tranzakcióinak megerősítése időigényes lehet, a stablecoinok gyakorlatilag azonnali átutalást tesznek lehetővé. Ezenfelül stabil árfolyamuk miatt különösen alkalmassá válnak nagy volumenű pénzmozgások lebonyolítására, mivel minimalizálják az árfolyam-ingadozásokból eredő kockázatot.

Fontos azonban megjegyezni, hogy noha a stablecoin tranzsferek aggregáltan kiemelkedők, ezek több különböző kriptovalutát foglalnak magukban, így nem értelmezhetők egyetlen kriptovalutaként a használati gyakoriság szempontjából. A 3. ábra további adataiból kiolvasható tendencia az ethereum növekvő szerepe a bűncselekményekhez köthető tranzakciók terén, amely az ökoszisztéma technológiai sokszínűségével és a decentralizált pénzügyi (DeFi)¹⁷ protokollok integrációjával magyarázható.



3. ábra: Bűncselekményekhez kapcsolódó tranzakciók eloszlása kriptovaluta-típusok szerint (2020–2024)

Forrás: a szerző szerkesztése Chainalysis 2025 alapján

¹⁵ ZHANG et al. 2020.

¹⁶ A stablecoinok olyan kriptovaluták, amelyek értéküket egy stabil árfolyamú gazdasági eszközhöz (pl. amerikai dollár, euró vagy arany) kötik annak érdekében, hogy elkerüljék a kriptopiacra jellemző volatilitást.

¹⁷ A decentralizált pénzügyi (DeFi) protokollok olyan blokláncalapú alkalmazások, amelyek központi pénzügyi közvetítők (pl. bankok, brókerek) nélkül teszik lehetővé pénzügyi műveletek lebonyolítását. Ezek az okosszerződésekre épülő rendszerek átlátható módon működnek, de gyakran névtelenül használhatók, így a szabályozás és ellenőrzés szempontjából komoly kihívást jelentenek.

Meglepő módon a kifejezetten anonimitásra épülő privacy coinok, amelyek az altcoinok körébe tartoznak (például Monero), a Chainalysis adatai alapján mindössze marginális arányban fordulnak elő az illegális tranzakciók teljes volumenében.¹⁸

Pénzmosás

A bűncselekménytípusok vonatkozásában a pénzmosás az egyik legfontosabb, amelynek elősegítésében szerepet játszanak a kriptovaluták. A pénzmosás olyan többlépcsős folyamat, amelynek célja, hogy a jogellenes forrásból származó bevételeket – például drogkereskedelemből, csalásból vagy korrupcióból eredő jövedelmeket – látszólag legális eredetű jövedelemmé alakítsák. Ennek eredményeként az illegális tőke problémamentesen visszaáramolhat a formális gazdaságba, a hatósági ellenőrzés elkerülésével.¹⁹

A pénzmosás folyamata a szakirodalomban hagyományosan három egymást követő szakaszra tagolódik (4. ábra):

1. Elhelyezés

Az első fázisban az illegális forrásból származó jövedelmet bevezetik a hivatalos pénzügyi rendszerbe, jellemzően banki befizetések, pénzváltások, tárgyak vásárlása vagy digitális eszközök – például kriptovaluták, NFT-k – vásárlása útján. Ebben a fázisban a legmagasabb annak a kockázata, hogy a pénzmosás lelepleződik.

2. Rétegzés

A második szakasz során a bűnözők többszörös tranzakciós műveletekkel igyekeznek eltüntetni az eredeti jövedelem nyomait. Ekkor gyakori a tőke különböző kriptovalutákba történő átváltása, coin mixerek vagy DeFi protokollok használata, valamint a pénzeszközök különböző országokon keresztül történő mozgatása. A folyamat során jelentős mértékben megnő a tranzakciók száma, mivel az elkövetők ismétlődő átutalásokkal és összetett pénzmozgásokkal igyekeznek a tranzakciós láncot széttagolni és a nyomon követhetőséget csökkenteni.

3. Integráció

Az utolsó fázisban a megtisztított vagyon visszakерül a formális gazdasági rendszerbe. Ez például ingatlanvásárlás, üzleti befektetés vagy más pénzügyi művelet révén

¹⁸ Chainalysis 2025.

¹⁹ LEVI 2002.

valósulhat meg. Az integráció gyakran olyan országokban történik, amelyek kedvező pénzügyi szabályozást kínálnak – ezek az úgynevezett adóparadicsomok.²⁰



4. ábra: A pénzmosás három szakasza kriptovalutákkal

Megjegyzés: Az illegális forrásból származó kriptovaluták elhelyezése után a rétegzés során kriptovaluta-keverők és privacy coinok alkalmazásával rejtik el a forrását, majd az integrálás során a „megtisztított” összegeket fiat valutára váltják vagy közvetlenül felhasználják

Forrás: a szerző szerkesztése SCHNEIDER–WINDISCHBAUER 2008 alapján

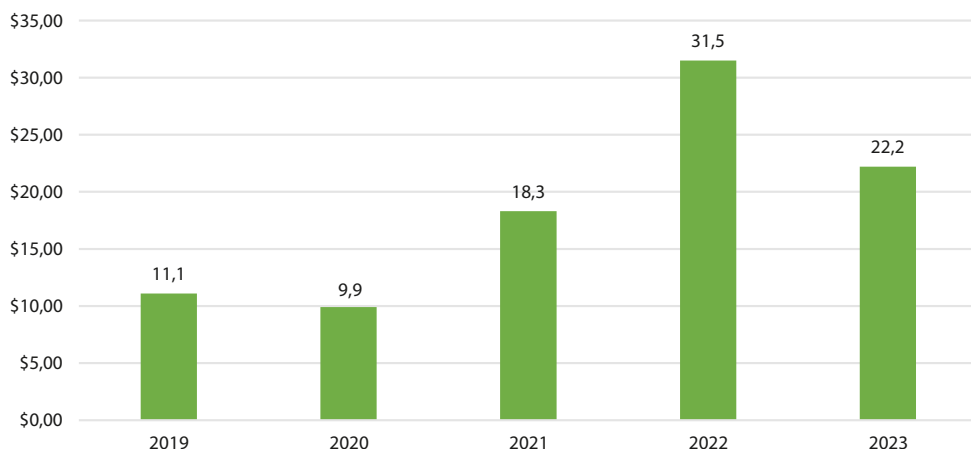
Az utóbbi években a bűnözők forradalmasították a pénzmosás folyamatát a kriptovaluták révén, hogy elkerüljék a szabályozó hatóságok ellenőrzését. A kriptovaluták megjelenése előtt a bűnözők kénytelenek voltak illegális módon szerzett kriptovalutáikat a központi bankrendszeren keresztül mozgatni és elrejteni. Ennek következtében különböző kormányok képesek voltak közvetett módon ellenőrizni a pénzmosást azáltal, hogy szigorúbb szabályozásokat és nagyobb bírságokat róttak ki a bankokra és pénzintézetekre, ami egyre nehezebbé tette az illegális tőkék mozgását. Ezzel szemben, mivel a kriptovaluták nem igényelnek központi banki közreműködést, képesek teljesen megkerülni a hagyományos bankrendszert. A kriptovaluták további gazdasági ösztönzőket biztosítanak a bűnözők számára, így még vonzóbbá téve számukra ezt a rendszert. Az egyik növekvő előny számukra az, hogy a kriptovaluták egyre szélesebb körben elfogadott fizetőeszközként jelennek meg az áruházlancok és kereskedők körében. Jelenleg ez az elfogadottság még korlátozott, mivel a kriptovalutákat gyakran át kell váltani hagyományos, fiat pénznemekre.²¹ Egy másik, még meghatározóbb előnye a kriptovaluták használatának, hogy rendkívül könnyen lehet velük pénzt mozgatni egyik országból a másikba. A pénzmosás rétegzési szakaszában az illegális úton szerzett összegeket nemcsak számos pénzügyi tranzakció lebonyolítására használják, hanem más pénzügyi joghatóságokba is átutalják, ahol a bűnelkövetők könnyen hozzáférhetnek forrásaikhoz, ezáltal védve vagyonukat a lefoglalás ellen. A kriptovaluták pénzmosásban betöltött szerepének növekedését jól szemlélteti az 5. ábra, amely az éves kriptovaluta-pénzmosási összegek alakulását mutatja be 2019 és 2023 között, milliárd amerikai dollárban kifejezve.²²

²⁰ SCHNEIDER–WINDISCHBAUER 2008.

²¹ A fiat pénz olyan hivatalos fizetőeszköz, amelyet az állam bocsát ki, és amelynek értékét nem valamilyen mögöttes termék – például arany vagy ezüst – biztosítja, hanem az adott ország kormányába és gazdaságába vetett bizalom. Ez azt jelenti, hogy azért fogadjuk el fizetesként, mert a törvény érvényes fizetőeszközként ismeri el, és mert bízunk benne, hogy stabilan megőrzi az értékét.

²² ALBRECHT et al. 2019.

Amennyiben európai uniós szemszögből vizsgáljuk a kriptovaluták és a pénzmosás jogi szabályozását, rendkívül fontos az Európai Parlament és a Tanács 2024/1624 (AMLR) rendelete, amely a pénzügyi rendszer pénzmosás vagy a terrorizmus finanszírozása céljára történő felhasználásának megelőzését hivatott szolgálni. A rendelet többek között előírja a kriptovaluta-szolgáltatók számára az ügyfél-azonosítási (KYC²³) kötelezettségek szigorítását, tiltja az anonimizáló eszközök alkalmazását, mint például a coin mixereket, illetve a privacy coinokat, mint a Monero, Zcash vagy Dash.²⁴



5. ábra: Éves kriptovaluta-pénzmosás összegei (milliárd dollárban) 2019–2023 között

Forrás: a szerző szerkesztése Chainalysis 2024 alapján

Fontos megemlíteni továbbá, hogy a legnagyobb kriptovaluta-tőzsdék – köztük a Binance – már eltávolították platformjukról a monero és a zcash kereskedési lehetőséget, ami jól tükrözi a szabályozói nyomás erősödését.²⁵

Csalások

A kriptovaluták gyors ütemű elterjedése és a köztudatba való beépülése jelentős hatást gyakorolt a digitális pénzügyi ökoszisztéma fejlődésére. A technológia újszerűsége, valamint a gyakran irreálisan magas hozamígéretet következtében mind több magánszemély és befektető dönt úgy, hogy befektet különféle kriptovalutákba. Ezzel párhuzamosan azonban az elmúlt években a csalások számának folyamatos emelkedése is megfigyelhető, ami a bűnözői körök gyors alkalmazkodását jelzi az új pénzügyi technológiákhoz. A kriptovalutákhoz kapcsolódó csalások számos formában

²³ A *know your customer* (KYC) elv olyan azonosítási és ellenőrzési folyamat, amelyet a pénzügyi szolgáltatók – például bankok, tőzsdék vagy kriptovaluta-platformok – kötelesek elvégezni annak érdekében, hogy azonosítsák ügyfeleiket (pl. személyazonosító okmány vagy lakcímgigazolás alapján), valamint meggyőződjenek arról, hogy az ügyfél jövedelmei jogszerű forrásból származnak.

²⁴ European Union 2024b.

²⁵ CoinMarketCap 2024.

jelennek meg, amelyek közül az egyik leggyakoribb a magas hozamú befektetési csalások kategóriájába tartozó Ponzi-séma. Ez a megtévesztési forma arra épül, hogy az elkövetők az újonnan belépő befektetők által befizetett tőkéből fizetik ki a korábbi befektetőknek ígért hozamokat. A rendszer hosszú távon fenntarthatatlan, mivel mögötte nem húzódik meg valódi gazdasági tevékenység vagy jövedelemtermelő modell, csupán a folyamatos új befektetők bevonása biztosítja ideiglenes működését. Az új befektetőket gyakran manipulatív eszközökkel, például hamis hozamjelentésekkel, mesterségesen generált pozitív visszajelzésekkel és a már meglévő résztvevők ajánlásaival próbálják meggyőzni a csatlakozásról. Az ilyen típusú csalási technikák különösen ott bizonyulnak eredményesnek, ahol a kriptovaluták iránt érdeklődő, de pénzügyileg kevésbé tájékozott felhasználókat könnyen be lehet vonni a piacra, és ahol a szabályozási keretek hiányosak, illetve a jogérvényesítés nem működik kellő hatékonysággal.²⁶

Az egyik legismertebb Ponzi-séma típusú csalási eset a Bitconnect platform 2018-as összeomlása volt. A szolgáltatás a felszínen legitim, felhasználóbarát kriptovalutaként és kereskedési felületként működött, ám valójában egy klasszikus Ponzi-sémát valósított meg, több ezer befektetővel. A rendszer működésének korai szakaszában akár évi 120%-os hozamot ígért a befektetőknek, amennyiben azok Bitconnect Coin (BCC) nevű tokenjeiket a platformon tárolták és ott kereskedtek velük. Ennek következtében a BCC-tranzakciók mintegy 95%-a házon belül zajlott, erősen korlátozva az átláthatóságot. További gyanúra adott okot, hogy a BCC kizárólag bitcoinért volt megvásárolható, fiat pénz nemek használata nem volt lehetséges. Ez a működési modell nyilvánvalóan a nyomon követhetőség csökkentését szolgálta. A Bitconnect rendszeresen küldött hamisított kamatjelentéseket a befektetőknek, ám ezek a „hozamok” valójában az újonnan belépő felhasználók befizetéseiből származtak. 2018. január 17-én a BCC árfolyama drasztikusan összeomlott, és rövid időn belül 400 dollárról 27 dollárra zuhant. Ez a hirtelen árfolyamcsökkenés annak tudható be, hogy egyre több befektető ismerte fel a csalást, és megpróbálta minél gyorsabban kivenni a még elérhető tőkéjét a rendszerből. A befektetések teljes egészében kriptovalutában zajlottak, ami jelentős akadályt jelentett a bűnüldöző szervek számára a felelősök beazonosításában és az elkövetési lánc feltárásában. Bár néhány kulcsszereplőt sikerült azonosítani és bíróság elé állítani, több gyanúsított továbbra is ismeretlen vagy nem tudták előállítani őket, így a nyomozás máig sem zárult le teljes egészében.²⁷

A Ponzi-séma mellett egy másik gyakran alkalmazott csalási forma a kriptovaluták esetén a pump and dump (P&D) módszer. A P&D ármanipulációs technika lényege, hogy egy fizetőeszköz árát mesterségesen felhajtják, mielőtt a korábban olcsón megvásárolt kriptovalutát magasabb áron értékesítik. Miután a kriptovalutát eladják, az árak drasztikusan visszaesnek, és a befektetők jelentős veszteségeket szenvednek el. A folyamat illusztrációja a 6. ábrán szerepel.

²⁶ KERR et al. 2023.

²⁷ BAUM 2018.



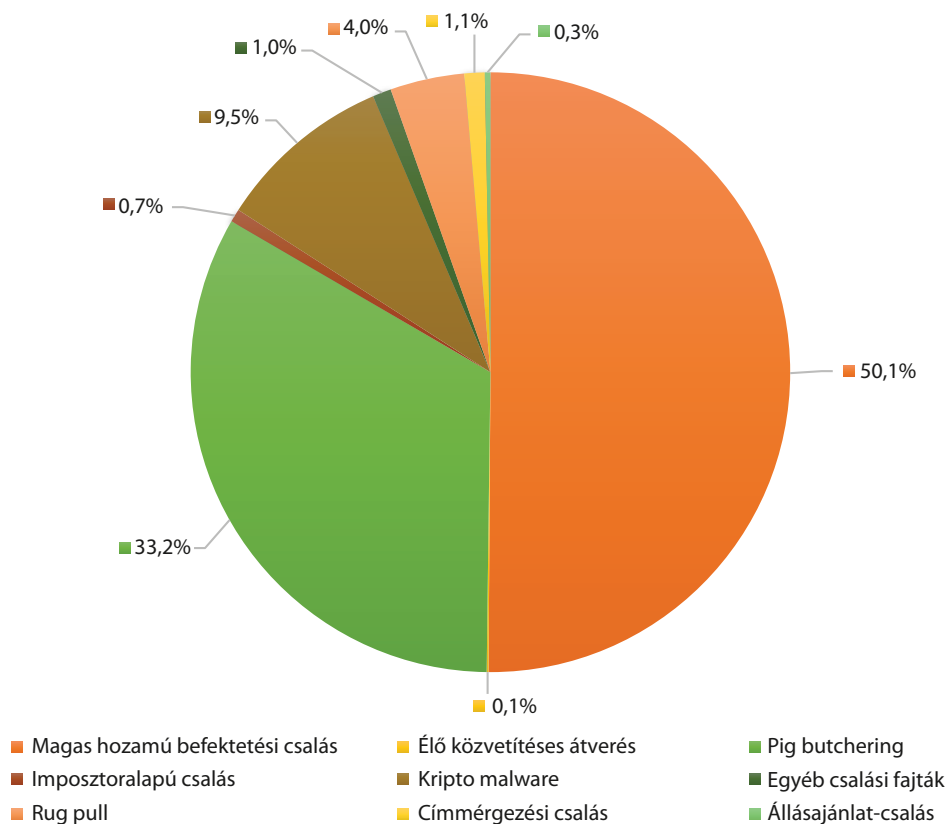
6. ábra: A pump and dump csalási módszer modellje

Forrás: a szerző szerkesztése KAMPS–KLEINBERG 2018 alapján

Több kutatás is rámutatott arra, hogy a P&D típusú ármanipulációk jellemzően szervezett módon valósulnak meg, úgynevezett P&D-csoportok létrejöttével. Ezek a közösségek kifejezetten azzal a céllal jönnek létre, hogy előre kiválasztott kriptovaluták árfolyamát mesterségesen felhajtásák, majd az így generált nyereséget realizálják. A csoportok elsősorban online platformokon – például Discordon vagy Telegramon – szerveződnek, ahol a manipulációt összehangoltan hajtják végre. Annak érdekében, hogy a lehető legnagyobb nyereséget ériék el, a rendelkezésre álló jelentések szerint ezek a csoportok szinte kizárólag alacsony piaci kapitalizációjú, kis forgalmú és kevésbé ismert kriptovalutákat céloznak. Az ilyen típusú eszközök árfolyama ugyanis sokkal érzékenyebb a hirtelen megnövekedett keresletre, ezáltal könnyebben manipulálható rövid időtávon belül.²⁸ A P&D-csalások egyik várható jövőbeli trendje a gyorsan változó globális témákhoz kapcsolódó, úgynevezett hype-tokenek létrehozása. Az elkövetők gyakran olyan új digitális tokeneket indítanak, amelyek aktuális társadalmi, politikai vagy kulturális jelenségekre építenek, így rövid idő alatt jelentős felhasználói érdeklődést generálnak. A kezdeti árfolyam-emelkedés után a szervezők hirtelen kivonják a befektetett tőkét, és a piac összeomlik. Egy szintén manapság elterjedt csalási módszer a pig butchering, amely a Chainalysis 2025-ös Crypto Crime Reportja szerint a második legtöbb bevételt hozó kriptocsalási forma. A módszer érzelmi manipuláción – leggyakrabban színlelt romantikus kapcsolaton – alapul, amely során a csalók hosszú bizalomépítés után veszik rá áldozatukat hamis kriptobefektetésekre. A jelentésben szereplő legelterjedtebb csalástípusok a 7. ábrán tekinthetők meg. A megoszlásból kitűnik, hogy a klasszikus pénzügyi átverések (például befektetési csalások és pig butchering) dominálnak, míg a kifinomult technológiai jellegű csalások kisebb, de nem elhanyagolható szeletet képviselnek. Ez a tendencia arra utal, hogy a kriptovaluta-alapú csalások sikerességében a pszichológiai manipuláció továbbra is nagyobb szerepet játszik, mint a tisztán technikai eszközök.²⁹

²⁸ KAMPS–KLEINBERG 2018.

²⁹ Chainalysis 2025.



7. ábra: Kriptovaluta-alapú csálásokból szerzett bevételek altípusok szerint

Forrás: a szerző szerkesztése Chainalysis 2025 alapján

Zsarolóvírusok, váltságdíjfizetések kriptovalutában

A zsarolóvírusos támadások az elmúlt évek egyik legtöbbet elkövetett és legsúlyosabb következményekkel járó kiberbűnözési formájává váltak. Ezek a rosszindulatú programok a megfertőzött eszközökön tárolt adatokat titkosítják, és azok visszafejtéséért váltságdíjat követelnek az áldozattól. A váltságdíjakat jellemzően kriptovalutákban határozzák meg, ami nagymértékben hozzájárul a támadók anonimitásának fenntartásához.

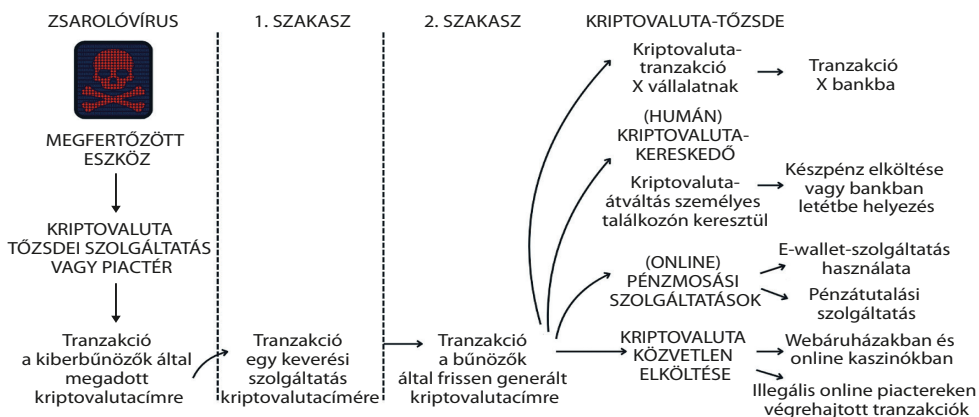
A Chainalysis 2025-ös jelentése szerint 2024-ben a zsarolóvírus-támadásokhoz köthető váltságdíj-kifizetések összege 2%-kal emelkedett az előző évhez képest, és elérte a 459,8 millió dollárt, szemben a 2023-as 449,1 millió dolláros adattal.³⁰ A növekedés hátterében több tényező áll, amelyek közül kiemelkedik a zsarolóvírus

³⁰ Chainalysis 2024.

mint szolgáltatás³¹ (RaaS-) modell térnyerése. Ez a szolgáltatásalapú megközelítés lehetővé teszi, hogy technikai háttérrel kevésbé rendelkező elkövetők is hozzáférjenek professzionálisan fejlesztett zsarolóvírusokhoz, ezzel jelentősen növelve a támadások számát és hatékonyságát. A TRM Labs 2025-ös jelentése szerint a RaaS-modell térnyerésével párhuzamosan 2024-ben több új zsarolóvírus-csoport is megjelent, például a Brain Cipher, dAnOn, DragonForce, Fog, Funksec, RansomHub, Sarcoma és Trinity, ami jelzi a piaci szereplők folyamatos bővülését és a támadások diverzifikálódását.³²

A kriptovaluták részleges anonimitást biztosító jellege szintén elősegíti a zsarolóvírus-támadások sikerét, mivel lehetővé teszi, hogy az elkövetők személyazonosságuk felfedése nélkül követeljenek és fogadjanak el váltságdíjat. A támadók anonimitását nem kizárólag a kriptovaluták technikai sajátosságai biztosítják, hanem gyakran további eszközöket is igénybe vesznek, mint például coin mixereket vagy a dark weben működő escrow szolgáltatásokat, amelyek még inkább megnehezítik az azonosítást és a tranzakciók visszakövetését. A váltságdíjak kifizetésére továbbra is a bitcoin a leggyakrabban használt kriptovaluta, mivel széles körben hozzáférhető és a legtöbb szereplő által elfogadott fizetőeszköz a kiberbűnözői ökoszisztémában. Ugyanakkor megfigyelhető, hogy a monero egyre népszerűbbé válik az elkövetők körében, mivel jelentősen magasabb szintű tranzakciós anonimitást kínál a bitcoinhoz képest.³³

Hazai eset a 2021 márciusában bekövetkezett zsarolóvírus-támadás, amely az UNIX Autó Kft.-t érte, és ahol a váltságdíjat moneróban követelték.³⁴ Egy másik jelentős eset 2021 áprilisában történt, amikor a Colonial Pipeline, az USA legnagyobb üzemanyagvezeték-hálózatának üzemeltetője, zsarolóvírus-támadás áldoztatá vált. A támadók, a DarkSide nevű kiberbűnöző csoport, 75 bitcoin (akkoriban körülbelül 4,4 millió USD értékben) váltságdíjat követeltek és szereztek meg³⁵ (8. ábra).



8. ábra: A zsarolóvírusokból származó nyereség pénzmosási modellje

Forrás: a szerző szerkesztése CUSTERS–OERLEMANS–POOL 2020 alapján

³¹ Illegális üzleti modell, amelyben a zsarolóvírusok készítői szoftverként kínálják fel a kártékony programokat más bűnözőknek, akik így technikai tudás nélkül is képesek zsarolóvírus-támadásokat végrehajtani. A támadók általában megosztják a befolyt váltságdíjat a RaaS-szolgáltatóval, aki cserébe technikai támogatást, frissítéseket és infrastruktúrát biztosít.

³² TRM Labs 2025.

³³ CUSTERS–OERLEMANS–POOL 2020.

³⁴ UNIX Autó Kft. 2024.

³⁵ BEERMAN et al. 2023.

A *The Evolution of Cryptocurrency and Cyber Attacks* című tanulmány, azt vizsgálta, hogy van-e kimutatható összefüggés a zsarolóvírusok terjedése és a kriptovaluták egyre szélesebb körű használata között. A kutatás egyik központi kérdése az volt, hogy a zsarolóvírusok kialakulása és fennmaradása független lehet-e a kriptovalutáktól, vagy pedig ezek kulcsszerepet játszanak a kibertámadások ezen formájának terjedésében. Az eredmények arra mutattak, hogy nem feltételezhető közvetlen korreláció a két jelenség között, és a zsarolóvírusok kriptovaluta nélkül is létezhetnek. Ezt támasztja alá az a tény is, hogy zsarolóvírusok már jóval a kriptovaluták megjelenése előtt, például a bitcoin elterjedését megelőzően is jelen voltak. Ennek egyik legkorábbi példája az AIDS Trojan (vagy más néven PC Cyborg), amely 1989-ben jelent meg, amikor is egy konferencián húszezer résztvevőnek osztották szét floppylemezeket. A megfertőzött számítógépek felhasználóitól 189 dollárt követeltek.³⁶

Bár a kutatás nem talált egyértelmű korrelációt a kriptovaluták és a zsarolóvírusok elterjedése között, manapság a zsarolóvírusok túlnyomó többsége mégis kriptovalutában követeli a váltságdíjat. Ez azt sugallja, hogy a kriptovaluták anonimitása és nehezebb nyomon követhetősége olyan tényezők, amelyek hozzájárulhatnak e bűncselekmények fennmaradásához és terjedéséhez, mivel megkönnyítik a támadók számára az illegális pénzügyi tranzakciókat.

Terrorizmus finanszírozása kriptovalutákon keresztül

A terrorizmus finanszírozása azon folyamatokat foglalja magában, amelyek során terrorista szervezetek pénzügyi forrásokat szereznek és használnak fel tevékenységeik előkészítésére, megszervezésére és végrehajtására. A pénzügyi támogatás nemcsak konkrét terrortámadások megvalósításához szükséges, hanem a szervezetek mindennapi működésének fenntartásához is, beleértve a toborzást, a kiképzést, a fegyverbeszerzést, a logisztikai háttér biztosítását, valamint a tagok és hozzátartozók anyagi támogatását.³⁷ Bár egy-egy támadás viszonylag alacsony költségű lehet, a terrorszervezetek működtetése jelentős anyagi forrásokat igényel. A szigorodó pénzügyi ellenőrzések miatt ezek a csoportok egyre gyakrabban fordulnak alternatív eszközökhöz, mint például a kriptovalutákhoz. Egy sikeres terrorszervezet – hasonlóan a bűnözői csoportokhoz – olyan, amely képes hatékony pénzügyi infrastruktúrát kiépíteni és fenntartani. Ennek érdekében a csoportnak különféle finanszírozási forrásokat kell kialakítania, valamint olyan eszközöket kell fejlesztenie, amelyek megnehezítik a források és a finanszírozott tevékenységek közötti kapcsolatok felderítését. A kriptovaluták vonzó megoldásnak tekinthetők a terrorizmus finanszírozására, mivel olyan jellemzőkkel rendelkeznek, mint a letagadhatatlanság, a központi felügyelet hiánya, az alacsony használati költség, a viszonylag egyszerű használat, valamint a helyszín és a valuta változtathatóságának rugalmassága, a tranzakciók feldolgozási sebessége, a működés bonyolultsága és a globális elérhetőség, illetve a már említett anonimitást elősegítő módszerek. A dark web felületet biztosít a terrorszervezetek számára, hogy kriptovalutában adományokat gyűjtsenek céljaik finanszírozására, amely

³⁶ BERRY 2022.

³⁷ ALFIERI 2022.

összegeket később fegyverek és robbanóanyagok beszerzésére fordíthatnak különböző, szintén dark webes piactereken keresztül. Példaként említhető a „Támogasd az Iszlám Harcot nyom nélkül” nevezetű dark webes oldal (9. ábra), amely bitcointranzakciók útján gyűjt adományokat egy adott Bitcoin-címre a dzsihád támogatására. A felületen emellett egy PDF-fájl is elérhető, amely útmutatóként szolgál az anonim pénzáttalások végrehajtásához.³⁸

A Chainalysis megállapítása alapján a Hamasz Izz ad-Din al-Kassám Brigádja (AQB) „az egyik legnagyobb és legkifinomultabb kriptovaluta-alapú terrorizmusfinanszírozási kampányt valósította meg, amit valaha tapasztaltak”. 2019-ben az AQB megpróbált bitcoint használva adományokat gyűjteni támogatóitól, és módszereit folyamatosan finomította, ahogy a bűnüldöző szervek akadályozni próbálták erőfeszítéseit. A csoport egy QR-kódot helyezett el a weboldalán, amely egy Bitcoin-címhez irányította az adományozókat. Nem sokkal később azonban a hatóságok befagyasztották a számlát, és megvizsgálták annak tulajdonosát és tranzakcióit. Az AQB erre reagálva lecserélte a QR-kódos Bitcoin-címet egy privát tárcához tartozó új címre. Bár az AQB úgy gondolta, hogy ez a privát tárca növeli az anonimitást, a bűnüldöző szervek elemzői képesek voltak nyomon követni a csoport tárcatranzakcióit és adományait. A tárcát végül leállították. Az AQB ismét változtatott a bitcoinadományok gyűjtésének módszerén. Ezúttal a weboldal minden egyes adományozó számára külön-külön Bitcoin-címet generált, amelyre a támogatók pénzt küldhettek. A weboldal egy oktatóvideót is tartalmazott, amely részletesen bemutatta, hogyan lehet a legnagyobb anonimitás mellett adományozni. A videó két adományozási lehetőséget ajánlott: a hawalat³⁹ vagy egy privát Bitcoin-tárca használatát. A hawala egy informális pénzáttalási rendszer, amely a bizalmon alapul. Ha ezt a módszert választották, az adományozók megadhatták a Bitcoin-címet, valamint az adomány összegét fiat pénzben, amit a hawala szolgáltató bitcoinban utalt tovább a megadott címre. Az útmutató emellett azt is elmagyarázta, hogyan lehet privát Bitcoin-tárcát létrehozni, és egy ajánlott kriptotőzsdén keresztül bitcoint vásárolni, majd azt átutalni a megfelelő címre. Ez a kifinomult rendszer egyre nehezebbé tette a pénzügyi tranzakciók nyomon követését. Az AQB több mint 10 000 dollárnyi adományt gyűjtött össze, amíg az amerikai hatóságok 2020-ban le nem foglalták az adománygyűjtő oldalt. Ez az eset is rávilágít arra, hogy az AQB nemcsak sikeresen használta ki a kriptovalutát, hanem folyamatosan alkalmazkodott is, amikor a bűnüldöző szervek akadályozták tevékenységét.⁴⁰

A kriptovaluták felhasználása a dark web piacokon

A dark webes piacterek által nyújtott technológiai anonimitás kiemelkedően kedvező feltételeket teremt az illegális tevékenységek lebonyolításához. Ezekben a platformokon széles skálán mozognak az elérhető illegális termékek és szolgáltatások – például

³⁸ MAJUMDER–ROUTH–SINGHA 2019.

³⁹ A hawala egy alternatív pénzáttalási rendszer, amelyben a pénz fizikailag nem hagyja el a küldő országot, mégis eljut a címzetthez. A folyamat alapját két egymással kapcsolatban álló és egymásban megbízó közvetítő – úgynevezett hawalaügynökök – közti informális megállapodás képezi. Ők egyeztetik egymással a szükséges összeget, amelyet banki vagy hivatalos pénzügyi csatornák igénybevétele nélkül adnak át.

⁴⁰ ALFIERI 2022.

kábítószerek, fegyverek, hamis iratok vagy kiberbűnözési eszközök –, amelyek folyamatosan változó kínálata dinamikus és nehezen kontrollálható környezetet hoz létre. A kriptovaluták, különösen a bitcoin és a privacy coinok, jelentős szerepet játszanak a piacterek működésében, mivel decentralizált és részben vagy teljesen anonimizált fizetési lehetőséget biztosítanak. Ezáltal a felhasználók úgy tudják lebonyolítani tranzakcióikat, hogy személyazonosságuk rejtve maradjon. A The Onion Router (TOR) hálózat technikai infrastruktúrája tovább fokozza a résztvevők anonimitását. A TOR úgynevezett réteges titkosítási technológiát alkalmaz, amely lehetővé teszi, hogy a felhasználók internetes forgalma többlépcsős csatornákon keresztül, véletlenszerűen kiválasztott csomópontokon haladjon át. Ennek köszönhetően a felhasználók tevékenységei és IP-címeik rejtve maradnak, így mind a piacterek üzemeltetői, mind pedig a vásárlók számára fokozott védelmet nyújt a digitális nyomon követhetőséggel szemben.⁴¹

ALLAH YOLUNDA
MAL İLE CİHAD

ALLAH ﷻ ŞÖYLE BUYURMUŞTUR:
"Ey iman edenler! Sizi elem dolu bir azaptan kurtaracak bir ticaret göstereyim mi size? Allah'a ve O'nun Resulü'ne iman edersiniz, mallarınızla ve canlarınızla Allah yolunda cihad edersiniz. Eğer bilerseniz, bu sizin için çok hayırlıdır." [Saf, 10-11]

RASÜLÜLLAH ﷺ ŞÖYLE BUYURMUŞTUR:
"Her kim Allah yolunda savaşan birini donatırsa, o da savaşmış olur. Yine her kim Allah yolunda savaşan birinin ailesi için (ailesinin ihtiyaçlarını karşılayarak) hayırlı yerini tutarsa, o da savaşmış olur." [Buhârî]

Gerek Medya süğüründeki, gerekse de bilfiil sahada olan Mücahid kardeşlerimize yardım ederek mal ile cihad etmek isteyen kardeşlerimiz aşağıdaki Kripto Para Hesabına dilekçeleri miktarda gönderim yapabilirler.

Cüzdan İsmi: Monero (XMR)
Hesap Numarası:

PLEASE DONATE FOR WAGING
JIHAD with WEALTH

ALLAH ﷻ SAID:
"O believers! Shall I guide you to an exchange that will save you from a painful punishment? It is to have faith in Allah and His Messenger, and strive in the cause of Allah with your wealth and your lives. That is best for you, if only you knew." [Al-Saff, 10-11]

Please donate with safe cryptocurrency Monero (XMR) for waging jihad with wealth and financing those who are waging the same with their lives.

Monero (XMR)

9. ábra: Dzsihadista és terrorista szervezetek támogatására irányuló adománygyűjtő kampányt hirdető weboldalak

Megjegyzés: A weboldal az adományozást moneróban bonyolítja.

Forrás: TRM Labs 2025

A Chainalysis 2024-es Crypto Crime Reportja szerint a dark web piacterek 2023-ban 1,7 milliárd dollárnyi bevételt generáltak, amely jelentős növekedést jelent a megelőző év adataihoz képest. A bővülés hátterében részben a Hydra Market 2022-es bezárása állt, amely alapvetően alakította át a dark web illegális kereskedelmi ökoszisztémáját.

⁴¹ KAVALLIEROS et al. 2021.

A Hydra korábbi dominanciája miatt annak megszűnése nem visszaesést, hanem szerkezeti átrendeződést eredményezett: új szereplők léptek a piacra, és a Hydra egykori felhasználói más platformokra migráltak. A jelentés adatai alapján a dark web piacterek nem gyengültek, csupán átszerveződtek, ami teret nyitott új szolgáltatóknak és üzleti modelleknek.⁴²

A 2025-ben publikált *Crypto Crime Report* szerint bár a kriptovaluta-alapú bűncselekmények volumene történelmi csúcstól ért el, a dark web piacterek és a személyazonosság-lopással kapcsolatos szolgáltatások bitcoinalapú bevételei csökkentek. 2024-ben a dark web piacterek bevétele több mint 2 milliárd, ami jelentős visszaesés az előző évekhez képest. A Hydra Market megszűnését követően új szereplők vették át a vezető pozíciót, közülük a Kraken piactér emelkedett ki, amely 737 millió dollár értékű bitcoinforgalmat bonyolított le, így vált piacvezetővé. A jelentés azt is megállapítja, hogy a Bitcoin transzparenciája miatt egyre több szereplő tér át a monero használatára.⁴³

A kriptovaluták használata mellett a dark web piacterein a tranzakciók biztonságát és titkosságát gyakran escrow (letéti) mechanizmusok alkalmazásával biztosítják. Az escrow rendszer lényege, hogy egy harmadik fél ideiglenesen tárolja a kriptovalutát, amíg az eladó teljesíti az ígért szolgáltatást, ezáltal csökkentve a csalások kockázatát. A hagyományos dark webes piacokon a vásárlók összegeit először levonják a digitális pénztárcából, majd egy escrow számlára helyezik, amelyet a piactér vagy egy harmadik fél kezel. Ez a folyamat biztosítja, hogy a pénz csak a vásárlás véglegesítésekor kerüljön át az eladóhoz. Az escrow rendszerek azonban nem teljesen kockázatmentesek. A pénzt kezelő harmadik fél visszaélhet a felhasználók bizalmával, például „kilépési csalás” (exit scam⁴⁴) formájában, amikor a szolgáltató váratlanul eltűnik a letéti pénzekkel. Egy figyelemreméltó eset 2015 márciusában történt, amikor az Evolution dark web piactér hirtelen bezárta kapuit, és az üzemeltetők több mint 11 millió euró értékű kriptovalutával tűntek el. Ez az eset kiemeli a bizalom fontosságát az escrow rendszerek működésében.⁴⁵

Nemcsak a kilépési csalások, hanem a hatósági rajtaütések is jelentős kockázatot jelentenek a dark webes piacokon. Például 2024 októberében a hatóságok felszámolták a világ legnagyobb dark web piacát, amely a Bohemia és a Cannabia platformokból állt. A művelet során több mint 6,5 millió font értékű kriptovalutát foglaltak le, és letartóztatták a két adminisztrátort. A hatósági rajtaütések és a kilépési csalások egyaránt rávilágítanak arra, hogy az escrow rendszerek használatával a felhasználók gyakran kiszolgáltatottá válnak olyan tényezőknek, amelyek felett nincs kontrolljuk.⁴⁶

⁴² Chainalysis 2024.

⁴³ Chainalysis 2025.

⁴⁴ Az *exit scam* (kilépési csalás) olyan szándékos és előre megtervezett csalási forma, amely során egy – kezdetben megbízhatónak vagy legitimnek tűnő – szolgáltató (pl. kriptovaluta-tőzsde, befektetési platform vagy *dark net* piactér) hirtelen leállítja működését, és az ügyfelek letéti összegeit eltulajdonítja. A csalás a felhasználók bizalmára és a platform korábbi jó hírnevére épít, amelyet a későbbi tőkekiáramlás maximalizálása érdekében tudatosan építenek fel.

⁴⁵ Intel 471 2021.

⁴⁶ LAKSHMANAN 2024.

Diszkusszió

A kutatás eredményei alátámasztják azt a feltételezést, hogy a kriptovaluták technológiai sajátosságai, különösen az anonimitás kiemelt szerepet játszanak a kiberbűnözés új formáinak kialakulásában és terjedésében. A Chainalysis 2024-es és 2025-ös jelentési adatai alapján kirajzolódik, hogy bár a bitcoin továbbra is dominál az illegális tranzakciók során, de az újabb típusú kriptovaluták, mint a stablecoinok vagy az ethereum gyors térnyerése új kihívásokat jelent a nyomozó hatóságok számára. Ezzel párhuzamosan megállapítható, hogy a privacy coinok marginális piaci súlyuk ellenére kiemelt szerepet töltenek be a pénzmosásban, a zsarolóvírusos támadások lebonyolításában, valamint a dark webes piactereken végbemenő tranzakciók anonimizálásában.

A coin mixer szolgáltatások elemzése megerősítette azt a hipotézist, miszerint a bűnelkövetők tudatosan alkalmaznak olyan technológiai megoldásokat, amelyek jelentősen rontják a visszafejthetőség esélyét. A Monero esete különösen jól példázza, hogy a natív anonimizálási mechanizmusok mennyiben képesek kiváltani a hagyományos coin mixerek funkcióit, sőt meghaladni azok hatékonyságát. A kutatás során feltárt esettanulmányok szemléletesen mutatják be, hogy a kriptovaluták alkalmazása messze túlmutat a pusztá pénzmozgatáson. A kriptovaluta a kiberbűnözés eszközévé válik, amely egyszerre szolgál tranzakciós infrastruktúraként, álcázási technikaként és pénzügyi motivációs közegként.

Ezen eredmények tükrében a kutatás két tézise fogalmazható meg:

T1: A Chainalysis 2024-es és 2025-ös jelentései alapján az elmúlt években markáns eltolódás figyelhető meg a bűnözők által használt kriptovaluták körében. Míg korábban a bitcoin dominanciája volt egyértelmű az illegális tranzakciókban, 2024-re a stablecoinok vették át a vezető szerepet, amint az a 3. ábrán is látható. Ugyanakkor – ahogy azt az ábra magyarázatánál az alapfogalmak fejezetben kifejtettük – a stablecoinok több tokenből álló kategóriát alkotnak, ezért továbbra is megalapozottan kijelenthető és alátámasztható a hipotézis, miszerint a bitcoin még mindig a vezető kriptovaluta az illegális tevékenységekben. A stablecoinok és az ethereum szerepe azonban folyamatosan növekszik, elsősorban a DeFi-ökoszisztéma, az okosszerződések és a széles körű piaci integráció következtében. A privacy coinok globálisan marginális volumennel rendelkeznek, ugyanakkor bizonyos bűncselekménytípusokban – különösen a zsarolóvírusos váltságdíjak kifizetésében és a dark webes tranzakciókban – felülreprezentáltak. A szigorodó szabályozások, például az EU 2024/1624 AMLR rendelete és a nagy kriptotőzsdék privacy coin kivezetései paradox módon tovább növelik az anonim platformok iránti keresletet az illegális piacon. Emellett egyre elterjedtebbek a bűnelkövetők körében a többlépcsős tranzakciós minták, amelyek során különböző kriptovaluták között váltanak – például a bitcoinból etherumra, majd moneróra – kifejezetten a tranzakciók nyomon követhetőségének csökkentése érdekében. Ez a gyakorlat a nyomozó hatóságok számára összetett technológiai és jogi kihívásokat eredményez. A jövőbeni empirikus és kvantitatív elemzések során indokolt lehet részletesen vizsgálni, hogy a stablecoinok egyes tokenjein belül melyek mutatnak kiemelkedő illegális forgalmi aktivitást.

T2: A kriptovaluta-tranzakciók visszakövethetőségét akadályozó technológiák (például coin mixerek, privacy coinok, escrow rendszerek) nem csupán elméleti lehetőségek,

hanem a kiberbűnözésben széles körben alkalmazott eszközök. Ez a gyakorlat közvetlenül alátámasztja a második hipotézist, miszerint a bűnelkövetők folyamatosan alkalmazzák az anonimizálást és a blokkláncon való visszakövethetőség akadályozását szolgáló technológiákat, ami állandó kihívást jelent a bűnüldöző szervek számára. A macska-egér játék logikája egyértelműen megfigyelhető: a technológiai fejlődés mindkét felet egyre kifinomultabb, fejlettebb és innovatívabb módszerek bevetésére ösztönzi, így a nyomozások folyamatosan új akadályokba ütköznek. A kutatás azt is feltárta, hogy a coin mixerek és privacy coinok használata már nem kizárólag a technikailag felkészült bűnelkövetők kiváltsága, hanem felhasználóbarát formában szélesebb kör számára is hozzáférhetővé vált. Ezzel párhuzamosan a bűnüldöző hatóságok a nemzetközi együttműködések erősítésével, valamint a transzparenciát növelő szabályozási keretek, például az FATF Travel Rule és a MiCA alkalmazásával igyekeznek ellensúlyozni ezt a tendenciát.

A fentiek alapján összegzésként kijelenthető, hogy a kriptovaluták jogi, technológiai és bűnüldözési szempontból is egy olyan hibrid kihívást képeznek, amely nem kezelhető pusztán szabályozói, informatikai vagy rendészeti válaszokkal. A hatékony fellépéshez szükség van multidiszciplináris megközelítésre, amely ötvözi a bűnügyi pénzügyi elemzést, a blokklánc elemzést, a nemzetközi együttműködést és a szabályozói eszköztár folyamatos frissítését.

A cikksorozat második része azon technikai és nyomozati módszerek bemutatására fókuszál, amelyek révén a rendvédelmi szervek képesek fellépni a kriptovalutákhoz köthető bűncselekményekkel szemben. Bemutatjuk azokat az eszközöket és eljárásokat, amelyek révén lehetővé válik a kriptovalutákkal összefüggő jogsértések felderítése, a tranzakciók visszaköveteése, valamint a digitális bizonyítékok büntetőeljárásban való felhasználása, ezáltal gyakorlati válaszokat adva a jelen tanulmányban feltárt elméleti kihívásokra.

Felhasznált irodalom

- ALBRECHT, Chad et al. (2019): The Use of Cryptocurrencies in the Money Laundering Process. *Journal of Money Laundering Control*, 22(2), 210–216. Online: <https://doi.org/10.1108/JMLC-12-2017-0074>
- ALFIERI, Carolyn (2022): Cryptocurrency and National Security. *International Journal on Criminology*, 9(1), 21–48. Online: <https://doi.org/10.18278/ijc.9.1.3>
- BAUM, Stafford C. (2018): *Cryptocurrency Fraud: A Look Into the Frontier of Fraud*. Honors College Theses, 2018. november 19. Online: <https://digitalcommons.georgiasouthern.edu/honors-theses/375>
- BEERMAN, Jack et al. (2023): A Review of Colonial Pipeline Ransomware Attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 8–15. Online: <https://doi.org/10.1109/CCGridW59191.2023.00017>

- BERRY, Hala Strohmer (2022): The Evolution of Cryptocurrency and Cyber Attacks. *2022 International Conference on Computer and Applications (ICCA)*, 1–7. Online: <https://doi.org/10.1109/ICCA56443.2022.10039632>
- Chainalysis (2024): *The 2024 Crypto Crime Report*. Online: <https://go.chainalysis.com/crypto-crime-2024.html>
- Chainalysis (2025): *The 2025 Crypto Crime Report*. Online: <https://go.chainalysis.com/2025-Crypto-Crime-Report.html>
- CoinMarketCap (2024): *Binance Delists Privacy-Focused Cryptocurrencies in Multiple European Countries*. Online: <https://coinmarketcap.com/academy/article/binance-delists-privacy-focused-cryptocurrencies-in-multiple-european-countries>
- CUSTERS, Bart – OERLEMANS, Jan-Jaap – POOL, Ronald (2020): Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies. *European Journal of Crime, Criminal Law and Criminal Justice*, 28, 121–152. Online: <https://doi.org/10.1163/15718174-02802002>
- Europol (2015): Darknets–IOCTA 2015. Online: www.europol.europa.eu/iocta/2015/darknets.html
- FATF (2021): *12 Month Review of the Revised FATF Standards. Virtual Assets and VASPs*. Online: www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html
- Intel 471 (2021): *How Cryptomixers Allow Cybercriminals to Clean Their Ransoms*. Online: <https://intel471.com/blog/cryptomixers-ransomware>
- KAMPS, Josh – KLEINBERG, Bennett (2018): To the Moon: Defining and Detecting Cryptocurrency Pump-and-Dumps. *Crime Science*, 7, 18. Online: <https://doi.org/10.1186/s40163-018-0093-5>
- KAVALLIEROS, Dimitrios et al. (2021): Understanding the Dark Web. In AKHGAR, Babak et al. (szerk.): *Dark Web Investigation. Security Informatics and Law Enforcement*. Cham: Springer, 3–26. Online: https://doi.org/10.1007/978-3-030-55343-2_1
- KERR, David S. et al. (2023): Cryptocurrency Risks, Fraud Cases, and Financial Performance. *Risks*, 11(3). Online: <https://doi.org/10.3390/risks11030051>
- LAKSHMANAN, Ravie (2024): Bohemia and Cannabia Dark Web Markets Taken Down After Joint Police Operation. *The Hacker News*, 2024. október 11. Online: <https://thehackernews.com/2024/10/bohemia-and-cannabia-dark-web-markets.html>
- LEVI, Michael (2002): Money Laundering and Its Regulation. *The ANNALS of the American Academy of Political and Social Science*, 582(1), 181–194. Online: <https://doi.org/10.1177/000271620258200113>
- LI, Yannan et al. (2021): Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability. *IEEE Transactions on Dependable and Secure Computing*, 18(2), 679–691. Online: <https://doi.org/10.1109/TDSC.2019.2910058>
- MAJUMDER, Amit – ROUTH, Megnath – SINGHA, Dipayan (2019): A Conceptual Study on the Emergence of Cryptocurrency Economy and Its Nexus with Terrorism Financing. In DAS, Ramesh Chandra (szerk.): *The Impact of Global Terrorism on Economic and Political Development*. Emerald Publishing Limited, 125–138. Online: <https://doi.org/10.1108/978-1-78769-919-920191012>

- MARIANI, Juraj – HOMOLIAK, Ivan (2025): SoK: A Survey of Mixing Techniques and Mixers for Cryptocurrencies. *arXiv*, 2025. április 28. Online: <https://doi.org/10.48550/arXiv.2504.20296>
- Monero (2024): *Moneropedia: Ring Signature*. Online: www.getmonero.org/resources/moneropedia/ringsignatures.html
- MUKHOPADHYAY, Ujan et al. (2016): A Brief Survey of Cryptocurrency Systems. *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 745–752. Online: <https://doi.org/10.1109/PST.2016.7906988>
- NAKAMOTO, Satoshi (2008): *Bitcoin: A Peer-to-Peer Electronic Cash System*. Online: www.researchgate.net/publication/228640975_Bitcoin_A_Peer-to-Peer_Electronic_Cash_System
- NOETHER, Shen (2015): *Ring Signature Confidential Transactions for Monero*. Cryptology ePrint Archive. Online: <https://eprint.iacr.org/2015/1098>
- SCHNEIDER, Friedrich – WINDISCHBAUER, Ursula (2008): Money Laundering: Some Facts. *European Journal of Law and Economics*, 26(3), 387–404. Online: <https://doi.org/10.1007/s10657-008-9070-x>
- Southern District of New York (2025): *Founders of Samourai Wallet Cryptocurrency Mixing Service Plead Guilty*. United States Department of Justice, 2025. augusztus 6. Online: www.justice.gov/usao-sdny/pr/founders-samourai-wallet-cryptocurrency-mixing-service-plead-guilty
- TEKINER, Ege et al. (2021): SoK: Cryptojacking Malware. *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, 120–139. Online: <https://doi.org/10.1109/EuroSP51992.2021.00019>
- TRM Labs (2025): *2025 Crypto Crime Report*. Online: www.trmlabs.com/resources/reports/2025-crypto-crime-report
- UNIX Autó Kft. (2024): Hackertámadás – 2021. 03. 30. Online: www.unixauto.hu/hirlevel/hackertamadas
- ZHANG, Zongyang et al. (2020): A Refined Analysis of Zcash Anonymity. *IEEE Access*, 8, 31845–31853. Online: <https://doi.org/10.1109/ACCESS.2020.2973291>

Jogi források

- Az Európai Parlament és a Tanács (EU) 2023/1114 rendelete (2023. május 31.) a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról
- Az Európai Parlament és a Tanács (EU) 2024/1624 rendelete (2024. május 31.) a pénzügyi rendszer pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről
- Az Európai Parlament és a Tanács (EU) 2024/1640 irányelve (2024. május 31.) a pénzügyi rendszer pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzése érdekében a tagállamok által létrehozandó mechanizmusokról, az (EU) 2019/1937 irányelv módosításáról, és az (EU) 2015/849 irányelv módosításáról és hatályon kívül helyezéséről

Bottyán Sándor¹

Nagy nyelvi modellek az internetes nyílt forrású információgyűjtésben

Alkalmazások és védelmi stratégiák

Large Language Models in Online Open-Source Intelligence

Applications and Defensive Strategies

Absztrakt

A tanulmány az internetalapú nyílt forrású információgyűjtésben (open source intelligence, OSINT) megjelenő nagy nyelvi modelleket (large language models, LLMs) és az ezzel kapcsolatos kihívásokat vizsgálja. Bemutatja az internetalapú OSINT-tevékenység forráskörnyezetét és alkalmazási területeit, továbbá az LLM-ek szerepét ezen a területen. A kutatás fókuszában két olyan alkalmazás (LLM OSINT PoC és InfoHound) áll, amelyek kifejezetten nagy nyelvi modelleket integráltak internetes nyílt forrású információgyűjtésre tervezett keretrendszerekbe. A szerző összehasonlítás keretében vizsgálja a rendszerek architektúráis jellemzőit és utasításait, elemzi továbbá azok hatékonyságát és fenyegetéseit. A tanulmány eredményei között javaslatokat találunk a keretrendszerek képességeivel szembeni olyan védelmi stratégiákra, amelyek mérsékelhetik az LLM-ek segítségével végzett OSINT eredményességét.

Kulcsszavak: OSINT, LLM, információgyűjtés, mesterséges intelligencia

¹ Doktori hallgató, Nemzeti Közszerológati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola.

Abstract

This study examines the emergence of large language models (LLMs) in internet-based open source intelligence (OSINT) and the associated challenges. It presents the source environment and application domains of internet-based OSINT, as well as the role of LLMs in this area. The research focuses on two applications (LLM OSINT PoC and InfoHound) that specifically integrate large language models into frameworks designed for internet-based open source intelligence. The author analyses and compares the architectural characteristics and prompts of these projects, while also assessing their efficiencies and threats. The study concludes with proposals for defensive strategies against the capabilities of such frameworks, aiming to mitigate the effectiveness of LLM-supported OSINT operations.

Keywords: OSINT, LLM, intelligence, artificial intelligence

Bevezetés

Napjainkban a nagy nyelvi modelleket (*large language models*, LLM) alkalmazó interaktív csevegőbotok (például *ChatGPT*, *Gemini*, *DeepSeek*) megjelenése a társadalmi és a gazdasági területeken egyaránt jelentős hatást váltott ki. A jelenség körüli társadalmi népszerűség oka valószínűsíthetően a széles témakörben emberszerű interakciót prezentálni képes alkalmazások megjelenése. A gazdasági felkapottság pedig abban feltételezhető, hogy a transzformátoralapú modellek számos eljárást képesek potenciálisan gyorsítani, részben vagy egészben automatizálni, különösen az adatfeldolgozás, a kommunikáció és döntéstámogatás területén. E két perspektívából a nagy nyelvi modellek körüli diskurzus élénk, ugyanakkor polarizált is. Míg a társadalmi vonatkozásban számos szabályozási, etikai és filozófiai kérdés vetődik fel a témában, a gazdasági területen az LLM-ek alkalmazása új eredményeket és hatékonyabb folyamatokat ígér. Mindazonáltal az ilyen rendszerek széles körű elterjedése mindkét területre egyfajta veszélyt is jelent, így ezek megértése és előrejelzése akár tudományosan is értelmezhető feladat. Különösen figyelemre méltó kockázati szegmens a nagy nyelvi modellek alkalmazása a nyílt forrású információgyűjtésben (*open source intelligence*, OSINT). A nagy nyelvi modellek tanítóanyagát valós, időszerű, hiteles és nyers adatokból állítják elő, továbbá ugyanezek az adatok az OSINT-tevékenység forrásai is. Elgondolkodtató, hogy ez az unió hogyan gyakorol kölcsönhatást mindkét szereplőre, így hát ez az elméleti kérdés határozottan megfogalmazható néhány tudományos feltételezésben is.

Kutatási célok és hipotézisek

Jelen tanulmány alapvető célja, hogy áttekintse az LLM-ek alkalmazását az interneten végzett nyílt forrású információgyűjtésben, valamint speciális célkitűzése azon OSINT-LLM keretrendszerek részletes elemzése, amelyek hatékonyan képesek ötvözni

a hagyományos OSINT-eszközöket a nagy nyelvi modellek képességeivel. Ennek érdekében a kutatás során három fő hipotézist vizsgálunk:

H1: Feltételezhető, hogy a nagy nyelvi modelleket már aktívan alkalmazzák az internetalapú nyílt forrású információgyűjtés (OSINT) területén.

H2: Feltételezhető, hogy a nagy nyelvi modellek internetalapú OSINT-célú alkalmazása esetén azok új típusú, LLM-specifikus kiberbiztonsági fenyegetést jelentenek.

H3: Amennyiben a H1 és H2 hipotézisek igaznak bizonyulnak, feltételezhetően azonosíthatók olyan védelmi stratégiák, amelyek kifejezetten az LLM-ekkel végzett internetalapú OSINT-tevékenységekhez kapcsolódó fenyegetések megelőzésére és kezelésére alkalmasak.

A fenti célok elérése érdekében a hipotézisek mentén többértű módszertant alkalmazunk. Az OSINT-témakör szükségszerű leíró feldolgozása mellett az internetes tartalomkutatásban (leginkább szürkeirodalomnak tekinthető esettanulmányok alapján) azonosított LLM-ágensek technológiai rendszerelemzése (architektúra és utasításkészlet) és ezek összehasonlításának leírása történik meg. A vizsgálathoz szükséges adatokat egy korábbi, a 2024. év második félévében végzett szekunder kutatás szolgáltatta. Ennek során kulcsszóalapú (kulcsszavak: OSINT, LLM, *open source intelligence*, OSINT-AI) kereséssel weboldalakról, dokumentációkból, GitHub oldalakról származó olyan projektek, szoftverek, keretrendszerek azonosítása ment végbe, amelyek az interneten történő nyílt forrású információgyűjtéshez nagy nyelvi modell képességet alkalmaznak architektúrájukban. Keresési követelményként lett megfogalmazva az OSINT-LLM funkcionalitás részletekbe menő megismerhetősége, a forráskódok elérhetőségén alapuló architektúra- és utasításvizsgálat. A tanulmány az összeállított információk szintézisével megállapítottak mellett a védelmi lehetőségek meghatározásával és predikciók alkotásával próbál hozzájárulni az esetleges új fenyegetésekből fakadó kockázatok kezeléséhez.

Az internetes nyílt forrású információgyűjtés

Az információgyűjtés konvencionálisan a különféle hírszerző szervek feladata volt,² így az OSINT is kizárólag nemzetbiztonsági és katonai hírszerzési tevékenységként jelent meg kezdetben. Ezt igazolja az Amerikai Egyesült Államok katonai fogalomtára is, amely alapján a teljes spektrumú hírszerzési tevékenység (*all-source intelligence*, ASI) három fő (ügymond hagyományos) kategóriából áll: emberi ügynökökön alapuló hírszerzés (*human intelligence*, HUMINT), technikai eszközökkel támogatott hírszerzés (*technological intelligence*, TECHINT), valamint a nyílt forrásokból történő információgyűjtés (OSINT).³ Az elmúlt évtizedek során mindazonáltal jelentős változások következtek be a hírszerzés forráskörnyezetében és annak művelői körében egyaránt. Egyrészt a digitalizáció robbanásszerű fejlődésének köszönhetően a kibertérben található adatok mennyisége drámai módon megnövekedett, ami költséghatékonyabban feldolgozható, részben nyíltan elérhető információforrásként szolgál.

² VADÁSZ 2018: 64.

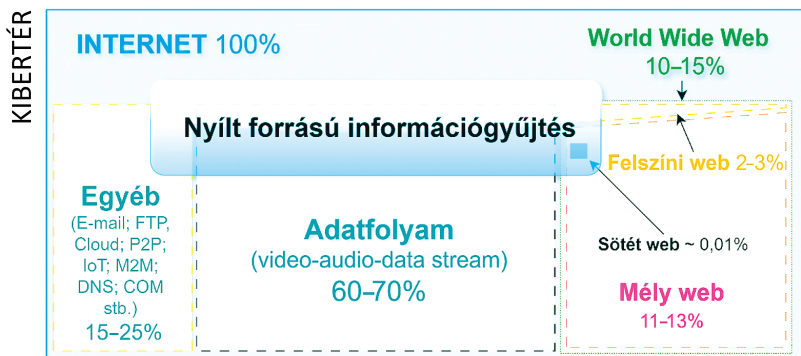
³ Department of Defense 2010.

Másrészt ez a jelenség létrehozta azt a változást, amely során a hírszerző tevékenység eredményei iránt érdeklődő entitások köre is bővült, ezáltal természetesen a korábbi hagyományosnak mondható cél és módszertan is megváltozott.

Az utóbbi időszakban az OSINT már bőven túllépett az állami alkalmazás privilégiumán és a versenyszférában is egyre jelentősebb szerepet tölt be. A gazdasági szervezetek partner-, konkurencia- és beszállítóelemzésre, az újságírók tényfeltáró munkára, a pénzügyi intézetek ügyfél-azonosításra és kockázatelemzésre használják, e mellett a kiberbiztonsági vizsgálatok egyik meghatározó biztonsági eljárásává is vált.⁴ E többreű folyamat céljának, feladatainak, eszközrendszerének és módszertanának pontos meghatározása nehéz feladat, kiváltképp hogy annak határa az adatvédelem szempontjából különösen elmosódott.⁵ Bár az OSINT forrásai változatosak lehetnek (például nyomtatott média, nyílt rendezvények, közvetlen megfigyelés stb.), jelen tanulmány kizárólag az internetes nyílt forrású információgyűjtés területén tájékozódik. Ez a tevékenység lényegében az interneten nyíltan és bárki számára elérhető, transzparens és legitim módszertannal megszerzett adatok összegyűjtését, előre meghatározott cél szerinti elemzését, értékelését (együttesen feldolgozását) és továbbítását jelenti.

Az internetalapú OSINT forrásai

Az internetes információgyűjtés kapcsán lényeges megemlíteni, hogy az internet ismert információforrásait rétegekre tagolhatjuk, és megbecsülhetjük azok egymáshoz viszonyított terjedelmének arányát (1. ábra).



1. ábra: Az internet rétegeinek becsült összetétele és a nyílt forrású információgyűjtés viszonya

Forrás: a szerző szerkesztése

⁴ Precognox 2022.

⁵ Az itt említett konfliktus alatt azt értjük, hogy nyílt forrású adatnak minősül a legális módon, vagyis jogszabályba nem ütközően megszerezhető adat. Az internetalapú OSINT adatforrásait tekintve az azokkal szemben felállított legfőbb kritérium az, hogy nyíltak legyenek, tehát bárki számára elérhetők. Ugyanakkor az eltulajdonított, majd nyilvánosan közzétett személyes vagy védett adat is ide tartozik, amelyet ugyanakkor továbbra is véd az adatvédelmi jog.

Teljes internetes információgyűjtés alatt az interneten fellelhető bármely adatforrás felhasználását értjük, amelybe természetesen beletartozik a teljes világháló (*world wide web*, *www*), valamint annak mélyebb rétegei is. A legszélesebb körben ismert felszíni web (*surface web*) a nyilvános és könnyen hozzáférhető weboldalak csoportja, amely technikailag a legkönnyebben elérhető OSINT-forrás. A mély web (*deep web*) tartalmai hagyományos keresőmotorokkal már nem érhetők el. Ez leginkább autentikációt követően elérhető weboldalak tartománya, például vállalati intranetek,⁶ privát vagy előfizetési tartalmak, jelszóval védett fórumok és a közösségi oldalak csoportjai sorolhatók ide. A közösségimédia-platformok látszólag ellentmondanak a nyílt forrású információgyűjtés alapdefiníciójának, de ki kell emelni, hogy a legtöbb ilyen mély webes weboldalhoz a hozzáférés nyilvánosan elérhető. Ilyenkor technikailag *nyíltan hozzáférhető mély webtartalomról* beszélünk, ami OSINT-szempontról forrásnak minősítendő, csak a módszertan eltérő némileg. Azonban vannak korlátozott hozzáférésű (például előfizetési weboldalak vagy szervezeti intranet) mély weboldalak, amelyek már nem tartoznak az OSINT forrásai körébe. A *deep web* egy kisebb tartománya a sötét web (*dark web*), amely bár méretét tekintve elhanyagolható, de funkciója (főként illegális kereskedelmi tevékenységeknek vagy az anonimitás megőrzésére törekvő egyéb tartalmaknak ad helyet) okán közismert terület.⁷ Ez a világháló egy olyan speciális része, amely kizárólag anonim hálózatokon (például Tor, I2P, Freenet) érhető el. Ezzel összefüggésben itt is ki kell térni a meghívásos rendszer keretében vagy költség ellenében hozzáférhető weboldalakra, amelyek feldolgozása szintén nem felel meg a nyílt forrású információgyűjtés módszertani követelményének.

Emellett az internet jelentős adatforgalmat generáló része az adatfolyam (*streaming*), amely olyan platformoknak ad otthont, mint a videószoftverek (például YouTube, Netflix stb.), az audio- vagy zeneszoftverek (például Spotify, online rádiók stb.), illetve az élő közvetítések (például Twitch). Továbbá az internet szintén önálló részébe soroljuk a kisebb szolgáltatásokat, amelyek a teljesség igénye nélkül a fájlátviteli (például FTP, SFTP stb.), az e-mail (például SMTP, IMAP stb.), a kommunikációs (például IRC, WhatsApp, Messenger), a felhőtárhely (például Google Drive, Onedrive stb.), a *peer-to-peer* (P2P-) szolgáltatások, valamint az IoT (*internet of things*) és az M2M (*machine-to-machine*) kommunikációs és hálózati szolgáltatások (például DNS, DHCP). Tekintve, hogy ez az információforrás-csoport számtalan forrástípust tartalmaz, az OSINT-forrásként való értelmezésük nem homogén. A nyíltan hozzáférhető streamingből kinyerhető adatok (például videók tartalma, képi információk, helyszínek, személyek, időpontok, kommentek, reakciók, metaadatok) megfelelnek e tekintetben. Ugyanakkor a privát elektronikus levelezések természetesen nem, de a nyíltan hozzáférhető e-mailek és archívumok tartalmaikkal és metaadataikkal viszont már a legitim források közé sorolhatók. A többi említett szolgáltatásnál (például FTP, IoT, P2P stb.) is azonos elveket kell használni a forrásként való validálás során.

⁶ Az intranet egy zárt, belső számítógépes hálózat, amelyet egy szervezet használ az információk és erőforrások megosztására a munkatársai között.

⁷ ROSENGREN 2022: 24.

Az internetalapú OSINT eszközei

Az internetes források vonatkozásában értelmezett OSINT-eszközök olyan célszoftverek, platformok, vagy egyéb informatikai megoldások (valamint a használatukkal megvalósított technikák), amelyeket az interneten található nyilvánosan hozzáférhető információk hatékony megszerzésére és feldolgozására (strukturálásra és elemzésre) fejlesztettek. Az ilyen eszközök leltárának az információbiztonsági indíttatásból létrejött OSINT Framework⁸ platform ad otthont, de azok színes skáláját mutatja be a svájci i-Intelligence vállalat által készített *Open Source Intelligence Tools and Resources Handbook*, vagyis a nyílt forrású információgyűjtési eszközök és források kézikönyve is, amelyet elsődlegesen nyomozók és információbiztonsági szakemberek támogatására hoztak létre.⁹

Az internetalapú OSINT-eszközöket alkalmazási területük és funkciójuk szempontjából megkülönböztethetjük az alábbi csoportok szerint:

- adatgyűjtő, adatfeldolgozó és adatvizualizációs eszközök (például RSS-olvasók, *scraping*¹⁰ eszközök, hálózatelemző és infografika-készítő szoftverek és szolgáltatások stb.);
- általános keresőmotorok, dokumentumkutató és dokumentumelemző eszközök (például piacvezető keresők, metaadat-keresők stb.);
- infokommunikációs felderítő eszközök (például informatikai hálózati információk felderítésére, sebezhetőségazonosításra alkalmazott szoftverek stb.);
- közösségimédia-elemző eszközök (például főbb közösségimédia-platformok, blogok, fórumok és Q&A¹¹ oldalak kereső- és elemzőeszközei stb.);
- multimédiás eszközök (például képkereső, arcfelismerő, videó- és hangelemző eszközök stb.);
- személykereső és -ellenőrző eszközök (például nevek, felhasználónevek, telefonszámok és e-mailek keresésére, nyilvántartások forrásfelhasználására fejlesztett eszközök stb.);
- térinformatikai és közlekedésvizsgáló eszközök (például online térképek, műholdfelvételek, repülő-, hajó- és járműkövető szoftverek stb.);
- üzleti célú eszközök (például cégalapbázisok, állás- és béradatbázisok kezelésére, versenytársak feltérképezésére, üzleti partnerek megbízhatóságának vizsgálatára készült alkalmazások és szolgáltatások stb.).

Az eszközökkel szemben megfelelőségi követelményeket is meghatározhatunk, bár meg kell jegyezni, hogy ezek leginkább csak elvi követelmények, hiszen a többnyire ingyenesen elérhető OSINT-alkalmazásokat – a maximális hatékonyság elérése okán – nem készítik fel az elméleti alapvetések maradéktalan teljesítésére. Ezek a következők:

⁸ BIELSKA 2020.

⁹ BIELSKA 2020; BOTTYÁN 2024:16.

¹⁰ Az *internet scraping* (vagy *web scraping*) olyan automatizált folyamat, amellyel weboldalakról adatokat gyűjtnek le strukturált formában.

¹¹ *Questions and answers* (kérdések és válaszok).

- kizárólag nyíltan, külön engedély vagy jogosultság nélkül elérhető adatot használhat fel forrásként;
- az eszköz által begyűjtött információk eredete visszakövethető és ellenőrizhető;
- az információkhoz való hozzáférés nem lehet sértő szándékú, tehát nem tartalmazhat etikailag kifogásolható technikai tevékenységet (például *brute-force*, tiltott *scraping* stb.);
- az eszköz információgyűjtési mechanizmusa összhangban van a hatályos adatvédelmi jogszabályokkal (például GDPR,¹² Infotv.¹³), és működése transzparens (átlátható és dokumentált).

Az eszközöknek széles körű alkalmazási területe van, többek között:

- katonai hírszerzés: hadászati, hadműveleti és harcászati támogatás (például információk műveletek azonosítása, saját katonai műveletek támogatása);
- kiberbiztonság: saját infrastruktúra sérülékenységeinek felkutatása, fenyegetés-hírszerzés (*cyber threat intelligence*, CTI);
- nemzetbiztonsági hírszerzés: stratégiai (például geopolitikai) információgyűjtés, humanitárus válsághelyzetek követése, radikalizáció és terrorizmus-felderítés;
- nyomozó hatóságok és rendvédelmi szervek tevékenysége: gyanúsítottak, tanúk vagy eltűnt személyek azonosítása, kapcsolati hálók meghatározása, tartózkodási helyük megállapítása;
- oknyomozó újságírói kutatás: információk keresése, háttér-információk ellenőrzése;
- piackutatás, üzleti intelligencia: versenytársak elemzése, trendek felkutatása;
- politikai tevékenység: politikai ellenfelek elemzése, választói hangulat monitorozása, reputációmenedzsment, narratívátámogatás, civil szerveződések monitorozása.

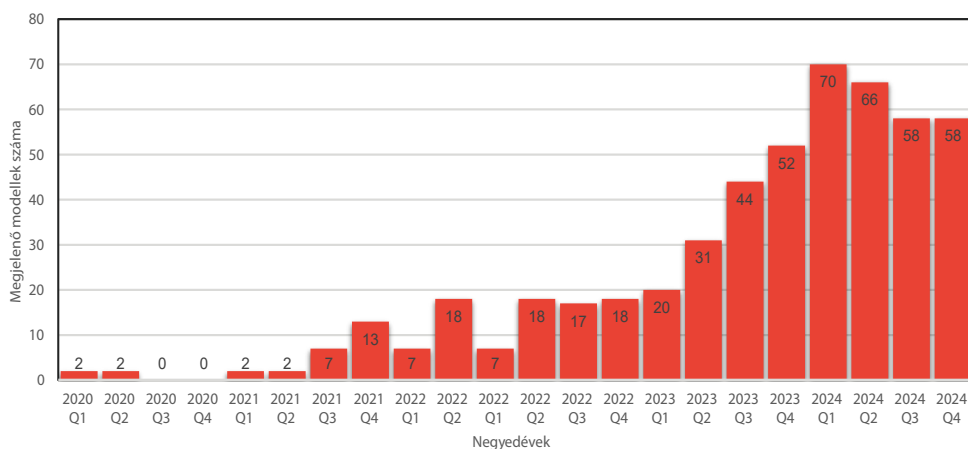
A nagy nyelvi modellek

A legtöbb ezzel a témával foglalkozó tudományos értekezés a nagy nyelvi modellek népszerűségének alapkövét egy 2017-ben történt eseményhez, vagyis a Google által fejlesztett transzformátormodell és annak figyelemmechanizmusának bemutatásához köti. Ez az esemény jelentős lendületet hozott a természetes nyelvi feldolgozás (*natural language processing*, NLP) tudományos területén, csakhogy a társadalmi és gazdasági rétegeket egyaránt megmozgató jelenség a ChatGPT megjelenése volt 2022 novemberében. A hétköznapi emberek nyilvánosan ekkor léptek kapcsolatba egy kifejezetten emberi csevegésre finomhangolt nagy nyelvi modell interaktív felületével, megismerhették annak megdöbbentő képességeit. A megjelenéssel járó popularitás

¹² Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).

¹³ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

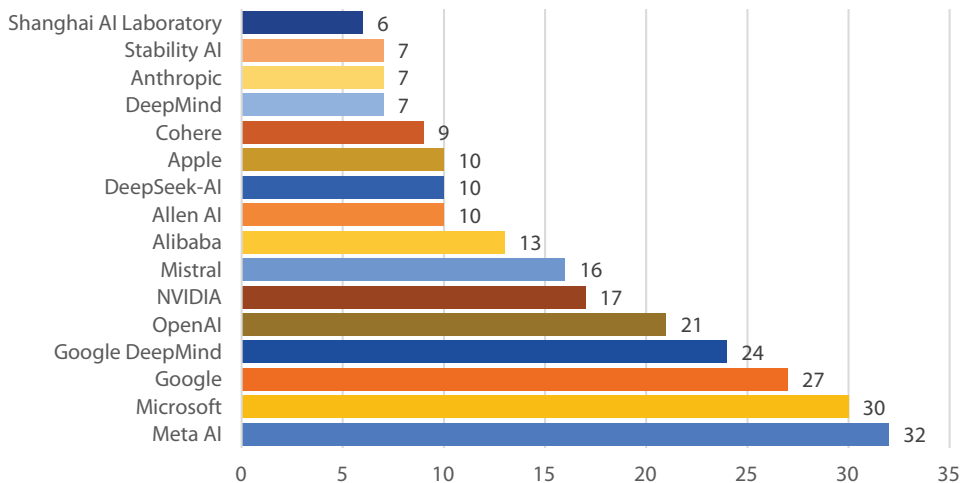
olyan globális gazdasági hatásokat eredményezett, amelyeknek köszönhetően az óriásvállalatok jelentős tőkét csoportosítottak át a mesterséges intelligencia, különösen az LLM fejlesztésébe. E mellett számos infokommunikációs ipari szervezet gondolta újra innovációs politikáját és dinamikusabban fordult az AI- (*artificial intelligence*, vagyis mesterséges intelligencia) fejlesztések irányába. Természetesen az olyan AI-terület, mint a gépi tanulás (*machine learning*, ML) továbbra is dinamikusan fejlődő megközelítés maradt, de a nagy nyelvi modellek egy negyedévre jutó megjelenéseiből egyértelműen megállapítható a közel négyszeres növekedés 2022 utolsó (Q4) és 2024 első negyedéve (Q1) között. Ez a magas számú LLM-eredménytermék-növekedés valószínűsíthetően a 2022 utolsó negyedévében (Q4) történt tőkeinjektálással meginduló, kifejezetten gyors ciklusú kutatási-fejlesztési (K+F-) folyamatok eredménye (2. ábra).



2. ábra: A nagy nyelvi modellek megjelenése 2020–2024 között

Forrás: a szerző szerkesztése a *lifearchitect.ai* 2025. 02. 10-ei adatai alapján

A növekedés azért is figyelemre méltó, mert a nagy nyelvi modellek fejlesztése kifejezetten összetett feladat. Szignifikáns mértékű interdiszciplináris humán szakértelmet igényel, hiszen több kutatói és mérnöki szerepkör (például adatmérnökök, nyelvészek, NLP-szakértők, szoftverfejlesztők, adatvédelmi és jogi szakértők stb.) együttes alkalmazása, valamint számos monumentális információs és kommunikációs technológiai (*information and communication technology*, ICT) erőforrás megléte indokolt. Ezeket a jelentős mennyiségű és szerteágazó szükségleteket csak a világviszonylatban legnagyobb szoftver- és technológiai ipari, kutatási fejlesztési képességekkel is rendelkező óriásvállalatok tudják biztosítani. Ilyen piaci szereplők az Amerikai Egyesült Államokban (Apple, NVIDIA, OpenAI, Google, Microsoft, Meta AI, Allen AI, Anthropic), Kínában (Shanghai AI Laboratory, Alibaba, DeepSeek-AI), az Egyesült Királyságban (DeepMind, Stability AI) és Kanadában (Cohere) vannak, az általuk 2020–2024 között létrehozott nagy nyelvi modellek számát a 3. ábra mutatja.



3. ábra: A legnagyobb technológiai nagyvállalatok által bemutatott LLM-megjelenések száma 2020–2024 között

Forrás: a szerző szerkesztése a lifearchitect.ai 2025. 02. 10-ei adatai alapján

Bár a nagy nyelvi modellek népszerűsége töretlen, valószínűsíthető, hogy a jövőben a modelltípusok száma csökkenni fog, és bár alacsonyabb számban, de eredményesebb architektúrák megjelenésére lehet számítani. A modellek az NLP területén elért eredményeikkel számottevő hatást gyakorolnak az élet számos területére, hiszen az emberszerű automatizáltság növelésére mindenhol igény van. Ezt a tényezőt használják fel egyesek a nyílt forrású információgyűjtés területén is, de mielőtt rátérnénk a gyakorlati alkalmazásra, röviden bemutatjuk az LLM-modellek jellemzőit.

A nagy nyelvi modellek csoportosítása

A nagy nyelvi modelleket elérhetőségük szerint két csoportba sorolhatjuk, vannak nyílt forráskódú (*open-source*) és zárt (esetleg részben zárt rendszerként működő, felhőalapú) úgynevezett *hostolt* modellek. Az előbbi csoportba tartozó LLM-ek esetében a modell forráskódját, a tanítási adatokat, súlyokat, dokumentációkat nyilvánosan – részben vagy egészben – bárki számára elérhetővé teszik, ennek köszönhetően a fejlesztők és kutatók szabadon módosíthatják azokat. A zárt vagy *hostolt* modellek esetében általában a fejlesztést végrehajtó nagyvállalat üzemelteti a modellt, és előfizetés (legtöbbször *pay as you go*¹⁴ fizetési rendszer alkalmazásával) ellenében, általában API-n¹⁵ vagy felhőszolgáltatáson keresztül, valamint interaktív webfelületen biztosítja a hozzáférést. Ez esetben a fejlesztő nem osztja meg a modell forráskódját

¹⁴ A *pay as you go* (PAYG) egy fizetési modell, amelyben a felhasználó kizárólag a termék használatáért fizet. Leginkább technológiai szolgáltatásoknál (például felhőalapú szolgáltatások, API-k, mesterségesintelligencia-modellek használata stb.) alkalmazzák.

¹⁵ *Application programming interface* (alkalmazásprogramozási interfész).

és a hozzá tartozó egyéb információkat, ellenben korlátozott lehetőséget biztosít a modell bizonyos képességeinek használatához. Általánosságban elmondhatjuk, hogy a nyíltan elérhető modellek képességei alulmúlják a *hostolt* modellekét, a különböző *benchmarkok*¹⁶ listáját általában a legnagyobb óriásvállalatok kutatóközpontjai által létrehozott csúcsmodellek vezetik.

Az LLM-ek valós idejű információgyűjtési képessége

Az információkeresés az NLP egyik olyan területe, amelyben az LLM-ek elismerten kiváló teljesítményt nyújtanak. A kontextuális jellemzőkkel együttesen beágyazott vektorértékeknek köszönhetően hatékonyan képesek a szöveges tartalmak közötti kapcsolatok azonosítására, így képesek a keresések során megfelelő információt szolgáltatni. Ugyanakkor az LLM-ek tanítóadatai múltbéliak, így bizonyos kérdésekben nem képesek aktuális (időszerű) információkat szolgáltatni, ami ellenben lényegi jellemzője és követelménye is az információgyűjtésnek. Az utóbbi években, a nagy nyelvi modellek elterjedésével megjelent az igény arra, hogy annak kontextuális képességeit valamilyen módon internetes keresési funkcióként is alkalmazzák. A közismert ChatGPT-t üzemeltető OpenAI először 2023 nyarán egyfajta béta teszt jelleggel a Bing keresőmotorjának integrálásával lehetővé tette a modellen keresztül internetes keresés lehetőségét. Az eseményt követően probléma merült fel, mert a Bing modullal végzett LLM-keresések képesek voltak hozzáférni bizonyos híroldalak alapvetően felhasználói előfizetéssel elérhető szöveges tartalmaihoz, majd az információt ingyen megosztani a ChatGPT felhasználóival.¹⁷ Az OpenAI ekkor eltávolította a Bing modult a *chatbotból*, majd a hiba javítását követően újra visszahelyezte 2023 őszén.¹⁸ A keresőfunkció néhány *ChatGPT release*¹⁹ esetében a mai napig elérhető, de alkalmazása közben észlelhetjük a *chatbot* szigorú energiagazdálkodási konfigurálásának következményét, miszerint a keresési munkamenetet gyorsan lefuttatja, és minimális információt gyűjtve tér vissza a válasszal. A modellek által megszerzett információk mennyisége csekély, további feldolgozásra nem alkalmas, így önálló OSINT-eszközként valószínűleg nem tekinthetők hatékonynak.²⁰

A kutatás

A kutatási cél érdekében végzett keresés során mindösszesen két olyan keretrendszert sikerült azonosítani, amelyek az előzetesen meghatározott követelményeknek evidenciákkal alátámaszthatóan eleget tesznek. A következőkben e projekteket mutatom be,

¹⁶ A *benchmark* kifejezés általában egy standard teszt vagy referenciaérték, amelyet teljesítmény mérésére használnak.

¹⁷ OKEMWA 2023; Holupredictions 2023.

¹⁸ ROGERS 2023.

¹⁹ A *release* kifejezés az adott modell új változatának kiadására, vagyis megjelenésére utal.

²⁰ BOTTYÁN 2024: 54.

megemlítve architekturális jellemzőiket, kiemelten vizsgálva LLM-komponenseiket és -utasításait (*prompt*).

LLM OSINT

Az ingyenesen használható LLM OSINT komplex keretrendszer, amelynek célja, hogy az interneten elérhető források felhasználásával minél többet tudjon meg egy adott személyről, szervezetről, helyről, dologról stb. Tekintve, hogy a projekt nem kapott sajátos elnevezést és csak *proof of concept* (PoC),²¹ a következőkben a könnyebb azonosíthatóság okán LLM OSINT PoC-ként hivatkozunk rá. Ez a keretrendszer-architektúra több szálon, több típusú nagy nyelvi modellt vesz igénybe az információgyűjtés során. A koncepció már a kezdeti web ágensében (*initial web agent*, IWA) egy GPT-4.0-t kér fel az internetes nyílt információgyűjtésre, egy kifejezetten OSINT-ügynök persona²² használatával (4. ábra).²³

PREFIX = Te egy automatizált OSINT-ügynök vagy, aki kiválóan képes információt felkutatni személyekről, vállalatokról, helyekről és más témákról. A kérdés/gondolat/tevékenység/megfigyelés formátumot használd a keresések során. Ha kimerítetted a rendelkezésre álló forrásokat, NE ÁLLJ MEG, végezz újabb keresést bármilyen olyan részletről, amelyről további információt szerezhetsz! Válaszold meg a felhasználó kérdéseit az internet átvizsgálásával és légy nagyon alapos!

Tippek:

Mindig olvasd el a hivatkozott weboldalakon szereplő tartalmakat, amelyek további információt nyújthatnak a kérdés megválaszolásához!

A weboldalak tartalmát rekurzívan használd fel újabb információk felfedezéséhez! Kövesd a linkeket, amelyek további adatokkal szolgálhatnak!

4. ábra: Az LLM OSINT PoC IWA által futtatott angol nyelvű prompt magyar nyelvre fordítva

Forrás: a szerző szerkesztése és fordítása a https://github.com/sshh12/llm_osint oldalon található információk alapján

Az IWA által visszajuttatott információkból a mélyelemző webes ügynökök (*deep dive web agents*, DDWA) Serper²⁴ API felhasználásával olyan internetes hivatkozásokat kutatnak fel, amelyek tartalmazzák a megjelölt információkat. Ezt követően a weboldalak forráskódjait Scrapingbee API segítségével (ezt nevezik *web scrapingnek*²⁵)

²¹ A *proof of concept* kifejezés jelentése: koncepció igazolása vagy próbaüzem, műszaki és üzleti szférában is használatos fogalom.

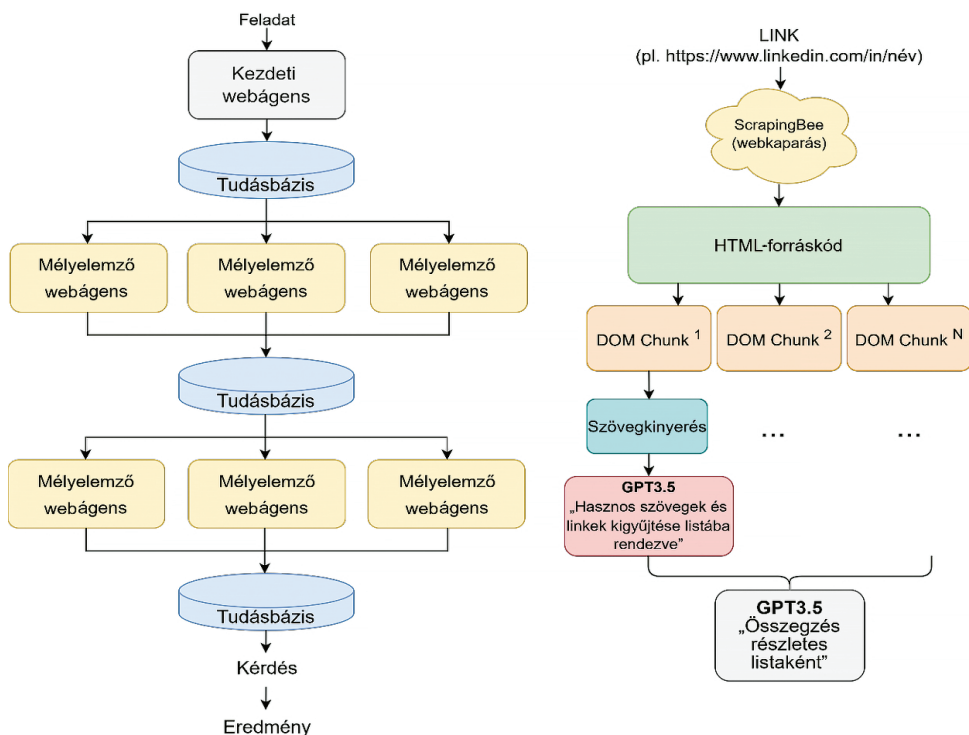
²² A kifejezés a nagy nyelvi modellek esetében arra a mesterséges szerepre vagy személyiségre utal, amelyet a modell vesz fel a felhasználóval folytatott kommunikáció során. Ez a szerep meghatározhatja a beszédstílust, a szóhasználatot, az ismeretek körét, sőt azt is, hogy a rendszer milyen nézőpontból válaszoljon.

²³ BOTTYÁN 2024: 62.

²⁴ A Serper egy gyors és költséghatékony Google-kereső, amely lehetővé teszi a felhasználók számára, hogy automatizált módon hozzáférjenek a Google keresési eredményeihez.

²⁵ A *web scraping* folyamán – emberi olvasásra alkalmas, de közvetlen gépi feldolgozásra alkalmatlan – adatot gyűjtünk weboldalakról.

további feldolgozás céljából letöltik. A keretrendszer a kinyert adatokat (HTML-forráskód) – azok méretbeli nagysága miatt – tovább tisztítja olyan formátumú DOM-*(document object model)*²⁶ *chunkokra*,²⁷ amelyek már alkalmasak a GPT-3.5 általi reprezentálásra.²⁸ A modell ebből a nagyszöveges *promptból*²⁹ kivonatolja a leg-
hasznosabb adatokat egészen addig, amíg a GPT-3.5 tokenizálási korlátját³⁰ el nem éri, majd ez addig ismétlődik, amíg a legutolsó műveletnél elfogy a feldolgozandó tartalom. Az eredményként kinyert részletek újfent visszacsatolódnak a GPT-3.5-be, és az adatok összegzése történik meg végeredményként (5. ábra).³¹



5. ábra: Bal oldalt az OSINT-LLM PoC web ügynökeinek működése, jobb oldalt a web scraping adatfeldolgozás szemléltetése

Forrás: a szerző szerkesztése és fordítása a https://github.com/sshh12/llm_osint alapján

²⁶ Platformfüggetlen, fa struktúrájú programozási modell, amely lehetővé teszi a HTML- vagy XML-dokumentumok elemeinek dinamikus elérését és módosítását.

²⁷ A *chunk* egy adott hosszúságú szövegrészlet (pl. mondat, bekezdés vagy fix hosszúságú tokensorozat), amelyet a modell egyszerre képes feldolgozni.

²⁸ A nagy nyelvi modellek során a reprezentálás azt jelenti, hogy a nyelvi elemeket (szavakat, mondatokat) olyan matematikai struktúrákká, például többdimenziós vektorokká alakítják, amelyeken a modell képes elvégezni a matematikai műveleteket.

²⁹ A *prompt* egy szöveges bemenet vagy utasítás, amelyet a felhasználó megad a modellnek annak érdekében, hogy a modell az adott szövegre reagálva választ, tartalmat vagy információt generáljon.

³⁰ *Token limit*. A nagy nyelvi modellek esetében azt a maximális mennyiségű tokenre (a szöveg egyik feldolgozási egysége) vonatkozó határt jelöli, amelyet a modell egy adott bemeneten belül kezelni tud.

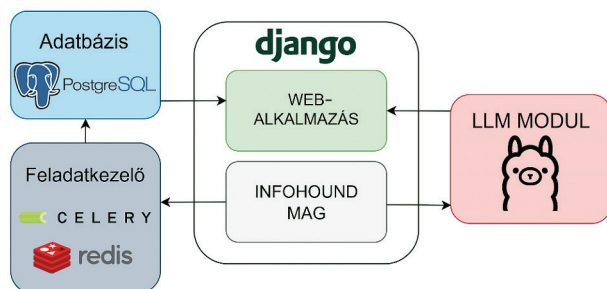
³¹ BOTTYÁN 2024: 63.

Az összegyűjtött információkat LLM-utasításban felhasználva a *hostolt* GPT – a korábbi tanítóanyagából kikövetkeztetve – képes akár a célszemély pszichológiai jellemzőit is (például személyiségvonások, motivációs tényezők, viselkedési mintázatok) feltárni.

InfoHound

Az InfoHound egy információgyűjtő és -feldolgozó OSINT-eszköz, amely képes jelentős mennyiségű adatot feltárni az előzetesen megcélzott domainről. Az i2CAT³² által kifejlesztett eszköz leginkább személyekre vonatkozó információkat (például személyneveket, e-mail-címeket, felhasználóneveket), valamint aldomaineket, fájlokat, URL-³³ címeket gyűjt össze. Az adatvizualizáció mellett képes kimutatást készíteni a begyűjtött URL-ek, a felfedezett aldomainek, a felfedezett személyek, az észlelt fájlok, az észlelt e-mailek számáról.³⁴

Architektúráját tekintve nyílt forráskódú modulokból áll (6. ábra). Egy Django keretrendszeren fejlesztett webes alkalmazás szolgáltatja a felhasználófelületet, a webalkalmazáson indított adatgyűjtési háttér folyamatok futtatása Celery-n történik meg, amely a gyűjtés eredményeit a PostgreSQL adatbázisba továbbítja. A végleges adatokat a webalkalmazás jeleníti meg. A webalkalmazásból indított elemző feladatok során a feladatok munkafolyamatát szintén a Celery végzi, a Redis³⁵ szoftver a kommunikációért felel. Specifikuma, hogy több Python könyvtár alapú OSINT-eszköz (például BeautifulSoup, DNSPython, E-mail-validator, Holehe, Shodan stb.) van integrálva a keretrendszerbe. Az InfoHound önmagában is kifinomult OSINT-eszköz, de legújabb verziója már LLM-támogatással is rendelkezik, méghozzá az Ollama felhasználásával.³⁶



6. ábra: az InfoHound keretrendszerének kialakítása

Forrás: a szerző szerkesztése és fordítása a GitHub Fundacio-i2CAT/InfoHound 2024 alapján

³² Fundació Privada Internet i Innovació Digital a Catalunya.

³³ *Uniform resource locator* (egységes erőforrás-azonosító) rövidítése. Az interneten fellelhető erőforrások (pl. weboldalak, képek vagy videók) elérési útvonalát és címét határozza meg.

³⁴ CyberRaya 2023.

³⁵ A Redis nyílt forráskódú, memóriában futó kulcsértékalapú adatbázis, amelyet elsősorban gyors adatkezelésre és gyorsítótárazásra használnak.

³⁶ BOTTYÁN 2024: 67.

Az Ollama egy nyílt forráskódú keretrendszer, amely biztosítja a szintén nyílt forráskódú LLM-ek futtatását felhő- és internetszolgáltatás nélkül saját számítógépen (vagy úgy mond *on-premise*³⁷ megoldásként). Praktikus eszköz azok számára, akik a klasszikus operációs rendszereken (macOS, Linux, Windows) kívánnak nagy nyelvi modelleket (például Llama 2, Mistral, Dolphin Phi, Phi-2, Neural Chat, Starling, Code Llama stb.) futtatni. Az InfoHound legújabb verziója alapértelmezetten az Ollama által futtatott Llama 2 nagy nyelvi modellt alkalmazza – az OSINT-eszközök által összegyűjtött adatok felhasználásával – a szervezeti struktúra meghatározásához vagy a személyek szervezeten belüli szerepének azonosításához.

```
summarize_prompt = "Foglalja össze a személy foglalkozását mindössze 150 szóban a  
következő adatok alapján:"  
raw_data = entry.raw_metadata  
print ("Az AI-alapú profilelemzés végrehajtása:" + entry.name)  
entry.occupation_summary = ollama.ollama_flexible_prompt(summarize_prompt +  
raw_data)  
print ("Összegzés: " + entry.occupation_summary)  
entry.save()
```

7. ábra: Az InfoHound azon forráskódrészlete, amely a Llama 2 részére kiadott utasítást tartalmazza (magyarra fordítva)

Forrás: a szerző szerkesztése és fordítása a <https://github.com/ollama/ollama> alapján

Annak ellenére, hogy az InfoHound OSINT szempontból egy igen komplex rendszer, az LLM-komponenst utasító prompt (7. ábra) egyszerűnek mondható, pedig a témában már igen részletes utasításábrázolás is létezik.³⁸ Eszerint a fejlesztő nem törekedett az LLM-képességek hatékonyabb kihasználására, bár természetesen e tekintetben a Llama 2 nyelvi funkciói is lényegesen korlátozottabbak *hostolt* társainál.

A két vizsgált megközelítés között egyértelműen azonosíthatók megegyező és diverzív architektúráis jellemzők is, ami alapján klasszifikálhatók az LLM-et integráló OSINT-architektúrák.

Az OSINT-LLM-keretrendszerek azonosított típusai és jellemzői

A kutatás során feltárt OSINT-LLM-integrációk elemzése alapján megállapítható, hogy bár azok architektúrája, funkciója és jellemzője némileg különbözik, a vizsgált keretrendszerek azonos alapvető komponensekből épülnek fel.

Az OSINT-LLM-keretrendszer fő elemei:

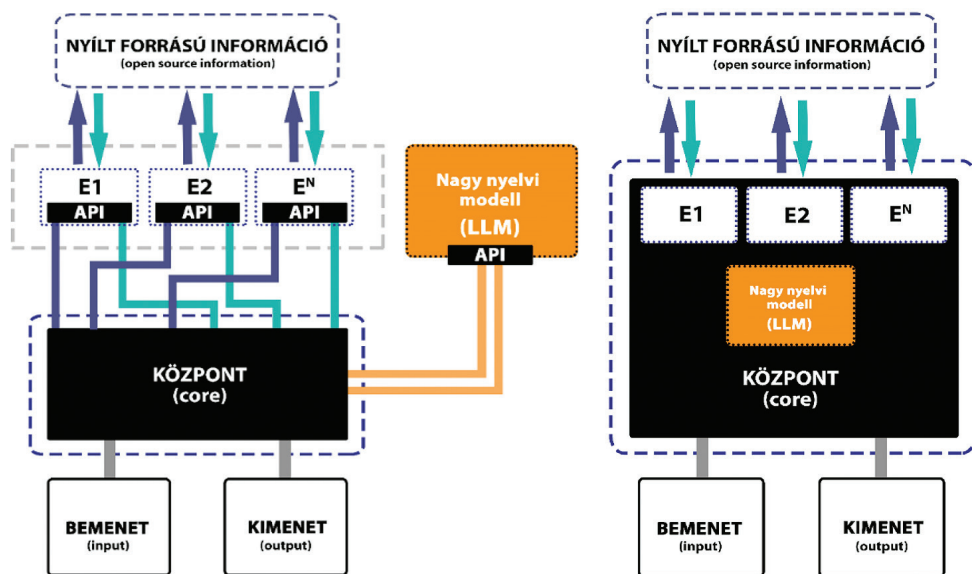
1. Internetes nyílt forrású adatgyűjtő komponens (OSINT-modul): ez az egység felelős a nagy mennyiségű, feldolgozásra szánt nyílt forrású adatok felkutatásáért

³⁷ A kifejezés az informatikában arra utal, hogy a szoftver, alkalmazás vagy adatbázis a vállalat/szervezet saját fizikai környezetében – például a cég saját szervertermében vagy adatközpontjában – fut és van telepítve, nem pedig felhőalapú szolgáltatásként külső szolgáltató infrastruktúráján.

³⁸ ČERNÝ 2024: 120.

- és összegyűjtéséért. A modul külső szolgáltatók által biztosított megoldásokat, illetve szabadon elérhető, integrálható OSINT-eszközöket is tartalmazhat.
2. Nagy nyelvi modell (LLM-) modul: ez a komponens egy vagy több LLM-integrációt foglal magában, amely lehet külső szolgáltatón keresztül elérhető *hostolt* modell, vagy helyben telepített (*on-premise*) megoldás. Feladata az OSINT-modul által begyűjtött információk, elsősorban szöveges adatok feldolgozása és utasításalapú kivonatolása. Továbbá az API-n keresztül megszólított keresőfunkció alkalmazása esetén OSINT-eszközként is értelmezhető, valamint lehetőséget nyújt generatív feladatok elvégzésére is, például egy adott személy pszichológiai profiljának elkészítésére.
 3. Központi vezérlő modul (*core*): ez az elem biztosítja az összeköttetést és az adatáramlást a rendszer különböző moduljai között, valamint irányítja azok működését. Kezeli a felhasználói bemeneteket (utasításokat), továbbítja és feldolgozza az adatokat, illetve biztosítja a felhasználó számára az eredmények megjelenítését. Ebbe a modulba integrálódnak azok az eszközök is, amelyek az OSINT- és LLM-modulok közötti adatkompatibilitást támogatják (például a webes adatgyűjtés során kinyert HTML-forráskód tisztításával).³⁹

A keretrendszereken belül a modulok architektúrális elhelyezkedése bizonyos mértékű aszimmetriát mutat, amely alapján két alapvetően különböző megközelítésű rendszerkialakítás állapítható meg: az egyik a külső szolgáltatás alapú (*third-party dependent*), míg a másik a lokálisan integrált modell (8. ábra).



8. ábra: Balról a külső szolgáltatás alapú, jobbról a helyi (*on-premise*) OSINT-LLM-architektúra-típusok
Forrás: a szerző szerkesztése

³⁹ BOTTYÁN 2024: 74–75.

A szolgáltatásra épülő architektúra esetén a felhasználói bemenet – például egy adott személyre irányuló információs igény – először a központi egységhez érkezik. Ezt követően a rendszer a szükséges adatok lekérdezését különféle OSINT-eszközök API-interfészein keresztül hajtja végre (például Google Search, Shodan vagy ScrapyBee használatával).⁴⁰

Az OSINT-eszközök visszajuttatják a nagyhalmazú adatot a központi egységbe, ahonnan viszont *LLM-prompt(ok)* kíséretében megküldik egy szintén külső szolgáltatású LLM-nek. Ezt követően a meghívott LLM-képesség (például elemzés, kivonatolás stb.) érvényesítése után az információ az utasítás szerinti tartalom formájában visszaérkezik kimenetként. A keretrendszer előnye, hogy skálázható, a kapcsolt szolgáltatások száma elméletben korlátlan.

Gyakorlati megközelítésben forrásigénye alacsony, hiszen a nagyobb számítási kapacitást igénylő feladatokat a kapcsolt szolgáltatások végzik. Ebből az okból kitettsége jelentős, alkalmazhatósága függ a szolgáltatások rendelkezésre állásától. Rejtve maradása végponttól végpontig nem értelmezhető, hiszen a behívott szolgáltatások megkapják a célpontra vonatkozó információkat. Erőssége a rendszernek, hogy az integrált szolgáltatások a piacon elérhető leghatékonyabbak, és kielégítő eredményt nyújtanak. Ugyanakkor problémásan felel meg az OSINT-tevékenységgel szembeni transzparenciakövetelménynek, hiszen a behívott szolgáltatók gazdasági érdekük alapján nem biztosítanak teljes és maradéktalan átláthatóságot az általuk szolgáltatott eszközökkel és eljárásaikkal összefüggésben.⁴¹

A másik csoport a helyi integrációban (*local integration*) létrehozott típus, amelyben nem találunk külső szolgáltatói kapcsolatot, és minden OSINT-LLM-funkció egy helyi keretrendszerbe építve jelenik meg (8. ábra jobb oldali kép). Az előző modellarchitektúrától eltérően itt az OSINT-eszköz és LLM-képesség önálló modulokként épülnek be, tehát nincs szolgáltató irányába megjelenő kitettség és költségvonzat, valamint biztosított a rejtve maradás, hiszen alapértelmezetten nincs harmadik félen keresztülmenő kommunikáció. Az integrált OSINT-modulok korlátozottabb hatékonysággal bírnak, továbbá a nyílt forráskódú LLM-ek sem a legeredményesebbek, ugyanakkor az üzemeltetési költségek is alacsonyabbak. Ez a keretrendszer szintén skálázható, hiszen az integrációk száma elméletben itt is korlátlan, azonban már megjelenik a rendelkezésre álló erőforrások okozta korlátozottság. Mivel a keretrendszer elemei integrálva vannak, így az OSINT-tevékenység transzparenciája is biztosítható. Annak okán, hogy megőrzi a használója anonimitását, sajnos a rosszindulatú tevékenységek végzésére is kiválóan alkalmas.⁴²

OSINT-LLM-tevékenység elhárítását támogató javaslatok

A korábban tett megállapításokra hivatkozva kijelenthetjük, hogy az OSINT-LLM-megoldások jelenlegi alkalmazási formái nem jelentenek kiemelkedően új fenyegetést

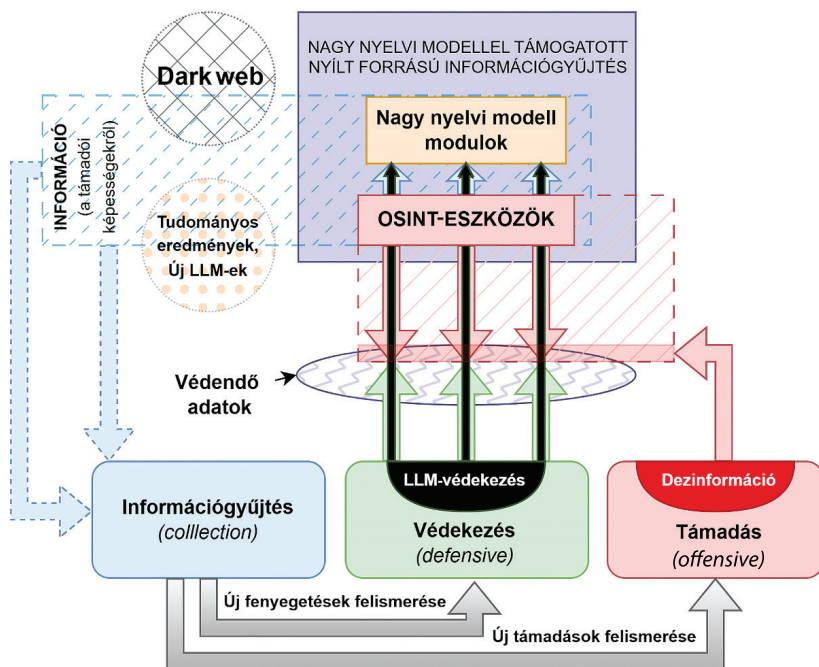
⁴⁰ BOTTYÁN 2024: 75–76.

⁴¹ BOTTYÁN 2024: 74–76.

⁴² BOTTYÁN 2024: 76–78.

a nyílt forrású információszerzés elleni védekezés területén, ellenben az adatmennyiség kezelésében az eddigi korlátok többszörösére lesznek képesek. Az LLM-innovációnak köszönhetően az internetes nyílt forrású információgyűjtés valószínűbb kockázattá válik, így kibebiztonsági szempontból felértékelődik annak kezelése. Egyetlen lehetőségünk az érzékeny adatok (például személyes adatok, üzletmenet-folytonosságot veszélyeztető adatkörök) eltávolítása vagy eltávolíttatása az aktív forrásokból, valamint a jövőbeni tudatosság gyakorlása mellett belenyugvás abba a felismerésbe, hogy az archívumokban továbbra is megtalálhatók korábban közzétett adataink.

Szervezeti szempontból jelentősebb a felelősség, hiszen munkavállalóink személyes és szervezetünk védett adataira egyaránt hat az LLM-OSINT-fenyegetés. Az eredményes védekezés legelső eleme az OSINT elleni módszerek és eljárások (például digitális lábnyom csökkentése) alkalmazása, amelyet ez a tanulmány részletekbe menően nem kíván tárgyalni. Helyette inkább azon speciális lehetőségeket kívánja azonosítani, amelyek felhasználása redukálhatja az LLM-mel támogatott OSINT hatékonyságát. Ezeket a klasszikus kémelhárítási (*counterintelligence*) kategóriák⁴³ szerint azonosítva tárgyaljuk és egyúttal a 9. ábrán szemléltetjük.



9. ábra: A nagy nyelvi modellel támogatott nyílt forrású információgyűjtés elleni védelmi stratégiák szemléltetése

Forrás: a szerző szerkesztése

⁴³ LOWENTHAL 2003: 263.

Információgyűjtés

Ez a típusú elhárítási forma információkat szerez az ellenfél hírszerzési képességeiről. Ebből következően az LLM-OSINT-megoldások megjelenésének rendszeres kutatása (*CTI feed*)⁴⁴ és elemzése hozzájárulhat a időszakos kockázat-felülvizsgálatok eredményességéhez. A témában releváns új tudományos publikációk, esettanulmányok, a nyílt forrású projektek vizsgálata és tesztelése, valamint a technológiai óriások által szolgáltatott LLM-képességek rendszeres elemzése megfelelő információt szolgáltat a fenyegetettségek jellemzőiről. A dark weben fellelhető információk, különösen az illegális piactereken áruba bocsátott LLM-technológiák (például FraudGPT vagy WormGPT⁴⁵) elemzése rámutathat a legújabb fenyegetések indikátoraira, de ugyanez vonatkozik az OSINT-eszközökre is. Értékes információt lehet szerezni a felismert OSINT-tevékenységgel kapcsolatos esettanulmányok vizsgálatából is, kifejezetten az LLM-alkalmazás szemszögéből megvizsgálva a tapasztalatokat.

Defenzív elhárítás

A védekező jellegű elhárítás alapvető célja az ellenséges hírszerzési tevékenységek megakadályozása. Ebből a szemszögből célszerű az OSINT- és LLM-rendszerek gyengeségeinek és fenyegetéseinek együttes, védekezési szempontú elemzése és hasznosítása. Az alkalmazható eszközök között szerepelhet egy speciálisan kialakított *honeypot*⁴⁶ is, amely képes csökkenteni a nagy nyelvi modellek általi feldolgozás hatékonyságát. Ezen túlmenően a digitális lábnymban (például weboldalak forráskódjaiban) elhelyezett *prompt injection*⁴⁷ sebezhetőséget kihasználó utasítások szintén károsan hathatnak az LLM-ek működésére, különösen, ha ezek az adatok az indexelés során létrejövő archívumokba (alias későbbi tanítóanyagba) jutva megzavarják az LLM-mel történő adatfeldolgozást. Hasonló eredményt lehet elérni a toxicitás módszeres alkalmazásával is, kihasználva a nagy nyelvi modellek azon sérülékenységet, hogy „megmérgeezhetők”. Ebben az esetben a digitális lábnymba (például a *deep webre*) helyezünk el olyan mennyiségű és típusú toxikus adatot, amely az általános felhasználásban nem okoz fennakadást, ám az LLM-ek tanítását vagy működését jelentősen megzavarhatja. Vizsgálat tárgyát képezheti az is, hogy milyen védelmi hatást érhetünk el azzal, ha a digitális környezetet úgy alakítjuk át, hogy az ne legyen ideális az LLM-alapú feldolgozásra – például angol nyelvű modellek esetében a különösen nehezen kezelhető

⁴⁴ A kiberbiztonságban a *CTI feed* (*cyber threat intelligence feed*) egy folyamatosan frissülő adatforrás, amely ismert fenyegetésekről, támadási mintákról és indikátorokról (pl. IP-címek, *domainek*, *hash*-ek) szolgáltat információt a védekezés támogatására.

⁴⁵ A FraudGPT és a WormGPT két GPT-modellen alapuló, kifejezetten kiberbűnözők számára készült eszköz, amelyeket a *dark weben* és Telegram-csatornákon terjesztenek. Olyan illegális tevékenységek támogatására tervezték őket, mint a célzott adathalászat, rosszindulatú kódok generálása és sebezhetőségek kihasználása.

⁴⁶ A kiberbiztonságban a *honeypot* egy csapda, amely úgy van kialakítva, mintha értékes célpont lenne. Így szándékosan vonzza a hackereket és más rosszindulatú felhasználókat, azonban valójában izolált és ellenőrzött környezetben működnek, így nem jelentenek valódi kockázatot a szervezet számára.

⁴⁷ A *prompt injection* (utasításbefecskendezés vagy injekció) a nagy nyelvi modellek egyik legjelentősebb sebezhetősége, amely során a modellutasításokat úgy módosítják, hogy reprezentálás során eltérítse a modellműködést az alapértelmezettől.

nyelvek (mint az orosz vagy a kínai) használatával. Ezenkívül érdemes a *honeypotok* szöveges tartalmait tokenizálni, mivel így a nagy nyelvi modellek könnyebben képesek azokat feldolgozni, ami fokozza a megtévesztő hatást.

Jogi eszközök is bevetethetők, bár ezen a területen a lehetőségek korlátozottak. A jogalkotás hagyományosan késve követi a technológiai fejlődést, ennek ellenére indítványok megküldésével elérhető például, hogy a keresőmotorokból vagy archiváló szolgáltatók adatbázisaiból eltávolítsanak bizonyos tartalmakat, ami szintén befolyásolja az OSINT-LLM-rendszerek adathozzáférését. Védekezésünk során az OSINT-LLM-rendszerek kitettségéből (mint egyfajta ellátásilánc-sebezhetőség) is előnyt kovácsolhatunk azzal, hogy technikai intézkedéseket alkalmazunk a legelterjedtebben használt *web scraping* eszközök vagy LLM-alkalmazások ellen. Ezzel a lépéssel csökkenthetjük a feltérképezés kockázatát, és így fokozottabban védhetjük adatainkat.⁴⁸

Offenzív elhárítás

Az offenzív típusú védekezés célja az ellenfél rendszererősségeinek feltérképezése, majd annak félrevezetése szándékosan torzított információkkal. Ez lényegében egy OSINT-LLM megtévesztési (dezinformációs) stratégia. A gyakorlatban ez megvalósulhat például *honeypot* rendszerek alkalmazásával, eredeti weboldalak forráskódjaiba ágyazott manipulált elemekkel, vagy akár *deep webes* felületeken közzétett tartalmakkal is. Hatékony módszer lehet olyan adatsomagok elhelyezése, amelyek elavult vagy teljes mértékben valótlan információkat tartalmaznak. A megtévesztés eredményességét tovább fokozhatja, ha a szöveges anyagokat nagy nyelvi modellek segítségével állítjuk elő, mivel ezek tokenizált formában jobban illeszkednek az LLM-ek feldolgozási mechanizmusaihoz, ezáltal technikailag hatékonyabb a félrevezetés.⁴⁹

Összefoglalás és eredmények

A vizsgált rendszerek vonatkozásában sikerült azonosítani és részletesen bemutatni az architektúrák legfőbb azonosságait (főbb komponenseit), azonban az eltérések részletes vizsgálatát egyfajta összefoglalásként az 1. táblázat szemlélteti.

Az alábbi táblázatból megállapítható, hogy bár csekély számú elemet érintett vizsgálat, ez a két projekt is bőven eltér a főbb LLM- és OSINT-funkciók tekintetében. Az eltérésekből azt is megállapíthatjuk, hogy az LLM OSINT PoC architektúrája az LLM-modul jellemzői tekintetében mutat fejlettebb szintű megvalósítást, míg az InfoHound vonatkozásában a csökkent LLM-funkciók mellett az OSINT-eszközök széles körű alkalmazásán van a hangsúly. Ez arra enged következtetni, hogy mindkét projekt esetében az adott modulok még bőven fejleszthetők, és a technológiai lehetőségek nincsenek maradéktalanul kihasználva.

⁴⁸ BOTTYÁN 2024: 84.

⁴⁹ BOTTYÁN 2024: 84.

1. táblázat: A vizsgált projektek további architektúráis jellemzői

Architektúrajellemzők	LLM OSINT PoC	Infohound
LLM-verzió	GPT-4 és GPT-3.5	Llama 2 (Olama)
LLM-komponens	Többszintű (multi-agent)	Egyszintű (single-agent)
LLM-munkamenet	Ismétlődő (triggered process)	Egyszeri (one-time session)
LLM-funkció	Információkereső ügynök, szöveg összefoglalása és generatív szövegalkotás (abstractive summarisation and content generation)	Szöveg összefoglalása (only content generation)
LLM-utasítás (prompt)	Alapvető (structured)	Rövid, egyszerű (naive)
OSINT-eszközök	Egyszerűbb keresőmotorok, adatgyűjtő eszközök	Számos OSINT eszköztípus
OSINT-tevékenység	Webkaparás (web scraping)	Többféle tevékenység, de főként web scraping

Forrás: a szerző szerkesztése

Az eredmények tekintetében az H1 hipotézis bizonyítása sikeres, hiszen az LLM-alkalmazás már nem példa nélküli az internetes nyílt forrású információgyűjtésben, ugyanakkor a vizsgált elemek architektúrái tekintetében az LLM-komponensek kihasználása még nem kidolgozott. Ez a megállapítás bizonyítja azt a felvetést, hogy az LLM funkcionalitása harmonizálható az OSINT adatfeldolgozási folyamatában. Bizonyos az is, hogy az LLM-ek innovációs hatást gyakorolnak az OSINT-eszközök alkalmazására, és valószínűsíthetően a nagyobb, korábban leküzdhetetlennek hitt adatmennyiségek feldolgozásában fognak hatékonyan közreműködni.

A második hipotézis hamisnak bizonyult, amelynek oka, hogy e kutatás fókuszába olyan felhasználási módok kerültek, amelyekben az LLM-komponenseket főként az internetalapú OSINT adatfeldolgozási folyamatába integrálják azért, hogy a kívánt célok szerint kivonatolják a releváns információkat a nagy mennyiségű adatból. Önálló internetalapú OSINT-eszközként is alkalmazhatók, de valószínűleg nem hatékonyak. A nagy nyelvi modellek jellemzőiből kiindulva valószínűsíthető a hatékonyságnövelésük az internetalapú OSINT-folyamatokban, sőt képesek lehetnek redukálni vagy megoldani az OSINT néhány elemi nehézségét (például adatdömping, elemzési képességek). Egyértelmű azonban, hogy a nagy nyelvi modell komponensek alkalmazása a vizsgált projektek architektúrái jellemzői alapján nem nyitnak meg új kockázati területeket, az ezzel összefüggő támadási vektor azonos. Ugyanakkor növelik az internetalapú OSINT kiberbiztonságra irányuló fenyegetettségét, hiszen a kibertámadások időigényes felderítési fázisa gyorsabb és hatékonyabb lesz, időigénye valószínűsíthetően töredéke lesz a korábbiak.

A harmadik hipotézis bizonyított azzal, hogy az elhárítási stratégiai megközelítések (információgyűjtés, defenzív és offenzív elhárítás) tartalmaznak olyan speciális elemeket (például az LLM-sebezhetőségek és hatékonyságcsökkentő intézkedések

alkalmazása védelmi céllal), amelyeket kifejezetten az LLM-OSINT-tevékenységekkel szembeni kockázatok mérséklésére alkalmazhatunk. A továbbiakban egy prediktív kitekintést teszünk, és a feltárt információk figyelembevételével valószínűsíthető változásokat azonosítjuk a jövőre nézve.

Az OSINT és az LLM jövője

A korábban megfogalmazott megállapítás, miszerint az OSINT-LLM-keretrendszerek fejlődése még a vizsgált rendszerek alapján kezdetleges, felveti a kérdést, hogy a jövőben várható-e ebben változás, és ha igen, milyen irányokban. Valószínűsíthető, hogy az LLM-architektúrák tovább fejlődnek, kompaktabbá és ezáltal könnyebben testre szabhatóvá válnak, amely helyzet jól hasznosul az OSINT-ben. Manapság a technológiai nagyvállalatok egyre inkább integrálják az LLM-alapú megoldásokat saját szolgáltatásaikba (például a Microsoft CoPilot vagy a Google Assistant with Bard⁵⁰) egyfajta asszisztensként. Hasonló fejlődési irány várható az OSINT területén is: az LLM-ek itt is támogató és hatékonyságnövelő szerepet fognak betölteni. Mindemellett várható, hogy a már azonosított keretrendszertípusokba fokozatosan egyre több OSINT-eszközt fognak beépíteni, mivel az LLM-ek adatfeldolgozó kapacitása még messze nincs maximálisan kihasználva, továbbá egyre hatékonyabb és erőforrás-takarékosabb LLM-verziók megjelenése is előrevetíthető.

A jövőben a kifejezetten hírszerzési célokra összeállított domainspecifikus korpuszok is megjelenhetnek, amelyekre a finomhangolt LLM még hatékonyabb komponenssé válhat az internetes adatgyűjtésben. Ezzel összefüggésben számos további olyan fejlődő tényező felmerülhet, amely szintén pozitívan hathat a nagy nyelvi modellel végzett nyílt forrású információgyűjtésre. Biztosra vehető a jövőben a mesterséges intelligencia képességeinek általános bővülése – különösen a nagy multimodális modellek (LMMs) fejlődése – is, ami további új megközelítések kidolgozásához járulhat hozzá, akár kihasználva az internet eddig kevésbé feltárt rétegeit is.

A kutatás eredményei rámutatnak arra is, hogy az LLM-ek és az OSINT közötti kapcsolat nem csupán technológiai, hanem stratégiai jelentőséggel is bír, különösen a kiberbiztonság területén. A vizsgált projektek ugyan csak pillanatképet nyújtanak az LLM-ek jelenlegi OSINT-alkalmazásairól, mégis jól érzékelhető belőlük a jövőbeni tendenciák iránya. Ennek megfelelően a témában elengedhetetlen a tudományos diskurzus fenntartása. Ehhez a megállapítások kellő alapot nyújthatnak, és hozzájárulhatnak új tudományos kérdések kidolgozásához olyan tudományterületeken, mint a jogtudomány, a rendészettudomány, a hadtudomány és a katonai műszaki tudomány. Emellett eredményei és ajánlásai érvényesíthetők olyan területeken, mint az adatvédelem, a katonai és nemzetbiztonsági hírszerzés és a védelmi ipar. Az sem kizárt, hogy a jövőben az OSINT-LLM-rendszerek fejlődése új kutatási irányokat nyithat meg, különös tekintettel a stratégiai kiberfenyegetés-értékelés és a dezinformációs kampányok elleni fellépés területén.

⁵⁰ HSIAO 2023.

Felhasznált irodalom

- BIELSKA, Aleksandra (2020): *Open Source Intelligence Tools and Resources Handbook*. Online: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf
- BOTTYÁN Sándor (2024): *Nagy nyelvi modellel támogatott nyílt forrású információgyűjtés a kibertérben*. Tudományos diákköri dolgozat. Budapest: Nemzeti Közszerződési Egyetem Államtudományi és Nemzetközi Tanulmányok Kar.
- CyberRaya (2023): *Infhound: Enumerate Emails, Usernames, Subdomains, Names and Other Information*. Online: <https://osintteam.blog/infhound-enumerate-emails-usernames-subdomains-names-and-other-information-828bb9b8ac8e>
- ČERNÝ, Jan (2024): Implications of Large Language Models for OSINT: Assessing the Impact on Information Acquisition and Analyst Expertise in Prompt Engineering. *Proceedings of the 23rd European Conference on Cyber Warfare and Security*, 23(1). Online: <https://doi.org/10.34190/eccws.23.1.2261>
- Department of Defense (2010): *Dictionary of Military and Associated Terms*. Online: https://irp.fas.org/doddir/dod/jp1_02.pdf?utm_source=chatgpt.com
- Holupredictions (2023): *It Looks Like You Can Use ChatGPT to Bypass Paywalls*. Online: www.reddit.com/r/ChatGPT/comments/14j8q1u/it_looks_like_you_can_use_chatgpt_to_bypass/
- HSIAO, Sissie (2023): *Assistant with Bard: A Step Toward a More Personal Assistant*. Online: <https://blog.google/products/assistant/google-assistant-bard-generative-ai/>
- InfoHound – OSINT Tool for Domain Profiling (2024). Fundacio-i2CAT/InfoHound, GitHub. Online: <https://github.com/Fundacio-i2CAT/InfoHound?tab=readme-ov-file>
- LOWENTHAL, Mark. M. (2003): *Intelligence: From Secrets to Policy*. Washington, DC: CQ Press. Online: https://archive.org/details/intelligencefrom0000lowe_g9z8
- Mi az a proof-of-concept (PoC) exploit?* (2023). Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet. Online: <https://nki.gov.hu/it-biztonsag/tudastar/mi-az-a-proof-of-concept-poc-exploit/>
- OKEMWA, Kevin (2023): ChatGPT Pauses Bing Integration to Stop People From Bypassing Paywalls. *Windows Central*, 2023. július 4. Online: www.windowscentral.com/software-apps/chatgpt-pauses-bing-integration-to-stop-people-from-bypassing-paywalls
- Precognox (2022): *A hírek és információk megszerzése még nem hírszerzés*. Online: <https://precognox.hu/blog/a-hirek-es-informaciok-megszerzese-meg-nem-hirszerzes/>
- ROGERS, Reece (2023): How to Use ChatGPT's 'Browse With Bing' Tool – Plus 6 Starter Prompts. *Wired*, 2023. október 25. Online: www.wired.com/story/chatgpt-browse-with-bing-internet-connected-openai/
- ROSENGREN, Kim (2022): *Contribution of Open-Source Intelligence to Social Engineering Cyberattacks*. Bachelor's Thesis. Turku University of Applied Sciences. Online: www.theseus.fi/bitstream/handle/10024/754826/Rosengren_Kim.pdf?sequence=2
- VADÁSZ Pál (2018): *A szemantikus keresés módszerei és alkalmazási lehetőségei a védelmi szférában, a közigazgatásban, illetve a gazdasági életben*. PhD-értekezés. Budapest: Nemzeti Közszerződési Egyetem Katonai Műszaki Doktori Iskola. Online: www.uni-nke.hu/document/uni-nke-hu/Vadasz-Janos-Pal_Doktori-ertekezes_2018.pdf

Attila Hammas¹

More Data, More Problems?

Exploring the Impacts of Using External Datasets when Training Deep Learning Models for Remote Sensing Applications

Abstract

The resurgence of large-scale conventional warfare, exemplified by the ongoing conflict in Ukraine, has highlighted the critical importance of modern technologies in enhancing situational awareness and target acquisition on the battlefield. In particular, the integration of unmanned aerial vehicles (UAVs) and artificial intelligence (AI)-driven computer vision systems has emerged as a key enabler of real-time intelligence and precision engagement. This paper presents an approach to enhance object detection models on aerial imagery for military applications. Initial experiments revealed shortcomings in detecting certain object classes, particularly in complex environments and under variable lighting conditions. To address these issues, the paper investigates impacts of cross-dataset training to improve the robustness and accuracy of object detection models. Through selective label integration and careful dataset curation, the paper demonstrates that incorporating assets from external sources significantly enhances generalisation and detection performance. The results underline the potential of leveraging large-scale annotated datasets to augment domain-specific applications with minimal additional labelling cost.

Keywords: reconnaissance, IMINT, artificial intelligence, machine learning

Introduction

The full-scale invasion of Ukraine by Russia in 2022 sent shockwaves across the international community, not only due to its humanitarian and geopolitical implications

¹ PhD student, Ludovika University of Public Service Doctoral School of Military Engineering, e-mail: hammas.attila@stud.uni-nke.hu

but also because it signified a dramatic resurgence of high-intensity, conventional warfare between sovereign states – something Europe had not witnessed on such a scale since World War II. For decades, armed conflicts in the post-Cold War era were predominantly characterised by asymmetrical warfare, insurgencies and proxy battles. The re-emergence of large-scale, state-versus-state conflict – complete with tanks, artillery and mass mobilisations – was seen as an anachronism by many, a relic of 20th-century military history that had no place in modern geopolitics. Yet, the events in Ukraine challenged that assumption. This war has prompted a re-evaluation of European defence strategies, NATO readiness and global power dynamics. It has also raised urgent questions about the role of deterrence, the importance of military alliances and the stability of the international rules-based order. As such, the invasion is not just a regional crisis, it is a pivotal moment in global history, redefining how war is perceived and prepared for in the 21st century.

In addition to its geopolitical and strategic consequences, the war in Ukraine has also served as a proving ground for a new era of military technology and innovation. One of the most striking features of the conflict has been the widespread use of drones – not only by state actors but also by irregular forces – ranging from inexpensive commercial quadcopters used for reconnaissance and targeting, to advanced loitering munitions capable of precision strikes. The fusion of Intelligence, Surveillance and Reconnaissance (ISR) capabilities has dramatically increased situational awareness on both sides, with real-time battlefield intelligence. Moreover, artificial intelligence has begun to play a significant role, from the automatised image analysis and the identification of targets to enhancing electromagnetic warfare systems and optimising logistics. This blending of traditional combat with digital innovation has underscored a new model of hybrid warfare, where software, data and autonomous systems can be as decisive as tanks and artillery. The Ukraine conflict is not just a return to conventional war; it is a glimpse into the future of how wars will be fought from now on.

ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) stands at the forefront of this technological evolution, serving as a critical military capability that integrates diverse intelligence streams and sensor inputs to generate comprehensive situational awareness, enabling faster and more informed decision-making.² In the context of modern warfare, ISTAR capabilities have become increasingly intertwined with disruptive technologies such as drones, autonomous weapon systems and artificial intelligence. These advancements hold the promise of not only strengthening operational effectiveness but also significantly reducing risks for human personnel.³ By leveraging autonomous systems to perform dangerous reconnaissance missions or precision strikes, human soldiers are kept at safer distances from frontline threats. AI-driven analysis of vast datasets can rapidly identify threats, improve targeting accuracy and reduce collateral damage.

During the progress of research and development of a platform for processing and analysing data provided by Unmanned Aerial Vehicles (UAV) to intensify situational awareness and target acquisition capabilities, notable shortcomings in object

² BODA 2024.

³ BALOGH 2012.

detection performance were identified, particularly regarding specific object classes. This study investigates whether the integration of external datasets improves accuracy and robustness of the employed object detection models. Accordingly, the research addresses whether supplementing synthetic and limited real-world data with large-scale external datasets can enhance accuracy and generalisation in UAV-based ISTAR applications. It further examines the extent to which cross-dataset training contributes to improved performance. In the following sections, the impact of incorporating annotated data from additional sources on model performance is evaluated.

Theoretical overview

Machine learning, particularly through Convolutional Neural Networks (CNN), has revolutionised computer vision by enabling machines to recognise patterns in images. CNNs utilise multiple layers, including convolution, pooling and fully connected layers, to process and classify images. Deeper and more complex CNN architectures require significantly more computational resources for training and inference.⁴ Deep networks are also prone to overfitting, especially when trained on small datasets, this issue can be addressed using techniques such as dropout and data augmentation.⁵

In the field of computer vision, several important applications can be identified (Figure 1):

- *Image classification*: CNNs have achieved state-of-the-art results in image classification tasks by effectively learning hierarchical representations of images.⁶
- *Object detection, recognition and tracking*: CNNs are widely used in object detection frameworks such as YOLO (You Only Look Once)⁷ and Faster R-CNN (Region based Convolutional Neural Network),⁸ which can identify and localise objects within images.⁹
- *Image segmentation*: CNNs divide an image into multiple segments, often with pixel-level precision, allowing computer vision systems to more accurately detect and interpret objects by outlining their exact shapes rather than using simple bounding boxes.
- Other applications include video analysis, face recognition and human pose estimation, showcasing the versatility of CNNs in handling various visual tasks.¹⁰

While CNNs have become a cornerstone of computer vision, they are not without limitations. The complexity of CNNs can lead to high computational costs, making them less accessible for applications with limited resources. Additionally, the reliance on large, labelled datasets for training poses challenges in domains where such data is scarce.

⁴ VAN DOORN 2014; ZHAO et al. 2024.

⁵ ZHAO et al. 2024.

⁶ SHETTY et al. 2022; ZHAO et al. 2024.

⁷ REDMON et al. 2015; REDMON–FARHADI 2016; 2018; BOCHKOVSKIY et al. 2020.

⁸ REN et al. 2017.

⁹ SHETTY et al. 2022; RANA–CHAUHAN 2021.

¹⁰ SHETTY et al. 2022; VOULODIMOS et al. 2018.

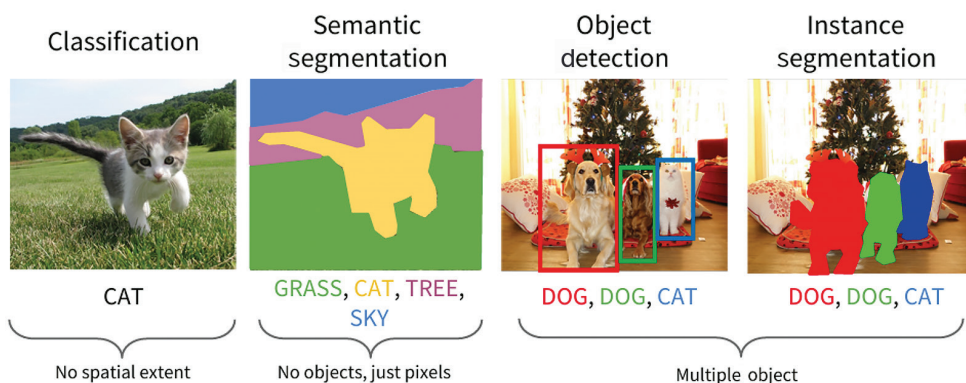


Figure 1: Visualisation of different computer vision tasks

Source: LI-ADELI 2024: 14.

The size and quality of a training dataset are pivotal factors that significantly influence the performance of machine learning models. The interplay between these two elements determines the model's ability to generalise its accuracy and its efficiency. While larger datasets generally provide more learning opportunities, the quality of the data is often more critical in ensuring reliable deep learning model outputs. The scarcity of data is a core issue in training Machine Learning (ML) application. Big preexisting datasets like MS COCO (Microsoft Common Objects in Context)¹¹ and PASCAL VOC (Pascal Visual Object Classes)¹² contain a wide range of object classes and scenarios, which can significantly boost the diversity of training data. This diversity helps in improving the generalisation ability of models, makes them more robust to different environments and conditions. In those cases when the label provided by these large datasets do not exactly cover the required label set, cross-dataset training can be applied, allowing models to learn from a union or an intersection of different object classes without the need for exhaustive labelling across all datasets.¹³ This approach is efficient for industrial applications where object classes frequently increase. By leveraging the work done for the already existing datasets, we can reduce the costs of labelling.

Methodology

The original dataset consisted of synthetic images generated using Unreal Engine based AirSim simulator complemented with real-world images collected by using drones and downloaded from the internet. Based on the analysis of our previous results, our trained models fail to generalise enough, and they underperform in detecting people not in uniforms or certain cars. As shown in Figure 2, the model can detect soldiers in uniforms but struggles detecting people in civilian clothing. The synthetic datasets generated using the simulator and other 3D game engines are designed to emphasise objects of military relevance.¹⁴

¹¹ LIN et al. 2014.

¹² EVERINGHAM et al. 2010.

¹³ YAO et al. 2020.

¹⁴ HAMMAS 2023; BRASSAI et al. 2024.

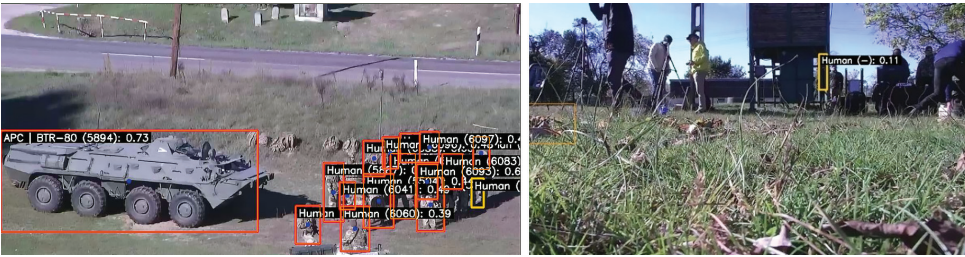


Figure 2: Example outputs of our models before including external datasets

Note: Left: soldiers in uniforms; right: people in civilian clothing.

Source: compiled by the author

To extend the dataset while minimising acquiring and labelling costs, preexisting datasets containing people and different vehicle categories were employed:

- *Microsoft Common Objects in Context*:¹⁵ Includes images from everyday scenes with objects in *natural and complex contexts*, helping models generalise better to real-world environments compared to synthetic or simplified datasets. It contains over 200 thousand images with 80 different labels. As illustrated in Figure 3, the dataset includes people in various poses, which can help improve robustness when they are crouching or crawling on frames.

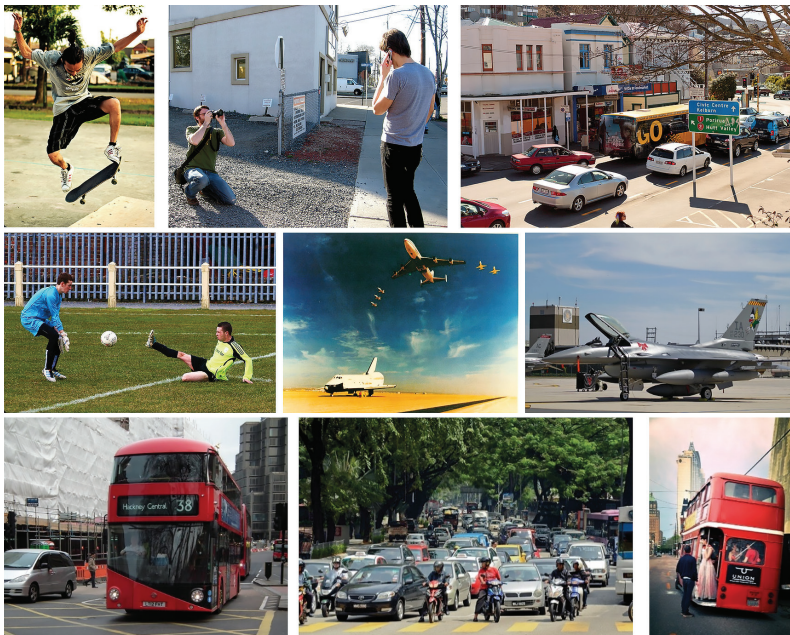


Figure 3: Example images from MS COCO dataset

Source: LIN et al. 2014

¹⁵ LIN et al. 2014.

- *VisDrone*:¹⁶ Contains drone footage in urban areas with complex scenes, varying light conditions and perspectives specifically tailored for object detection tasks in aerial imagery as can be seen in Figure 4. The dataset presents video sequences and still images predominantly from urban environments, which are characterised by their high level of scene complexity. It includes a diverse range of labelled object categories such as pedestrian, people, bicycle, car, van, truck, tricycle, bus and motorcycle.

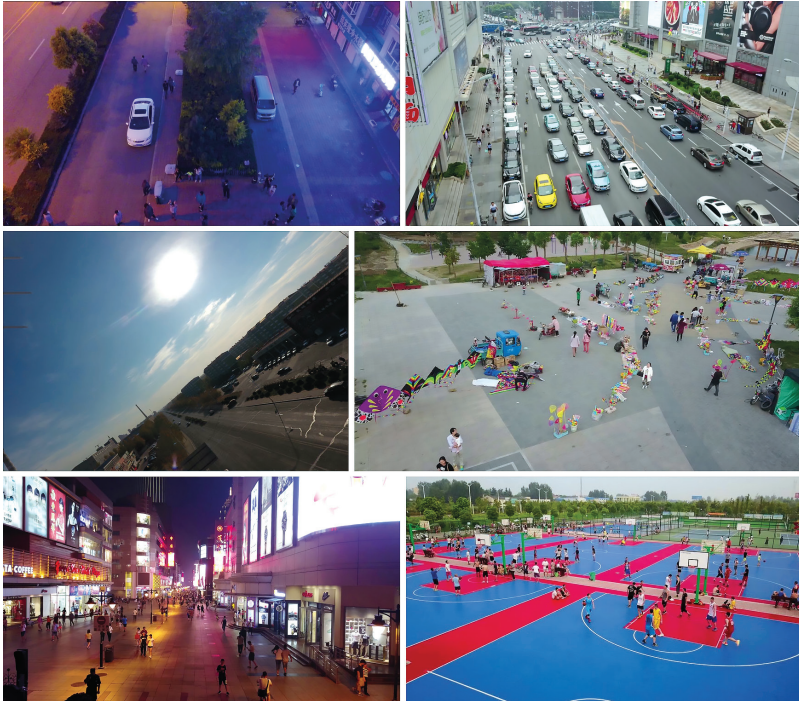


Figure 4: Example images from VisDrone dataset

Source: ZHU et al. 2018

These datasets also contain irrelevant object classes (e.g. food items, toys, household objects). These labels were removed from the images which resulted in many images remaining without any annotation.

More datasets were considered, then excluded due to conflicts:

- *DOTA (Dataset for Object Detection in Aerial Images)*:¹⁷ Provides high-resolution aerial imagery with objects annotated in arbitrary orientations. It mainly uses rotated bounding boxes but it is also available with horizontal bounding boxes. It does not include people since it was created for object detection on satellite imagery.

¹⁶ ZHU et al. 2018.

¹⁷ XIA et al. 2018.

- *UAVDT (Unmanned Aerial Vehicle Detection and Tracking)*:¹⁸ It is very similar to VisDrone, but with emphasis on vehicle detection and tracking. It conflicts with our classes since the images contain people, but they are not annotated. If the dataset is combined with VisDrone without further annotation it may reduce the recall and accuracy of detecting people.

The classes selected from the MS COCO and VisDrone datasets were carefully adapted to align with the objectives of this study, which focus on improving situational awareness through the reliable detection of humans and vehicles relevant to UAV-based ISTAR operations. After filtering out irrelevant categories, the following classes were retained and harmonised across the combined dataset: (index: class name):

- 0: Human
- 1: Car
- 2: Truck
- 3: Bus
- 5: Train
- 31: Unknown Aircraft

The rules for adapting the classes found in this external dataset were as follows:

Table 1: The rules for transferring labels from external dataset into the combined dataset

Dataset	Class name in external dataset	Class name in combined dataset
MS COCO	Person	Human
	Car	Car
	Bus	Bus
	Train	Train
	Truck	Truck
	Other classes were removed.	
VisDrone	Pedestrian	Human
	People	Human
	Car	Car
	Van	Car
	Truck	Truck
	Bus	Bus
	Other classes were removed.	

Source: compiled by the author

For testing purposes, the Ultralytics¹⁹ framework was used for training and evaluation. We trained both models for 240 epochs with the following parameters: learning rate: 0.01 (with 3 warmup epochs – the value was gradually increased in the first 3 epochs), momentum: 0.9, and with an input image size of 1280 × 1280.

¹⁸ DU et al. 2018.

¹⁹ Ultralytics s. a.

Results and discussion

Due to the size of the selected datasets the final combined dataset is unbalanced. This is a limitation of this research. The number of instances is orders of magnitude larger compared to the other classes which are not in the selected external datasets. As shown in Figure 5, the Human (0) and Car (1) classes are overrepresented in this dataset. This issue is not addressed in this research but as can be seen in Figure 7 it does not impact precision and recall.

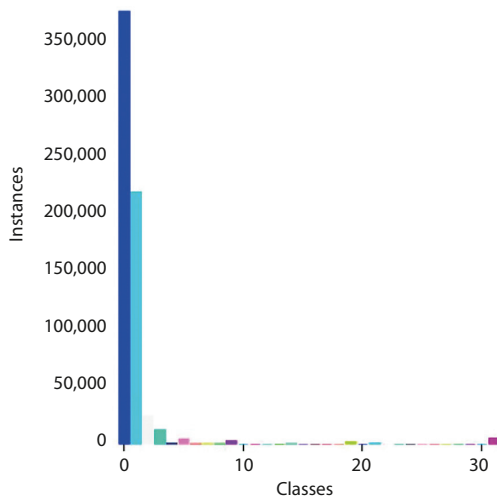


Figure 5: Distribution of classes in the training dataset

Source: compiled by the author

As was emphasised in the introduction, the model trained solely on our internal dataset performed poorly when detecting people in civilian clothing or civilian vehicles (e.g. cars, trucks). The extended dataset samples from the validation and testing subset of the selected external datasets were added in unchanged form. This is also evident in Figure 6, where the model's precision is substantially lower.

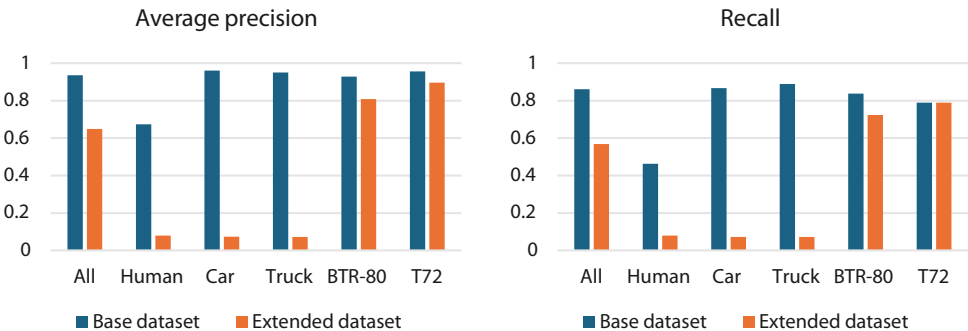


Figure 6: Comparison of the initially trained model on the base dataset and validated on the extended dataset

Source: compiled by the author

Compared to the models trained in the original base dataset, the newly trained models show significant improvements, as shown in Figure 7. The precision and recall values are not negatively impacted by the imbalance between the classes of the dataset.

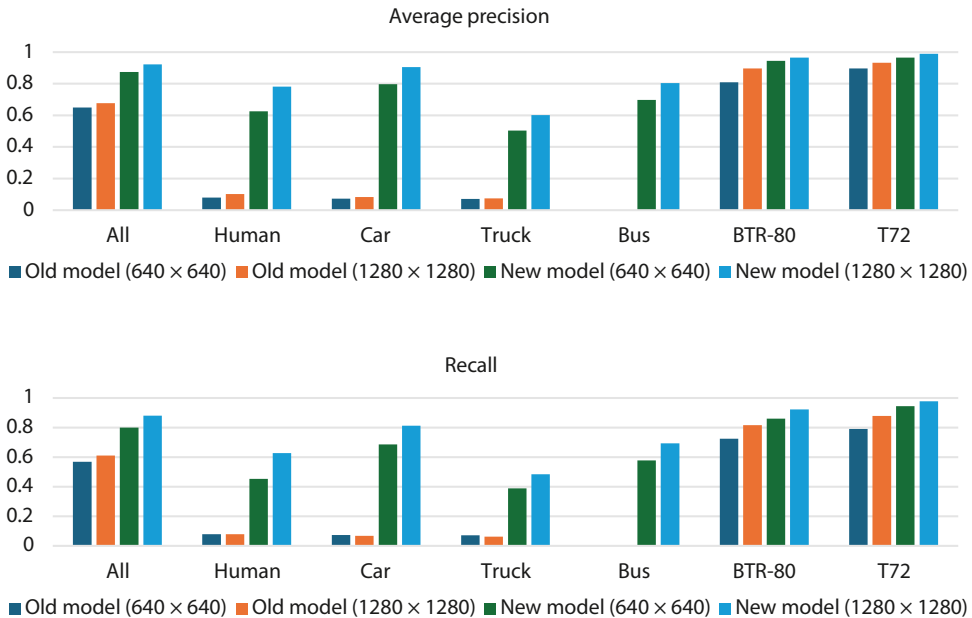


Figure 7: Comparison of the base model trained on the initial dataset and the new model trained on the extended dataset with multiple input resolutions (640 × 640 and 1280 × 1280)

Source: compiled by the author

In some rare cases, the newly trained model detected and identified object instances which were not labelled by the authors of the dataset, as shown on Figure 8. In the example on Figure 8, the image had no relevant labels but was left in as a negative example. The phone class were removed since they do not align with the objectives of this work (as explained in the methodology section). Surprisingly, the object detector still managed to identify people in the image. As shown in the left-hand image of Figure 8, the screen displays pictures of people.



Figure 8: One of the images in the validation set with desired output on the top and predicted output on the bottom

Source: compiled by the author based on image found in the dataset presented by LIN et al. 2014

The image used for example comes from the validation subset of the MS COCO dataset, where phones were labelled from various angles, but the people visible on the screen were not annotated. Thanks to the inclusion of numerous small-scale human instances in both the VisDrone and our internal datasets, the model was able to learn to detect these as well.

Another issue identified involves false positive detections, particularly during takeoff, landing, or when the drone encounters certain textures, as shown in Figure 9. The VisDrone dataset contains numerous small objects, as illustrated in Figure 10. These objects often occupy only a few dozen pixels and lack significant detail, appearing mostly as dark shapes on a gray background. During takeoff and landing, the video stream tends to be unstable, and compression artifacts increase, which occasionally results in false positives.



Figure 9: Example of false positive instances on roof with a texture

Note: Detections on the left and zoomed-in texture on the right.

Source: compiled by the author

Figure 10 further illustrates a zoomed-in image from the VisDrone dataset. A magnified section can be seen on the left; the full image is on the right, where a car is shown in a blue frame, a human in a red frame and the zoomed-in section in a yellow frame.

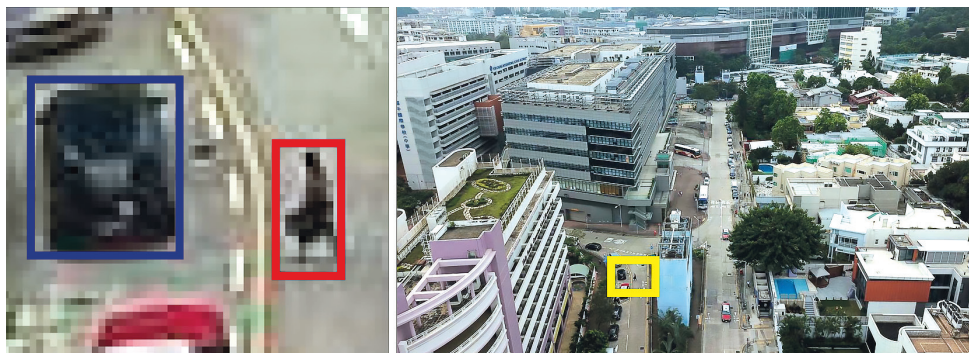


Figure 10: Example of a zoomed-in image from VisDrone dataset

Source: compiled by the author based on image found in the dataset presented by ZHU et al. 2018

Conclusion

This study highlights the challenges and opportunities of improving object detection models for UAV-based ISTAR applications by leveraging external datasets and cross-dataset training. While the initial models, trained solely on synthetic and limited real-world data collected by us, underperformed in recognising civilian objects under varied conditions, integrating large-scale datasets such as MS COCO and VisDrone significantly improved generalisation and detection performance.

However, this approach also introduced certain limitations, notably dataset imbalance and an increased risk of false positives in complex or noisy environments. Despite these challenges, the expanded training data enhanced the model's ability to detect people and vehicles in more realistic and diverse scenarios. Negative examples – images with no valid labels – further contributed to reducing false detections, demonstrating the importance of including such samples in training. This research demonstrates that supplementing domain-specific data with curated external datasets is an effective, low-cost strategy to improve the robustness and accuracy of object detection models for UAV operations. Future work may focus on addressing dataset imbalance, refining label consistency across combined datasets, and developing techniques to mitigate false positive detections caused by sensor artifacts or environmental noise. These improvements will advance further deployment of reliable AI-powered situational awareness systems in real-world defence and security applications.

References

- BALOGH, Péter (2012): A magyar honvédség ISTAR (ISR) képességei, a fejlesztés lehetséges irányai, különös tekintettel az elektronikai hadviselésre. *Hadmérnök*, 7(4), 75–94. Online: http://hadmernok.hu/2012_4_balogh.pdf
- BOCHKOVSKIY, Alexey – WANG, Chien-Yao – LIAO, Hong-Yuan Mark (2020): YOLOv4: Optimal Speed and Accuracy of Object Detection. *arXiv*. Online: <https://doi.org/10.48550/arXiv.2004.10934>
- BODA, Mihály (2024): A kockázatkerülő háború és a bátorság a 20–21. század fordulóján. *Honvédségi Szemle*, 152(3), 113–125. Online: <https://doi.org/10.35926/HSZ.2024.3.9>
- BRASSAI, Sándor Tihamér – SZÁNTÓ, Norbert – BAJKA, Adorján – BÁRDI, Olivér – NÉMETH, András – HAMMAS, Attila (2024): *Simulation Environment Implementation for Generation of Training Samples*. 2024 25th International Carpathian Control Conference (ICCC), Krynica Zdrój, Poland, 22–24 May 2024. Online: <https://doi.org/10.1109/ICCC62069.2024.10569502>
- DU, Dawei – QI, Yuankai – YU, Hongyang – YANG, Yifan – DUAN, Kaiwen – LI, Guorong – ZHANG, Weigang – HUANG, Qingming – TIAN, Qi (2018): The Unmanned Aerial Vehicle Benchmark: Object Detection and Tracking. *arXiv*. Online: <https://doi.org/10.48550/arXiv.1804.00518>
- EVERINGHAM, Mark – VAN GOOL, Luc – WILLIAMS, Christopher K. I. – WINN, John – ZISSERMAN, Andrew (2010): The Pascal Visual Object Classes (VOC) Challenge.

- International Journal of Computer Vision*, 88(2), 303–338. Online: <https://doi.org/10.1007/s11263-009-0275-4>
- HAMMAS, Attila (2023): *Harcjárművek észlelése szintetikus előállított mintákon tanított mélytanuló algoritmusok segítségével*. Budapest: Nemzeti Közzolgálati Egyetem.
- LI, Fei-Fei – ADELI, Ehsan (2024): *CS231n: Deep Learning for Computer Vision*. Online: https://cs231n.stanford.edu/slides/2024/lecture_1_part_2.pdf
- LIN, Tsung-Yi – MAIRE, Michael – BELONGIE, Serge – HAYS, James – PERONA, Pietro – RAMANAN, Deva – DOLLÁR, Piotr – ZITNICK, C. Lawrence (2014): Microsoft COCO: Common Objects in Context. In FLEET, David – PAJDLA, Tomas – SCHIELE, Bernt – TUYTELAARS, Tinne (eds.): *Computer Vision – ECCV 2014. Lecture Notes in Computer Science*. Cham: Springer, 740–755. Online: https://doi.org/10.1007/978-3-319-10602-1_48
- RANA, Ajay – CHAUHAN, Kuldeep (2021): Computer Vision and Machine Learning for Image Recognition: A Review of the Convolutional Neural Network (CNN) Model. *Asian Journal of Multidimensional Research*, 10(10), 1023–1029. Online: <https://doi.org/10.5958/2278-4853.2021.00920.4>
- REDMON, Joseph – DIVVALA, Santosh – GIRSHICK, Ross – FARHADI, Ali (2015): You Only Look Once: Unified, Real-Time Object Detection. *arXiv*. Online: <https://doi.org/10.48550/ARXIV.1506.02640>
- REDMON, Joseph – FARHADI, Ali (2016): YOLO9000: Better, Faster, Stronger. *arXiv*. Online: <https://doi.org/10.48550/arXiv.1612.08242>
- REDMON, Joseph – FARHADI, Ali (2018): YOLOv3: An Incremental Improvement. *arXiv*. Online: <https://doi.org/10.48550/arXiv.1804.02767>
- REN, Shaoqing – HE, Kaiming – GIRSHICK, Ross – SUN, Jian (2017): Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 39(6), 1137–1149. Online: <https://doi.org/10.1109/TPAMI.2016.2577031>
- SHETTY, Ksheera R. – SOORINJE, Vaibhav S. – DSOUZA, Prinson – SWASTHIK (2022): Deep Learning for Computer Vision: A Brief Review. *International Journal of Advanced Research in Science, Communication and Technology*, 2(2), 450–463. Online: <https://doi.org/10.48175/IJARSCT-2898>
- Ultralytics (s. a.): *Ultralytics Documentation*. Online: <https://docs.ultralytics.com/>
- VAN DOORN, Joost (2014): *Analysis of Deep Convolutional Neural Network Architectures*. Proceedings of the Twenty First Twente Student Conference on IT, Enschede, The Netherlands, 1–7.
- VOULODIMOS, Athanasios – DOULAMIS, Nikolaos – DOULAMIS, Anastasios – PROTOPAPADAKIS, Eftychios (2018): Deep Learning for Computer Vision: A Brief Review. *Computational Intelligence and Neuroscience*, 2018(1), 1–13. Online: <https://doi.org/10.1155/2018/7068349>
- XIA, Gui-Song – BAI, Xiang – DING, Jian – ZHU, Zhen – BELONGIE, Serge – LUO, Jiebo – DATCU, Mihai – PELILLO, Marcello – ZHANG, Liangpei (2018): *DOTA: A Large-Scale Dataset for Object Detection in Aerial Images*. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, 18–23 June 2018. Online: <https://doi.org/10.1109/CVPR.2018.00418>

- YAO, Yongqiang – WANG, Yan – GUO, Yu – LIN, Jiaojiao – QIN, Hongwei – YAN, Junjie (2020): Cross-dataset Training for Class Increasing Object Detection. *arXiv*. Online: <https://doi.org/10.48550/arXiv.2001.04621>
- ZHAO, Xia – WANG, Limin – ZHANG, Yufei – HAN, Xuming – DEVECİ, Muhammet – PARMAR, Milan (2024): A Review of Convolutional Neural Networks in Computer Vision. *Artificial Intelligence Review*, 57(4). Online: <https://doi.org/10.1007/s10462-024-10721-6>
- ZHU, Pengfei – WEN, Longyin – BIAN, Xiao – LING, Haibin – HU, Qinghua (2018): Vision Meets Drones: A Challenge. *arXiv*. Online: <https://doi.org/10.48550/arXiv.1804.07437>

Szabolcs Jobbágy¹

The Convergence of the Digital Virtual World and Artificial Intelligence – Or What the Future Symbiosis Brings in the Synergy of the Metaverse and AI

Abstract

Utopia, fiction or tangible digital reality, a projection of the physical world in virtual space? The metaverse, as a phenomenon, as another milestone in the revolution of technological development speeding along the digital superhighway, is much more in today's information-digital society than just another big hit in the service, gaming and entertainment industry. It is far from being in its infancy, with antecedents linked to, among others, Neal Stephenson's cyberpunk novel Snow Crash or Ernest Cline's novel Ready Player One.

It has surpassed its time, exceeded its limitations, and has long since left the ranks of primitive implementations such as the WoW, Fortnite, Roblox or Minecraft game softwares that can be considered the predecessors of its technological evolution. The investments of the technological giants and startups of our time, which at their inception took the form of implementations such as Horizon Worlds, Workrooms, Home, Venues, Microsoft Mesh, Roblox, Fortnite, XiRang, Decentraland, Sandbox, TCG World, Next Earth, Axie Infinity, Neos, Yield Guild, Genesis Worlds, MetaverseZ, vPark, OVR, Bizverse, Challau, Meta-vice, Blankos Block Party, My Neighbor Alice, Somnium Space video games, already seem to be paying off. Nowadays, AI is one of the pillars of the metaverse. The big data available in the metaverse is like oil that fuels AI, as the digital engine of the virtual world, which operates and advances the digital projection of physical reality. Their technological integration is inevitable in order to further blur the boundaries between the real and virtual worlds. The combined effect of this new digital alloy² can be the driving force behind the increasing spread of digitalisation,

¹ Associate Professor, Ludovika University of Public Service Faculty of Military Science and Officer Training, Department of Information Technology, e-mail: jobbagy.szabolcs@uni-nke.hu

² In my own interpretation, I use the term to refer to a new type of digital environment created by the convergence of metaverse and artificial intelligence, based on existing technologies. Their synergy results in new technological and service opportunities for users.

the emerging new era, the revolution of newer and newer technological possibilities, and the development of ever-higher levels of connectivity in the digital space. Technological synergy can bring mutual benefits to these emerging and disruptive technologies for their future development.

Keywords: metaverse, digital world, virtual and physical reality, artificial intelligence, convergence, synergy, fusion, digital alloy, connectivity, symbiosis, digital hybrid technology

Introduction

At the outset, I would like to make it clear that I do not want to look at the subject under consideration through the lens of engineering, by examining it in depth. Rather, I would like to give a general, summary outlook and vision of the future, without claiming to be exhaustive, by reviewing and analysing current technological trends and expert predictions, and supplementing this with subjective insights and thoughts.

Metaverse and Artificial Intelligence (AI) are two Emerging and Disruptive Technologies (EDT)³ that are fundamentally no longer new entities in the technological repertoire of the digital world, but their impact is all the greater. They are prominent milestones in the evolution of different digital technologies that are having a huge impact on the digital transformation of the globalised world around us, on all aspects of the daily lives of digital citizens. Their introduction, deployment, technological evolution and, as a result, convergence are inevitable.

However, it is a different matter to apply them responsibly and judiciously for the benefit of humanity, with positive effects in the information-digital society they permeate. It is important to mention this, among other things, because today, in the age of the 4th generation warfare, as a result of the information-digital theatre of war that has emerged, the primary use of all new technological waves is typically in the defence sphere. Although it is also true that today the vector of development has reversed. This means that new technologies are increasingly being developed in the civilian sphere and then adapted or further developed in the defence sphere. Evidence of this can also be found in the case of one of the current military conflicts, the Russian–Ukrainian confrontation, which presents experts with a picture of a multi-faceted war. Looking at the situation through the lens of technology, we can observe, for example, that the Ukrainian army has been greatly helped on the battlefield by the crowdsourcing database system provided by the U.S. Company Palantir Technologies.⁴ With the help of this system, the Ukrainian forces were able to attack

³ A collective terminology for technological innovations that strengthen the digital achievements of today. Basically, we can include not only new technologies here, but also already introduced but constantly developing and transforming technologies, such as cloud computing, 5G–6G technologies, various xR solutions (VR, AR, MR implementations), big data, autonomous systems (AS), quantum computing, which, in a good sense, fundamentally shake up almost every segment of the information-digital society of the 21st century (PORKOLÁB–HÖNICH 2024).

⁴ A mysterious American commercial data analytics and software development company that offers technological implementations for the defence sector, among other things, and is at the forefront of AI development (Palantir Technologies s. a.).

with much greater precision, they had much more information about the opposing side, and they could see Russian positions much better than before.

Previously, the opposite trend was observed. Although it is true that it is not possible to draw such a sharp line in terms of the flow of technology, the transfer of the knowledge base (know-how), because, for example, in the case of AI, the U.S. Department of Defense's research arm, the Defense Advanced Research Projects Agency (DARPA), has also had AI developments in the last 10–15 years.

So, to return to the basic idea, why is it reasonable to say that we are talking about technological innovations that are not so recent? In the case of AI, this factual statement can be based, for example, on the fact that, by turning back the clock, we can recall events that led to the opening of a certain Pandora's box. Namely, that the first AI conference was convened on the East Coast of the United States of America as early as 1956, at which the basic idea of creating AI that would be equivalent or even rival human cognitive abilities was already being mooted.

Similar evidence can be found for the metaverse. The digital world, the virtual projection of physical reality is not without precedent. Although we may not have used this technological terminology at the time, experts agree that WoW, Fortnite, Roblox and Minecraft are already a kind of rudimentary, primary metaverse implementation, which are certainly familiar buzzwords for all Generation Y, Z and Alpha players.

In the conceptual maze of interpreting the metaverse and AI

In light of all these introductory thoughts, in view of the continuous and exponential technological evolution that has been going on for decades, it is difficult to paddle into the waters of conceptualisation. Regardless of this, however, in order to have a unified interpretation, complex, systemic thinking, and to examine the convergence of these two areas, it is necessary to define a basic terminology for both of the issues examined.

Thus, if we first examine the issue of the metaverse, we can rely on the previous basic concept explanation, which was defined based on my own interpretation. In general, the

"metaverse can be interpreted as a new, large and unprecedented digital world, offering new user experiences and countless opportunities, the next major development milestone of the internet, web 3.0, a virtual universe, partly a digital projection of the world around us, a utopian world influenced by the interaction of users' metaclasses (digital twin)".⁵

⁵ JOBBÁGY 2022: 134. Digital twin, avatar, metaclass: In my own interpretation, these synonymous terms can be interpreted in various ways depending on their application and usage areas. However, their common characteristic, which helps to define them, is the following: an accurate, virtual representation of a physical object, system, process, etc. in the metaverse, in the virtual space, in such a way that it copies and carries with it almost all the characteristics of the thing it represents. It must 100% reflect what happens in physical reality. Their size can be of different magnitudes depending on their application area and the physical pair to be represented digitally. We can interpret them in terms of the size of a user, an object, a process, or even an entire city.

In an initial interpretation by Mark Zuckerberg, the brainchild of Meta, the metaverse is a vision that is much more than VR, which will affect countless companies that will affect the entire industry and that will not just be about gaming. The metaverse, which is being talked about as the successor to the mobile internet, can also be seen as the internet incarnate, where instead of just looking at content, the user can be part of it, interacting with others. Connecting to it on different device platforms, they can have experiences that are not possible through two-dimensional applications and websites, although he believes that people will first see the potential of the internet through these, in commerce and entertainment. In the metaverse, many physical objects will be mere holograms and users will be able to teleport as holograms.⁶

However, despite all the technological evolution and the billions of dollars spent, Zuckerberg is starting to retreat from the meta-future concept of the metaverse. The reason for this is not so much prosaic as technical: there are still a number of problems, many of which remain unresolved, in terms of creating a fully-fledged, practical utopian world that permeates all aspects of the daily lives of digital users. Furthermore, the main focus of future developments will clearly shift to AI, which is also a more tangible and meaningful EDT technology for the average digital user, much, much closer to their interactions in the digital world. However, we can only make cautious predictions about this, as there is a lot of hype around this tech craze, and we are currently in the summer of the AI seasons.⁷ On top of this, at the altar of marketing, developers often sacrifice real technological content in order to make a newer implementation more marketable or to get that coveted superintelligence tag.

This shift in the technological balance is not only the case for Meta, but also for many other technology giants, startups and all the technology-related players that were previously among the biggest advertisers in the metaverse, such as Microsoft, Tencent,⁸ Decentraland⁹ or even Disney.

Perhaps it is at this point that the basic idea of the present paper might make sense, that it is precisely AI that might save the metaverse from technological extinction, from evolutionary dead-end. Maybe it is the convergence and synergy of the two technologies that could bring the big breakthrough for metaverse, which could be an excellent digital atmosphere, an ecosystem, for a possible use of AI. These may seem bold and overly presumptuous statements, as if they were coming from a futurologist. The explosive development of these technologies cannot be treated as a *fait accompli*, and now we can only envisage the likely technological direction and product, depending on their current development. In any case, the spectacular decline in the number of users of various metaverse implementations and the Google Trends search statistics shown in the picture (Figure 1) all prove that the concept

⁶ NEWTON 2021.

⁷ Experts often compare the major milestones and intensity of AI technological development to the change of seasons, which is synonymous with its momentum, the hype surrounding it, etc.

⁸ It is one of the largest Chinese-owned video game publishers in the world (Tencent s. a.).

⁹ A web platform-based 3D virtual world in which users can purchase land for themselves using various virtual currencies (Decentraland s. a.).

of metaverse is in its current state increasingly distancing itself from reality and its rate of development has slowed down. It is in a kind of lifeless state, perhaps due to poor communication, creating a kind of misconception about it in the minds of users, making it difficult for it to penetrate digital society.¹⁰

For the sake of a broader interpretation, referring to a previous article I wrote on this topic, which at that time was still a completely different guise of ideas related to the metaverse, the following terminology explanations were previously formulated.

According to David Baszucki, CEO of Roblox, the metaverse is a persistent, shared universe of virtual worlds, an online place where users from different walks of life work, play and have fun. According to him, the future metaverse should have eight defining characteristics: an avatar with a virtual identity, social connections, an immersive, reality-destroying experience, high-speed connections, the possibility of adventuring in the virtual world without geographical boundaries, diversity, a vibrant economy, and security and stability. All of these will put the possibility of connecting people on a completely new basis.¹¹

Epic Games CEO Tim Sweeney's vision for the metaverse was an expansive, digitised community space, a kind of online playground, the virtual equivalent of the real world, where people could interact with each other and engage in a myriad of activities. He agrees with David Baszucki's view that the metaverse will be created and shaped by users, and that interoperability and a unified technological regulatory framework are essential to achieve this.¹²

Finally, I would like to conclude my thoughts on the terminological discussion with a conceptual interpretation by Jensen Huang, the head of Nvidia. Huang also characterises the metaverse as a kind of virtual world universe, for the realisation of which artificial intelligence (AI) and the evolution of graphic innovations are indispensable, because of which we can reach the 3D extension of the internet.¹³

All these initial conceptual definitions clearly show what kind of future was once envisioned for the metaverse, and what is even more striking is how the development of this technology was transformed in the period following its explosion, which, relying fundamentally on various xR technologies, considered the gaming, entertainment and service industries its primary field of application. Furthermore, there was no real talk at the time about its intertwining with AI technology, although Nvidia's CEO already envisioned such a development trend. In light of the AI developments that are booming today, in my opinion, the need for a joint, mutually influencing examination of these two areas may rightly arise.

¹⁰ FLACHNER 2023.

¹¹ TAKAHASHI 2021a.

¹² PARK 2021.

¹³ TAKAHASHI 2021b.

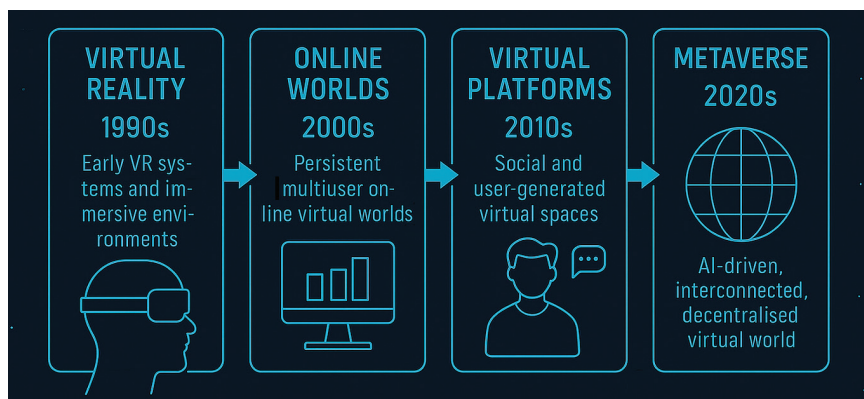


Figure 1: The history of the development of metaverse

Source: Microsoft Copilot

However, before I do all this, I consider it necessary to provide a terminological interpretation of AI, similarly to the conceptual definition of the metaverse. All this in order to be able to map out possible areas of connection and joint development. Furthermore, let us envision a kind of future, taking into account the opinions of experts and the trends of current developments.

Although AI technology has only recently become widely known, like the metaverse, it is not a completely new technological trend. AI developments, although once only in rudimentary form, have been the subject of technological development for several decades. Researchers, developers and professionals are still primarily motivated to try to model human intelligence with the help of machines and to try to automate activities that require human intelligence, such as decision-making, problem solving, or recognising repeating patterns and drawing conclusions based on them. Of course, the goal of mechanising and automating these activities, like the metaverse, was to make people's everyday lives easier and revolutionise certain industries. The first results in this regard were published as early as 1943. Subsequently, more and more innovations appeared in this field, starting with various learning models and ending with the creation of rudimentary neural network computers.

As a result of the increasingly rapid pace of research and development, experts have come to the conclusion that AI should be separated from cybernetics. In response, in 1956, a cybernetics conference held at Dartmouth University in New Hampshire accepted the proposal of John McCarthy, a pioneering expert and visionary of AI, who played a key role in laying the foundations of AI, in a paper. As a result, the term artificial intelligence, which he proposed, is still used today to describe this technology. The essence of this is a machine with intelligence similar to human intelligence, which is able to learn, recognise patterns and make decisions.

The aim of the conference, organised by a specialist with a doctoral degree in mathematics, was precisely to examine the basic philosophy related to AI, the creation of machines capable of intelligent behaviour, with scientific demands. Based on unanimous opinions, we can consider this event as the birth of thinking about

AI, which acted as the engine and driving force of later research and development advances. Among other things, he is credited with developing the LISP (LISt Proces-sing) programming language¹⁴ and creating numerous mathematical models and algorithms. Despite his professional status, or even in parallel with it, he consciously sought to convince and familiarise society with this new technology. Reacting to the criticisms and negative suggestions he received, he sought to draw attention to its responsible, fair, ethical and human values-oriented application and development, taking into account many aspects.

McCarthy thus provided the conceptual and technological framework for AI, which meant the formulation of a vision, the need for a kind of striving for innovation, and the laying of the foundations for the necessary inspiration for this. He created the term itself, designated the main direction in terms of the history of the development of AI, the related dream, the creation of machines with human-level intelligence, the development and creation of general artificial intelligence, superintelligence, is for now only a long-term goal.¹⁵

After the initial conceptualisation, let us review some of the terminological interpretations used today, highlighting the changes this field has undergone during its nearly 80-year development history, and what factors influenced its development. Another pioneer of great importance in terms of the rise of AI is the British–Canadian computer scientist Geoffrey E. Hinton, Professor Emeritus at the University of Toronto, who received the Nobel Prize in Physics in 2024 for his research on AI. He is one of the three people who are called the godfathers of AI, and who also received the ACM (Association for Computing Machinery)¹⁶ A.M.¹⁷ Turing Award,¹⁸ the computer science equivalent of the Nobel Prize, for his work. In Hinton's formulation, AI is defined as computer systems that perform tasks that typically require human intelligence. Like McCarthy, he also emphasises his concerns about the development of technology, its risks, stating that he is shocked by the intensity of its development rate. According to his statement, contrary to previous forecasts, AI is developing at a much faster and more advanced pace than anyone would have ever thought. This is one of its greatest dangers, which may also carry the possibility that the technology will slip out of human control and, above all, out of the regulatory frameworks aimed at safe application. Therefore, in his opinion, great emphasis should be placed on the regulatory background, which requires a behaviour expected from all actors involved in the technology, whether we look at the technology from the government side, from the developer side, or from the user side. The development of a system more intelligent

¹⁴ It is the oldest programming language developed to facilitate AI research and is still of decisive importance today (LISP s. a.).

¹⁵ SZABÓ 2024.

¹⁶ U.S. based international scientific society, the world's largest scientific and educational computing society (ACM s. a.).

¹⁷ The ACM A.M. Turing Prize is also often referred to as the Nobel Prize in Computer Science. The prize is named after Alan M. Turing, the British mathematician who laid the mathematical foundations of computer science (The ACM A.M. Turing Prize s. a.).

¹⁸ Although John McCarthy is also cited as one of the pioneers of AI, surprisingly his name is not included in this triumvirate. The three pioneers in this respect are Yann LeCun (a leading AI scientist at Meta, staff member of New York University), Geoffrey E. Hinton and Yoshua Bengio (staff member of Microsoft, IBM and McGill University) (The ACM A.M. Turing Prize s. a.).

than humans, the creation of so-called superintelligence, carries enormous dangers if it is not used properly and in a sufficiently regulated, safe manner, not to mention the possibility of it falling into the wrong hands.¹⁹

We could continue the endless list of the most famous AI experts and their opinions on the definition of technology. Instead, let us take a brief look at the situation in Hungary in this regard.

One of the documents of decisive importance in this regard is the Artificial Intelligence Strategy of Hungary 2020–2030, which, among other things, uses the following two conceptual definitions regarding AI: "Artificial intelligence (AI) as a set of algorithmic systems capable of learning and improving themselves based on input data."²⁰ On another page of the strategy, we can read the following terminological interpretation:

"Artificial intelligence is software suitable for mapping some part of human intelligence, which is able to support or autonomously perform perception, interpretation, decision-making or action processes. A technology that has special capabilities, nevertheless receives special attention both at the economic and social levels."²¹

The strategy also clearly states that when it comes to the interpretation of AI, we mean narrow AI systems capable of mapping only one area of human intelligence. Research on general AI is still so rudimentary and underdeveloped that these conceptual explanations are probably not clearly equivalent to it.

We can also read numerous terminological explanations in relevant documents on the international scene regarding the interpretation of AI. One of the prominent regulators is the EU AI Act issued by the European Union, which states as follows:

"'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."²²

The significance of AI's impact on the defence sphere is demonstrated by NATO's strategic engagement with the technology. As a result, in October 2021, following a meeting of member countries' defence ministers in Belgium, it published the first version of this strategy, followed by a second revised version in 2024. In the alliance's short, concise and to the point definition, "AI is the ability of machines to perform tasks that typically require human intelligence".²³ Based on NATO's dual view, this new technology will have a fundamental impact on both the global defence and security environment, as a result of which it can provide a technological advantage on the one hand, but also present member countries with new challenges and threats, with a combined impact on the pillars of collective defence, crisis management and cooperative security. What is also a welcome moment in this strategic framework,

¹⁹ MILMO 2024.

²⁰ Ministry of Innovation and Technology 2020: 6. Translated by the author.

²¹ Ministry of Innovation and Technology 2020: 9. Translated by the author.

²² European Parliament 2024.

²³ STANLEY-LOCKMAN – HUNTER CHRISTIE 2021.

as a formulated strategic goal, is, among other things, the safe and responsible application of technology for defence and security purposes, emphasised as the stated intention of all experts, researchers, developers and all stakeholders. In addition, this principle is accompanied by strategic objectives such as the acceleration and general dissemination of the application of AI in capability development, the need to protect self-developed AI technologies and related innovation capabilities, and the need to identify threats arising from the malicious use of AI by state and non-state actors and to create effective protection against them.²⁴

Starting from all this terminological reasoning, it can be seen that almost all definitions and explanations include the main characteristics attributed to this technology – mapping human intelligence, pattern recognition, decision-making, etc. –, which sufficiently define and, in their complexity, frame its nature and perhaps its right to exist. In addition to all this, what perhaps all unanimous opinions welcome is that we must strive for the possibility of using this new opportunity responsibly, safely, consciously and in a way that serves the purpose of humanity.

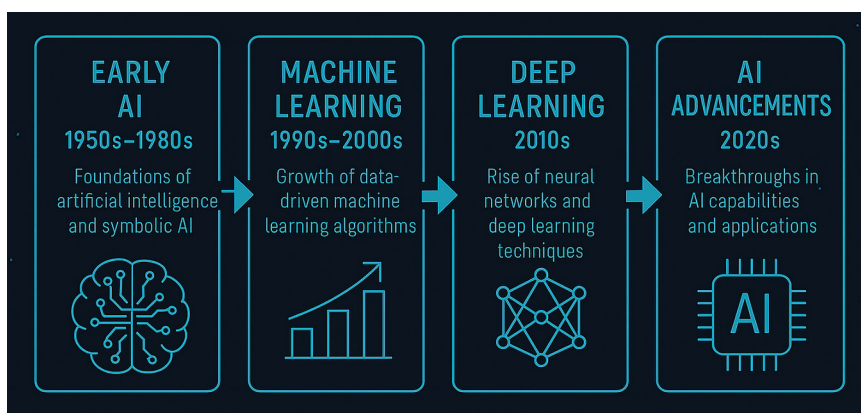


Figure 2: The history of the development of AI

Source: Microsoft Copilot

The synergy of the metaverse and AI

After we have managed to put some order in the conceptual maze of the metaverse and AI, and to establish the underlying content of the technologies involved on a theoretical level, in connection with the ideas formulated in the introduction, let us review what new opportunities and possible directions these two innovations, which have permeated and defined our time to such a significant extent, offer each other. Do they need each other at all, do they give each other something new and different, is there a new potential brewing, or is it just another great epoch-making madness that, after a while, will suffocate under the current over-mystified state, leading to a dead end and sinking into stagnation and complacency?

²⁴ NATO 2021.

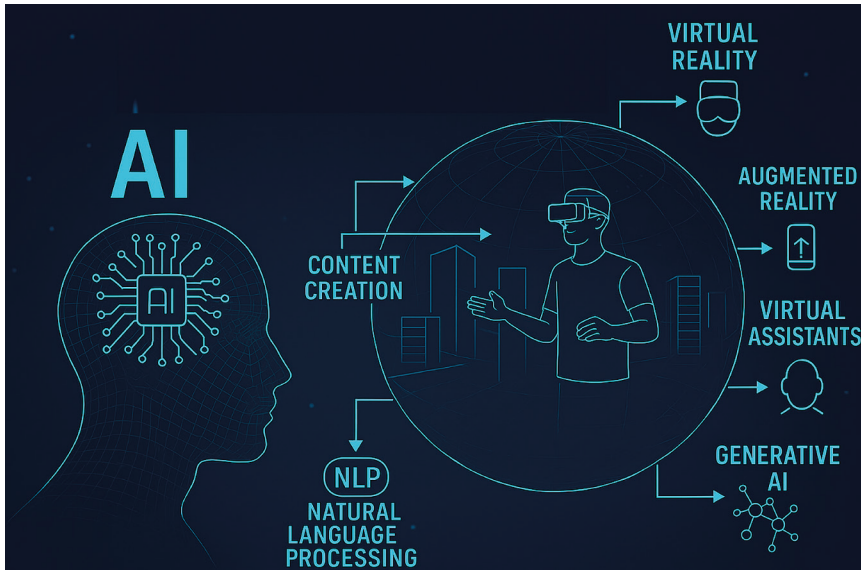


Figure 3: The convergence of AI and the metaverse

Source: Microsoft Copilot

As Figure 3 tries to illustrate in a simplified way, we can certainly conclude that we cannot draw a sharp and clear dividing line between them, as they each carry with them a myriad of new technological opportunities and perspectives, which, through their synergy, could lead to significant breakthroughs in almost all areas of our digital world. In my opinion, their technological impact on each other is unquestionable. It is obvious to everyone that one of the main building blocks of the metaverse is the digital projection of our real physical being, the appearance of our own digital clone in a collective virtual space, connected with the help of the new great era of the internet, Web 3.0, realised as a result of physical reality and virtual space, relying on various xR technologies. The interaction of these digital avatars, interwoven with intelligent behavioural patterns, with each other or with real users in the metaverse, controlled by AI, can result in the implementation of an ever more enhanced, more lifelike digital user experience.

With the help of AI, we can generate significantly more realistic, complex, dynamically changing, intelligent digital environments than before. In contrast to the previous manual planning, design and 3D modelling, these processes can be automated and optimised with the help of generative AI. As a result, digital content production becomes significantly simpler and more diverse in terms of customising both the world of the metaverse and the digital characters appearing in it.

At the same time, this digital space can offer, among other things, an excellent development environment, a kind of digital ecosystem for the development and improvement of AI. It can result in a data set, big data and a continuous data flow for AI professionals, who as a result can test the self-learning process of AI much

more freely, flexibly, and by pushing the physical or virtual limits of the available possibilities in a way never seen before. All the training sets, generated or injected data that are essential for teaching AI can be generated, injected and transformed much more easily in such a digital environment according to the needs and the pace of development of technology. Overall, the metaverse can be an excellent teaching and simulation incubator for technologies, tools and services permeated by AI.

We can witness this kind of powerful intertwining in everyday life because of the emergence of AI and metaverse implementations, such as the emergence of various digital assistants and teachers in order to revolutionise language learning, but also any learning and knowledge acquisition process. As a result of this kind of intertwining, in the metaverse, translation programmes supported by different AI models eliminate language barriers between digital avatars of different nationalities, thus expanding the interactions that can be interpreted in it between users.

If we examine the possible application areas of each technology, we cannot draw a clear and distinct boundary line to separate these two technologies. Although initially, as I mentioned in my previous relevant publication, the metaverse was predicted to gain ground in the service, entertainment and gaming industries, this vision has been significantly re-evaluated and transformed today. Because of the various metaverse implementations, its appearance can already be seen to a significant extent in industry, healthcare, education, training, etc., among others. In addition, the impact of AI on the industrial segment, the economy, medical diagnostics or research–development–innovation, etc. is also indisputable. As a result of these developments, for example, in manufacturing processes, in the diagnosis of various diseases, in the planning of treatments, in scientific research, in various economic transactions and processes, the degree of autonomy, efficiency and optimisation of various processes can be increased to an unprecedented extent.

We must also not forget that the convergence of these technologies may result in not only a significant transformation of existing professional fields, but also the creation of new ones because of the creative power of technology. They may result in the development of new professions, specialists, expertise and professional competencies that have not been needed until now, or that must be fundamentally reinterpreted and transformed. It is no coincidence that the need for programmers to identify with the approach that AI should not be programmed, but taught, appears as a new expectation. Moreover, if we interpret all this teaching process under the protective umbrella of security, then the emphasis should be on human-centred teaching of algorithms.

Speaking of ethical behaviour, we can also predict the emergence of new professionals and fields of expertise that will be responsible for developing the ethical behaviour of AI, or for creating a kind of digital legal culture and regulatory environment.

The creativity of professionals, which focuses on creating and shaping virtual worlds, or on how we can harmonise and fine-tune the interactions between digital twins and real users, may also gain new meaning.

The emergence of this kind of creativity will not only be evident in the development of the visual world of the metaverse, but also in the world of fine arts, music and other areas of culture, where average users, supported by these technologies, can

unleash their imagination and creativity, take their self-expression to new heights, and they can realise their full potential.

The synergy of these two technologies will certainly bring about the explosive development of related technologies, the emergence of new devices and the spread of new services. For example, in the case of the metaverse, the technological spread has long been hampered by the development of the necessary equipment – various xR devices – their cost, the supporting software platform, and other technical obstacles, such as the wearability of these devices and their user ergonomic design. Nowadays, all of these are available in an increasingly mature form and at increasingly affordable prices. Moreover, many, mainly Chinese developers – such as DeepSeek²⁵ cloud-based AI – are trying to circumvent the fact, with more or less success, that the development of AI costs, say, billions of dollars, or that it would require extremely expensive hardware with enormous processing power.

What is certain is that creating an immersive metaverse and operating the AI that supports it necessitates huge computing capacity, a resilient, stable, digitally based and converged network infrastructure, and the availability of hardware and software infrastructure capable of serving it. In the case of AI, such related areas include, among others, the development of certain programming languages, such as Python, as one of the basic pillars of AI development.

The globalisation of the 21st century will reach a new level with the help of these technologies, as because of these technologies, almost all obstacles such as geographical borders, physical distances and language barriers will disappear, and collaboration will reach a higher level than ever before. This kind of blurring and mutual, shared thinking, everyday activity and work were already present in the metaverse from the beginning. Let us just think of the previously mentioned service, gaming and entertainment industries, and the creation of virtual shopping malls, virtual concerts or conference rooms in this digital world that still seemed utopian at the time.

In the case of AI, an interesting and increasingly popular area of application in the repertoire of application areas can be its use in global climate research and climate change. In this segment, the technology can help us in processing the available big data, making forecasts, and, let us hope, in creating urgent, effective solutions, if you like, emergency scenarios. Complementing this with the possibilities of the metaverse, as in a simulated laboratory, the causes, results and effects of extreme changes in the weather become interpretable and verifiable in a tangible way, as well as the measures applied against them, the expected results of the decisions made, and various scenarios and their outputs can be tested in a simulated virtual environment. This is

²⁵ A startup that grew out of the High-Flyer Capital Management hedge fund and was founded in 2023 by Liang Wenfeng. Wenfeng's primary goal was to connect AI and the financial sector. However, he subsequently separated the AI segment from the financial part by founding DeepSeek. He has already introduced new AI implementations such as DeepSeek Coder, DeepSeek LLM, DeepSeek Chat, DeepSeek V2 and V3. However, the real breakthrough was the R1 model, which debuted in early 2025, which is a reasoning-based AI technology (DeepSeek s. a.).

similar to the industrial metaverse,²⁶ where, for example, various production processes can be designed, simulated, tested, optimised and automated in virtual factories.

Closing thoughts

The explosive development of AI technology is being hailed as a new industrial revolution. However, one of the biggest differences between this technological revolution and the previous ones is that while in the case of the previous three major industrial revolutions, humanity had time to prepare for the technological and technical innovations that changed their everyday lives, in the case of AI, we can witness an intensity of development that surpasses even the vision of experts, researchers, professionals and developers, for which there is almost no or very little time available to prepare. This creates an interesting paradox, since we ourselves, humans, are the creators of everything. At the same time, what is unusual in this regard is that if the technological singularity²⁷ (or artificial superintelligence) occurs, which in this case means the creation of an AI that surpasses our capabilities, then how can it be imagined that a creator with a lower level of intelligence will want to control, regulate and keep within limits a system that is much more intelligent than him. We must therefore be very careful in this regard. Furthermore, the much-mentioned lifelong learning will really make sense now, if ever. After all, the development of AI does not require natural resources, but only the available human resource competencies will provide and overcome its limitations.

In addition to all this, we must also keep ethical issues in mind in order to use it responsibly, safely and within a regulated framework. We must raise user safety, data protection, the possibility of attribution and accountability of decisions made by AI in the metaverse to an unprecedented level. Although one of the keys to the survival or renewal of the metaverse is, for example, the pursuit of personalised experiences as a result of the effective application of AI, this can also carry dangers such as the analysis of users' behaviour for non-ethical purposes, the mapping of their personalities, and profiling, which can result in them becoming victims of various attacks, harassment

²⁶ A metaverse implementation in which the digitalisation and optimisation of the industrial segment, supported by AI technology, with innovative solutions to increase production efficiency and supply chain security is the primary goal. This includes, for example, the mapping of production lines, production processes, manufacturing technology, prototyping, testing, product development, research and innovation, production support, standardisation, quality assurance, business development, etc. into virtual space. In addition, workers, development engineers, industrialists can of course actively and collaboratively engage all these processes, either in their physical reality through the various xR technologies or through the interaction of their digital clones. As a result, for example, unprecedented horizons can be opened up not only for the participation of workers in specific work processes, but also for their training, education and coaching processes (Industrial Metaverse s. a.).

²⁷ It is a future period during which the pace of technological change will be so rapid, its impact so deep that human life will be irreversibly transformed. Although neither utopian nor dystopian, this epoch will transform the concepts that we rely on to give meaning to our lives, from our business models to the cycle of human life, including death itself. Understanding this Singularity will alter our perspective on the significance of our past and the ramifications for our future. To truly understand it inherently changes one's view of life in general and one's own particular life (KURZWEIL 2006).

and manipulation. All of this can also raise the awareness of a kind of reinterpreted law-abiding behaviour and the dilemma of legal accountability in this case.

One thing is certain, no matter through which lens we examine the potential of the interaction of technologies, one of the most important factors in their adoption and penetration at the level of the information-digital society will be trust in them, unlimited accessibility, the development of user awareness and the acquisition of the necessary competencies.

In my opinion, especially in the case of AI, we can talk about a technological innovation that almost no user will be able to avoid interacting with, regardless of the different user generations. Thus, these technologies will certainly be part of the everyday lives of all ages and social groups in some form. As a result, although in some cases we protest against it, we must at some level know and make friends with the positive effects of these technologies for humanity – let us trust in them. Of course, without falling overboard and becoming completely dependent on these technological innovations.

In terms of the topic under study, one of the key moments will probably be the level and form at which they will be able to develop together, interact with each other, open up new horizons of innovation, digitalisation and connectivity, and revolutionise new major breakthroughs in their own and related technologies. In addition, to do all this in a way that will serve the long-term and lasting benefit of humanity, dominating the course of technological development. We trust that as a result of symbiosis, we will be witnesses and active participants of a technological development that will result in a hybrid implementation in which one technology benefits from the impact of the other, they mutually influence each other's development, and their development and the opportunities they offer will have some positive added value for all involved.

Overall, if we wanted to summarise the expected main benefits of the synergy of the metaverse and AI in a few thoughts, then without claiming to be exhaustive, we could attach the following adjectives to the new technological future that will emerge as a result of their symbiosis: automation, optimisation, efficiency enhancement, creativity, innovation, boundlessness, unrestrictedness, collaboration, connectivity, simulation, decision support and problem solving.

References

- ACM (s. a.): *ACM (Association for Computing Machinery)*. Online: www.acm.org/
 Decentraland (s. a.). Online: <https://decentraland.org/>
 DeepSeek (s. a.). Online: www.deepseek.com/en
 European Parliament (2024): *The EU Artificial Intelligence Act*. Up-to-date developments and analyses of the EU AI Act. Online: <https://artificialintelligenceact.eu/article/3/>
 FLACHNER, Balázs (2023): Így működik el a metaverzum dicsősége. *Telex*, 26 April 2023. Online: <https://telex.hu/techtud/2023/04/26/metaverzum-meta-microsoft-disney-web3-nft>

- JOBBÁGY, Szabolcs (2022): Metaverzum, a virtuális univerzum, világunk digitális kivetülése. Utópia vagy kézzelfogható valóság a digitális jövőben? *Hadtudományi Szemle*, 15(2), 131–160. Online: <https://doi.org/10.32563/hsz.2022.2.8>
- KURZWEIL, Ray (2006): *The Singularity Is Near*. New York: Viking Press. Online: <https://doi.org/10.1145/1119621.1117663>
- LISP (s. a.): *LISP (LISt Processing) programming language*. Online: www.britannica.com/technology/LISP-computer-language
- MILMO, Dan (2024): 'Godfather of AI' Shortens Odds of the Technology Wiping Out Humanity over Next 30 Years. *The Guardian*, 27 December 2024. Online: www.theguardian.com/technology/2024/dec/27/godfather-of-ai-raises-odds-of-the-technology-wiping-out-humanity-over-next-30-years
- Ministry of Innovation and Technology (2020): Magyarország Mesterséges Intelligencia Stratégiája 2020–2030 [Artificial Intelligence Strategy of Hungary 2020–2030]. Online: <https://cdn.kormany.hu/uploads/document/6/67/676/676186555d8df2b1408982bb6ce81c643d5fa4ab.pdf>
- NEWTON, Casey (2021): Mark in the Metaverse – Facebook's CEO on Why the Social Network Is Becoming a Metaverse Company. *The Verge*, 22 July 2021. Online: www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview
- Palantir Technologies (s. a.). Online: www.palantir.com/about/
- PARK, Gene (2021): Epic Games Believes the Internet is Broken. This Is Their Blueprint to Fix It. *The Washington Post*, 28 September 2021. Online: www.washingtonpost.com/video-games/2021/09/28/epic-fortnite-metaverse-facebook/
- PORKOLÁB, Imre – HÖNICH, Artúr (2024): A stratégiai előrelátás operatív hatása: A NATO technológiai prioritásai és a magyar védelmi innováció fókuszterületei. *Honvédségi Szemle*, 152(1), 3–16. Online: <https://doi.org/10.35926/HSZ.2024.1.1>
- Industrial Metaverse (s. a.). Online: www.siemens.com/global/en/company/digital-transformation/industrial-metaverse.html
- NATO (2021): *Summary of the NATO Artificial Intelligence Strategy*. Online: www.nato.int/cps/en/natohq/official_texts_187617.htm
- STANLEY-LOCKMAN, Zoe – CHRISTIE, Edward H. (2021): *An Artificial Intelligence Strategy for NATO*. Online: www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html
- SZABÓ, László (2024): Az AI eredete: John McCarthy, a mesterséges intelligencia mögött álló látnok. *NowadAI*s, 29 February 2024. Online: www.nowadais.com/hu/mi-john-mccarthy-mesterseges-intelligencia/
- TAKAHASHI, Dean (2021a): Roblox CEO Dave Baszucki Believes Users Will Create the Metaverse. *Venture Beat*, 27 January 2021. Online: <https://venturebeat.com/games/roblox-ceo-dave-baszucki-believes-users-will-create-the-metaverse/>
- TAKAHASHI, Dean (2021b): Jensen Huang Interview: The Physical World and the Metaverse Can Be Connected. *Venture Beat*, 21 August 2021. Online: <https://venturebeat.com/games/jensen-huang-interview-the-physical-world-and-the-metaverse-can-be-connected/>
- Tencent (s. a.). Online: www.tencentgames.com/
- The ACM A.M. Turing Prize (s. a.). Online: <https://amturing.acm.org/>

Pál Károly Laska¹

Empirical Analysis of the Impact of Personality Traits on Cybersecurity Awareness

A Scientometric and Network-Based Approach

Abstract

This study investigates the relationship between personality traits and cybersecurity awareness through a bibliometric and network analysis of scientific publications indexed in Scopus between 2000 and 2023. Using VOSviewer software, the research identifies keyword co-occurrence patterns, thematic clusters and temporal research trends in this interdisciplinary domain. The scientometric approach is complemented with theoretical insights from psychology – particularly the Big Five personality model – and cybersecurity behaviour research. Results indicate that personality traits significantly shape security awareness, influencing susceptibility to social engineering, phishing and compliance behaviour. Network analysis highlights the increasing integration of psychological constructs into cybersecurity education and policy. The study argues for the adoption of personality-based adaptive training programmes, particularly in the public sector, where tailored interventions can enhance resilience against human-factor-related security breaches.

Keywords: cybersecurity awareness, personality traits, Big Five model, scientometric analysis, network analysis, social engineering, adaptive training

¹ Doctoral candidate, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: [Laska. Pal.Karoly@uni-nke.hu](mailto:Pal.Karoly@uni-nke.hu)

Introduction

Cybersecurity has evolved from a purely technical discipline into a complex, multidisciplinary field that increasingly recognises the human factor as a critical component of security resilience. While technological solutions such as encryption, firewalls and intrusion detection systems remain essential, empirical evidence suggests that human behaviour often constitutes the weakest link in the security chain.² Among the various human factors influencing security outcomes, personality traits have emerged as a significant determinant of cybersecurity awareness, decision-making and policy compliance.³

The Big Five personality model – openness, conscientiousness, extraversion, agreeableness, and neuroticism – has been widely studied in psychology as a predictor of behaviour across diverse domains, including workplace performance, health behaviour and risk-taking.⁴ In the cybersecurity context, these traits influence not only the likelihood of engaging in risky online behaviour but also the capacity to detect and resist social engineering attacks.⁵ For example, high conscientiousness has been associated with greater adherence to security protocols, whereas high openness may correlate with exploratory behaviour that increases exposure to threats.⁶

Despite these insights, the integration of psychological constructs into cybersecurity strategy remains limited. Existing research is fragmented, with studies dispersed across information systems, psychology, criminology and behavioural sciences.⁷ This fragmentation complicates the development of unified, evidence-based interventions that could enhance security awareness through personality-tailored training programmes.

To address this gap, the present study applies a scientometric and network analysis approach to systematically map the literature on personality traits and cybersecurity awareness. By analysing keyword co-occurrence patterns, thematic clusters and temporal evolution in the research landscape, we aim to:

1. Identify the central concepts and dominant research themes in this interdisciplinary field.
2. Examine the degree to which psychological frameworks have been incorporated into cybersecurity studies over time.
3. Highlight potential directions for future empirical research and policy development.

Ultimately, the study seeks to contribute to the emerging paradigm of psychologically informed cybersecurity, advocating for adaptive awareness programmes that align

² PONT-MATA 2016; AMANKWA et al. 2020.

³ BARABÁSI-ALBERT 1999; BLASCO-QUAGLIA 2018.

⁴ BOBAN 2014.

⁵ WANG et al. 2021.

⁶ MCCORMAC et al. 2017; PADAYACHEE 2022.

⁷ DOUCEK et al. 2019; UFFEN et al. 2012.

with individual differences in personality.⁸ This approach aligns with recent calls for moving beyond “one-size-fits-all” training and towards personalised, data-driven interventions.⁹ Moreover, latest developments in cybersecurity education emphasise the implementation of adaptive learning frameworks that dynamically respond to individual learner profiles. For instance, the Adaptive Cybersecurity Training Framework for Social Media Risks (ACSTF-SMR) demonstrated significant improvements in employee engagement and learning outcomes by customising training modules to individual preferences and proficiency levels.¹⁰ This evidence underscores the feasibility and effectiveness of personalised, psychology-informed interventions, which align precisely with the evolving paradigm of human-centred cybersecurity.

Research objective

The overarching objective of this research is to conduct a comprehensive scientometric and network-based investigation into the relationship between personality traits and cybersecurity awareness, with the aim of advancing both the theoretical understanding and the practical application of psychologically informed cybersecurity strategies. While isolated studies have examined the influence of specific psychological variables on security-related behaviour, there is a notable lack of integrative, cross-disciplinary mapping of the field. This study addresses this gap by systematically analysing the global body of research indexed in the Scopus database over the period 2000–2023, thereby identifying conceptual patterns, thematic clusters and temporal dynamics.

The research is guided by three interrelated objectives:

1. *Conceptual Mapping of the Field*: To identify and categorise the dominant themes, frameworks and methodological approaches in the literature on personality traits and cybersecurity awareness. This includes examining the prevalence of psychological constructs – particularly the Big Five personality model¹¹ – and their integration into cybersecurity-focused research. Mapping the conceptual terrain provides a clearer picture of the intellectual structure of the field and reveals underexplored intersections between disciplines such as psychology, information systems and criminology.¹²
2. *Network Structure and Interdisciplinary Linkages*: To perform a co-occurrence network analysis using VOSviewer in order to visualise the relationships among keywords, authors and thematic clusters. The analysis seeks to determine the degree of interdisciplinarity, the centrality of key concepts and the presence of network properties such as *small-world* and *scale-free* characteristics.¹³ These structural properties can reveal how knowledge flows within the research

⁸ This is also supported by Weems et al. in their study, when they state that insecure cyber behaviours were associated with lower levels of conscientiousness, higher levels of psychological symptoms such as somatic and depressive symptoms (WEEMS et al. 2018).

⁹ UFFEN–BREITNER 2015; WANG et al. 2023.

¹⁰ BEN SALAMAH et al. 2023.

¹¹ BOBAN 2014.

¹² MCCORMAC et al. 2017; UFFEN et al. 2012.

¹³ BARABÁSI–ALBERT 1999; WATTS–STROGATZ 1998.

community and whether certain clusters function as bridges between otherwise disconnected domains.¹⁴

3. *Implications for Adaptive Cybersecurity Interventions:* To derive actionable insights for policymakers, educators and organisational leaders on how personality assessment can be systematically incorporated into cybersecurity awareness programmes. The study argues that tailoring training content to personality profiles – rather than relying on uniform, generic approaches – can enhance engagement, retention and ultimately behavioural change.¹⁵ This is particularly relevant for high-risk sectors such as government agencies, health-care providers and critical infrastructure operators, where human error can have severe consequences.¹⁶

From a scientific contribution perspective, this research offers several advancements. First, it synthesises a fragmented literature base, bridging the gap between psychological theory and cybersecurity practice. Second, it applies bibliometric techniques to quantify and visualise the structural evolution of the field, enabling a more objective understanding of how research trends have shifted towards greater psychological integration over the past two decades. Third, it proposes a conceptual framework for the incorporation of personality-based tailoring into cybersecurity awareness interventions, grounded in empirical evidence from the analysed literature.

In sum, the research objective is not merely to describe the existing literature, but to generate a strategic, evidence-based roadmap for advancing psychologically informed cybersecurity. By integrating scientometric mapping with behavioural theory, this study seeks to facilitate a paradigm shift from reactive, technology-centred security measures to proactive, human-centred resilience strategies.

Methodology

This study adopts a mixed-method scientometric approach combining *bibliometric analysis* and *network analysis* to systematically explore the relationship between personality traits and cybersecurity awareness in academic literature. The methodological design follows three core principles: transparency, reproducibility and integration of quantitative mapping with qualitative interpretation.

Data source and search strategy

The primary data source was the Scopus database, selected for its comprehensive coverage of peer-reviewed journals, conference proceedings and book chapters

¹⁴ DOUCEK et al. 2019.

¹⁵ McCORMAC et al. 2017; PADAYACHEE 2022; UFFEN-BREITNER 2015.

¹⁶ WANG et al. 2023; YENG et al. 2021.

across disciplines. The search strategy was defined to maximise precision (minimising irrelevant results) and recall (capturing the broadest relevant set of publications).¹⁷

This search string ensures inclusion of studies explicitly addressing both cybersecurity and personality-related variables, in line with the research objective. The publication period 2000–2023 was chosen to encompass the emergence of human-centric security research in the early 2000s and the recent acceleration of psychological integration in security studies.¹⁸

Inclusion and exclusion criteria

From the initial 1,082 records, a two-stage screening process was applied:

1. Title and abstract screening – Excluded papers not focusing on the human aspect of cybersecurity or personality-related constructs.
2. Full-text screening – Excluded works that:
 - focused solely on technical aspects without behavioural analysis
 - addressed personality traits but in non-cybersecurity contexts
 - were duplicates or non-peer-reviewed sources

The final dataset comprised 50 publications, representing the most relevant and methodologically rigorous contributions to the field.

Data extraction and pre-processing

For each selected publication, the following metadata were extracted:

- authors and affiliations
- year of publication
- source type (journal, conference, book chapter)
- keywords (author keywords and indexed keywords)
- abstract and full-text content (when accessible)
- citation counts
- DOI and Scopus identifiers

To ensure consistency, keyword harmonisation was performed, merging synonyms (e.g. *cyber security* to *cybersecurity*) and unifying American/British spelling variations (*behaviour* vs. *behavior*).

¹⁷ Scopus 2023.

¹⁸ McCORMAC et al. 2017; PADAYACHEE 2022; UFFEN-BREITNER 2015.

Network analysis procedure

Bibliometric mapping was conducted using VOSviewer 1.6.19 to visualise keyword co-occurrence networks. Network parameters were configured as follows:

- counting method: full counting
- minimum keyword occurrence threshold: 3
- layout algorithm: VOS mapping with normalisation
- clustering resolution: 1.0 (default)
- attraction and repulsion parameters: default (2 and -1)

The resulting network graphs allowed the identification of clusters, each representing a thematic concentration in the literature. The size of nodes reflects the frequency of occurrence, while the proximity and link strength between nodes indicate conceptual relatedness.

To deepen the structural analysis, network metrics were calculated:

- degree centrality: measures the number of direct connections a keyword has
- betweenness centrality: indicates keywords acting as bridges between clusters
- closeness centrality: reflects the average shortest path length to all other keywords
- clustering coefficient: measures the extent to which nodes tend to cluster together

These metrics provided a quantitative basis for interpreting the role of central concepts such as *personality traits*, *security awareness* and *human behaviour*.

Validation and reliability measures

To ensure methodological robustness:

- search results were cross-validated with a secondary search in Web of Science
- two independent reviewers conducted screening to minimise selection bias
- network visualisations were replicated with alternative clustering resolutions to check stability
- all data processing steps were documented for reproducibility

Results

The bibliometric and network analysis revealed several distinct thematic clusters in the literature on personality traits and cybersecurity awareness. These clusters reflect the evolving interdisciplinary integration between *psychology*, *information security* and *human behaviour research*.

Cluster analysis

The co-occurrence network generated from the dataset identified four major clusters:

1. Cluster 1 – Human Factors in Cybersecurity Awareness
 - Core keywords: *cybersecurity, security awareness, information security, training, human error*
 - This cluster represents research focusing on awareness programmes, training effectiveness and behavioural interventions. Personality traits are examined in the context of susceptibility to phishing, password management habits and compliance with security policies.
2. Cluster 2 – Psychological Models and Personality Frameworks
 - Core keywords: *personality traits, Big Five, individual differences, risk perception*
 - This cluster links psychometric models to security behaviours, often testing how openness, conscientiousness, extraversion, agreeableness and neuroticism affect security decision-making.
 - Several studies within this cluster explore risk-taking behaviour and impulsivity as predictors of vulnerability to cyber threats.
3. Cluster 3 – Social Engineering and Insider Threats
 - Core keywords: *social engineering, phishing, insider threats, trust*
 - Here, personality traits are related to social manipulation susceptibility, with emphasis on trust propensity and agreeableness as double-edged factors – facilitating collaboration but also increasing vulnerability.
4. Cluster 4 – Network Security and Behavioural Modelling
 - Core keywords: *network analysis, behavioural modelling, resilience, incident response*
 - This cluster focuses on modelling human-in-the-loop security systems, often combining graph theory with behavioural parameters to predict system resilience.

Cross-cluster interactions

Analysis of inter-cluster links showed strong conceptual ties between:

- Psychological Models (Cluster 2) and Social Engineering (Cluster 3), indicating the increasing role of personality profiling in phishing defence strategies.
- Human Factors (Cluster 1) and Network Modelling (Cluster 4), suggesting that behavioural metrics are now integrated into system resilience simulations.

These connections indicate a paradigm shift from purely technical safeguards towards human-centric, behaviourally adaptive security systems.

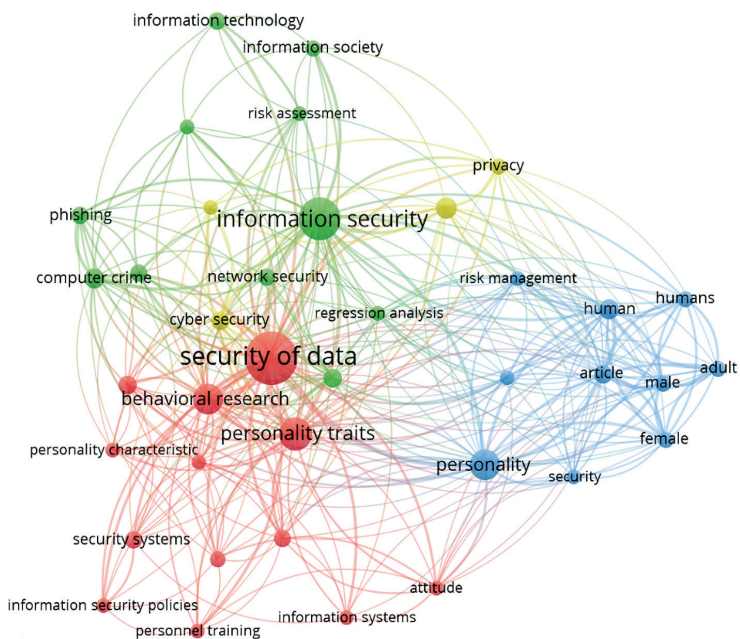


Figure 1: Keyword co-occurrence network – colour-coded clusters

Source: compiled by the author

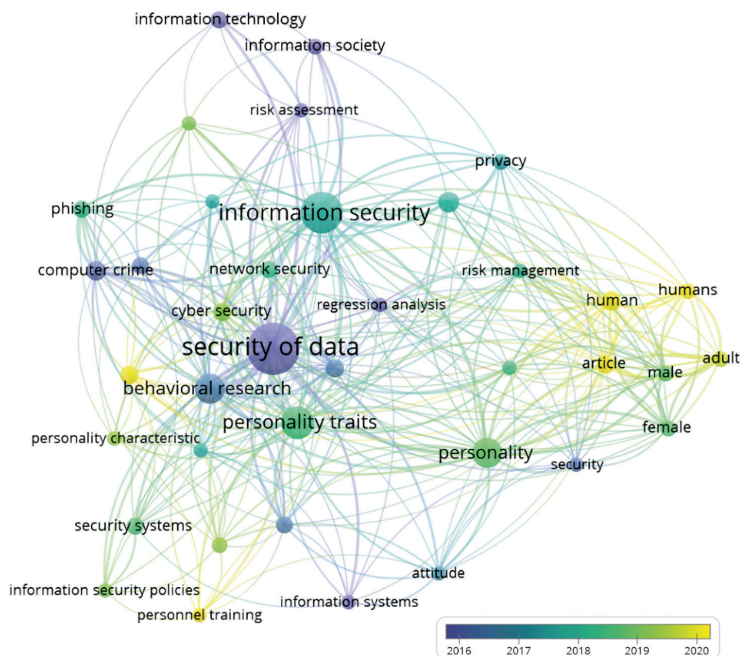


Figure 2: Inter-cluster connection map

Source: compiled by the author

Discussion

The results of this study confirm that personality traits exert a measurable and significant influence on cybersecurity awareness and related behaviours. This aligns with prior empirical findings,¹⁹ which have repeatedly demonstrated that *individual differences* – particularly in the domains of conscientiousness, openness to experience and neuroticism – affect the degree to which users comply with security policies, detect phishing attempts and adhere to safe digital practices.

From a network analysis perspective, the high degree and betweenness centrality scores of *personality traits* and *security awareness* highlight their bridging role between the psychological and technical domains of cybersecurity. This suggests that the interdisciplinary integration of these domains is not only theoretical but is also reflected in the structure of the scientific literature itself.

Notably, the cross-cluster connections between *psychological models* and *social engineering* studies underline the critical role of personality profiling in countering phishing and manipulation attacks. For example, individuals with high agreeableness may be more prone to trust unsolicited communications, while those with high openness may be more likely to engage with unfamiliar digital content – both traits that can be leveraged in targeted attacks if not addressed in training.

The implications for policy and practice are clear:

- Cybersecurity awareness programmes should integrate personality-based risk assessments to optimise content delivery and engagement.
- Public sector organisations and critical infrastructure operators, which face heightened risks from targeted social engineering, could significantly improve resilience by embedding psychological screening and tailored training into security protocols.
- Network-based monitoring of research trends can help policymakers and educators anticipate emerging vulnerabilities, ensuring that awareness initiatives remain current and evidence-based.

At the same time, the study's reliance on secondary data and bibliometric analysis presents limitations. While network analysis reveals structural relationships within the literature, it does not capture causal mechanisms between personality traits and security behaviours. Thus, the next stage of research should combine scientometric insights with *primary* empirical data – for instance, controlled experiments or large-scale surveys – to validate and expand upon the observed patterns.

Furthermore, advanced network metrics such as modularity scores, eigenvector centrality and temporal clustering coefficients could be incorporated in future analyses to deepen the understanding of how research themes evolve and interconnect. These metrics, when combined with content analysis, could identify not only *what* is being studied but also *how* the conceptual framing of personality in cybersecurity shifts over time.

¹⁹ MCCORMAC et al. 2017; PADAYACHEE 2022; UFFEN-BREITNER 2015.

Ultimately, the evidence points towards an emerging research paradigm in which human factors, particularly personality traits, are not peripheral considerations but central determinants of cybersecurity strategy effectiveness. Recognising and operationalising this fact in both academic research and practical training design will be critical to strengthening digital resilience in an era of increasingly sophisticated cyber threats.

Conclusion

This study has demonstrated that personality traits play a decisive role in shaping cybersecurity awareness, influencing not only users' adherence to security protocols but also their susceptibility to social engineering and other human-targeted attacks. Through bibliometric and network analysis of literature indexed in the Scopus database between 2000 and 2023, the research has mapped the intellectual structure of this interdisciplinary field, revealing that the connection between psychological science and cybersecurity practice has become increasingly prominent over time.

The scientometric mapping confirms that the domain is characterised by a "small-world" and partially "scale-free" network structure, indicating the existence of highly connected research nodes that facilitate cross-disciplinary knowledge exchange. This network configuration also suggests that targeted integration of concepts from psychology – such as the Big Five personality dimensions – into cybersecurity strategies could have an outsized impact on both academic discourse and applied training methodologies.

From a practical perspective, the findings point towards a paradigm shift:

1. Moving from uniform, technical training modules towards adaptive, psychologically-informed security awareness programmes.
2. Incorporating personality-based profiling into both public and private sector security policies to tailor interventions more precisely to user risk profiles.
3. Leveraging network monitoring of research trends to maintain up-to-date, evidence-based awareness initiatives that anticipate emerging threats.

However, the present study is not without limitations. As the analysis relied exclusively on secondary data, causal inferences regarding the influence of personality traits on cybersecurity behaviours cannot be drawn. Future research should therefore complement bibliometric analysis with primary empirical methods – including experimental designs, longitudinal surveys and sector-specific case studies – to validate and extend the observed relationships.

In addition, the methodological framework could be enhanced by incorporating advanced network indicators (e.g. betweenness and closeness centrality, modularity optimisation) and by integrating quantitative content analysis of the most influential works in the field. This would provide not only a structural but also a substantive understanding of how key concepts are operationalised across disciplines.

In conclusion, recognising and systematically integrating personality traits into cybersecurity awareness frameworks represents both a scientific opportunity and

a practical necessity. The resilience of individuals and organisations against cyber threats will increasingly depend on the ability to merge human factors research with technical security measures – creating holistic, adaptive and psychologically grounded defence strategies that are responsive to the evolving threat landscape.

References

- AMANKWA, Eric – LOOCK, Marianne – KRITZINGER, Elmarie (2020): A Composite Framework to Promote Information Security Policy Compliance in Organizations. In SERRHINI, Mohammed – SILVA, Carla – ALJAHDAI, Sultan (eds.): *Innovation in Information Systems and Technologies to Support Learning Research*. Cham: Springer, 458–468. Online: https://doi.org/10.1007/978-3-030-36778-7_51
- BARABÁSI, Albert-László – ALBERT, Réka (1999): Emergence of Scaling in Random Networks. *Science*, 286(5439), 509–512. Online: <https://doi.org/10.1126/science.286.5439.509>
- BEN SALAMAH, Fai – PALOMINO, Marco A. – CRAVEN, Matthew J. – PAPADAKI, Maria – FURNELL, Steven (2023): An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work. *Applied Sciences*, 13(17). Online: <https://doi.org/10.3390/app13179595>
- BLASCO, Jorge – QUAGLIA, Elizabeth A. (2018): *InfoSec Cinema: Using Films for Information Security Teaching*. ASE 2018 – USENIX Workshop on Advances in Security Education, Co-Located with USENIX Security 2018. Conference Paper. Online: www.usenix.org/system/files/conference/ase18/ase18-paper_blasco.pdf
- BOBAN, Marija (2014): *Information Security and the Right to Privacy in Digital Economy – The Case of the Republic of Croatia*. 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 26–30 May 2014, Opatija, Croatia. Online: <https://doi.org/10.1109/MIPRO.2014.6859804>
- DOUCEK, Petr – BASL, Josef – PAVLICEK, Antonin M. – TJOA, A. Min – DETTER, Katrin – RAFFAI, Maria eds. (2019): *Research and Practical Issues of Enterprise Information Systems*. Cham: Springer. Online: <https://doi.org/10.1007/978-3-030-37632-1>
- MCCORMAC, Agata – ZWAANS, Tara – PARSONS, Kathryn – CALIC, Dragana – BUTAVICIUS, Marcus – PATTINSON, Malcolm (2017): Individual Differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151–156. Online: <https://doi.org/10.1016/j.chb.2016.11.065>
- PADAYACHEE, Keshnee (2022): Understanding the Effects of Situational Crime Prevention and Personality Factors on Insider Compliance. *Journal of Information Security and Applications*, 70. Online: <https://doi.org/10.1016/j.jisa.2022.103338>
- PONT, Ana – MATA, Francisco J. eds. (2016): *ICT for Promoting Human Development and Protecting the Environment*. Cham: Springer. Online: <https://doi.org/10.1007/978-3-319-44447-5>
- Scopus (2023): *Content Coverage Guide*. Online: https://assets.ctfassets.net/o78em1y1w4i4/EX1iy8VxBeQKf8aN2XzOp/c36f79db25484cb38a-5972ad9a5472ec/Scopus_ContentCoverage_Guide_WEB.pdf

- UFFEN, Jörg – GUHR, Nadine – BREITNER, Michael H. (2012): *Personality Traits and Information Security Management: An Empirical Study of Information Security Executives*. International Conference on Information Systems, ICIS 2012. Conference Paper. Online: <https://aisel.aisnet.org/icis2012/proceedings/ISSecurity/5>
- UFFEN, Jörg – BREITNER, Michael H. (2015): Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions. In *Standards and Standardization: Concepts, Methodologies, Tools, and Applications*. Hershey: IGI Global, 836–853. Online: <https://doi.org/10.4018/978-1-4666-8111-8.ch039>
- WANG, Dawei (David) – DURCIKOVA, Alexandra – DENNIS, Alan R. (2023): Security Is Local: The Influence of the Immediate Workgroup on Information Security. *Journal of the Association for Information Systems*, 24(4), 1052–1101. Online: <https://doi.org/10.17705/1jais.00812>
- WANG, Zuoguang – ZHU, Hongsong – SUN, Limin (2021): Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access*, 9, 11895–11910. Online: <https://doi.org/10.1109/ACCESS.2021.3051633>
- WATTS, Duncan J. – STROGATZ, Steven H. (1998): Collective Dynamics of "Small-World" Networks. *Nature*, 393(6684), 440–442. Online: <https://doi.org/10.1038/30918>
- WEEMS, Carl F. – AHMED, Irfan – RICHARD, Golden G. III – RUSSELL, Justin D. – NEILL, Erin L. (2018): Susceptibility and Resilience to Cyber Threat: Findings from a Scenario Decision Program to Measure Secure and Insecure Computing Behavior. *PLoS One*, 13(12). Online: <https://doi.org/10.1371/journal.pone.0207408>
- YENG, Prosper K. – FAUZI, Muhammad A. – YANG, Bian (2021): Assessing the Effect of Human Factors in Healthcare Cybersecurity Practice: An Empirical Study. In VASSILAKOPOULOS, Michael Gr. – KARANIKOLAS, Nikitas N. (eds.): *PCI 2021: Proceedings of the 25th Pan-Hellenic Conference on Informatics*. New York: Association for Computing Machinery, 472–476. Online: <https://doi.org/10.1145/3503823.3503909>

Pataki János Imre,¹ Sulányi Péter²

Az autóipari vállalatok és beszállítók integrált biztonsági és védelmi stratégiája

Security and Defence Strategy of Companies in the Automotive Industry

Absztrakt

Napjaink biztonsági kihívásai világszerte jelentősen befolyásolják a multinacionális vállalatok biztonságos működését. Ezt a problémát a multinacionális vállalatok korán felismerték, ezért különböző elméletek és módszerek alkalmazásával alkották meg saját válságkezelő szabályait és folyamataikat. A különböző elgondolások alkalmazása több vállalatnál nem működött hatékonyan, ezért a nemzetközi szervezetek és intézmények megalkottak egy sor jogszabályt és ajánlást, amelyek válaszokat adnak a 21. század biztonsági kihívásaira, veszélyeire és kockázataira. A privát szektorban jelenleg két fontos nemzetközi/nemzeti jogszabály jelent meg, amelyek bevezetése és alkalmazása jelentős terhet jelent a vállalkozói szféra számára. A jelenlegi biztonsági helyzet a vállalatok számára integrált biztonsági és védelmi stratégia kidolgozását teszi szükségessé, amely figyelembe veszi az új jogszabályoknak való megfelelést.

Kulcsszavak: biztonsági stratégia, integrált biztonsági és védelmi koncepció, fizikai védelem, Helyzetelemző Központ

¹ AUDI HUNGARIA Zrt., e-mail: janos.pataki@audi.hu

² Suprex Kft., e-mail: speter@suprex.hu

Abstract

Today's security challenges have significant impact on large enterprises worldwide. Multinational companies recognised this problem early on and used different theories and methods to create their own crisis management rules and processes. The application of different concepts has not worked well in many companies, so international organisations and institutions have created a series of laws and recommendations that respond to the security challenges, threats and risks of the twenty-first century. In the private sector, two important international/national laws have emerged at present, the introduction and operation of which represent a significant burden for the business sector. The current security situation makes it necessary for companies to develop a Security and Defence Strategy that takes into account compliance with the new legislation.

Keywords: security strategy, integrated security and defence system, physical security, Situation Centre

„Élet és halál alapja, a túlélés vagy a megsemmisülés Útja (Tao).
Éppen ezért alapos vizsgálatot és mérlegelést kíván.”
Szun-Ce³

Bevezetés

A stratégiai gondolkodás a nagy földrajzi felfedezések és a haditechnikai eszközök fejlődésével⁴ új korszakba lépett. Új katonai intézmények alakultak, amelyekben új eljárásokat és módszereket dolgoztak ki, amelyek maig hatást gyakorolnak a jelen kor stratégiai gondolkodóira. Viszont Montecuccoli⁵ kijelentése, hogy a háborúhoz csak pénz, pénz, pénz szükséges, ez maig érvényes.

Napjainkban a geopolitikai helyzet változását a civilizációk közötti ellentétek generálják,⁶ amelyek helyi szinten törésvonal-konfliktusokat⁷ okoznak a különböző civilizációkat képviselő nemzetállamok között, illetve egy országon belül polgárháború⁸ vagy konfliktus⁹ törhet ki. Ez negatívan befolyásolja a globális gazdaság működését, ami működési zavarokat okoz a multinacionális vállalatoknál.¹⁰

2013 februárjában jelent meg Valerij Geraszimov tábornok cikke, amelyben a Varsói Szerződés totális háborús doktrínáit és taktikáját vette alapul, és ötvözte azokat a mai stratégiai katonai gondolkodással. Kidolgozta a modern hadviselés egy új elméletét. Ez az elmélet inkább egy ellenséges hatalom megdöntésére irányul és nem közvetlen támadásra. Azt írta: „A háború szabályai megváltoztak. A politikai és stratégiai célok

³ Szun-Ce 2012: 17.

⁴ A lovagvilág megszűnése, tűzfegyverek megjelenése.

⁵ PARET 1986: 32–40.

⁶ HUNTINGTON 2006: 343–346.

⁷ Orosz–ukrán háború.

⁸ Húsz felkelők Jemenben, évtizedes polgárháború, hajóforgalom támadása a Vörös-tengeren.

⁹ Gázában: izraeli–palesztin konfliktus.

¹⁰ Zavar az ellátási láncban, közvetlen és közvetett költségek növekedése.

elérésében a nem katonai eszközök szerepe megnőtt, és hatékonyságuk sok esetben meghaladta a fegyverek erejét. Mindezt rejtett katonai eszközök egészítik ki.¹¹ Oroszország 2014-ben megszállta a Krím félszigetet, és céljait a különleges erők,¹² a helyi fegyveres szereplők, a gazdasági befolyás, a dezinformáció és az ukrajnai társadalmi-politikai polarizáció kihasználásával érte el.

Az unió területén több kibertámadás történt az elmúlt években. A közműrendszerek és vállalkozások kiberbiztonsági sérülékenysége magas kockázati szintet jelent. A támadások elkövetőinek fő célja a közműrendszerek és a vállalkozások működésének akadályozása, amivel veszélyeztetik a lakosság és a fontosabb létesítmények ellátását, illetve működését. A támadásokkal az adott állam működőképességét is veszélyeztethetik.¹³ 2024-ben világszerte megnőtt a vállalatok elleni kibertámadások száma, mert a támadások átlagos száma 44%-kal magasabb volt, mint 2023-ban. A támadások elleni védekezés jelentős költséggel jár a közüzemek és a vállalatok számára. Átlagosan 75 napot vesz igénybe, hogy egy szervezet visszanyerje működőképességét egy kiberincidens után.

A járműiparban kiemelt feladat a járművek IT-biztonsági szempontok alapján történő fejlesztése, gyártása, valamint az értékesített járművek folyamatos felügyelete. Az Automotive Security Management System (ASMS) előírásainak betartása kiemelt feladat a járművek intenzívebb adatforgalma miatt. Ez vonatkozik a *cyber security* (kiberbiztonság) és a *software update* (szoftverfrissítés) feladatokra is. A kibervédelmet a járművek teljes életciklusára ki kell terjeszteni.

A reziliencia kérdése mint új kihívás a 2016-os varsói NATO-csúcson¹⁴ merült fel, ahol megfogalmazták az ezzel kapcsolatos feladatokat szövetségi és tagállami szinten. A kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény (CER¹⁵), a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (NIS 2¹⁶), valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló módosított 2021. évi XCIII. törvény¹⁷ megkövetelik a vállalatok biztonsági és védelmi rendszereinek felülvizsgálatát és a szükséges intézkedések bevezetését, valamint alkalmazását.

A 21. században a multinacionális vállalatok felismerték, hogy a biztonságos működés elengedhetetlen feltétele a biztonsági és védelmi intézkedések bevezetése és folyamatos működtetése. Ez viszont megnöveli a vállalatok működési költségeit, amit már nem terhelhetnek tovább a fogyasztókra, mert az már a piaci pozíciójukat veszélyeztetné. Mindez indokolja, hogy miért Montecuccoli gondolataival kezdtem a stratégiai gondolkodás jelentőségét. A jelenkor biztonsági kihívásainak kezelése a vállalatoktól egyre nagyobb anyagi ráfordítást követel meg.

¹¹ HAMELEERS 2025: 90–100.

¹² „Kicsi zöld emberek” jöttek és elfoglalták a félsziget stratégiai pontjait, majd biztosították a területet. Azonosító nélküli fegyveresek, akik egyértelműen orosz katonák voltak, de ezt hivatalosan nem tudták bizonyítani.

¹³ DÉNES-KOVÁCS 2019: 52–84.

¹⁴ NATO 2016.

¹⁵ Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályaon kívül helyezéséről.

¹⁶ Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2555 irányelve az Unió egész területén egyenesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályaon kívül helyezéséről (NIS 2 irányelv).

¹⁷ Továbbiakban Vbő.

A stratégiaalkotás nagyon fontos *vezetői funkció*.¹⁸ Ezért fontos szempont a megfelelő vezető, módszer kiválasztása és alkalmazása, ami jelentősen befolyásolja az új stratégia bevezetését. A magyarországi nagyvállalatok biztonsági vezetői a velük folytatott informális beszélgetések során elmondták, hogy különböző szintű biztonsági szabályokkal, előírásokkal vagy szabályzatrendszerekkel rendelkeznek, de a biztonsági stratégiával mint témakörrel még nem foglalkoztak. A „Biztonsági stratégia és keretei” fejezetben ismertetjük azon feltételeket és követelményeket, amelyek mintaként szolgálhatnak az autóipari vállalatok saját stratégiájának kialakításához.

A tudományos probléma megfogalmazása

Kutatásunk során megállapítottuk, hogy nemzetközi és nemzeti szinten még nincs releváns szakirodalom, amely a két hipotézisben megfogalmazott stratégiai szintű kihívásokra és az összetett biztonsági kérdésekre választ adna. Kutatásunkban bemutattuk azt, hogyan befolyásolja a stratégiai gondolkodás egy vállalkozás biztonságát, és milyen adminisztratív és technikai intézkedésekkel garantálható az üzletmenet folytonossága és az új jogszabályoknak való megfelelés.

Kutatási hipotézisek

Kutatómunkánkban alapvetően két hipotézisben fogalmazhatjuk meg a felmerült kihívásokat.

- Biztonsági stratégiában szükséges rögzíteni azokat az iránymutatásokat, amelyek alkalmazásával a vállalkozások meg tudnak felelni napjaink biztonsági kihívásainak, illetve az új jogszabályi kereteknek.
- A költségek – köztük a védelmi költségek – csökkentése alapvető elvárás a jelen gazdasági környezetben. Ezért szükséges a biztonsági koncepciók újragondolása, ami magába foglalja a szervezeti keretek optimalizálását, valamint a biztonsági rendszerek és a beavatkozó erők létszámának felülvizsgálatát.

Kutatási módszerek

A tanulmányunkban a már közzétett tudományos eredményekre hivatkozva (alkalmazott kutatás) dolgoztuk ki azokat a szabályokat és módszereket, amelyek a gyakorlatban már beváltak. A különböző biztonsági intézkedéseket interjúk és a kvantitatív statisztikai módszerek szabályai alapján vizsgáltuk. Ezen folyamatok és módszerek alkalmazásával fogalmaztuk meg hipotéziseinket, és ezeket elemeztük és hasonlítottuk össze más vállalatok biztonsági rendszereivel. A vállalatok biztonsági vezetői csak anonim módon nyilatkoztak.

¹⁸ TURI-RESPERGER-TÚRI 2012: 8.

Biztonsági stratégia és keretei

A biztonság fogalmát átfogóan kell értelmezni, mivel a biztonsági környezet is folyamatosan változik. Ma a globális kihívások, fenyegetések, veszélyek és kockázatok több szinten jelentkeznek, egyének, közösségek, államok és régiók szintjén.

A biztonsági stratégia kidolgozásánál figyelembe kell venni a Magyarország Nemzeti Biztonsági Stratégiájáról szóló kormányhatározatot.¹⁹ A biztonság – vagy annak hiánya – közvetlen hatással van a vállalat teljes termelésére és működésére. Az összes üzleti egységre kiterjedő és átfogó biztonsági stratégia hiánya hatékonysági problémákat és erőforrás-pazarlást okozhat, ami sebezhetővé teszi a vállalatot a külső kihívásokkal és a belső fenyegetésekkel szemben. A vállalatot fenyegető veszélyek változó jellege miatt a vállalatbiztonság évente felülvizsgálja a biztonsági stratégiát. Erre azért kerül sor, hogy a terveket és tevékenységeket úgy igazítsák ki, hogy azok tükrözzék az új információkat és tanulságokat. A vállalatbiztonság jövőképe, küldetése és célja a stratégia hosszú távú elemeit alkotják. A vállalat felső vezetésének létre kell hoznia és meg kell bíznia egy vállalatbiztonsági tanácsadó csoportot (VTCS),²⁰ hogy tervezze meg, koordinálja és rangsorolja a vállalat biztonságával és védelmével kapcsolatos döntéseket, valamint hozzon létre és felügyelje a biztonsági szintet emelő projekteket, amelyek jelentősen csökkentik a vállalat biztonsággal kapcsolatos költségeit. A stratégia végrehajtása során új célkitűzéseket és kezdeményezéseket határoznak meg. A dokumentumban foglalt célkitűzések és kezdeményezések a vállalat általános stratégiájának egyik kiindulópontját képezik.

Ezen túlmenően a stratégia eredményeként szükség lehet a jelenlegi vállalati politikák és ágazati stratégiák megváltoztatására, és ez fordítva is igaz. Az új vállalati politikák megkövetelik a stratégiák finomítását és összehangolását. A vállalatbiztonság egyik fontos feladata, hogy évente vagy szükség esetén felülvizsgálja és módosítsa a stratégiát. A biztonsági stratégiát a vállalat felső vezetése hagyja jóvá.

Biztonsági vízió

A vízió a biztonság kívánt végállapotának megfogalmazása. A jövőkép kihívást jelent a vállalat számára, és minden üzleti egység minden szintjét egyetlen átfogó eredményre összpontosítja, amely a biztonságos működés és zavartalan üzletmenet biztosítása. Ez a kockázatalapú biztonsági és védelmi intézkedések kidolgozását és megvalósítását jelenti a vállalatnál, figyelembe véve azokat a kihívásokat, fenyegetéseket és biztonsági sebezhetőségeket, amelyek a vállalat működését befolyásolják.

A jövőképeknek több fontos összetevője van:

- a stratégiát alakító fenyegetési és kockázati környezet rendkívül dinamikus, és folyamatosan új fenyegetések jelennek meg;

¹⁹ 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

²⁰ Mátrixszervezet, tagjai olyan vezető beosztású személyek, akik olyan szervezeti egységet (osztályt) vezetnek, amely „biztonsági” funkcióval is rendelkezik (pl. egészségmenedzsment, rizikómenedzsment, compliance, munkavédelem, környezetvédelem, IT-biztonság stb.).

- a jövőkép a kockázatértékelés során beazonosított fenyegetések és sebezhetőségek kezelésén alapul;
- a kihívások, fenyegetések és biztonsági rések csökkentése;
- a rendelkezésre álló eszközök²¹ alkalmazása a vállalaton belül.

Küldetés

A küldetés egyszerű magyarázat arra, hogy mit csinál a vállalatbiztonság. A küldetés magában foglalja a vállalatbiztonság tevékenységét, függetlenül attól, hogy melyik szint²² hajtja végre.

A vállalatbiztonság partnerség és együttműködés révén integrálja és folyamatosan javítja a különböző kompetenciák²³ biztonsági szintjét tanácsadással, koordinációval és ellenőrzésekkel. A küldetés nem foglalja magában a kompetenciaterületek felügyeletét, az alapvető biztonsági funkciók adminisztrációját vagy a fenti küldetésben kifejezetten nem tükröződő egyéb tevékenységek teljesítményének irányítását. A vállalatbiztonság célja a Biztonsági stratégiában megfogalmazott követelmények megvalósítása, a feladatok azonosítása és azon konkrét intézkedések végrehajtása, amelyek javítják a vállalatbiztonság alaprendeltetéséből adódó funkcióit.

Fő célok

A biztonsági stratégia célja, hogy az értékek és érdekek figyelembevételével, valamint a biztonsági környezet elemzésével meghatározza a vállalat biztonsági és védelmi céljait, feladatait és eszközeit, amelyek révén a vállalat garantálja az emberek életét és egészségét, valamint a vállalat biztonságos működését egy globalizált világban.

A vállalat vezetése két átfogó célt tűz ki a vállalat számára:

- közös biztonsági szabályok és rendszerek,
- védelmi költségek optimális meghatározása.

Közös biztonsági szabályok és rendszerek:

- szabványosítják a biztonsági funkciók szinergikus végrehajtását a működés javítása érdekében;
- ezeknek a funkcióknak a szabványosítása növeli a folyamatok hatékonyságát, és egyre zökkenőmentesebbé teszi a tevékenységek integrációját és szinkronizálását a vállalat üzleti egységei között.

Biztonsági funkciói fejlesztése érdekében a vállalatnak nagy hangsúlyt kell fektetnie küldetésére, jövőképre és céljaira. A vállalatbiztonsági tanácsadó csoport felelőssége a specifikus feladatok meghatározása, amelyek irányíthatják a napi tevékenységet. Minden ilyen feladat maximum 10 éves időtartamra fogalmaz meg célkitűzéseket,

²¹ Az eszközök közé tartoznak az emberek, rendszerek, berendezések, létesítmények és információk.

²² Munkatárs, vezető, szervezeti egység, üzleti egység.

²³ Biztonsági helyzetelemzés, információvédelem, *know-how* védelem, prototípus-védelem, utazásbiztonság, objektumvédelem, tűzvédelem, iparbiztonság, katasztrófavédelem, munkabiztonság, környezetvédelem, egészségmenedzsment stb.

amelyek célja, hogy mérhető kiindulási alapot biztosítsanak az üzleti egységek számára, és ez alapján a fejlesztések hatékonysága mérhetővé válik. Ahogy a biztonsági funkciók és feladatok végrehajtása javul, és a fejlesztések megvalósulnak, a vállalatbiztonsági tanácsadó csoport felülvizsgálja a vállalat biztonsági helyzetét a célokhoz képest, és szükség szerint módosítja a korábban meghatározott mérföldköveket. Az egységes szabály- és biztonságtechnikai rendszerek alkalmazásával a különböző üzleti egységek biztonsági személyzeti létszáma csökkenthető.

A védelmi költségek közgazdasági elmélete és gyakorlata

A vállalatok biztonsági kérdéseivel foglalkozó menedzsment tagjainak és munkatársainak folyamatosan figyelemmel kell kísérniük a saját szakterületükön bekövetkezett változásokat. Ennek megfelelően új eljárásokat és módszereket kell kidolgozni és alkalmazni annak érdekében, hogy a vállalat felső vezetése időszerű és megfelelő információk birtokában tudja meghozni döntéseit.

Alapvetően azt kell mérlegelni, milyen költségeket kíván a vállalat ebben a témakörben *cash flow*²⁴ szinten internalizálni. Nyilvánvalóan felmerül az a kérdés, hogy egy konkrét kiadásnak van-e vállalatbiztonsági dimenziója, vagy nincs. Például, ha egy nagy kiterjedésű telephellyel rendelkező vállalat a telephelyen egy új utat épít vagy egy meglévőt kijavít, akkor ez például a beavatkozó egységek²⁵ elérési útvonalának optimalizálása révén védelmi költségnek minősül-e, avagy inkább a telephelyen belüli árumozgatás támogatása miatt logisztikai kiadás. Hasonló kérdés számos esetben felmerülhet, alapvető fontosságú tehát ezen kérdések gondos mérlegelése és a különböző költséghelyek, erőforrások és kivitelezések megfelelő csoportosítása, illetve hozzárendelése. A kellő gondossággal kimutatott védelmi költségek esetén a következő kérdés, hogy milyen védelmi dimenzióban szükséges a vállalatnak gondolkodnia ahhoz, hogy jól hasznosítható keretek között történjen az idevonatkozó elemzés.

A vállalat több tényezőhöz kötheti az általa szükségesnek ítélt védelmi képességeket, és ennek megfelelően biztosíthat ezek eléréséhez erőforrásokat. Ez a csoportosítás két dimenzióban összegezhető. Egyfelől meg kell határozni, hogy pontosan milyen képességeket igényel a vállalat, és utána meg kell határozni, hogy minden egyes képesség elfogadható szintű eléréséhez milyen időtávon és milyen erőforrások szükségesek. (Az időtáv már csak likviditási szempontokból is lényeges.) Ez a csoportosítás természetesen a megfelelő szintű, azaz igazgatóság általi jóváhagyást követően folyamatos nyomon követést igényel annak érdekében, hogy pontosan követhetők legyenek azok a lehetséges hatások, amelyek a vállalatot érik, illetve érhetik, valamint hasznosíthatók legyenek a vállalaton belüli szinergiahatások. A vállalatot érő hatások csoportosítása és elemzése annál bonyolultabb feladat, és annál magasabb szintű elemzőcsapatot igényel, minél nagyobb kiterjedésben dolgozik a vállalat. Könnyű belátni, hogy a világméretben tevékenykedő nagyvállalat világméretű veszélyekkel kell hogy szembenézzen, vagy legalábbis az egész világon szóba jöhető veszélyek érinthetik

²⁴ Pénzügyi kimutatás, amely összefoglalja a készpénz és készpénzhez kapcsolódó eszközök mozgását.

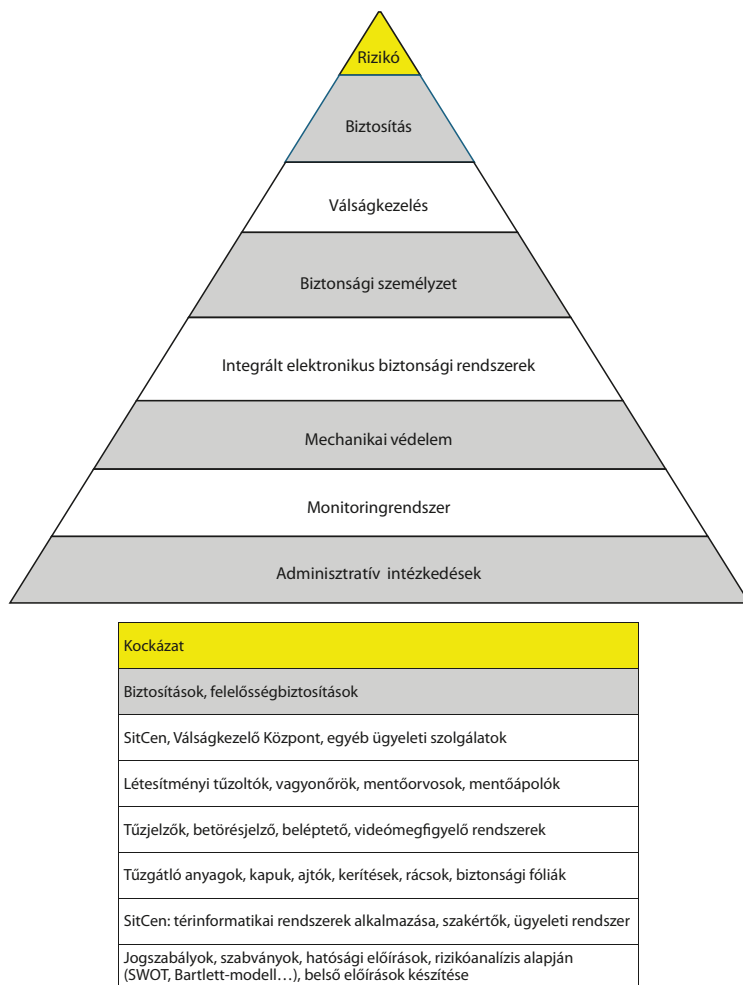
²⁵ Létesítményi tűzoltóság, mentőszolgálat, járőrszolgálat.

tevékenységét. Ugyanakkor minél több ilyen veszélynek, illetve fenyegetettségnek kitett a vállalat, annál nagyobb a valószínűsége annak, hogy valamely telephelyén már merült fel olyan igény, illetve intézkedés, amely megkönnyíti más telephelyeken is a hasonló fenyegetettségekre való reagálást. Ezen tényezők statikus vizsgálata természetesen nem elégséges, azok folyamatos és dinamikus vizsgálatot igényelnek.²⁶

A következő kérdés, hogy milyen időtávra próbál meg az elemzőcsapat előre tekinteni. Különböző és nagyon gondosan összeállított szempontok alapján kell meghatározni az elemzés célzott időtávját. Ennek során értelemszerűen nemcsak gazdasági, hanem politikai tényezőket is célszerű elemezni, amelyek különböző földrészek különböző országaiban, különböző telephelyeket közvetlenül érinthetnek. Ugyanilyen fontos kérdés lehet a lehetséges intézkedéseket, illetve felhasznált berendezéseket befolyásoló jogszabályi környezet változásának kérdése. Voltaképpen a kérdés úgy tehető fel összegzőképpen: a világ mely táján, mely hatások alapján létező, illetve várhatóan kialakuló, mely fenyegetésekkel szemben, milyen védelmi képességek alkalmazását, illetve kifejlesztését látja szükségesnek a nagyvállalat. Figyelembe kell venni ehhez természetesen saját termelési ciklusait is, valamint portfóliója folyamatos módosulását, ami szintén befolyásolhatja a biztonsági igényeket (lásd többcélú felhasználási termékek). Ha sikerült összeállítani a fenti igényeket, akkor nagyon gondosan össze kell állítani az ezek lefedéséhez szükséges költségstruktúrákat is. Amennyiben ez sikerült, úgy el kell fogadtatni a vállalat vezetésével az ehhez szükséges költségvetést. Adott esetben a költségeket persze csökkentheti a különböző együttműködési lehetőségek köre, de végső soron a kérdés az, hogyha lebontjuk a költségeket, akkor egy dolgozó biztonságos jelenlétének költségét kell meghatározni, egy termék biztonságos előállításához a nagyvállalat összes egyéb funkciójának biztonságos megvalósítása mellett. Ez természetesen az egyes tényező szintjére lebontva éppoly nehéz feladat, mint amikor a kérdés úgy merül fel, hány reklámforint, hány eladott terméket eredményez – amivel kapcsolatban óhatatlanul fel kell idézni azt a megközelítést, miszerint a reklámköltségek fele mindig felesleges, ugyanakkor aligha lehetséges meghatározni, hogy melyik fele. Voltaképpen egyfajta diszkontált nettó jelenérték-számítást célszerű elvégezni, ily módon szembe állítva egymással a biztonságot és a munkatársak számára biztonságos körülmények között zajló termelést. Innentől kezdve voltaképpen a két tervező-elemző csapatnak kell dinamikus kölcsönhatásban működnie: hogyan alakulnak a kölcsönösen meghatározott súlypontok eredőjeként meghatározott időtávok vonatkozásában a biztonságos körülmények által előidézett működésbeli, illetve termelékenységi előnyök egyfelől, illetve a kellő gondossággal és a mindenkori várható veszélyek elemzése kapcsán meghatározott képességek finanszírozását szolgáló költségek másfelől. Felmerül a kérdés, mi az, amit a vállalat elfogadhatónak tart, mi az, amit szükségesnek vél, mi az, amire már csak presztízsokból is szüksége van, hogyan változik mindez napról napra, és a diszkontált nettó jelenértéken számított költségek, illetve forgalomnövekmények aránya milyen várható pontosság mellett, hogyan viszonyul egymáshoz.

²⁶ „Tényezők statikus vizsgálata” a már rendelkezésre álló adatok (jogszabályok, bekövetkezett események és statisztikák) elemzése. A „dinamikus vizsgálatok” egy konkrét esemény elemzését jelenti, amelyet a SitCen (lásd Security and Situation Centre fejezet) hajt végre. Ezen információk alapján van lehetőség a biztonsági előírások felülvizsgálatára.

Védelmi rendszer kiépítésénél és üzemeltetése során figyelembe kell venni a biztonsági rendszer elemeinek fontossági sorrendjét. Az elemek egymásra épülnek, és kiegészítik egymást. Az *integrált biztonsági és védelmi koncepció*²⁷ tartalmazza az összes elemet.



1. ábra: Integrált biztonsági és védelmi koncepció

Forrás: a szerzők szerkesztése PATAKI 2019a alapján

Ebben határozzák meg a különböző szakterületek és üzleti egységek feladatát és kötelezettségeit, valamint az alkalmazott biztonsági rendszerek teljes körű integrációját.²⁸

²⁷ PATAKI 2021: 151–152.

²⁸ PATAKI–SULÁNYI 2011.

- a vállalatbiztonságra fordított erőforrások és befektetések megtérülésének bizonyítása;
- értékalapú irányítási rendszert alkalmazunk, amelynek relatív mutatója a befektetés megtérülése (roi);²⁹
- érték-hozzájárulás és értékmutatók alkalmazása.³⁰

A biztonsági költségek üzleti titkoknak minősülnek. Így nehéz megfelelő adatok hiányában pontos adatokat publikálni, de informális beszélgetések alapján kijelenthetjük, hogy Magyarországon ma a vállalatok döntő többségénél ez pontosan ellentétes a szakmailag elvárt arányokkal. Jelentős projekteket kell indítani a vállalatoknál, hogy a szakmailag elfogadott optimális költségeloszlás valósuljon meg. Az új jogszabályok (NIS 2 és CER) és az ISO 27000-es sorozatok „rákényszerítik” az érintett vállalatokat, hogy a törvényi elvárásoknak megfeleljenek úgy, hogy a működési költségeik se nőjenek. Ezt csak az integrált biztonsági koncepcióval tudják megvalósítani. Ezen belül is az „Adminisztratív intézkedések”, „Monitoring” és „Biztonságtechnikai rendszerek” elemek erősítésével, annak érdekében, hogy a „beavatkozó erők” létszáma csökkenthető legyen. Így a biztonsági költségek is jelentősen csökkenthetők.

A koncepció „Biztosítás” elemének szerepét is át kell gondolni, mert jelentős költségeket jelent. Az utóbbi években a biztosítási költségek többszörösükre emelkedtek.³¹ A tapasztalatok alapján csak a közvetlen károk térülnek meg teljesen, a közvetett károk összegét a biztosítók már nem tudják teljes egészében megtéríteni.

Meg kell gondolni, hogy a biztosításokat úgy kössék meg a cégek, hogy a közvetlen károkat teljes egészében fizesse ki a biztosító, a közvetett károkat nem fogják tudni, mert ha történik egy olyan esemény, amely több multinacionális vállalatot érint, akkor több cég is benyújtja a számláit, így a biztosítók képtelenek kifizetni a teljes összegeket.

A vállalatbiztonság feladata egy sor eredményorientált intézkedés és kapcsolódó mérőszám³² kidolgozása kell hogy legyen, amelyek:

- segítik a felső vezetést a biztonsággal kapcsolatos kockázatok megértésében és a kockázattűrési paramétereinek kialakításában;
- biztosítják, hogy a pontok hatékonyan kapcsolódjanak egymáshoz a kockázati kitettség megbízható képe érdekében;
- nyomon követési ajánlásokat és intézkedéseket tesznek lehetővé;
- lehetővé teszik a kockázatsökkentési tevékenységek eredményeinek nyomon követését; valamint
- keretet biztosítanak a biztonság értékének értékeléséhez mint az üzleti stratégia központi eleméhez egy egyre kockázatosabb világban.

²⁹ *Return on Investment* – beruházások megtérülése.

³⁰ NEMESSÁLYI 2005.

³¹ European Insurance and Occupational Pensions Authority 2024.

³² Teljesítménymutató (*performance indicator*, PI) a kitűzött cél elért eredményét objektíven, számokkal írja le. Ez a tömörített információ lehetővé teszi a terv/tényértékek összehasonlítását. Ezt az adott vállalat biztonsági stratégiájából kell levezetni, kidolgozni és követni. Ezek alapul szolgálnak az üzleti és szervezeti egységek céljainak meghatározásához. Minden biztonsággal kapcsolatos teljesítménymutatót az adott vállalat felső vezetése hagyja jóvá, de a vállalatbiztonság készíti el.

A munkaerő technológiával való felváltása

A nagyvállalati szegmens valószínűleg gyors ütemben fog növekedni a globális fizikai biztonsági piacon. Az üzleti egységeket olyan tényezők vezérlik, mint az új EU-irányelvek bevezetése, valamint a megnövekedett védelmi infrastruktúra, az érzékeny információk védelme és a megnövekedett befektetési költségek.

A költséghatékonyság egyik fő ösztönzője az új technológiák alkalmazása tekintetében az, hogy a biztosítási és védelmi feladatok elvégzéséhez szükséges személyzet létszámának csökkentésével mérsékelhetik a személyzeti költségeket. A hatékonyság ugyanakkor javítható: kamerák vagy drónok figyelhetik a nehezen vagy költségesen hozzáférhető területeket. A telefonok, az AI³³-alapú videómegfigyelés vagy más érzékelők által gyűjtött és a mesterséges intelligencia által feldolgozott adatok képesek azonosítani és felismerni azokat a mintákat, amelyekre az emberek nem képesek. A technológia a biztonsági alkalmazottak biztonságérzetét is javíthatja, mivel kevesebb kockázatnak teszi ki őket azáltal, hogy lehetővé teszi azok távoli értékelését és javítja a munkahelyi kommunikációt. Jó példa erre a CCTV és a drónok közös használata nagy területek megfigyelésére vagy az incidens bejelentését követő helyzet gyors felmérésére. A fejlődő technológiák és a változó biztonsági igények miatt a szervezetek és az egyének folyamatosan értékelik eszközeik védelmének legjobb módjait. Az egyes biztonsági megoldások árnyalatainak megismerése során szem előtt kell tartani annak fontosságát, hogy a választást az egyedi biztonsági igényekhez és célokhoz igazítsák.³⁴

Az objektumok/épületek az elmúlt években folyamatosan fejlődtek, és az „egyszerű” riasztástól eljutottunk a mesterséges intelligencia alkalmazásáig. Az integrált biztonsági rendszerek alkalmazása költséghatékonyabb, mert egy biztonsági rendszer folyamatosan és stabilan működik – a megfelelő karbantartás mellett –, és ezzel a biztonsági személyzet létszáma csökkenthető. Viszont a rendszereknek is vannak korlátai, ezért fontos az egyensúly megteremtése a technológia és az ember között. Egy tökéletesen kiépített és működtetett integrált biztonsági rendszer nem tud úgy gondolkodni, mint egy ember. Egy rendszer csak azokat az eseményeket tudja detektálni és kezelni, amelyekre programozták, ha ettől eltérő esetet derít fel, akkor „összezavarodhat”, és riasztást generál, ha nincs is valós veszély, illetve figyelmen kívül hagyja az alattomos fenyegetéseket, amelyeket csak egy ember tud észlelni. Ha az emberek egy biztonsági őr látnak, nagyobb biztonságban érzik magukat. A biztonsági személyzet sokkal többet tesz annál, mint hogy csak figyel a veszélyre. Azért is ott vannak, hogy segítsenek a látogatóknak, útbaigazítást vagy segítséget nyújtsanak, amire egy biztonsági rendszer nem képes. Ezt az integrált biztonsági rendszerek nem tudják garantálni. Az emberi tényező előnye, hogy képes értelmezni az összetett és bonyolult helyzeteket, döntéseket hozni, és szükség esetén azonnali beavatkozást végrehajtani.³⁵

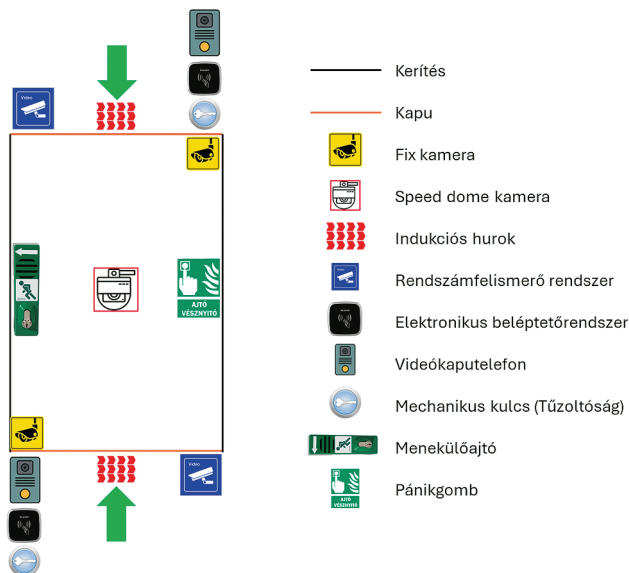
³³ *Artificial intelligence* – mesterséges intelligencia.

³⁴ HUSSEINI 2019.

³⁵ TÓTH 2018: 35–39.

Befektetésarányos megtérülés számítása

A járműforgalom ellenőrzésénél fontos szempont a „négy szem elv”,³⁶ vagyis a gépjárművek ellenőrzését két vagyonnőrnek kell végrehajtania. Ezt a feladatot automatizálhatjuk egy automata zsilipkapurendszer kiépítésével. Ezzel az egyszeri befektetéssel az élőerős őrzés kiváltható. Ha a vállalat már rendelkezik videómegfigyelő rendszerrel, illetve rendszámfelismerő rendszerrel, valamint elektronikus beléptetőrendszerrel, akkor csak a meglévő biztonságtechnikai rendszereink bővítéséről beszélünk. A zsilipkapurendszer létesítésénél a következő szempontokat kell figyelembe venni:



2. ábra: Automata zsilipkapu blokkvázlata

Forrás: a szerzők szerkesztése

Biztonságtechnikai rendszerek és felszerelések, valamint minimumkövetelmények:

- minimális kerítés/kapu magasság 2 m;
- vészhelyzetek kezeléséhez szükséges a mechanikus kulcs telepítése, párhuzamos zárással (tűzoltóság);
- „Tűzoltókapu” felirat szükséges, Megállni tilos tábla (KRESZ szerint);
- közlekedési lámpák;
- infravörös fotocellák és elektromos biztonsági érintkezőléc;
- vészajtó vagy biztonsági kézi vészkioldó;
- beléptetőrendszer; videómegfigyelés (fix, dóm és rendszámfelismerő kamera);
- videókaputelefon (segélyhívás opció);
- biztonsági központ: a vészhelyzetek kezelése és a rendszer felügyelete.

³⁶ A „négy szem elve” olyan ellenőrzési módszer, amelynek alkalmazásával egy adott feladatot, egy feladat/esemény szabályszerűségét két, egymástól függetlenül eljáró személy teljeskörűen vizsgál.



3. ábra: Automata zsiliprendszer járműforgalom számára

Forrás: a szerzők szerkesztése

A meglévő biztonságtechnikai rendszerek alkalmazásával építünk ki egy, a nap 24 órájában működő kaput, amely egysávos és kétirányú forgalmat biztosít. Ha egy rendelkező kaput telepítünk, a ROI-érték meghatározása a következő: ha egy vagyonőr óradíját 4000 forintban határozzuk meg, akkor két fő vagyonőr éves költsége 70 080 000 forint. Az automata zsilipkapurendszer összköltsége a beérkezett árajánlatok alapján 66 800 000 forint. Tehát az őrzés költségét elosztjuk a befektetés összköltségével, majd megszorozzuk 100-zal, és megkapjuk a befektetés ROI-mutatóját, így 105,98%-os ROI-val számolhatunk, vagyis jövedelmező lesz a befektetés már az első évben. A későbbi időszakban költségként már csak a karbantartási és javítási költségekkel kell számolnunk.

Gördülő tervezés

A gördülő tervezés³⁷ alkalmazásával a stratégia bevezetésének alapkövét jelenti a *pénzügyi mutatók* transzparensse tétele.

Az első években fix biztonsági költséggel kell számolnunk, amely tartalmazza a humán, a karbantartás és első alkalommal a beruházás költségeit. Az új elemként megjelenő beruházási költségeket belső átcsoportosítással teremthetjük meg, de ez megköveteli – egyidejűleg – a humán költségek csökkentését, amit az egységes adminisztratív intézkedések bevezetése tesz lehetővé. A stratégiában meghatározott

³⁷ *Rolling wave planning*, bizonyos elemeit alkalmazva a hosszú távú terveket a legmagasabb szinten határozzák meg. Ez folyamatos célkövetést igényel, és ezzel megvalósul a projekt kontrollálingyomata is. A stratégiai tervezés pénzügyi céljait, amikor még kevesebb információ áll rendelkezésre, a munkacsomagokat csak az ismert szintig bontják. Amint több ismeret válik tudottá a közeljövő eseményeiről, a munkacsomagokat tevékenységekre bontják.

időszakban el kell érni a kívánt 50-50%-os arányt, és így a jövőben már három költségnemmel kell számolni:

- humán,
- karbantartás,
- beruházás.

A tervezés során a létszám optimalizált legyen és ne a fűnyíró elvet alkalmazzuk. Az első lépés a már meglévő folyamatok felülvizsgálata és a nem működő vagy felesleges folyamatok megszüntetése. Így a bürokrácia csökkentésével más költségeket is csökkenthetünk, és a maradó alkalmazottak munkavégzése is hatékonyabbá válik. A létszám-optimalizálás során előállhat olyan helyzet, hogy egy új szervezeti egységet (osztályt) kell megalakítani. Ez első hallásra antagonisztikus kijelentésnek tűnhet, de ha megvizsgáljuk az így létrehozandó új szervezeti kereteket, akkor bebizonyosodik, hogy az új szervezeti egységgel a biztonsági szervezet összlétszáma csökken. Természetesen a különböző kompetenciaterületeknek továbbra is működnie kell, de ha az azt végző alkalmazottat leépítettük, akkor meglévő munkatársaknak kell továbbképzést szervezni, hogy *multitaskingban*³⁸ képesek legyenek további kompetenciaterületen érvényesülni.

A régi és az új biztonságtechnikai és IT-biztonsági rendszereknek meg kell felelni a CER és NIS 2 jogszabályokban megfogalmazott elvárásoknak. A már meglévő biztonságtechnikai rendszereket az új biztonsági kihívásokhoz kell igazítani. Kiemelt feladat, hogy az új rendszerek kiválasztásánál figyelembe kell venni a kompatibilitást a már meglévő rendszerekkel, mert a megfelelő kommunikáció nélkül az integrált biztonsági koncepció működésképtelen lesz. Automatizáljunk, szüntessük meg és/vagy szervezzük ki a felesleges folyamatokat!

A stábfunkcióval rendelkező személyi állomány³⁹ jelentősen csökkenthető, ha a központban szolgáltatást teljesítő alkalmazottak magasabb szintű szakmai végzettséggel rendelkeznek, és minden kompetenciaterületen képesek döntéseket hozni.⁴⁰

Security and Situation Centre (SitCen)

A SitCen⁴¹ központi irányító egységként szolgál a különböző beavatkozó egységekkel együtt. A SitCen folyamatosan felügyeli a vállalat biztonsági helyzetét, és az elvárt kockázati szinten tartja azt. A SitCen a vállalatbiztonság szervezetének része és két funkcióval rendelkezik.

³⁸ *Multitasking*: egyszerre több feladatot képes elvégezni a munkatárs.

³⁹ Saját mérnöki és/vagy adminisztratív munkatársak.

⁴⁰ Biztonságtechnikai mérnök (Tűzvédelem/Vagyonvédelem/Munkavédelem) + Környezetvédelmi technikus – OKJ-tanfolyamok.

⁴¹ PATAKI 2019a.

Biztonságtechnikai és IT-biztonsági rendszerek felügyelete és a beavatkozó erők irányítása

Felügyeli, feldolgozza, kiértékeli és dokumentálja a vállalat területén üzemeltetett biztonsági rendszerek jelzéseit, amelyekre a megfelelő intézkedéseket kiadja. Irányítja a beavatkozó egységek⁴² munkáját, koordinálja és támogatja egy adott esemény felszámolása során. Intézkedik a biztonsági rendszerekkel kapcsolatos hibák kijavításáról.⁴³

A SitCen-ben alkalmazott biztonságtechnikai rendszerekben sokféle hardver és szoftver üzemel. Ezeknek képeseknek kell lenni arra, hogy önállóan is működjenek, illetve egy integrált rendszerben legyenek felügyelve. Az egymásra épülésükből kialakított rendszer az integrált felügyeleti rendszer. Feladatai a jelzést adó alközpontok jelzéseinek vétele, értelmezése, megjelenítése, mentése (naplózás).⁴⁴ A lehetőség szerinti magas integráció lehetővé teszi a különféle releváns telepített biztonsági rendszerek vezérlését is. A megjelenítésnél mindig prioritást kapnak az életvédelmi rendszerek (például tűzjelző). Az egyes riasztási típusokhoz tartozó tevékenységi rend a háttérben jelenik meg. Ez esetben fontos az épületek és helyiségek grafikus megjelenítése (a riasztás helye, oka, a kamerák helyzete, a helyiségek, az ott-tartózkodó személyek létszáma, a veszélyforrások, például tárolt veszélyes anyagok). A kiértékelési terv közvetlen összeköttetésben van a riasztási tervvel, de manuálisan is elérhető.

Helyzetelemző funkció

Információ gyűjtése, információk kezelése, médiafigyelés, elemzés, várható khatások felmérése, szakértők bevonása, döntés-előkészítés, koordináció, kapcsolattartás, szakértők és érintett vezetők informálása. A SitCen időben való tájékoztatása nélkül – vagy hiányában – a válságkezelő szervezetek nem tudják tevékenységüket megkezdeni és a válságot megoldani. A válságkezelés feladatait a SitCen-ből irányítják, amelynek működési alapját az információk gyűjtése, elemzése, értékelése és terjesztése, a döntések meghozatala, a feladatok meghatározása és a végrehajtás eredményeinek értékelése jelenti.

Válságkezelés

Ezen alapvetések szerint a vállalatnak rendelkeznie kell a kor színvonalán álló válságkezelő szervezetekkel és módszerekkel, amelyek a menedzsmentfolyamatok fontos részét képezik.

⁴² Létesítményi tűzoltóság, vagyonvédelmi szolgáltató, mentőszolgálat.

⁴³ Helyzetelemző és Biztonsági Központ – Security and Situation Centre.

⁴⁴ BEREK 2014: 9–11.

DIADAL válságkezelési módszer

A módszert a konfliktuskezelés egyes szakaszainak kezdőbetűi alapján nevezték el DIADAL-nak.⁴⁵

A válságkezelés első lépése mindig a *diagnózis* megállapítása, amely a vállalat SitCen szervezeti egységének feladata. Az első azonnali feladat a kialakult helyzettel kapcsolatos információk gyűjtése, majd végre kell hajtani az elsődleges elemzést. A következő 2–4 órában az időszámvetés a legfontosabb: mit tudunk azonnal cselekedni, valamint az azonnal alkalmazandó rendszabályok, első intézkedések, utasítások, korlátozások bevezetése.

A válságkezelés második lépése a kríziskezelés *irányának* meghatározása. Ez a vállalati válságtáb és a vállalati felső vezetés feladata, és ezt a válság kitörését követő 3–4, maximum 5 órán belül kell megtenniük. Először közösen kell megfogalmazni a stratégiai célokat, beleértve a válságkezelés pozitív céljainak meghatározását (azaz az elérendő eredményeket); a negatív céljaink meghatározását (azaz az elkerülni kívánt eseményeket és következményeket) és az elkerülhetetlen következmények meghatározását. A stratégiai célokat követően meg kell határozni a válságkezelés fókuszát és fontosabb területeit. Az irány meghatározásának utolsó feladatai közé tartozik a médiakapcsolatok felkeresése: előzetes nyilatkozat kiadása, sajtótájékoztató megtartása, valamint egy szóvivő kijelölése a média folyamatos tájékoztatására.

A válságtáb feladata továbbá, hogy a válságot követő 12–24 órán belül kidolgozza a cselekvési lehetőségeket és *alternatívákat*. Ekkor a válságtáb kidolgozza a krízis lefolyásának legjobb, legrosszabb és legvalószínűbb változatait, felvázolja a válság valószínűsíthető irányait, előnyeit és hátrányait, valamint indokolja a feltételezéseket. Ezt követően a SWOT-módszerrel⁴⁶ értékeli a kidolgozott alternatívákat.

A negyedik lépésben arról kell dönteni, hogy a javasolt cselekvési irányok közül melyiket érdemes végrehajtani és részletesen *kidolgozni*. A választás során a döntéshozó a döntési mátrix (normál, súlyozott) alapján hozza meg döntését, figyelembe véve az adott lehetőségek előnyeit és hátrányait, a szükséges időt és a költségeket. A döntést a válság bekövetkezését követő 13–27 órán belül meg kell hozni.

Az ötödik lépés az *alkalmazás*: az érintett szervezeti egységek kidolgozzák és betervezik a kiválasztott cselekvési változat részletes feladattervét.

A válságkezelési folyamat *lezárása* a vállalati felső vezetőség feladata, amely magába foglalja a válságtáb és a beavatkozó erők ellenőrzését a cselekvés teljesítése során, továbbá a válságkezelésben részt vevők tapasztalatainak, benyomásainak és javaslatainak összegyűjtését.

⁴⁵ RESPERGER 2018: 16–20.

⁴⁶ SWOT-elemzés egy stratégiai tervezési eszköz: *strengths* (erősségek), *weaknesses* (gyengeségek), *opportunities* (lehetőségek), *threats* (veszélyek).

Biztonsági kockázatok meghatározása

- A biztonsági kockázatértékelések⁴⁷ átfogó értékelést nyújtanak a vállalatról (GRC).⁴⁸
- A biztonsági kockázatértékelési jelentés azonosítja a megfelelően biztonságos rendszereket és azokat, amelyek nem megfelelően működnek. Ezen rendszereket felül kell vizsgálni, valamint új biztonsági szabályokat és konkrét technikai ajánlásokat kell megfogalmazni.

A jóváhagyott biztosítási és védelmi tervekkel a kidolgozott scenáriók alapján kell a válsághelyzetet kezelni a térinformatikai/biztonsági rendszerek alkalmazásával. Így az előre nem látható események időben felderíthetők, ami lehetővé teszi a válságkezelő szervezetek és a beavatkozó erők előzetes figyelmeztetését és riasztását.

CER, NIS 2 és a módosított Vbő.-nek való megfelelés

A tanulmányunk első részében a globalizáció hatásait már vizsgáltuk, és megállapítottuk, hogy a legnagyobb problémát a törésvonal-konfliktusok okozzák. Ezek az ellentétek államok közötti szembenálláshoz, konfliktusok kialakulásához vezethetnek, amelyek során az államok a negyedik generációs hadviselés⁴⁹ módszereit alkalmazhatják egymással szemben. Ezért egységes fellépésre van szükség a nemzetközi szervezetekkel és intézményekkel közösen a kritikus területeken.⁵⁰

Az IT-technológia gyors fejlődésével a vállalatok egyre komplexebb biztonsági fenyegetésekkel szembesülnek mind a fizikai védelem kompetenciaterületén, mind a virtuális térben. Nagyon sok vállalatnál a fizikai biztonság és az IT-biztonság külön szervezeti egységek kompetenciaterületei, annak ellenére, hogy sok szálon kapcsolódnak egymáshoz. Ezeket egyedül az ISO 27000 szabványsorozatban kezelik egy egészként. A fizikai biztonság és az IT-biztonság közötti határok egyre inkább elmosódnak. Ezért véleményünk szerint a biztonsági stratégiának mindkettővel egyenrangú szinten kell foglalkoznia.

„Az IFSEC Global tanulmánya bizonyítja, hogy 2023-ban az informatikai és biztonsági szakemberek 36%-a tervez befektetni a fizikai biztonság fokozását célzó biztonsági rendszerekbe. Ezen adatok alapján kijelenthetjük, hogy a biztonsági infrastruktúra nagymértékben függ a hálózattól, valamint azt, hogy a »fizikai« és IT-biztonsági szakemberek hagyományos szétválasztása már nem hatékony.”⁵¹

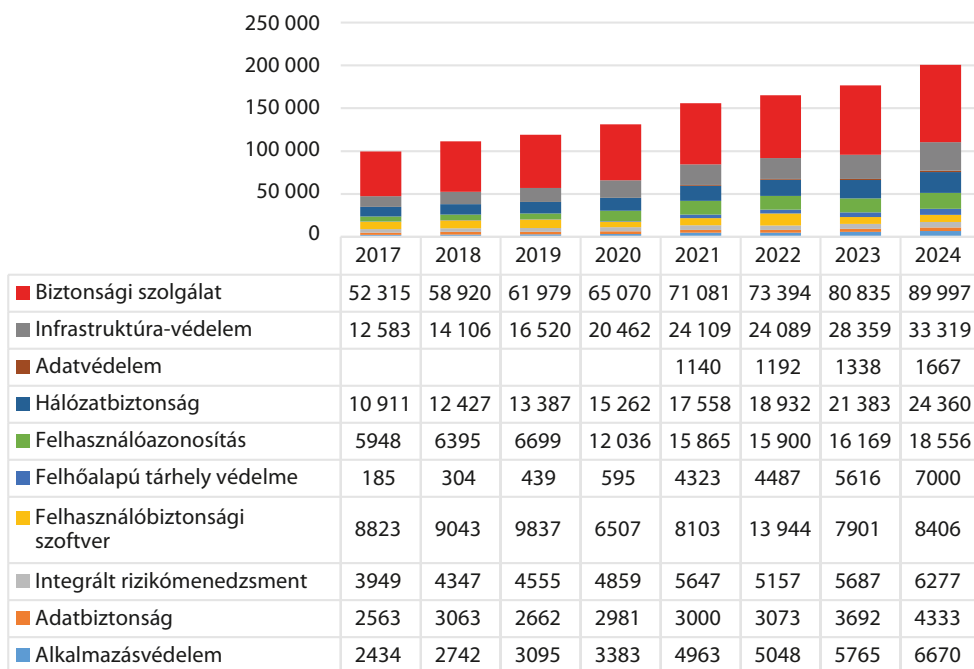
⁴⁷ CER, NIS 2, Vbő. szerinti kockázatok.

⁴⁸ *Governance, risk and compliance*.

⁴⁹ A háborút továbbra is hagyományos és aszimmetrikus katonai eszközökkel vívják meg, kiegészítve irreguláris erőkkel és más nem katonai szereplőkkel és eszközökkel, például hackertámadásokkal, terrortámadásokkal, médiafőlennyel, nyomásgyakorlással üzleti körökre, kiszivárogtatásokkal és álhírekkel.

⁵⁰ PATAKI 2019b.

⁵¹ MOORE 2023.



4. ábra: Információvédelmi költségek 2017–2024

Forrás: a szerzők szerkesztése Statista 2024 alapján

A biztonsági szektor költségeinek meghatározásánál csak az IT-biztonsági költségekről találtunk statisztikai adatokat, amelyek tartalmazzák az *általános* és fizikai biztonság költségeit is. Megfigyelhető, hogy 2017 és 2024 között a biztonsági költségek megduplázódtak. A költségek elemzése során megállapítottuk, hogy a fizikai biztonság költségei 2017-ben a biztonsági költségek 52,4%-át tették ki, ami 2024-re 44,4%-ra csökkent. Ez a biztonsági rendszerek integrálásának és a mesterséges intelligencia alkalmazásának tudható be. Nagyon kevés biztonsági szervezet rendelkezik az összes biztonsággal kapcsolatos kompetenciaterülettel egy szervezeti egységen belül. A jövő a biztonsági kérdések integrált megközelítése, mert a *fizikai biztonság* és az *információbiztonság* összekapcsolódik, a konvergencia a jelenlegi tendencia. Az *integrált biztonsági rendszer* egyre népszerűbb fogalom, azonban még mindig túl kevesen alkalmazzák, és a fogalom ki is zárja a biztonsági kompetenciák számos elemét, amelyek a vállalat védelme szempontjából alapvetők, mint például:

- hatékony, logikus kapcsolat az IT-biztonsági rendszerek és a fizikai biztonságot adó rendszerek között;
- valós kockázatot jelent, ha a biztonsági auditot egy olyan *nem minősített külső szolgáltató*⁵² végzi, aki érzékeny információkhoz vagy folyamatokhoz fér hozzá;
- a biztonsági stratégia, amelyben fontos szerepe van az alkalmazottak és a vezetők biztonságtudatának, nagyobb valószínűséggel csökkenti a bűncselekményeket

⁵² Lásd NIS 2 törvény, TISAX, ISO 2700 sorozat.

és köteleességszegéseket, és így gyorsabb reakció várható el a biztonsági személyzettől;

- az információbiztonsági kockázatok megelőzése kulcsfontosságú a vállalat üzletmenet-folytonosság- és hírnévvesztéssel járó eseményeinek kezelésében;
- a pénzügyi veszteséggel járó események kivizsgálása lehetőséget kínál az ismert sebezhetőségek azonosítására vagy kiküszöbölésére, amelyeket a jövőbeli kockázatok elkerülése érdekében le kell zárni;
- a különböző biztosított kockázatoknak megfelelő megelőző védelemi képességek hozzájárulnak az alacsonyabb biztosítási díjakhoz;
- a beléptető és behatolásjelző, illetve más fizikai biztonsági rendszerek közvetlenül hozzájárulnak a kockázatok korai azonosításához.⁵³

A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 4.) MK rendelet a 2. számú mellékletének 12. pontjában határozza meg a Fizikai és környezeti védelemmel kapcsolatos követelményeket, de a melléklet több ponton is kapcsolódik ehhez, és a vállalatbiztonság több kompetenciaterülete is érintett/együttműködő (például válságkezelés, információvédelem) a következő feladatokban:

- üzletmenet-folytonossági terv kidolgozása;⁵⁴
- biztonsági események kezelése;
- azonosítás és hitelesítés;⁵⁵
- személyek háttérellenőrzése;
- adathordozók védelme;⁵⁶
- karbantartás (TISAX⁵⁷).

A CER, NIS 2 és Vbö. törvényeknek megfelelő biztosítási és védelmi rendszert és tervet a már meglévő biztonsági előírásokra alapozva célszerű kidolgoznia a következő lépésekben:

1. biztonsági kihívások, veszélyek és rizikók azonosítása;
2. érvényben lévő biztonsági előírások felülvizsgálata;
3. új biztonsági szabályok, folyamatok kidolgozása és beillesztése a már meglévő biztonsági rendszerbe.

Ezt azért tartjuk jó megoldásnak, mert a változtatás nem az egész rendszert érinti, hanem annak csak bizonyos elemeit.

⁵³ CAMPBELL 2014: 31–39.

⁵⁴ Válságkezelés, krízismenedzsment, SitCen.

⁵⁵ Többfaktoros hitelesítés és azonosítás (pl. gyári belépőkártya: intelligens kártya és RFID-kódolás).

⁵⁶ A fizikai biztonságon túl, az üzleti utak során betartandó szabályok, *home office*.

⁵⁷ Trusted Information Security Assessment Exchange – német autóipari beszállítók részére kidolgozott IT-biztonsági követelményrendszer.

Összegzés, következtetések

A geopolitikai változások, valamint az új EU tanácsi irányelvek hatálybalépése miatt egy új biztonsági stratégiát szükséges megalkotni, amelyben meghatározzák a nagyvállalat biztonsági vízióit és küldetését, valamint a védelmi célokat. Ezen stratégiát mindig az adott vállalat legmagasabb döntéshozatali szervezete vagy vezetője hagyja jóvá.

Bizonyítottuk, hogy egy multinacionális vállalat biztonsági szabályainak, előírásainak és biztonsági szervezetének kidolgozásakor teljes mértékben figyelembe kell venni az ország nemzetbiztonsági stratégiáját, illetve meghatároztuk a biztonsági stratégia alapvető elemeit. A biztonsági és védelmi rendszerekkel és azok működtetésével kapcsolatban kidolgozott stratégiák olyan alapvető dokumentumok, amelyek meghatározzák a vállalat felső vezetése számára a hosszú távú biztonsági célokat és elvárásokat.

A biztonsági projektek (NIS 2, CER, Vbő.) kölcsönösen függenek egymástól, és ez nagyon fontos szempont a stratégiai tervezésnél, amelyet egy közös projektben lehet eredményesen teljesíteni, illetve a költségeket is így optimalizálhatjuk. Ezen tény meggyőzően bizonyítja, hogy egy szervezeti egységeken átnyúló, a beazonosított kockázatoknak megfelelő kompetenciaterületekkel rendelkező „vállalatbiztonság” szervezet megalakítására van szükség. Napjainkban a megszokott biztonsági modellekkel ezért szükséges egy mátrix szervezeti egységet kialakítani, amelyben a különböző szervezeti egységek (IT-biztonság és vállalatbiztonság) önállósága és felelőssége nemvész el. Ezzel a modellel lehet eredményesen és hatékonyan kezelni a jelen biztonsági kihívásait. Természetesen a jogszabályokban meghatározott biztonsági auditokat a hatóságok vagy az általuk megbízott vállalkozások egymástól függetlenül hajtják végre.

Igazoltuk, hogy a NIS 2 és CER törvények miatt új biztonsági stratégia kidolgozása szükséges, amely figyelembe veszi a jogszabályi keretek változását, a világszerte jelentkező új kihívásokat, veszélyeket és kockázatokat, valamint a vállalatok vezetőségének és a biztonsággal közvetlenül érintett szervezeti egységeknek nyomon kell követniük a saját szakterületükön jelentkező a multinacionális vállalat működését alapvetően befolyásoló tényezőket. Ennek megfelelően új eljárásokat és módszereket kell kidolgozni és alkalmazni, hogy a vállalat felső vezetése megfelelő információk birtokában, kellő időben tudjon döntéseket hozni.

Vizsgálataink alapján igazoltuk, hogy a SitCen meghatározó szerepet tölt be a vállalatok biztonsági helyzetének megítélésében, tervezésében és működtetésében, valamint a kialakult válsághelyzetek kezelésében. Ehhez magas képzettséggel rendelkező alkalmazottakra lesz szükség, akik folyamatos munkarendben képesek lesznek a megfelelő szakemberek, illetve előre definiált mátrixszervezetek alkalmazásával a különböző válsághelyzeteket kezelni. A biztonsági rendszerek az elmúlt években folyamatosan fejlődtek, és az „egyszerű” riasztástól eljutottunk a mesterséges intelligencia használatáig. Az integrált rendszerek alkalmazása költséghatékony, mert egy biztonsági rendszer folyamatosan és stabilan működik – a megfelelő karbantartás mellett –, és ezzel a biztonsági személyzet létszáma csökkenthető.

Elemzéseink és következtetéseink alapján rámutattunk, hogy a NIS 2 és a CER előírásai miatt a legtöbb vállalkozás esetében gondot jelentenek a megfelelés pénzügyi hatásai. Az irányelvek jelentősen kibővítik a szigorú biztonsági és védelmi intézkedések

betartására kötelezett iparágak és vállalkozások körét. Ezért a vállalatoknak erőforrásokat kell elkülöníteni a megfelelőség biztosítása érdekében. A biztonsági költségek növekednek, az előrejelzések szerint a vállalkozásoknak 10-20%-os költségnövekedéssel kell számolniuk.

Felhasznált irodalom

- BEREK Lajos (2014): *Biztonságtechnika*. Budapest: Nemzeti Közszoigálati Egyetem. Online: <https://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf>
- CAMPBELL, George K. (2014): *Measures and Metrics in Corporate Security*. Waltham, USA: Elsevier.
- European Insurance and Occupational Pensions Authority (2024): *European Insurance Overview 2024*. Online: https://nexteuropa-multisites.s3.eu-west-1.amazonaws.com/www.eiopa.europa.eu/assets/insurance-overview-report/European_Insurance_Overview_2024.html
- DÉNES Kálmán – KOVÁCS Zoltán (2019): Létesítmények közműrendszereinek robbantásos cselekmények általi veszélyeztetettsége és védelme. *Hadtudományi Szemle*, 12(Különszám), 82–84. Online: <https://doi.org/10.32563/hsz.2019.1.ksz.5>
- HAMELEERS, Michael (2025): The Visual Nature of Information Warfare: The Construction of Partisan Claims on Truth and Evidence in the Context of Wars in Ukraine and Israel/Palestine. *Journal of Communication*, 75(2), 90 – 100. Online: <https://doi.org/10.1093/joc/jqae045>
- HUNTINGTON, Samuel P. (2006): *A civilizációk összecsapása és a világrend átalakulása*. Budapest: Európa.
- HUSSEINI, Talal (2019): Ai In The Sky: Can Drone Surveillance Technology Replace CCTV? *Army Technology*, 2019. július 10. Online: www.army-technology.com/features/ai-drone-surveillance-cctv/
- MOORE, James (2023): *Editor's Viewpoint: 2023 Technology Trends Ahead for the Physical Security Industry*. Online: www.ifsecglobal.com/physical-security/editors-viewpoint-2023-technology-trends-ahead-for-the-physical-security-industry/
- North Atlantic Treaty Organisation (2016): *Commitment to Enhance Resilience*. Online: www.nato.int/cps/en/natohq/official_texts_133180.htm
- NEMESSÁLYI Zsolt (2005): Jövedelem, jövedelmezőség, versenyképesség a hatékonyság rendszerében. In *A mezőgazdaság tökeszükséglete és hatékonysága: Pfau Ernő professzor 70. születésnapja tiszteletére megrendezett tudományos ülés. 2005. május 26.* Debrecen: Debreceni Egyetem Agrártudományi Centrum, 199–208. Online: <https://real.mtak.hu/6738/1/1190849.pdf>
- PARET, Peter (1986): *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Princeton, New Jersey: Princeton University Press. Online: <https://doi.org/10.1515/9781400835461>
- PATAKI János (2019a): Situation Centre in the Private Sector. *Nemzetbiztonsági Szemle*, 7(3), 18–27. Online: <https://doi.org/10.32561/nsz.2019.3.2>

- PATAKI, János (2019b): NATO in 2030 and What the Future Will Bring „Essential Security, Dynamic Engagement”. *Nemzetbiztonsági Szemle*, 7(4), 61–70. Online: <https://doi.org/10.32561/nsz.2019.4.5>
- PATAKI János (2021): *A terrorizmus mint biztonsági probléma, a kritikus infrastruktúra védelmi szabályainak tükrében*. PhD-disszertáció. Nemzeti Közszerológati Egyetem Hadtudományi Doktori Iskola. Online: <https://doi.org/10.17625/NKE.2021.014>
- PATAKI, János – SULÁNYI, Péter (2011): Lage- und Analysezentrum bei einem internationalen Unternehmen. *Hadmérnök*, 6(3), 161–168. Online: http://hadmernok.hu/2011_3_pataki_sulanyi.pdf
- RESPERGER István (2018): *A válságkezelés és a hibrid hadviselés* [ePub]. Budapest: Dialóg Campus. Online: <https://bit.ly/3NxxVNG>
- Statista (2024): *Information Security Spending Worldwide from 2017 to 2024, by Segment*. Online: www.statista.com/statistics/790834/spending-global-security-technology-and-services-market-by-segment/
- Szun-Ce (2012): *A hadviselés tudománya*. Budapest: Göncöl.
- TÓTH Levente (2018): A komplex objektumvédelem kihívásai napjainkban. *Bolyai Szemle*, 1, 35–39. Online: www.szakmaikamara.hu/files/images/Orszagos/Szakmai_Kollegium/publikaciok/Bolyai_Szemle_2018_01_toth-levente.pdf
- TURI Laura Tamara – RESPERGER István – TURI Viktória (2012): *Stratégiaalkotás, stratégiai módszerek* [ePub]. Közigazgatási Vezetői Akadémia. Online: www.scribd.com/document/577246519/438

Jogi források

- Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről
- Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)
2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról
2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről
2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről
- 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

Szabó Gergő¹ 

A generatív mesterséges intelligencia használata a kibertudatosítási képzésekben, 2. rész²

The Use of Generative Artificial Intelligence in Cyber Awareness Training, Part 2

Absztrakt

A tanulmány célja annak vizsgálata, hogy miként alkalmazható a generatív mesterséges intelligencia (GenMI) a kibertudatosítási képzésekben, különös tekintettel az oktatás személyre szabhatóságára, hatékonyságára és elfogadottságára. A kutatás elméleti része az ADDIE modell mentén tárgyalja a GenMI szerepét az oktatástervezésben, bemutatva annak lehetőségeit a tananyagfejlesztés, személyre szabás és visszacsatolás területén. Részletesen ismerteti a RAG-technológia szerepét is, különösen a tartalmi pontosság és az adatbiztonság aspektusaira fókuszálva. Az empirikus kutatás egy 109 fő részvételével végzett kérdőíves vizsgálatra épül, amelyet a Technology Acceptance Model (TAM) keretrendszere szerint szerkesztettem. A kérdőív többek között phishing szimulációkat, egy generált scénáriót, valamint attitűdkérdéseket tartalmazott.

Kulcsszavak: GenMI, oktatás, kibervédelem, RAG, TAM

This study examines how generative artificial intelligence (hereinafter: GenAI) can be applied in cybersecurity awareness training, with particular emphasis on personalisation, effectiveness, and user acceptance. The theoretical section follows the ADDIE instructional design model and explores the role of GenAI in educational planning, highlighting its potential in content development, adaptive learning, and feedback mechanisms. Special

¹ Nemzeti Közszerológati Egyetem, e-mail: sz.gergo628@gmail.com

² A Kulturális és Innovációs Minisztérium EKÖP-24-2-49 kódszámú egyetemi kutatói ösztöndíj programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

attention is given to Retrieval-Augmented Generation (RAG) technologies, focusing on content accuracy and data protection considerations.

The empirical part of the research is based on a questionnaire survey conducted with 109 participants and designed according to the Technology Acceptance Model (TAM). The questionnaire included phishing simulations, an AI-generated cybersecurity scenario, and attitude-based questions. The aim of the study is to assess how non-expert users perceive and evaluate cybersecurity training materials generated by artificial intelligence, and to identify key factors influencing their acceptance and perceived usefulness.

Keywords: artificial intelligence, cybersecurity, awareness training, phishing

Bevezető

A kutatás első része elméleti és oktatástervezési szempontból közelítette meg a generatív mesterséges intelligencia szerepét a kiberbiztonsági képzésekben. Az elemzés fókuszában a tantervkészítés támogatása állt, különös tekintettel az ADDIE modell és a NIST CPLP keretrendszer egyes fázisaira. Bemutattam, hogy a GenMI képes hatékonyan támogatni az oktatási célú tartalomfejlesztést, ideértve nemcsak a szöveggenerálást, hanem az oktatási célokhoz igazított szcenáriók létrehozását is. Az érthetőség javítása érdekében a kutatási célkitűzéseket, kérdéseket és hipotéziseket a második rész elején mutatom be, ahol az empirikus kutatás részletes bemutatása is megtörténik.

A második részben az első részben felmerülő etikai és megbízhatósági kérdésekre felvetett megoldásként bemutatom a RAG-rendszerek működési elvét, valamint egy kérdőíves felmérés kvantitatív értékelésében bemutatom, hogyan értékelik a felhasználók a mesterséges intelligencia által előállított adathalász-szimulációkat és oktatási szcenáriókat. A kérdőív a Technology Acceptance Model (TAM) elméletére épült, és vizsgálta a tartalom érthetőségét, hasznosságát, a tanulási élményt, a technológia elfogadottságát, a jövőbeli használati szándékot és a válaszadók önértékelt tudásszintjének változását.

Kutatási célkitűzések és kutatási kérdések

A tanulmány célja kettős: egyrészt feltárni az elméleti háttér alapján, hogy a generatív mesterséges intelligencia miként támogathatja a személyre szabott, hatékony kibertudatosítási képzések kialakítását; másrészt empirikus úton vizsgálni, hogy a felhasználók miként viszonyulnak a GenMI által generált oktatási tartalmakhoz.

A kutatás során az alábbi célkitűzések mentén szerveződött az elemzés:

- KC1: A generatív mesterséges intelligenciával létrehozott kiberbiztonsági oktatási tartalmak elfogadottságának vizsgálata a felhasználók körében.
- KC2: A GenMI által generált tananyagok érthetőségének és tanulási élményének értékelése felhasználói visszajelzések alapján.
- KC3: Annak feltárása, hogy tapasztalható-e önértékelésen alapuló tudásszintváltozás egy GenMI-szcenárió elolvasását követően.

- KC4: Azoknak a tényezőknek az azonosítása, amelyeket a válaszadók a mesterségesintelligencia-alapú oktatás bevezetésének legnagyobb kihívásaiként jelölnek meg.
- KC5: Az MI-hez való hozzáállás különbségeinek feltérképezése demográfiai szempontok (például szakterület, életkor, iskolai végzettség) mentén.

A célkitűzésekhez kapcsolódón a tanulmány az alábbi kutatási kérdésekre keresi a választ:

- KK1: Milyen mértékben fogadják el a felhasználók a GenMI által létrehozott oktatási tartalmakat a kiberbiztonsági képzésekben?
- KK2: Hogyan értékeli a felhasználók a GenMI által generált tartalmak érthetőségét és tanulási élményét?
- KK3: Tapasztalható-e tudásszintbeli változás egy GenMI által generált kiberbiztonsági szcenárió elolvasását követően?
- KK4: Milyen tényezőket tartanak a válaszadók a legnagyobb kihívásnak a mesterségesintelligencia-alapú oktatás bevezetésében?
- KK5: Vannak-e különbségek az MI-hez való hozzáállásban a válaszadók szakterülete, életkora vagy iskolai végzettsége szerint?

Hipotézisek

A fenti kutatási kérdésekhez az alábbi hipotézisek tartoznak:

- H1: A válaszadók többsége elfogadja a GenMI által generált kiberbiztonsági oktatási tartalmakat hiteles és hasznos tananyagként.
- H2: A résztvevők a GenMI által generált tananyagot érthetőnek és tanulásra ösztönzőnek találják.
- H3: A GenMI szcenárió elolvasását követően a válaszadók magasabbra értékeli saját képességüket az adathalászat felismerésében.
- H4: A leggyakrabban említett kihívás a GenMI-alapú oktatásban a generált tartalom megbízhatósága és az oktatási rendszerbe vetett bizalom hiánya.
- H5: A GenMI-hez való pozitív hozzáállás szignifikánsan magasabb az informatikai szakterületen dolgozók körében, mint más területeken.

A hipotézisek tesztelése kvantitatív adatfeldolgozással történik, a kérdőíves válaszok statisztikai elemzése alapján. Az egyes hipotézisek alátámasztottságát a harmadik fejezet részletesen bemutatja.

Módszertan

A tanulmány két szinten közelíti meg a kutatási kérdéseket: egyrészt elméleti, másrészt empirikus alapon. Az elméleti rész célja a generatív mesterséges intelligencia oktatásban betöltött szerepének bemutatása, különös tekintettel a személyre szabható, adaptív tanulási folyamatok lehetőségeire a kiberbiztonsági tudatosság fejlesztésében. Ennek érdekében szakirodalmi áttekintést végeztem a releváns nemzetközi és hazai

források alapján, külön figyelmet fordítva a GenMI és a kiberbiztonsági oktatás kapcsolódási pontjaira.

Az empirikus kutatás online kérdőív formájában valósult meg, amelyet a Technológiaelfogadási Modell (Technology Acceptance Model, TAM) mentén építettem fel. A kérdőív célja az volt, hogy valóságghű, generatív MI által készített adathalászeszteken és komplexebb kiberbiztonsági szcenáriókon keresztül vizsgálja a felhasználói élményt, az észlelt hasznosságot, az érthetőséget, valamint a bizalmat és az elfogadottságot. A kitöltés során lehetőség nyílt szöveges válaszadásra is, amely az élmény minőségi értékelését segítette.

A kvantitatív adatok feldolgozása a leíró statisztikákon túl keresztábra-elemzéssel és Khi-négyzet-próbával történt, hogy feltárható legyen, mutatkozik-e szignifikáns különbség a különböző demográfiai csoportok (például nem, szakterület) között az MI-vezérelt oktatás elfogadottságában. Külön vizsgálat készült az IT-területen dolgozó és a nem informatikai területről érkező válaszadók válaszainak összevetésére is.

Információ-visszakereséssel kiegészített szöveggenerálás

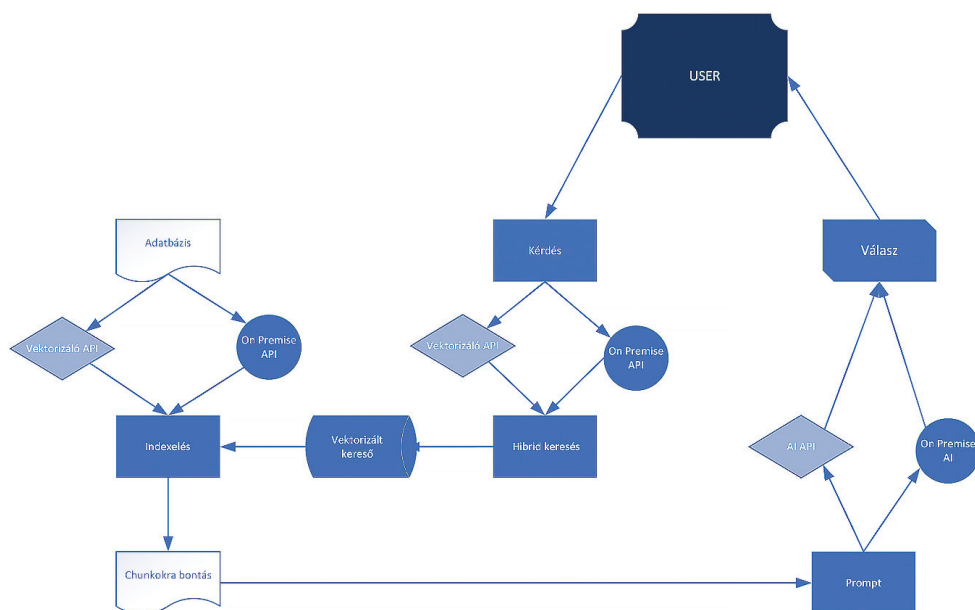
A RAG-rendszerek lényege, hogy a mesterséges intelligencia nem a tanított tudásból dolgozik, hanem valós időben keres információkat egy belső tudásbázisból. A vállalati képzések GenMI segítségével történő támogatásánál választható felhőalapú, szolgáltatott szoftver (*software as a service*, SaaS) vagy házon belüli (*on-premise*) RAG-megoldásrendszer. Különösen a szigorúan szabályozott iparágakban működő vállalatok preferálják, hogy az érzékeny adatokat saját infrastruktúrában tartsák, ahelyett, hogy azokat külső szolgáltatóra bíznák. Bár a legtöbb kész *awareness* tréning platform elsősorban SaaS-formában érhető el, bizonyos szolgáltatók kínálhatnak privát felhő- vagy virtuális *appliance* telepítést nagyvállalati ügyfeleknek egyedi megállapodás keretében.³

Alternatív megközelítés, hogy a vállalat saját maga épít RAG-alapú chatbotot vagy oktatórendszert nyílt forráskódú eszközökkel. A LangChain keretrendszer például lehetővé teszi egyedi, belső tudásbázison nyugvó chatbot kifejlesztését, amely házon belüli környezetben futó NNYM-ekkel működik.⁴ Ilyen *self-hosted* megoldásnál a cég egy nyílt nyelvi modellt, például a Llama 2-t, finomhangolhat saját adatokkal, vagy *retrieval-augmented generation* megközelítést alkalmazhat; az MI valós időben keres ki információkat egy belső tudásbázisból, ahelyett hogy minden vállalati adatot betanítanak a modellre.⁵ Ez a megközelítés hibrid modellként működik, mivel a generatív modell lehet felhőben, használhatja például az OpenAI API-t, de maga az adatkeresés és -tárolás helyben történik. Az 1. ábra szemlélteti a RAG általános működési elvét.

³ TitanHQ 2025.

⁴ HAYDOCK 2024.

⁵ HAYDOCK 2024.



1. ábra: A RAG általános működése

Forrás: NKE ÁNTK Kiberbiztonsági mesterképzés Hírszerzés a kibertérben tantárgy, Vadász Pál egyetemi előadása alapján (2025. március 1.)

A *hybrid* vagy *on-premise* megoldások előnye, hogy a vállalati dokumentumokat, tudásbázist helyben, például egy vektortárban kezelik, míg a generatív modell kizárólag lekérdezés útján fér hozzá az információhoz, szükség esetén. Ezáltal az üzleti titok nem kerül tartósan a modell paramétereire közé, csupán a kérdés megválaszolásának idejére.⁶ Ezzel elkerülhető egy problémás helyzet, mert ha érzékeny adatokkal tanítják be a modellt, később nem garantálható, hogy a betanításra használt adatok nem bukkannak-e fel valakinek a beszélgetésében, ami a GDPR szerint jogellenes adatkezelésnek minősülhet megfelelő törlési mechanizmus hiányában.⁷ Számos vállalat dönt a nyílt forráskódú nagy nyelvi modellek házon belüli alkalmazása mellett, ilyen esetben a modell betanítása és futtatása teljes mértékben az ő környezetükben történik, bár ennek erőforrásigénye jelentős lehet.

A RAG-rendszereknek biztosítaniuk kell az adatlekérdezések naplózását, és azt, hogy szükség esetén pontosan visszakereshető legyen, mely forrás alapján készült a generált válasz. Ez egyrészt a megbízhatóság miatt fontos, például azonosítható legyen, hogy a chatbot mely belső szabályzat melyik pontja alapján javasolt választ, ami nemcsak a megbízhatóságot, hanem az auditálhatóságot is támogatja. Sok megoldás ezért hivatkozásokat vagy forráslinkeket is mellékel az MI által generált válaszokhoz. Technikai szempontból elengedhetetlen, hogy a rendszer képes legyen az adatok osztályozására, érzékeny adatot ne jelenítsen meg illetéktelen felhasználónak még

⁶ HAYDOCK 2024.

⁷ HAYDOCK 2024.

akkor sem, ha az a tudásbázisban szerepel. Az AI Act várhatóan olyan előírásokat hoz, hogy a generatív modellek outputjainak bizonyos kockázatait, mint például a hallucináció, téves információ kezelve legyenek,⁸ erre a RAG részben válasz, hiszen a valós idejű információkeresés csökkenti a modellek hallucinációját azzal, hogy tényleges dokumentumokra támaszkodik.⁹ Mindazonáltal a vállalatoknak óvintézkedéseket kell bevezetniük, például felhasználói promptszűrés, nehogy üzleti titkot kérdezzenek be figyelmen kívül nyilvános modellhez, illetve hozzáféréskontroll az MI-eszközök felett.

Összességében elmondható, hogy a korszerű SaaS-plattformok vállalati kiadásai adatvédelmi szempontból egyre jobban kontrolláltak, szerződésben rögzítik az adatok tulajdonjogát, a modell nem tanul tovább az ügyfél adataiból, és gyakran tanúsítottak (SOC 2,¹⁰ ISO27001¹¹). További adatvédelmi garanciát jelenthet, ha a vállalat saját üzemeltetésű megoldás mellett dönt, ami teljes adatkontrollt ad, cserébe magasabb költséggel és komplexitással.

A RAG-alapú oktatórendszerek elsődleges célcsoportja a céges dolgozók széles köre, az újonnan csatlakozó munkavállalóktól kezdve a nem informatikai területen dolgozó alkalmazottakig. A platformok személyre szabott és interaktív tartalommal igyekeznek mindenki számára érthetővé és relevánssá tenni a kibervédelmi ismereteket. Generatív MI segítségével például valóság-hű támadási szimulációk készülnek: e-mailek, hanghívások, SMS-ek, QR-kódos támadások stb. A Keepnet Labs platformja MI-vel generált *phishing*, *vishing*, *smishing* és *quishing* (QR-kódon keresztül történő adathalászat) szimulációkat kínál, amelyeket az adott dolgozó munkakörére és korábbi teljesítményére szabnak.¹²

Hasonlóan a Hoxhunt nevű tréningplatform MI-vezérelt, adaptív mikroképzéseket nyújt, a rendszer minden egyes felhasználó viselkedése alapján egyénileg időzített és testre szabott adathalászat-e-maileket küld, ezzel kutatások szerint akár negyvenszeres növekedést is elér a felhasználói aktivitásban, és hosszú távú viselkedésváltozást ér el a hagyományos módszerekhez képest.¹³ Az MI a felhasználók eredményeit elemelve képes gyenge pontokat azonosítani és ezekre fókuszáló tartalmat ajánlani. Például ha egy osztályon sokan dőlnek be egy bizonyos típusú adathalásznak, a rendszer több ilyen példát küld, majd azonnali visszajelzést ad a tanulóknak a hibáikról, segítve a folyamatos fejlődést.¹⁴

Ezek a megoldások új belépők számára alapozótréninget nyújtanak, például jelzőkezelés, e-mail-biztonsági alapok, míg a régóta ott dolgozók számára friss, aktuális fenyegetési példákat mutatnak be, fenntartva a figyelmet, és elkerülik az úgynevezett tanulási kimerültséget vagy tréningfáradtságot, amely gyakran a túl sűrű vagy monoton oktatási programok esetén jelentkezik.

⁸ EU Artificial Intelligence Act. The AI Act Explorer 2025.

⁹ InterSystems 2025.

¹⁰ Az AICPA (American Institute of Certified Public Accountants) által meghatározott szabvány, amely azt értékeli, hogy a szolgáltató hogyan kezeli az ügyféladatokat az adatbiztonság, adatkezelés, rendelkezésre állás, titkosság és integritás szempontjából.

¹¹ Nemzetközi szabvány az információbiztonság-irányítási rendszerekre (ISMS), amely biztosítja, hogy a szervezet rendszerszinten kezelje és védje az információkat a jogosulatlan hozzáférés, módosítás vagy elvesztés ellen.

¹² Keepnet 2024.

¹³ TitanHQ 2025.

¹⁴ Keepnet 2024.

Egyes RAG-rendszereket kiterjesztettek a haladó felhasználók igényeire is. Bár a hagyományos biztonságtudatossági platformok (KnowBe4, Hoxhunt stb.) főként az általános munkaerőt célozzák, a közelmúltban olyan generatív MI-alapú eszközök váltak elérhetővé, amelyek közvetlenül a SOC-csapat munkáját támogatják. A 2023-ban bemutatott Microsoft Security Copilot jó példa erre: a GPT-4 alapú asszisztens a Microsoft globális fenyegetésfelderítési adatain (napi 65 billió biztonsági jelzés) és a vállalat saját biztonsági modelljén keresztül ad valós idejű biztonsági eseményelemzéseket.¹⁵

A Security Copilot képes bonyolult támadási mintázatokat természetes nyelven összefoglalni, javaslatokat adni az incidensek kivizsgálásához, és integrálódik a meglévő védelmi eszközökhöz, például a Microsoft Defender vagy Sentinel SIEM.¹⁶ A security operations center (SOC) támogatására tervezett funkciók közé tartozik, hogy ilyen MI-asszisztenssel a biztonsági elemzők rövid szöveges utasítások formájában, például csevegőfelületen keresztül kérhetnek le fenyegetettségi információkat, log elemzéseket, vagy akár komplett incidensriportokat. A generatív modell a háttérben lekérdez több adatforrást, például vállalati naplókat, ismert sebezhetőségi adatbázisokat, ami támogatja a gyorsabb döntéshozatalt és csökkenti az incidensek kezelési idejét.¹⁷

Friss kutatási eredmények is alátámasztják e megközelítés hasznát: az *IntellBot* nevű kísérleti RAG-chatbot például számos adatforrásból gyűjt össze kibertámadásokkal kapcsolatos fenyegetéseket, ismert sérülékenységeket, aktuális incidenseket, és a felhasználók kérdéseire az aktuális tudásbázisból generál választ. Ezzel azonnali hozzáférést nyújt releváns információkhoz, segítve a fenyegetéselemzést és az incidenskezelést, időt spórolva meg a szakembereknek.¹⁸

A SOC-támogató generatív MI-rendszerek jellemzően nem sorolhatók a klasszikus értelemben vett oktatási rendszerek közé, hanem inkább operatív eszközök. Épp ezért a SOC-orientált funkciókat az oktatási rendszerek dokumentációjában rendszerint külön jelölik. Ugyanakkor oktatási hozadékuk is van, támogatják a kevésbé tapasztalt elemzők tudásának bővítését vagy kompetenciafejlesztését azáltal, hogy javaslatokat és magyarázatokat fűznek a talált eredményekhez.¹⁹ Például a CrowdStrike Charlotte MI asszisztense a vállalat végponti védelmi platformjába épül be, és automatikusan képes riasztásokat kezelni és reagálni azokra (*triage*). A gyártó állítása szerint 98% feletti pontossággal leválogatja a triviális vagy ismert mintázatú riasztásokat, így a SOC-csapat csak a valóban kritikus esetekre fókuszálhat, ezzel átlagosan heti 40 órányi manuális munkát spórol meg a csapatnak.²⁰

A Microsoft Security Copilothoz hasonlóan a Charlotte MI is generatív interfészt kínál, például strukturált incidens-összefoglalót generál, amely támogatja az utólagos elemzést és a tudásmegosztást.²¹

¹⁵ JAKKAL 2023.

¹⁶ CHANDROTH 2025.

¹⁷ ARIKKAT et al. 2024.

¹⁸ ARIKKAT et al. 2024.

¹⁹ REED–RAY 2024.

²⁰ Crowdstrike 2025.

²¹ COLUMBUS 2023.

Összegzőként megállapítható, hogy a RAG-megközelítést alkalmazó generatív MI-rendszerek nemcsak az általános munkavállalók biztonságtudatosítási képését, hanem a kiberbiztonsági szakemberek napi munkáját és folyamatos szakmai fejlődését is képesek támogatni. Az ilyen eszközök bevezetése hozzájárulhat a gyorsabb incidenskezeléshez, a munkaterhelés csökkentéséhez, valamint a szervezeti tudás hatékonyabb hasznosításához.

A generatív mesterséges intelligencia által készített feladatok elfogadottsága Magyarországon

A technológiai megoldások elfogadottsága és hatékonysága nem csupán elvi kérdés, hanem mérhető élmény is. A generatív mesterséges intelligencia oktatási célú alkalmazása különösen érzékeny terület, mivel egyszerre érinti a tanulási folyamat minőségét, a bizalom kérdését és a felhasználói önreflexiót. A kérdőív válaszai nem pusztán véleményeket tükröznek, hanem különböző demográfiai és hozzáállásbeli mintázatokat is kirajzolnak. E fejezet célja ezen mintázatok feltérképezése és annak bemutatása, hogy a GenMI által előállított tartalmak milyen mértékben váltottak ki értelmezhető reakciókat a válaszadók körében. A statisztikai elemzés nemcsak az elfogadottságot, hanem a tanulási élményt, a viselkedésbeli változást és az MI-hez való viszonyulás sokféleségét is megvilágítja.

A kérdőív felépítése és célja

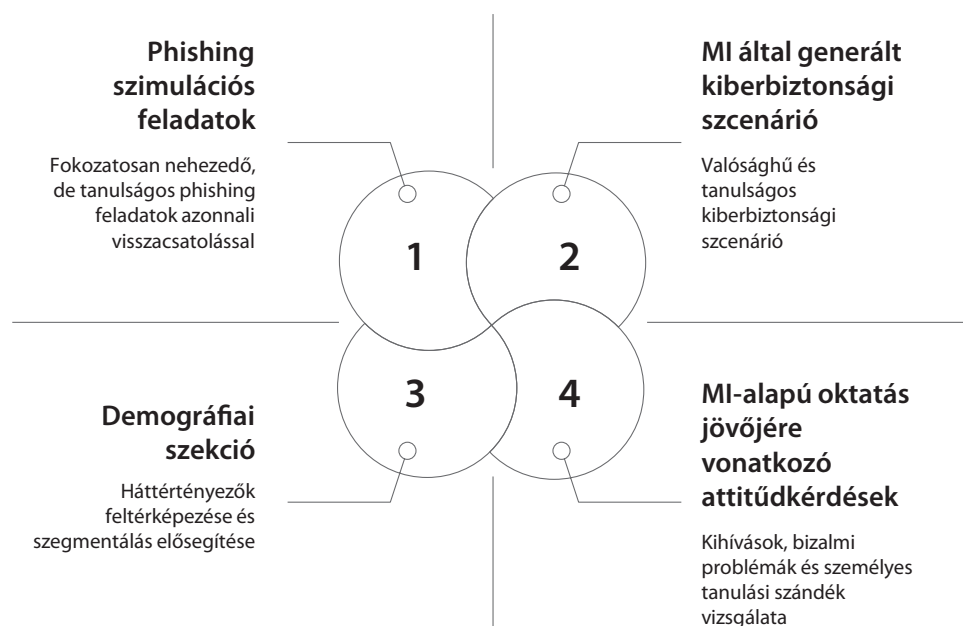
A kérdőíves kutatás célja az volt, hogy feltérképezze, miként viszonyulnak a válaszadók a generatív mesterséges intelligencia által létrehozott oktatási tartalmakhoz a kibertudatosítási képzések kontextusában. A kérdések kialakítását a Technology Acceptance Model elméleti kerete inspirálta,²² amely szerint egy új technológia elfogadottsága elsősorban két pszichológiai tényezőtől függ: az észlelt hasznosságtól és az észlelt használati könnyűségtől. Előbbi azt tükrözi, hogy a felhasználó mennyire látja értelmesnek és eredményesnek az adott technológia alkalmazását, míg utóbbi arra utal, mennyire tartja azt intuitívnak, érthetőnek vagy gyorsan elsajátíthatónak.

A kérdőívben az észlelt hasznosság két konkrét szempont mentén jelent meg, a tanulási érték és a jövőbeli alkalmazhatóság alapján. Ezek azért fontosak, mert nemcsak a GenMI-alapú scenárió azonnali megítélését tükrözik, hanem azt is, hogy a válaszadók hosszabb távon mennyire látják integrálhatónak ezt a technológiát a kiberbiztonsági képzésekbe. Az érthetőségi faktor vizsgálata, a scenáriók világossága és magyarázatai alapján, az észlelt könnyű használatot közelítette meg. Ezen túlmenően kérdések irányultak az MI-alapú oktatás elfogadási szándékára és a válaszadók érzelmi reakcióira is, így a kérdőív az elfogadás és érdeklődés, bevonódás összetett pszichológiai képét igyekezett feltárni.

²² DAVIS 1989.

A kérdőív négy nagyobb egységből épült fel:

- Három egymásra épülő *phishing* szimulációs feladat, amelyek fokozatosan komplexebbek lettek, de nem haladták meg a kitöltők általános információs műveltségét. A feladatok zárt végűek voltak, 4 válaszlehetőséggel. A válaszadók a visszacsatolások után három zárt kérdésre válaszoltak egy 1–5 fokozatú Likert-skálán (1 = egyáltalán nem, 5 = teljes mértékben), amelyek a feladat érthetőségére, a magyarázat világosságára és a tanulási élmény mértékére irányultak. A kérdések célja nem a válaszok helyességének vizsgálata volt, hanem a generált tartalom pedagógiai értékének mérése.
- Ezt követte egy MI által generált, interaktív kiberbiztonsági szcenárió, amely egy közel valósághű helyzetet modellezett. Az esettanulmány elkészítésekor igyekeztem egyensúlyozni a részletességet és az elolvasáshoz szükséges időt, aminek kihatása van arra, hogy mennyire lesz valósághű az esettanulmány. Ehhez kapcsolódva a válaszadók a szcenárió hasznosságát, érthetőségét, tanulságosságát, valamint saját érzéseiket és észrevételeiket is megoszthatták a fenti Likert-skálás módszerrel.
- A következő szakaszban az MI-alapú oktatás jövőjére vonatkozó attitűdkérdések lettek feltéve, amelyek a legnagyobb kihívásokra, bizalmi problémákra és személyes tanulási szándékokra kérdeztek rá.
- Zárásként egy demográfiai szekcióból, amely tartalmazta az életkort, nemet, legmagasabb iskolai végzettséget, gazdasági aktivitást, lakóhelytípust és a szakmai háttér megadását.



2. ábra: A kérdőív felépítése

Forrás: a szerző szerkesztése a Napkin.ai segítségével

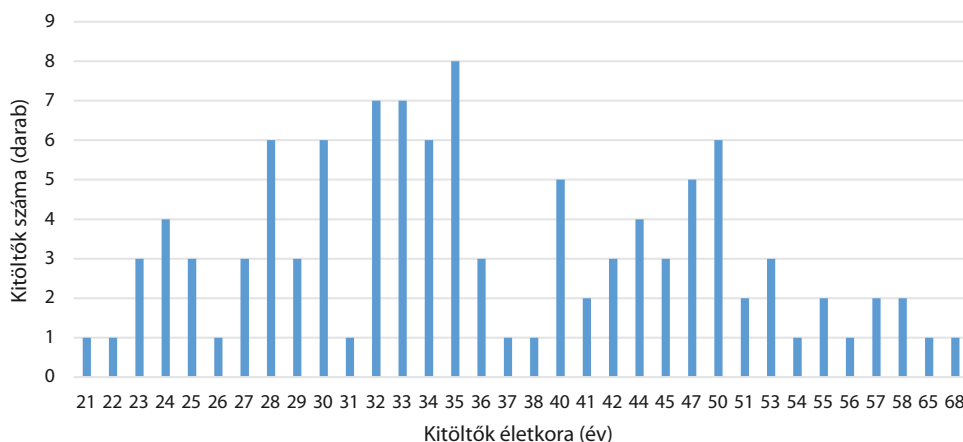
A kérdőívet Facebookon osztottam meg, kitölteni 2025. március 10. és április 10. között lehetett, ez idő alatt 109 fő töltötte ki, nem reprezentatív, de sokszínű minta alapján. A válaszadók között szerepeltek informatikai és kiberbiztonsági háttérrel rendelkezők is (27 fő), azonban a kérdőív célja nem szakmai mélységű értékelés, hanem a generált tartalmak általános használhatóságának és érthetőségének vizsgálata volt. A válaszok elemzése ennek megfelelően minden résztvevő válaszait figyelembe veszi, de az értelmezés során a nem szakértői nézőpontot tekintettük elsődlegesnek.

A válaszadók demográfiai jellemzői

A kérdőívet összesen 109 fő töltötte ki, önkéntes alapon. A minta nem reprezentatív, azonban célja nem is statisztikai általánosíthatóság, hanem annak vizsgálata volt, hogy a különböző háttérrel rendelkező felhasználók hogyan viszonyulnak a generatív mesterséges intelligencia által létrehozott kiberbiztonsági tartalmakhoz. A minta összetétele változatos, így alkalmas az elfogadottság, a tanulási élmény és az attitűdök közötti mintázatok feltérképezésére.

A válaszadók életkora 21 és 68 év között szóródott, az átlagéletkor 37,7 év, a szórás 10,5 év volt (3. ábra). A minta tehát alapvetően aktív korú felnőtteket reprezentál, akik potenciális célcsoportjai lehetnek egy valós vállalati vagy intézményi kibertudatosító programnak.

Egy válaszadó esetében az életkor mező nem numerikus formátumban szerepelt („3 x 5”), ezért ezt az adatpontot kizártam az életkorra vonatkozó statisztikai számításokból. Az érintett kitöltő többi válasza értelmezhető és konzisztens volt, így azok az elemzés részét képezték.



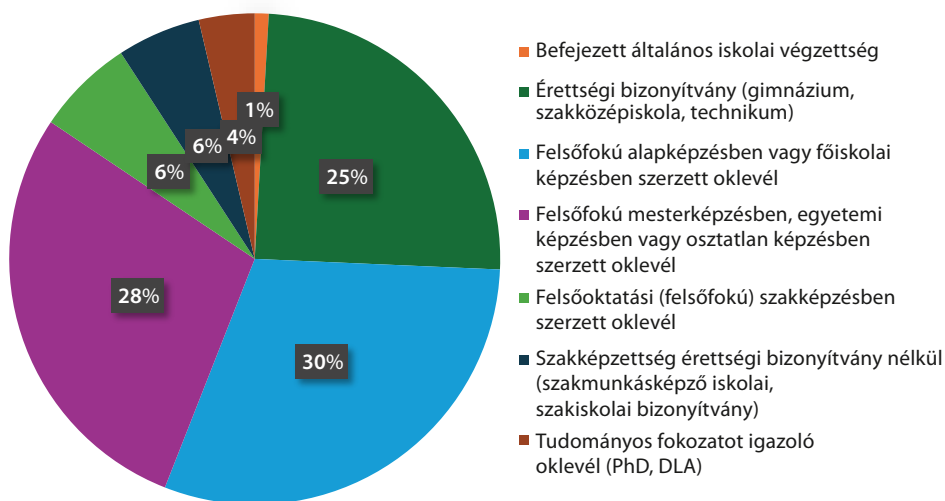
3. ábra: A kérdőívet kitöltők életkori megoszlása

Forrás: a szerző szerkesztése

A nemek megoszlása közel kiegyenlített: a válaszadók 55%-a férfi, 45%-a nő. Ez különösen fontos, mivel a kiberbiztonsági tudatosság vizsgálata során gyakran tapasztalható, hogy a minták nemi alapon torzulnak.

Az iskolai végzettséget tekintve a válaszadók többsége rendelkezik felsőfokú végzettséggel: leggyakoribb kategória a „Főiskolai vagy alapképzésben szerzett diploma”. Ezenkívül jelentős arányban szerepeltek mesterképzéses és középfokú végzettségű válaszadók is (4. ábra), ami lehetővé teszi az iskolai háttér hatásának vizsgálatát az MI-hez való viszonyulás szempontjából.

Mi a legmagasabb iskolai végzettsége?



4. ábra: A kérdőívet kitöltők legmagasabb iskolai végzettsége

Forrás: a szerző szerkesztése

A gazdasági aktivitás tekintetében a legtöbben alkalmazotti jogviszonyban dolgoznak (75 fő, a kitöltők 68%-a), de a mintában szerepeltek diákok, vállalkozók, szülési szabadságon lévők, nyugdíjasok és álláskereső is. Ez a sokféleség támogatja a viselkedésszerű és attitűdbeli különbségek feltárását.

A lakóhely típusa szerint a kitöltők legnagyobb része (40 fő) vármegyeszékhelyen vagy megyei jogú városban él, ami a digitális hozzáférés és a kibertérhez való viszonyulás szempontjából is releváns. Emellett kisebb városok, községek és a főváros is képviseltette magát.

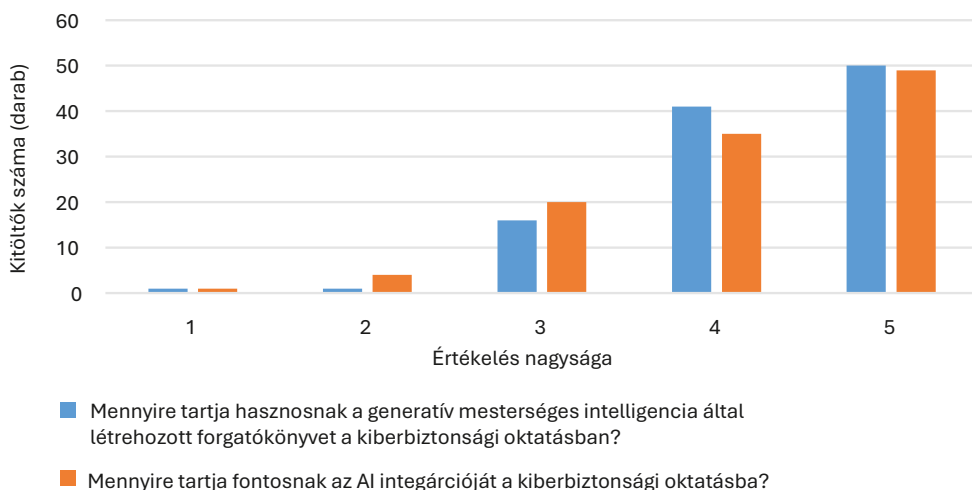
A szakterületi eloszlás igen változatos: 39 különböző megnevezés szerepel. A „Informatika / IT Biztonság” kategóriát 27 fő jelölte meg szakterületi háttérként. Mivel ez a megnevezés nem feltétlenül takar specializált kiberbiztonsági tudást, a tanulmány nem tekinti ezt a csoportot egységes szakértői kategóriának. Ugyanakkor a technológiai affinitás és informatikai háttér releváns szempontként jelenik meg az eredmények elemzése során, így az IT-s háttérrel rendelkező válaszadókat külön bontásban is vizsgálni kell.

A generatív mesterséges intelligencia alapú oktatási tartalmak elfogadottsága

A tanulmány bevezetőjében megfogalmazott első kutatási kérdés azt vizsgálta, hogy a nem szakmabeli felhasználók milyen mértékben fogadják el a generatív mesterséges intelligencia által létrehozott oktatási tartalmakat a kibertudatosítási képzésekben. A kérdéshez kapcsolódó első hipotézis szerint a válaszadók többsége elfogadja a GenAI által generált kiberbiztonsági oktatási szcenáriókat hiteles és hasznos tananyagként.

A kérdőív több szempontból is megvizsgálta az elfogadottság dimenzióját, három különböző kérdéssel, amelyek a TAM komponenseinek is megfeleltethetők. A „Mennyire tartja hasznosnak a generatív mesterséges intelligencia által létrehozott forgatókönyvet a kiberbiztonsági oktatásban?” kérdés az észlelt hasznosságra, míg a „Mennyire tartja fontosnak az AI integrációját a kiberbiztonsági oktatásba?” és az „El tudná képzelni, hogy hasonló interaktív forgatókönyvekkel tanuljon a kiberfenyegetésekről?” kérdések a használati szándékot jelzik.

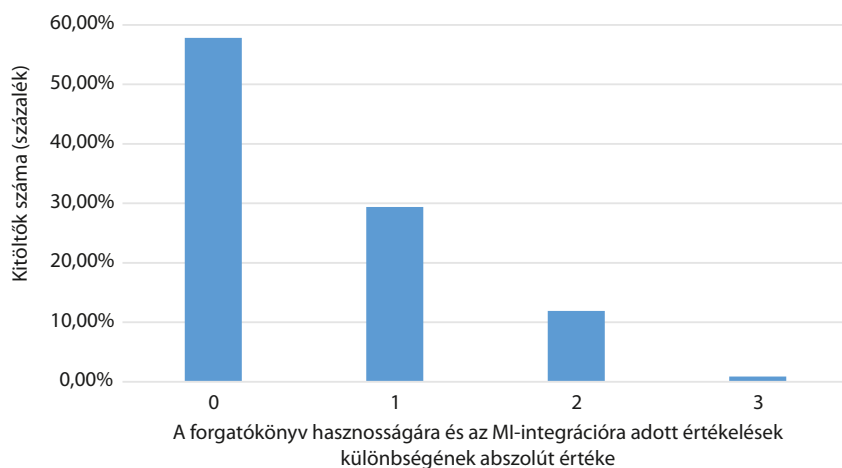
A válaszadás 1-től 5-ig terjedő Likert-skálán történt, a 109 fő által adott válaszok átlaga 4,27, szórása 0,81 volt az esettanulmány hasznosságánál, míg 4,17-os átlag és 0,92-os szórás mutatkozott az AI-integráció fontosságánál. Az eloszlás mindkét esetben enyhén torzult a magasabb értékek irányába, vizuálisan is jól elkülönülő csúcsponttal a 4–5-ös értékeknél (5. ábra).



5. ábra: A kérdőívet kitöltők válasza a fenti kérdésre

Forrás: a szerző szerkesztése

A két kérdés közötti kapcsolat közepesen erős pozitív korrelációt mutatott, azok, akik magasra értékelték a konkrét forgatókönyv hasznosságát, jellemzően az AI-integrációt is fontosnak tartották. A Pearson-féle korrelációs együttható értéke $r = 0,437$ volt ($n = 109$), ami statisztikailag közepesen erős pozitív kapcsolatot jelez a két változó között (6. ábra).

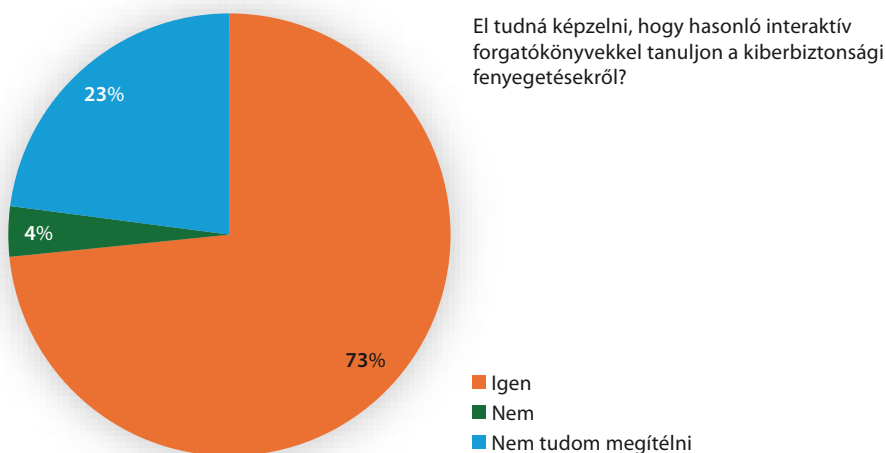


6. ábra: Különbségek eloszlása a két kérdés válasza között

Forrás: a szerző szerkesztése

A diagramon jól látható, hogy az esetek 57,8%-ában a két érték teljesen megegyezett, 29,4%-ban pedig csupán 1 pontos eltérés volt az értékek között. Mindössze 11,9%-nál fordult elő 2 pontos eltérés, és csupán egyetlen válaszadó esetén tért el három vagy több ponttal a két érték. Ez az eredmény jól szemlélteti, hogy a válaszadók nemcsak konzisztens véleményt formáltak, hanem a konkrét tapasztalat és a jövőbeni nyitottság között is szoros kapcsolat figyelhető meg.

A jövőbeni alkalmazhatóság vizsgálatára szolgáló „El tudná képzelni, hogy hasonló interaktív forgatókönyvekkel tanuljon a kiberfenyegetésekről?” kérdésre a 7. diagram szerint érkeztek a válaszok.



7. ábra: Válaszok megoszlása a jövőbeni interaktív forgatókönyveken történő részvételi szándékkal kapcsolatban

Forrás: a szerző szerkesztése

A válaszadók 73,4%-a igennel válaszolt erre a kérdésre, ami egyértelműen arra utal, hogy az MI-alapú tananyagokkal való tanulás nemcsak elfogadható, hanem kifejezetten kívánatos is a felhasználók többsége számára. Ez tovább erősíti a TAM-modell használati szándékra vonatkozó elemét, és azt mutatja, hogy a generatív MI alapú tanulási környezetek a jövőben is beilleszthetők lehetnek a tudatosítási programokba, különösen, ha azok interaktív és szituációalapú formában jelennek meg.

Összességében elmondható, hogy a H1 hipotézist igazoltuk. A válaszadók jelentős többsége hasznosnak találta a GenMI által generált forgatókönyvet, fontosnak tartja az MI integrációját az oktatásba, és nyitott a jövőbeli használatára. Ez az elfogadottság három külön dimenzióban is kimutatható volt: az aktuális tananyag megítélésében (észlelt hasznosság), az elvi támogatottságban (MI-integráció fontossága), valamint a jövőbeni használati szándékban (interaktív szcenáriók alkalmazhatósága). A statisztikai és vizuális eredmények alapján kijelenthető, hogy a generatív mesterséges intelligencia-alapú tananyagok alkalmasak lehetnek a kiberbiztonsági képzések kiegészítésére és fejlesztésére.

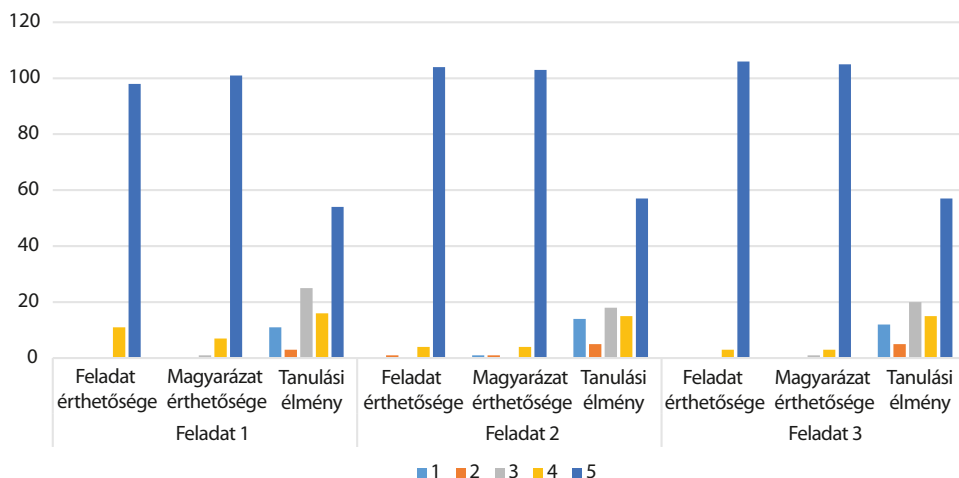
A generatív mesterséges intelligencia tartalmak érthetősége és tanulási értéke

A második kutatási kérdés azt vizsgálta, hogy a válaszadók hogyan értékelik a generatív mesterséges intelligencia által létrehozott kiberbiztonsági tartalmak érthetőségét és tanulási értékét. Az ehhez kapcsolódó második hipotézis szerint a résztvevők az MI által generált tananyagot érthetőnek és tanulásra ösztönzőnek találják.

A kérdőív három egymásra épülő *phishing* feladatot tartalmazott, amelyek fokozatosan növekvő bonyolultságot képviseltek, de nem haladták meg az általános felhasználói tapasztalatokat és technikai képességeket. Minden feladatra előre megadott válaszlehetőségek közül választhattak a kitöltők. A feladatok célja nem a kitöltők által adott válaszok helyességének az ellenőrzése, hiszen azt legjobban nyílt végű kérdésekkel lehetne figyelni, hanem a generatív mesterséges intelligencia által megírt feladat és magyarázat minőségének értékelése.

Minden feladatnál 4 választási lehetőség közül kellett választani a kitöltőnek, a válasz bejelölése és beküldése után azonnali visszacsatolást kapott a kitöltő, ahol a GenMI elmagyarázta, hogy a 4 válasz miért helyes vagy helytelen, valamint egy általános érvényű magyarázatot is adott. Mindhárom visszajelzés után három, azonos szerkezetű értékelő kérdés következett (1–5 skálán): a feladat érthetősége, a magyarázat érthetősége és a tanulás mértéke (8. ábra).

A vizuális eloszlások alapján megállapítható, hogy mind az érthetőség, mind a tanulási élmény többségében magas pontszámokat kapott. Az érthetőség eloszlása enyhén jobbra torzult, a legtöbben 4-es és 5-ös értékeket adtak.



8. ábra: A 3 phishing feladatra adott válaszok eloszlása

Megjegyzés: 1-től 5-ig terjedő skálán, ahol az 1 a legrosszabb, az 5 a legjobb értékelés.

Forrás: a szerző szerkesztése

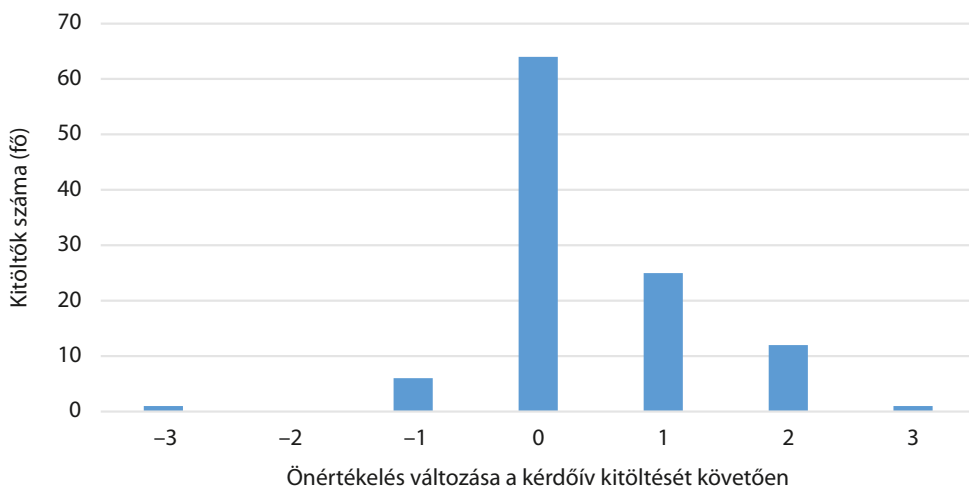
A tanulási élmény eloszlása szélesebb, és bár mediánban hasonló, szórása jóval nagyobb, mint az érthetőségi értékeké. Ez azt jelzi, hogy bár a legtöbben pozitív tanulási élményről számoltak be, az élmény szubjektívebb és egyénibb megítélés alá esik, mint a tartalom érthetősége. Érdeemes megfigyelni, hogy a feladatok fokozatos nehezedeése ellenére az értékelések nem estek vissza jelentősen.

A H2 hipotézis, miszerint a GenMI által generált tartalmak érthetőek és tanulásra ösztönzőek, igazolódott. A válaszadók a *phishing* feladatokat jellemzően jól értelmezhetőnek találták, és egyértelműen jelezték, hogy tanultak is belőlük. Mindez azt mutatja, hogy a GenMI képes a világos, strukturált és tanulást támogató tartalom előállítására nem szakmai célcsoportok számára is.

A tudásszint önértékelésének változása

A harmadik kutatási kérdés arra kereste a választ, hogy a válaszadók saját megítélése szerint mennyiben változott a tudásszintjük a kérdőívben bemutatott *phishing* szcenáriók és feladatok hatására. Az ehhez kapcsolódó harmadik hipotézis szerint a résztvevők az MI-szenárió és feladatok elolvasását követően magasabbra értékelik saját képességüket az adathalász-támadások felismerésében és kivédésében.

A kérdőív két kérdést tartalmazott ezzel kapcsolatban, azonos skálán (1 – egyáltalán nem, 5 – teljes mértékben) mérve az önértékelt jártasságot. Az első kérdés még a GenMI-feladatok és -szcenárió bemutatása előtt szerepelt, míg a második azokat követően. Ez lehetővé tette a közvetlen összehasonlítást, nemcsak statikusan, hanem dinamikus is, az önreflexió szintjén (9. ábra).



9. ábra: Az adathalászat felismerésére irányuló önreflexió változása

Forrás: a szerző szerkesztése

A kapott válaszok különbségének vizsgálatára páros t-próbát alkalmaztunk, amely azt méri, hogy az azonos válaszadók által megadott, szcenárió előtti és utáni értékek közötti eltérés statisztikailag szignifikáns-e. A párosított t-próba eredménye alapján a különbség szignifikáns volt, a $t(108)^{23} = 4,784$, $p < 0,001$, amely azt jelzi, hogy az önértékelt jártasság növekedése statisztikailag szignifikáns, azaz nem magyarázható véletlen ingadozással. Ez megerősíti, hogy a GenMI-feladatok és -szcenárió szignifikáns önértékelési javulást eredményeztek a válaszadók adathalászat elleni jártasságában. Bár az esetek túlnyomó többségében a változás pozitív vagy semleges volt, 7 válaszadónál enyhe csökkenés mutatkozott. Ez feltehetően nem a tudásszint csökkenését, hanem az önreflexió árnyaltabbá válását jelzi. A változatlan válaszadók között 24 fő már eleve maximális, 5-ös értékelést adott magának, ami azt jelzi, hogy az értékelés stabilitása sok esetben nem a hatás hiányát, hanem a meglévő kompetencia érzékelt teljességét tükrözi.

Összességében a H3 hipotézis igazolódott: a válaszadók átlaga szerint a GenMI-feladatokat követően magasabbra értékelték saját jártasságukat az adathalászat felismerésében. Bár a válaszadók több mint fele nem változtatott az értékelésén, a pozitív elmozdulások aránya, valamint az átlagos eltérés mértéke statisztikailag szignifikáns növekedést jelez. Mindez arra utal, hogy a generatív mesterséges intelligencia által előállított tartalom képes volt nemcsak az ismeretek aktiválására, hanem a tudatosság és önreflexió fejlesztésére is – különösen a nem szakmabeli felhasználók körében.

²³ A szabadsági fok ($df = 108$) a páros t-próbára jellemző módon az érvényes válasz párok számából adódik, azaz $df = n - 1$, ahol n azoknak a kitöltőknek a száma, akik mindkét – a szcenárió előtti és utáni – kérdésre válaszoltak.

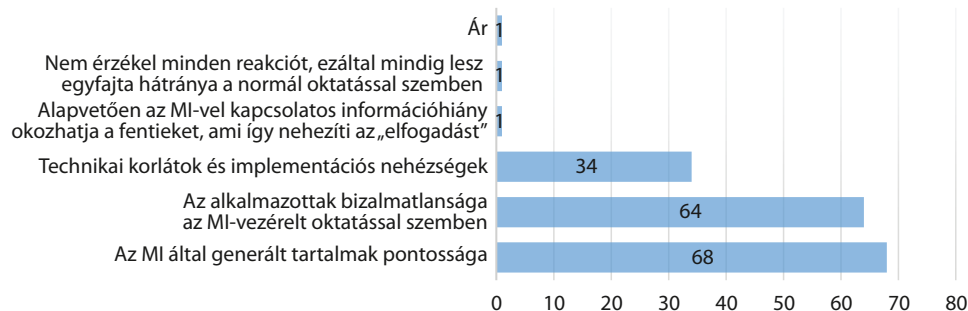
Kihívások a generatív mesterséges intelligencia alapú oktatás bevezetésében

A negyedik kutatási kérdés célja annak feltérképezése volt, hogy a válaszadók szerint mely tényezők jelentik a legnagyobb kihívást az MI-alapú oktatás bevezetése során. A hozzá kapcsolódó H4 hipotézis szerint a leggyakrabban említett kihívás az adatbiztonság és a tartalom megbízhatósága.

A kérdőívben szereplő zárt, többválaszos kérdés pontosan ezekre a tényezőkre kérdezett rá. A válaszadók 62,4%-a tartotta a legnagyobb kihívásnak az MI által generált tartalmak pontosságát, míg 58,7%-a említette az alkalmazottak bizalmatlanságát az MI-vezérelt oktatási rendszerekkel szemben. Ez a két tényező együttesen jól lefedi a H4 hipotézis kulcselemeit, hiszen a válaszok többsége a megbízhatóság és a bizalom hiányát jelöli meg akadályként.

A technikai korlátok és implementációs nehézségek a válaszadók közel egyharmada (31,2%) szerint szintén fontos szempont, de kevésbé meghatározó, mint a tartalmi és emberi tényezők. Az egyéb opciókat (például „információhiány”, „ár”, „nem érzékeli a reakciókat”) csak elenyészően kevesen választották (mindegyik 0,9% alatt), így ezek marginálisnak tekinthetők.

Mit tart a legnagyobb kihívásnak az MI-alapú oktatás bevezetésében?
(Több válasz is választható)



10. ábra: Az MI-alapú oktatás legnagyobb kihívásai

Forrás: a szerző szerkesztése

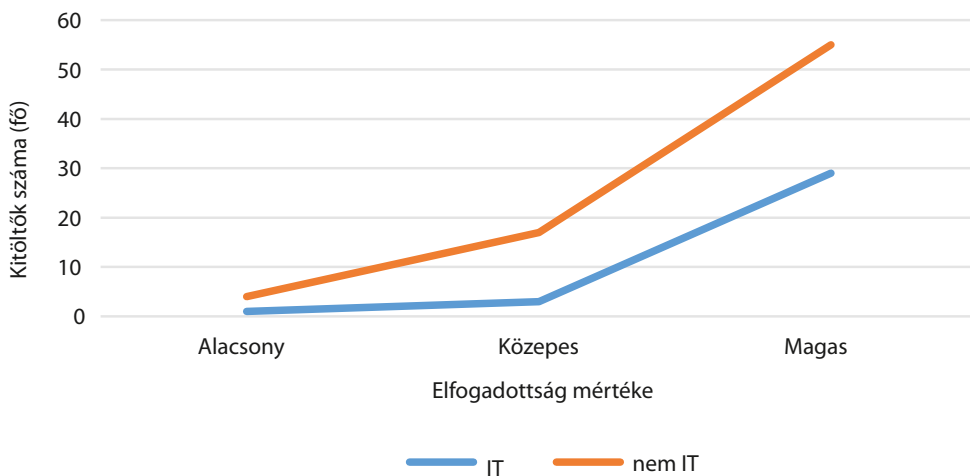
Az eredmények megerősítik azt a feltételezést, hogy a GenMI-alapú oktatás elfogadásának legnagyobb gátja nem technológiai, hanem elsősorban pszichológiai és bizalmi természetű. A válaszok alapján a felhasználók számára az információk pontossága és a rendszerbe vetett bizalom a két legkritikusabb tényező, míg a technikai kihívások másodlagos szerepet játszanak. A H4 hipotézis, miszerint a válaszadók elsősorban a tartalom megbízhatóságát és a bizalom hiányát tartják kihívásnak, igazolódott.

Különbségek generatív mesterséges intelligenciához való hozzáállásban demográfiai bontásban

Az ötödik kutatási kérdés célja annak feltárása volt, hogy a válaszadók MI-hez való hozzáállása eltér-e bizonyos demográfiai szempontok, például szakterület, iskolai végzettség vagy életkor alapján. A kapcsolódó H5 hipotézis szerint az informatikai szakterületen dolgozók szignifikánsan pozitívabb attitűddel viszonyulnak az MI-inTEGRÁCIÓHOZ, mint más területeken dolgozó társaik.

A kérdőív egyik zárt kérdése az MI-alapú oktatás fontosságának megítélésére irányult, amelyben a válaszadók egy ötfokozatú Likert-skálán értékelték, mennyire tartják lényegesnek a mesterséges intelligencia beépítését a kiberbiztonsági képzésekbe. Az elemzés során a válaszadókat szakterület alapján két csoportba soroltuk: informatikai (beleértve az IT-biztonságot) és nem informatikai háttérrel rendelkezők. A két csoport összehasonlításához független mintás t-próbát alkalmaztam. Az informatikai háttérrel rendelkező válaszadók átlaga magasabb volt, mint a más területekről érkezőké, azonban a statisztikai próba nem mutatott ki szignifikáns különbséget a két csoport között. Az eredmény, bár az elméleti elvárásokkal összhangban áll, nem volt elég markáns ahhoz, hogy kizárható legyen a véletlen szerepe.

A kvantitatív vizsgálatot egy keresztábrás khi-négyzet-próbával egészítettem ki, amelyben az MI-elfogadottságot három kategóriára bontottuk: alacsony, közepes és magas szintű elfogadottság. Ezt követően megvizsgáltam, hogy az egyes kategóriákban milyen arányban fordulnak elő informatikai, illetve nem informatikai háttérrel rendelkező válaszadók (11. ábra).



11. ábra: Az MI elfogadottsága az IT- és nem IT-kitöltők között

Forrás: a szerző szerkesztése

A khi-négyzet-próba eredménye megerősítette a t-próba következtetését: nem mutatható ki statisztikailag szignifikáns kapcsolat a szakterület és az MI-elfogadottság

között. A tendencia ugyan megfigyelhető, az informatikai háttérű kitöltők kissé pozitívabban értékelték az MI integrációját, ám a különbség mértéke nem haladta meg a szignifikancia határát.

Összességében a H5 hipotézist, miszerint az informatikai szakterületen dolgozók körében szignifikánsan magasabb az MI-integráció elfogadottsága, nem tudtuk megerősíteni. Bár az eredmények iránya az elvárásokkal összhangban áll, a mintában tapasztalt eltérések nem voltak elég erősek ahhoz, hogy egyértelmű következtetéseket vonjunk le. Az adatok arra utalnak, hogy az MI-hez való pozitív hozzáállás nem kizárólag a szakmai háttér függvénye, hanem valószínűleg összetettebb tényezők, például a technológiai nyitottság, az MI-vel kapcsolatos korábbi tapasztalatok, a munkahelyi kultúra vagy az oktatási módszerekkel szembeni nyitottság is befolyásolják a megítélést.

Összegzés

A kérdőív eredményei megerősítették, hogy a válaszadók alapvetően nyitottak a mesterségesintelligencia-alapú oktatási tartalmak iránt, és pozitívan viszonyulnak a generatív MI alkalmazásához a kiberbiztonsági tudatosságnövelésben. A KK1-re adott válaszok alapján elmondható, hogy a válaszadók túlnyomó többsége hasznosnak találta a GenMI által létrehozott scenáriót, és el tudja képzelni, hogy hasonló módszerekkel tanuljon kiberfenyegetésekről. A H1 hipotézist, miszerint a GenMI-tartalmak elfogadottak és hasznosnak ítélték, megerősítettük.

A KK2 és a H2 hipotézis a generatív mesterséges intelligencia által generált tartalmak érthetőségére és tanulási értékére fókuszált. A három *phishing* feladat kapcsán adott visszajelzésekből világosan kiderült, hogy a résztvevők a feladatokat és magyarázatokat túlnyomórészt jól érthetőnek ítélték, és egyértelműen jelezték, hogy tanultak is belőlük. A tanulási élmény szinte minden résztvevőnél magas szintet ért el, a skálán adott értékek torzítása pedig a pozitív irányba mutatott, megerősítve a H2 hipotézist.

A KK3 az önértékelt tudásszintváltozásra irányult, amelynek vizsgálatához páros mintás t-próbát alkalmaztam. A válaszadók a kérdőív kitöltését követően statisztikailag szignifikánsan magasabb értéket adtak az adathalászat felismerésére vonatkozó jártasságukra, mint a kitöltés előtt. A H3 hipotézis, hogy az MI-scenárió pozitív hatással van az önértékelt tudásszintre, igazolódott.

A KK4 azt vizsgálta, hogy milyen kihívások merülnek fel az MI-alapú oktatás bevezetésével kapcsolatban. A zárt kérdés válaszai alapján a leggyakrabban említett aggályok az MI által generált tartalmak pontossága és a rendszerbe vetett bizalom voltak. Az alkalmazottak bizalmatlansága az MI-vezérelt rendszerek iránt, valamint a technikai és implementációs nehézségek is megjelentek a válaszok között, de kisebb arányban. Ezek az eredmények alátámasztják a H4 hipotézist, amely szerint az MI-alapú oktatás legnagyobb kihívásai a tartalom megbízhatóságával és az emberi tényezőkkel kapcsolatosak.

Végül a KK5 és a H5 hipotézis azt vizsgálta, hogy van-e szignifikáns különbség az MI-integráció elfogadottságában a szakterület, iskolai végzettség vagy életkor szerint. A válaszadók szakterület szerinti bontásában bár megfigyelhető volt egy enyhe

tendencia az informatikai háttérű kitöltők közötti nagyobb elfogadottság felé, sem a független mintás t-próba, sem a khi-négyzet-teszt nem mutatott statisztikailag szignifikáns eltérést. A H5 hipotézist, miszerint az informatikai területen dolgozók körében kimutathatóan magasabb az elfogadottság, nem tudtuk megerősíteni. Az MI-hez való hozzáállás a jelek szerint nem kizárólag a szakmai háttér függvénye, hanem egyéni attitűdök, tapasztalatok és technológiai nyitottság is jelentős szerepet játszanak benne.

A tanulmány célja az volt, hogy feltárja, milyen lehetőségeket rejt a generatív mesterséges intelligencia alkalmazása a kibertudatosítási képzésekben, különös tekintettel a tananyagok személyre szabására, a tanulói élmény fokozására és a viselkedésváltozás támogatására. Az elméleti részben bemutattuk, hogy a GenMI hogyan tudja támogatni az oktatástervezést, például az ADDIE modell egyes fázisaiban, valamint milyen előnyökkel és kockázatokkal jár a tanulói oldalon történő alkalmazása. A vizsgálat figyelmet fordított az etikai, adatvédelmi és elfogadottsági kérdésekre is, amelyek elengedhetetlenek egy ilyen érzékeny területen, mint a kiberbiztonság.

Az empirikus részben egy kérdőíves kutatás segítségével vizsgáltam meg, hogy a magyar válaszadók miként értékelik a GenMI által generált kiberbiztonsági oktatási tartalmakat. A 109 fős minta nem reprezentatív, de kellően változatos volt ahhoz, hogy releváns mintázatokra lehessen következtetni. A kérdéseket a Technology Acceptance Model alapján alakítottam ki, és érintették a tartalom érthetőségét, tanulási értékét, elfogadottságát, jövőbeli alkalmazhatóságát, valamint a válaszadók saját tudásszintjükre vonatkozó önértékelését.

A kutatás főbb eredményei megerősítették a legtöbb hipotézist. A válaszadók többsége hasznosnak találta a GenMI által generált forgatókönyvet, és el tudja képzelni, hogy hasonló módon tanuljon kiberfenyegetésekről (H1). A *phishing* feladatok értékelései alapján a tartalmak érthetők és tanulásra ösztönzőek voltak (H2), és statisztikailag szignifikáns változást figyeltem meg az önértékelt jártasságban is az adathalászat felismerése terén (H3). A válaszadók a legnagyobb kihívásként az MI által generált tartalom megbízhatóságát és az alkalmazottak bizalmát nevezték meg, így a H4 hipotézis is igazolódott. A H5 hipotézis, amely az informatikai területen dolgozók pozitívabb MI-elfogadását feltételezte, nem nyert szignifikáns statisztikai alátámasztást, noha enyhe tendencia megfigyelhető volt.

A tanulmányban megfogalmazott hipotézisek többségét megerősítettük a kvantitatív vizsgálat során. Ezek alapján az alábbi tézisek vonhatók le:

T1: A válaszadók többsége elfogadja a generatív mesterséges intelligencia által létrehozott kiberbiztonsági oktatási tartalmakat hasznos és alkalmazható tananyagként.

T2: A GenMI által létrehozott tartalmakat a résztvevők világosan értelmezhetőnek és tanulásra ösztönzőnek találták.

T3: A GenMI-alapú szcenáriók és feladatok elolvasását követően statisztikailag szignifikáns növekedés figyelhető meg a válaszadók önértékelt jártasságában az adathalászat felismerésében.

T4: A válaszadók szerint a GenMI-alapú oktatás legnagyobb kihívása a tartalom megbízhatósága és az MI-rendszerekbe vetett bizalom hiánya.

T5: A kutatás nem mutatott ki statisztikailag szignifikáns különbséget az MI-integráció elfogadottságában az informatikai és nem informatikai háttérrel rendelkező válaszadók között.

Ezek a tézisek egyértelműen rávilágítanak arra, hogy a generatív mesterséges intelligencia nemcsak technológiai innovációként, hanem oktatási eszközként is releváns, ugyanakkor alkalmazása során elengedhetetlen a tartalom minőségének és a felhasználói bizalomnak a biztosítása. A tanulmányban bemutatott eredmények megalapozzák a jövőbeli kutatások irányait, amelyek vizsgálhatják a GenMI hosszú távú hatásait, a viselkedésváltozást, valamint az MI-alapú tartalom integrálásának lehetőségeit a különböző szervezeti kontextusokban.

A vizsgálat eredményei alapján elmondható, hogy a GenMI alkalmas lehet a kiberbiztonsági képzések támogatására, különösen, ha strukturált, kontextushoz illeszkedő tartalommal és megfelelő visszacsatolással működik. A válaszadók nyitottsága és pozitív visszajelzései alapján a generatív technológia nemcsak technikai lehetőség, hanem oktatásmódszertani innovációként is értelmezhető.

A tanulmány ugyanakkor nem törekszik gyakorlati implementációs javaslatok megfogalmazására, és nem vizsgálta kontrollált környezetben a tanulási hatékonyságot. A jövőbeni kutatások fókuszálhatnak az MI-alapú tartalom hosszú távú hatásaira, a viselkedésváltozás mérésére, valamint annak feltárására, hogy mely szakterületeken és milyen módszerekkel építhető be leghatékonyabban a GenMI a szervezeti oktatásba.

Felhasznált irodalom

- ARIKKAT, Dincy R. et al. (2024): IntellBot: Retrieval Augmented LLM Chatbot for Cyber Threat Knowledge Delivery. Arxiv. Online: <https://arxiv.org/html/2411.05442v1>
- CHANDROTH, Shiju (2025): Microsoft Security Copilot – Paramount is Excited about the most Awaited Generative AI for Cyber Security. Online: <https://paramountassure.com/cloud-security-solutions/microsoft-security-copilot/>
- COLUMBUS, Louis (2023): CrowdStrike Defines a Strong Vision for Generative AI at Fal.Con 2023. Zencoder, 2023. szeptember 21. Online: <https://venturebeat.com/security/crowdstrike-defines-a-strong-vision-for-generative-ai-at-fal-con-2023/>
- CrowdStrike (2025): CrowdStrike Delivers the Next Breakthrough in AI-Powered Agentic Cybersecurity with Charlotte AI Detection Triage. Online: www.crowdstrike.com/en-us/press-releases/crowdstrike-delivers-next-breakthrough-in-ai-powered-agentic-cybersecurity-with-charlotte-ai-detection-triage/
- 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>
- EU Artificial Intelligence Act. The AI Act Explorer (2025). Online: <https://artificialintelligenceact.eu/ai-act-explorer/>
- HAYDOCK, Walter (2024): Generative AI Risk Cheat Sheet: Training vs. RAG. *Stackaware Blog*, 2024. május 30. Online: <https://blog.stackaware.com/p/ai-training-retrieval-augmented-generation-rag>

- InterSystems (2025): *Retrieval Augmented Generation (RAG): Mi ez és hogyan előzi meg a mesterséges intelligencia hibáit?* Online: www.intersystems.com/hu/resources/retrieval-augmented-generation-rag-mi-ez-es-hogyan-eloz-meg-a-mesterseges-intelligencia-hibait/
- JAKKAL, Vasu (2023): Introducing Microsoft Security Copilot: Empowering Defenders at the Speed of AI. *The Official Microsoft Blog*, 2023. március 28. Online: <https://blogs.microsoft.com/blog/2023/03/28/introducing-microsoft-security-copilot-empowering-defenders-at-the-speed-of-ai/>
- Keepnet (2024): *How Generative AI Is Transforming Security Behavior and Culture Programs*. Online: <https://keepnetlabs.com/blog/how-generative-ai-is-transforming-security-behavior-and-culture-programs>
- REED, Jenn – RAY, Ayan (2024): CrowdStrike's Charlotte AI – Enhancing Productivity of Cyber Security Analysts with Generative AI Built-on AWS. *AWS Blog*, 2024. november 1. Online: <https://aws.amazon.com/blogs/apn/crowdstrike-charlotte-ai-generative-ai-on-aws/>
- TitanHQ (2025): *Hoxhunt and TitanHQ Security Awareness Training*. Online: www.titanhq.com/hoxhunt-vs-titanhq/

Somogyi János József,¹ Nagy Sándor²

A geopolitika és a lakosságvédelem kapcsolata

The Relationship between Geopolitics and Civil Protection

Absztrakt

A geopolitika és a lakosságvédelem közötti kapcsolatot az országok földrajzi helyzete, stratégiai erőforrásai és nemzetközi biztonsági környezete mellett a politikai akarat és a stratégiai mentalitás határozzák meg. A geopolitikai elemzések alapvetően befolyásolják a nemzeti lakosságvédelmi stratégiákat, amelyek alapvető célja a civil lakosság, a kritikus infrastruktúrák, kiemelt nemzeti vagyonelemek és a stratégiai erőforrások védelme.

Ez magában foglalja a természeti és ember okozta katasztrófákra való felkészülést, valamint a katonai védelmi intézkedések és a civil védelmi erőfeszítések összehangolását annak érdekében, hogy garantálják a lakosság biztonságát és az ország stabilitását geopolitikai feszültségek és konfliktusok esetén. Az államok geopolitikai helyzetének elemzése kulcsfontosságú a védelmi stratégiák megértésében, különös tekintettel arra, hogy milyen potenciális fenyegetések és kihívások érhetik az országot.

Ezek a tényezők együttesen formálják és befolyásolják a geostratégiai célok meghatározását, és azt, hogy az országok miként készülnek fel a potenciális fenyegetésekre, hogyan terveznek védekezni ellene, és hogyan működnek együtt más nemzetekkel geostratégiai célkitűzéseik harmonizálásával a közös biztonsági célok elérése érdekében. A geopolitika és a lakosságvédelem így összekapcsolódik egy komplex lokális, regionális vagy globális szintű multinacionális és multidiszciplináris megközelítésben, amely elengedhetetlen az országok jólétének és biztonságának fenntartásához a változékony biztonsági környezetben.

Kulcsszavak: geopolitika, lakosságvédelem, fenyegetések

¹ Dandártábornok; törzsigazgató-helyettes, Honvéd Vezérkar, e-mail: somogyi.janos@hm.gov.hu

² Alezredes, kiemelt főtiszt, Honvéd Vezérkar, Hadműveleti Csoportfőnökség, Stratégiai Tervező Főnökség, e-mail: nagysandor.phd@gmail.com

Abstract

The relationship between geopolitics and civil protection (civil defence) is determined by the geography, strategic resources and international security environment of countries, as well as by political will and strategic mentality. Geopolitical analyses have a profound influence on national civil protection strategies, which have the fundamental objective of protecting civilians, critical infrastructure, key national assets and strategic resources. This includes preparing for natural and man-made disasters and coordinating military protection measures and civil protection efforts to guarantee the security of the population and the stability of the country in the event of geopolitical tensions and conflicts. Analysing the geopolitical situation of states is key to understanding defence strategies, particularly with regard to the potential threats and challenges that may befall the country. Together, these factors shape and influence the definition of geostrategic objectives, how countries prepare for potential threats, how they plan to defend against them, and how they work with other nations to harmonise their geostrategic objectives to achieve common security goals. Geopolitics and civil protection are thus linked in a complex multinational and multidisciplinary approach at the local, regional or global level, which is essential to maintain the prosperity and security of countries in a volatile security environment.

Keywords: geopolitics, civil protection, hazards, threats

A geopolitika kialakulásáról röviden

A geopolitika jelenlegi rendszertani tudománya a 19. század végén és a 20. század elején alakult ki összetett folyamat eredményeként, amely a földrajz, a politika és a nemzetközi kapcsolatok összefonódásából származott, hiszen ez minden birodalomépítés alapja volt a történelem folyamán. A geopolitika az államok földrajzi helyzetét és az ebből következő hatalmi dinamikát vizsgálja. A hidegháború és a 21. századi globális verseny továbbra is fenntartja a geopolitika központi szerepét a nemzetközi kapcsolatok megértésében.

A geopolitika kifejezést Rudolf Kjellén svéd politológus használta először a 19. század végén. Kjellén a geopolitikát az állam politikai stratégiáinak földrajzi tényezőkkel való összefüggéseként határozta meg, ami új dimenziót adott a nemzetközi kapcsolatok elemzéséhez.³

A geopolitikai gondolkodás előzményei már korábban is megjelentek, különösen az államok földrajzi helyzetének jelentőségére vonatkozó elméletekben. A nagy birodalmak, mint például Napóleon Franciaországa vagy Oroszország I. Péter cár alatt, már a 18–19. században is alkalmazták a földrajzi adottságokat politikai és katonai stratégiáikban.⁴

³ TOAL 1996.

⁴ KENNEDY 1987.

Friedrich Ratzel német geográfus *Lebensraum* (élettér) koncepciója alapján állította, hogy az államok mint élő organizmusok folyamatos terjeszkedésre törekednek, ami későbbi politikai ideológiákra, mint például a náciizmusra is hatással volt.⁵

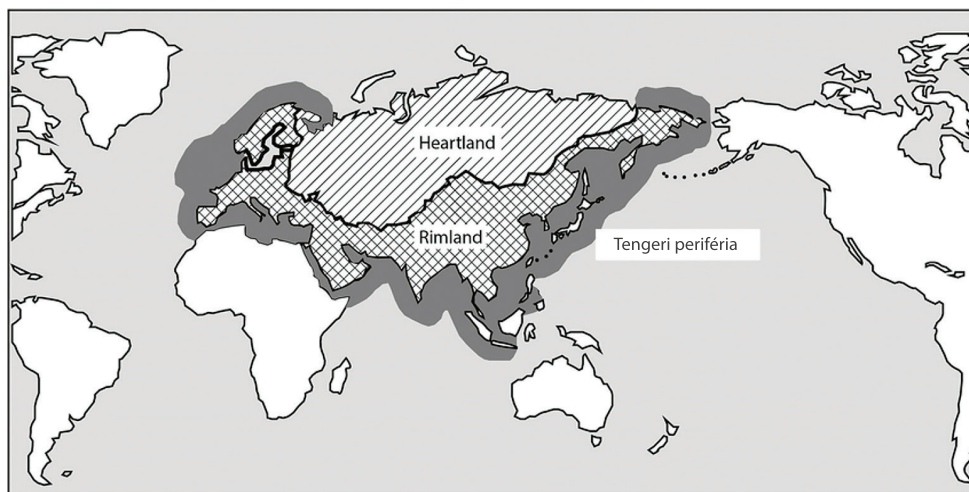
Alfred Mahan amerikai tengernagy a tengeri hatalom jelentőségét hangsúlyozta, amelyet *The Influence of Sea Power upon History* című művében fogalmazott meg. Mahan szerint a tengeri fölény kulcsfontosságú volt a világhatalommá válás szempontjából.⁶

Halford Mackinder híres heartland-elmélete szerint Eurázsia központi területének (*heartland*) ellenőrzése döntő szerepet játszik a globális hatalom megszerzésében. Ezt az elméletet a *The Geographical Pivot of History* című művében fogalmazta meg 1904-ben.⁷

Karl Haushofer német geopolitikai gondolkodó és tábornok volt, aki Ratzel elméleteit továbbfejlesztette. Haushofer fontos szerepet játszott a geopolitika népszerűsítésében a 20. század első felében, és hatással volt a náci ideológiára is, bár közvetlen politikai támogatásáról nincs bizonyíték.⁸

A két világháború közötti időszakban a geopolitika Németországban és más országokban is a terjeszkedési politikák és a hatalmi stratégiák alapjául szolgált. A német *Lebensraum* koncepció közvetlen hatással volt Adolf Hitler területi ambícióira.⁹

A hidegháború idején a geopolitika kulcsszerepet játszott az Egyesült Államok és a Szovjetunió közötti globális versenyben. Mackinder heartland-elmélete és Nicholas Spykman rimland-elmélete (1. ábra) formálta az amerikai külpolitikai gondolkodást, különösen a feltartóztatási politika (*containment*) megfogalmazásakor.¹⁰



1. ábra: Heartland-, rimland-elmélet

Forrás: MITCHELL 2020: 412.

⁵ BASSIN 1987.

⁶ MAHAN 1890.

⁷ MACKINDER 1904.

⁸ HERWIG 1999.

⁹ BLACK 2009.

¹⁰ KAPLAN 2012.

A 21. században a geopolitika továbbra is meghatározó szerepet játszik, különösen a globális erőforrásokért folytatott harcokban és a nagyhatalmak közötti rivalizálásban. A modern geopolitikai konfliktusok között említhetők a Közel-Keleten zajló olajért folytatott küzdelmek és a Dél-kínai-tenger térsége.¹¹

A geopolitika történelemformáló ereje

A geopolitika mint tudományág és gyakorlati politikai eszköz jelentős hatást gyakorolt a világtörténelemre. A nemzetek földrajzi elhelyezkedése, természeti erőforrásai és stratégiai döntései meghatározó szerepet játszottak abban, hogyan alakultak ki a világ nagyhatalmi viszonyai, hogyan zajlottak a terjeszkedések, háborúk és békekötések. Például a 15. századi európai felfedezések és a 20. századi dekolonizáció azt mutatják, hogy a geopolitikai elemzések meghatározók voltak a hódító birodalmak felemelkedésében és bukásában.¹²

A hidegháború idején a Szovjetunió és az Egyesült Államok közötti geopolitikai rivalizálás a világpolitika központi eleme volt.¹³ A két szuperhatalom globális befolyásért folytatott küzdelme és ideológiaexportja meghatározta a 20. század második felének nemzetközi kapcsolatait, beleértve a különböző regionális konfliktusokat és a katonai szövetségi rendszereket.

A Közel-Kelet geopolitikai dinamikája, különösen olajstratégiai jelentősége, az izraeli–palesztin konfliktus és az arab országok közötti feszültségek mind geopolitikai tényezőkön alapultak, és alapvetően befolyásolták a globális politikát.¹⁴

Végül az Orosz Birodalom geopolitikai és geostratégiai célkitűzései, mint az eurázsiai szívtérből (*heartland*) való kiindulással a peremterületek (*rimland*) és a meleg vízi kikötőkhöz való hozzáférés megszerzése, kulcsszerepet játszottak az ország történelmében.¹⁵ Napjainkban ugyanakkor az orosz történelmi geopolitika és stratégia kibővülni látszik, és az afrikai kontinensen való terjeszkedésével befolyásolási övezetének kiterjesztésével a világsgiget-koncepció megvalósítására törekszik kínai, indiai és közel-keleti támogatással, aminek az esetleges sikere megtöri Amerika jelenlegi globális hegemoniáját, és egy többpóluson alapuló *status quót* hoz létre.¹⁶

Ezek az események és politikai döntések nem csupán a földrajzi adottságok, hanem az erőforrások iránti igény és a stratégiai szempontok, nagyhatalmi érdekek tükrében értelmezhetők úgy napjainkban, amint azt a fent hivatkozott művek részletesen elemzik.

¹¹ FRIEDMAN 2009.

¹² KENNEDY 1987.

¹³ GADDIS 2005.

¹⁴ FRIEDMAN 1990.

¹⁵ TSYGANKOV 2013.

¹⁶ BERNEK 2023.

Általános geopolitikai kitekintés

A geopolitikai és geostratégiai elemzések, a geostratégia alakításának eredményessége attól függ, hogy milyen mértékben tudjuk időben felismerni és csökkenteni a nemzeti érdekeinket befolyásoló regionális és globális kockázatokat, hogyan tudunk adekvát válaszokat adni a biztonsági környezet kihívásaira. Mivel a Kárpát-medence geopolitikai és geostratégiai fontossága nem csökkent az elmúlt évszázadok alatt, így ebben segítségünkre lehetnek a történelmi példák elemzéseiből levont reális következtetések, amelyek alátámasztják a nemzeti geostratégiai célkitűzések megvalósíthatóságát az új típusú kockázatok és kihívások ellenében is. A stratégiai mélységet nemcsak földrajzi adottságok alapján kell vizsgálni, hanem történelmi, népességi, kulturális, gazdasági, technológiai kapacitás, haderőképeség, stratégiai mentalitás, valamint a tervezés és a politikai akarat komplex rendszerében.

A történelem folyamán többször, de a történelmi újkor végén a modern kor kezdetétől különösen előtérbe kerül a kérdés, hogy a kelet-közép-európai térség melyik nagyhatalom érdekszférájához tartozzon. A térség kisebb államainak nem maradt, és most sincs túl sok, mozgástere, és kisebb-nagyobb mértékben igazodniuk kell valamely nagyhatalomhoz. Nemzeti érdekeik védelmében, geopolitikai-geostratégiai céljaik elérése érdekében akaratlanul is súrlódhatnak a nagyhatalmi törekvésekkel, érdekekkel. A Kárpát-medence és annak központi része – Magyarország – jellegzetesen olyan állam, ahol számolni kell a nagyhatalmi érdekek fokozott megjelenésével, a térségi konfliktusok kihatásával, a nemzeti érdekeket közvetlenül érintő változásokkal.

A hidegháborút követően a NATO-hoz és az EU-hoz csatlakozó volt szocialista államok, kiemelten a balti országok, Lengyelország, Szlovákia, Magyarország, Románia a hidállamok szerepét töltötték be a Nyugat és a Kelet között. Az orosz–ukrán háború kirobbanása után potenciálisan ütközőzónává alakult a térség a NATO és Oroszország között. Ez közvetlenül hatással van Magyarországot geopolitikai, illetve abból eredő geostratégiai célkitűzéseire, nemzeti érdekeire.

A stratégiai mélység értelmezése

A stratégiai mélység fogalma a geopolitikában és a katonai stratégiában az a képesség, hogy egy ország késleltessen, megállítson vagy elhárítson egy támadást, biztosítva ezzel időt és teret a védekezésre és az ellenintézkedésre. A fogalom nemcsak fizikai területre utal, hanem a politikai, gazdasági és társadalmi stabilitásra is, amely lehetővé teszi egy állam számára, hogy hatékonyan reagáljon a kihívásokra és fenntartsa a függetlenségét.

A stratégiai mélység elemei közé tartozik a földrajzi elhelyezkedés, ami meghatározza az ország hozzáférhetőségét és védhetőségét. Az olyan országoknak, amelyek hatalmas területtel rendelkeznek, mint például Oroszország, természetes stratégiai mélységük van, ami nehezíti a megszállást és időt biztosít a mobilizációra. Ezzel szemben kisebb vagy sík területtel rendelkező országok, mint például Izrael vagy Magyarország, korlátozott fizikai stratégiai mélységgel rendelkeznek, ami fokozott kihívásokat jelent a védelmi stratégiák kialakításában.

Továbbá, a stratégiai mélység magában foglalja a gazdasági erőforrásokat, a politikai stabilitást és a nemzetközi szövetségeket is, amelyek kulcsfontosságúak egy ország hosszú távú biztonságának és stabilitásának fenntartásában. Például, a hidegháború alatt a NATO szövetségi rendszere biztosította Nyugat-Európa stratégiai mélységét azáltal, hogy kollektív védelmi garanciákat nyújtott a Szovjetunióval szemben.

Ezért a stratégiai mélység fogalmát szintén multidiszciplináris szempontból kell megközelíteni, figyelembe véve a katonai, gazdasági, társadalmi és politikai, diplomáciai dimenziókat is, hogy teljes képet kapjunk egy ország védelmi képességéről és stratégiai előnyeiről vagy hátrányairól.

A földrajzi stratégiai mélység hiánya

Magyarország földrajzi helyzete és mérete miatt stratégiai mélysége rendkívül korlátozott. A stratégiai mélység lényege, hogy egy ország elég nagy területtel rendelkezzen ahhoz, hogy időt és teret biztosítson a védekező erők számára a mozgósításra és manőverezésre. Magyarország esetében ez nem lehetséges, az államhatártól az ország kulcsfontosságú pontjai, például Budapest vagy a nagy ipari központok, gyorsan elérhetők egy esetleges támadó erő számára, valamint korlátozzák a lakosság távoltartásának lehetőségét a veszélyforrásoktól.

Ezt a problémát súlyosbítja, hogy Magyarország domborzati adottságai, a síkvidéki területek és a kevés természetes akadály miatt kicsiny lehetőség van arra, hogy természetes védvonalak segítségével lassítsák az esetleges támadókat. Az ország határai nagyrészt nyitottak, mivel Magyarország tagja a schengeni övezetnek, amely lehetővé teszi a szabad mozgást a határokon. Az ország teljes határhossza 2231 km, amely többnyire síkvidéki területeken húzódik. Az ország területének kétharmada, azaz 66%-a alföldi jellegű, ami kedvez a mezőgazdaságnak, ám a stratégiai védelem szempontjából is meghatározó lehet, mivel könnyen átjárható terep.

A lakossági koncentráció kiemelkedő a városokban, különösen Budapesten, ahol a főváros Magyarország területének mindössze 0,7%-át teszi ki, ám itt él az ország lakosságának mintegy 20%-a, ami több mint 1,7 millió fő (a teljes lakosság körülbelül 9,7 millió fő). Ez erősen befolyásolja az ország infrastrukturális és gazdasági politikáját is, mivel a gazdasági és kulturális élet jelentős része Budapestre összpontosul. Tíz vármegye székhelye a határtól 60 km-es távolságban található, emellett Magyarországon a városi lakosság aránya is magas, az ország teljes lakosságának körülbelül 72%-a él városokban. Ez a nagy fokú urbanizáció a városi térségeket kulcsfontosságúvá teszi mind a belpolitikai döntéshozatalban, mind a nemzetközi kapcsolatokban, mivel ezek a területek a leginkább érintettek a globális kihívások, például a migráció vagy az energiabiztonság kérdéseiben. A városi területeken történő gyors és hatékony válaszadás, például modern riasztási rendszerek, evakuációs útvonalak és vészhelyzeti kommunikációs csatornák fejlesztése elengedhetetlen a lakosság biztonságának garantálásához.

A földrajzi megközelítésnél fontos tisztázni a „hátsóország” fogalmát, különösen a kis- vagy közép méretű államok vonatkozásában, mint amilyen hazánk is. Esetükben a hátsóország nem területi, hanem az országvédelem szempontjából funkcionálisan

elkülönült feladatrendszereket jelent, hiszen a ballisztikus rakéták, a harcászati légi- és a gépesített, nagy mozgékonyosságú szárazföldi képességek korszakában a fizikai tér önmagában már nem ad kellő védelmet ezen országok lakossága, valamint a létfenntartáshoz szükséges anyagi javak számára. A globális képességű légi- és az interkontinentális ballisztikus rakéták és a kiber-támadóképesítések még a földrajzilag nagy kiterjedésű országokban is abszolút támadhatóvá teszik a klasszikus értelemben vett hátszín- és határterületeket. Így a lakosságvédelem és -felkészítés, a nemzeti vagyon, a kritikus infrastruktúrák védelme lényegesen nagyobb hangsúlyt kap, mint a második világháború után bármikor.

Népességi-kulturális alapú megközelítés

A stratégiai mélység népességi-kulturális kérdése Magyarország esetében elsősorban a demográfiai kihívásokból és kulturális identitás megőrzéséből fakad. A lakosság csökkenése, elöregedése, valamint a vidéki és határmenti területek elnéptelenedése csökkenti az ország belső stabilitását és ellenálló képességét. A határmenti régiókban élő nemzetiségi összetétel, valamint a városi és vidéki területek közötti egyenlőtlenségek tovább gyengítik ezt a stratégiai mélységet. A főváros és néhány nagyobb város dominanciája miatt az ország periferiái kevésbé védettek, míg a migráció és a nemzetközi kapcsolatok szintén jelentős kihívásokat jelentenek.

Magyarország számára a demográfiai stabilitás és a kulturális identitás megőrzése kulcsfontosságú a belső stabilitás és külső védekezőképesség fenntartása érdekében, amely közvetetten hatással van a lakosságvédelmi feladatokra is.

Határon túli magyar kisebbségek és a trianoni szerződés következményei

A trianoni békeszerződés következtében Magyarország elvesztette területének kétharmadát, ami jelentős magyar kisebbségeket hagyott hátra a szomszédos országokban, mint Románia, Szlovákia, Szerbia és Ukrajna. Ezek a jelentős kisebbségi csoportok feszültségeket generálhatnak a kétoldalú kapcsolatokban, és potenciálisan destabilizálhatják a regionális biztonságot. A kisebbségi kérdések kezelése kulcsfontosságú a konfliktusok megelőzésében és a stabil regionális kapcsolatok fenntartásában, ami közvetlen hatással van a közép-európai biztonsági környezetre.

A történelmi sebek és a kollektív emlékezet szerepe a kisebbségi konfliktusokban rendkívül fontos. A trianoni békeszerződés által kialakított határok jelentős hatást gyakoroltak a nemzeti identitásra és a nemzetközi kapcsolatokra a régióban.

A kisebbségek jogainak biztosítása és az etnikai feszültségek kezelése elengedhetetlen a biztonságos és stabil környezet megteremtéséhez, ami lehetővé teszi a hatékony válaszadást természeti és ember okozta katasztrófák esetén. A határmenti együttműködés erősítése, például közös lakosságvédelmi gyakorlatok és protokollok kidolgozása növelheti a reagálási képességeket. Ezenfelül, a regionális biztonsági együttműködések és az információcsera kiépítése kulcsfontosságú lehet a lakosságvédelmi

erőfeszítések koordinálása és a gyors reagálás biztosítása szempontjából, ami közvetlenül hozzájárulhat az érintett közösségek biztonságához és jólétéhez.

Gazdasági-technológiai megközelítés

Magyarország gazdasági-technológiai stratégiai mélysége a gazdasági stabilitás és technológiai fejlődés függvénye. Az autóipar és a külföldi tőkebefektetések nagy aránya elősegíti a rövid távú növekedést, de hosszú távon kiszolgáltatottá teheti az országot a globális piac ingadozásainak. Ugyanakkor a hazai gyártókapacitás, különösen a hadiipari beruházások és az akkumulátorgyárak kiépítése, jelentősen hozzájárulhat a gazdaság diverzifikációjához és az ország önellátó képességéhez. A hadiipari fejlesztések nemcsak a nemzetbiztonságot erősítik, hanem magas hozzájárulású munkahelyeket teremtenek, és elősegítik a technológiai innovációt, míg az akkumulátorgyárak a zöldátállásban és az elektromosjármű-iparban növelik Magyarország versenyképességét. Emellett az energiafüggetlenség növelése és a modern infrastruktúra kialakítása kulcsfontosságú az ország geopolitikai biztonsága és gazdasági ellenálló képessége szempontjából. A gazdasági diverzifikáció és a technológiai fejlesztések, valamint az infrastruktúra modernizálása közvetlenül hozzájárulnak a lakosság védelméhez, biztosítva, hogy az ország jobban felkészült legyen a jövő kihívásaira, legyen szó gazdasági ingadozásokról, természeti katasztrófákról vagy biztonsági fenyegetésekről.

Katonai képességek

Magyarország katonai stratégiai mélysége folyamatosan erősödik a hadsereg modernizációja és a nemzetközi szövetségi kapcsolatok fejlesztése révén. A hadiipari fejlesztések – mint például új harckocsik, légvédelmi rendszerek és helikopterek beszerzése – jelentősen növelik az ország védekezőképességét és technológiai felkészültségét. Emellett a hazai hadiipari beruházások tovább fokozzák az önellátást, csökkentve a külső beszállítóktól való függést, miközben új munkahelyeket teremtenek. A NATO-tagság biztosítja a kollektív védelem előnyeit, míg a kiberbiztonság és technológiai hadviselés fejlesztése a modern hadviselés új kihívásaira készíti fel az országot, ezzel is hozzájárulva a hosszú távú védelmi stratégia fenntarthatóságához.

A NATO-tagság által biztosított kollektív védelem mellett a kiberbiztonsági és technológiai hadviselési képességek fejlesztése kulcsfontosságú a lakosság védelmében a modern kihívásokkal szemben, így például kibertámadások vagy információs háború esetén. Az ilyen technológiai fejlesztések lehetővé teszik a hatóságok számára, hogy gyorsabban és hatékonyabban reagáljanak a fenyegetésekre, minimalizálva a lakosság kockázatait és növelve a biztonság érzetét. Ez a komplex védelmi stratégia nemcsak a katonai erőt, hanem a civil társadalom védelmét is magában foglalja, összekapcsolva a katonai és civil erőforrásokat a lakosság széles körű védelmében.

A stratégiai mélységgel kapcsolatos hiányosságok kezelése

A stratégiai mélység hiányának kezelése bonyolult kihívás, amely különféle megközelítéseket igényel a nemzeti érdekek védelme és a nemzet stabilitásának fenntartása érdekében. A stratégiai mélység arra utal, hogy egy állam mennyire képes rugalmasan és erőforrásokban gazdagon reagálni a geopolitikai kihívásokra, illetve hogyan tudja megőrizni függetlenségét és érdekeit a nemzetközi szinten. Kenneth Waltz elmélete szerint a nemzetközi rendszer anarchikus, és az államoknak önérdekeik mentén kell mozogniuk, hogy megőrizzék szuverenitásukat és túléljenek a globális versengésben.¹⁷

Saját dinamizmusát korlátozó stratégia (időnyerés)

Ez a megközelítés azt jelenti, hogy az ország passzív, kivárára épít, és megpróbálja átvészelni a nemzetközi változásokat anélkül, hogy aktívan beavatkozna. Mearsheimer¹⁸ szerint ez a realizmus egyik gyakorlati megvalósulása, amikor egy állam elkerüli a közvetlen konfliktust, és időt nyer a nemzetközi környezet csillapodásáig. Az alábbi elemek jellemzik ezt a stratégiát:

- *Kivárá a nemzetközi dinamizmus csillapodásáig.* Az ország nem próbál meg aktív szerepet játszani a globális folyamatokban, inkább megfigyel és védekező pozíciót vesz fel. Ez a stratégia lehetőséget ad arra, hogy időt nyerjen, amíg a nemzetközi helyzet megnyugszik, és a nagyobb hatalmak elosztják a befolyásukat. Waltz szerint az ilyen stratégia különösen a kisebb hatalmakra jellemző, amelyek nem rendelkeznek elegendő katonai és gazdasági erővel a nemzetközi rendszert aktívan alakítani.¹⁹
- *Az élettér védelme.* Ebben az esetben az ország társadalma nem rendelkezik elég önbizalommal ahhoz, hogy formálja vagy irányítsa a saját fejlődését. Az erőforrások és a figyelem leginkább a meglévő élettér és a nemzeti határok védelmére összpontosul, ahelyett, hogy új lehetőségeket keresne a globális porondon.

Ezzel a stratégiával az ország hosszú távon fennmarad, de hátránya, hogy nem tud versenyképes pozíciót kialakítani, és gyakran csak a nagyobb erők árnyékában képes életben maradni. Kissinger szerint az ilyen kivárá és defenzív stratégia könnyen nemzetközi elszigeteltséghez vezethet, ha az ország nem tudja kihasználni a nemzetközi rendszer változásait.²⁰

Fontos megjegyezni, hogy Ahmed Davutoğlu, Törökország volt miniszterelnöke, esetében az „időnyerés” stratégia egyes értékelések szerint olyan helyzetekben is megfigyelhető volt, amikor a regionális konfliktusok, mint például a szíriai polgárháború vagy a kurd kérdés kezelése került napirendre. Ilyen esetekben az időnyerés

¹⁷ WALTZ 1979.

¹⁸ MEARSHEIMER 2001.

¹⁹ WALTZ 1979.

²⁰ KISSINGER 1994.

lehetőséget adott Törökországnak, hogy felmérje a nemzetközi közösség reakcióit, ugyanakkor lehetőséget biztosított számára a belpolitikai helyzet stabilizálására is.²¹

Saját dinamizmus feladása (sodródás)

Ez a megközelítés reaktív, alárendelt pozíciót tükröz, ahol az ország képtelen saját érdekeit érvényesíteni a nemzetközi szinten, ezért kiszolgáltatottá válik a nagyhatalmak és globális folyamatok befolyásának. Nye *soft power* elmélete alapján az ilyen országok inkább sodródnak, mintsem aktívan alakítanak a saját sorsukat, mivel nem rendelkeznek elegendő hatalommal vagy befolyással ahhoz, hogy hatékonyan érvényesítsék érdekeiket.²²

Jellemzői:

- *Nem tudja értelmezni a hatalmi tényezőket.* Az ország nem tudja pontosan meghatározni, hogy milyen erők formálják a világpolitikát, így nehézségei vannak saját dinamizmusa fókuszálásával.
- *Történelmi identitászavar.* Az ilyen országok gyakran szenvednek identitás-zavartól, mivel a belső és külső tényezők hatására elbizonytalanodnak nemzeti céljaikban és értékeikben. Huntington *A civilizációk összecsapása* című művében rámutat arra, hogy a globális hatalmi központok befolyása alatt álló országok gyakran elveszítik nemzeti identitásukat és történelmi perspektívájukat.²³
- *Nemzetközi hatalmi központok befolyása alatt áll.* Az országokat ebben a stratégiában gyakran külföldi hatalmi központok irányítják, és az ő érdekeik szerint mozognak, ami a nemzeti szuverenitás elvesztéséhez vezethet.
- *Sodródás.* Ahelyett, hogy határozott lépéseket tenne, az ország inkább sodródik a globális változások áramlásában, passzívan reagálva a külső eseményekre.
- *A helyi egzisztenciáról a globálisra lépés vágya.* Az ilyen országok gyakran álmodnak arról, hogy részesévé válnak a globális gazdaságnak, politikának, ám ezt nem saját erejükből, hanem más nagyhatalmak segítségével próbálják elérni.

Ez a stratégia rövid távon biztosíthat bizonyos előnyöket, de hosszú távon az ország elveszítheti autonómiáját, és kiszolgáltatottá válhat a nemzetközi politika alakulásának. Nye szerint a *soft power* hiánya ebben az esetben veszélyezteti a nemzeti szuverenitást és az önállóságot.²⁴

Saját dinamizmus a nemzetközi dinamizmus befolyásolására

Ez a megközelítés a proaktivitásra épít, ahol az ország aktívan befolyásolja a nemzetközi dinamikát, és jövőformáló szerepet vállal. Wendt konstruktív megközelítése szerint

²¹ DAVUTOĞLU 2014.

²² NYE 2004.

²³ HUNTINGTON 1996.

²⁴ NYE 2004.

az államok nem csupán passzív szereplők a nemzetközi rendszerben, hanem aktívan alakítják azt a saját identitásuk és érdekeik szerint.²⁵ Főbb jellemzői:

- *Jövőformáló potenciálok építése.* Az ország célja, hogy ne csak reagáljon a nemzetközi változásokra, hanem aktívan formálja azokat. Ez magában foglalja a nemzeti gazdaság, technológia, katonai képességek és diplomácia fejlesztését. Allison szerint az Egyesült Államok és Kína közötti verseny ezen jövőformáló potenciálokra épít, ahol mindkét ország arra törekszik, hogy alakítsa a globális rendszert.²⁶
- *A kínálkozó alkalom elmulasztása elszalasztott stratégiai lehetőség.* Ebben a dinamikában fontos felismerni, hogy az elérhető lehetőségek elmulasztása nagy stratégiai hibát jelenthet. Az országoknak képesnek kell lenniük gyorsan reagálni a változó helyzetekre.
- *Történelemépítés.* Az ország aktív részt vállal a nemzetközi politika formálásában, és olyan intézkedéseket tesz, amelyek történelmi jelentőségűek, akár globális szinten is.
- *Kockázatvállalás.* Ez a stratégia nagyobb kockázatot hordoz magában, hiszen az ország aktívan beavatkozik a nemzetközi politikába, és saját erőforrásait használja fel arra, hogy befolyásolja a világ alakulását.
- *Jövőépítés.* Az ország hosszú távú célja a saját jövője alakítása, ami egy olyan erős nemzet megteremtését célozza, amely képes a nemzetközi szinten is versenyképes maradni.

Ez a stratégia nagy elkötelezettséget, erőforrásokat és jövőorientált gondolkodást igényel, de lehetővé teszi az ország számára, hogy vezető szerepet töltsön be a globális szinten, és saját érdekei szerint formálja a világpolitikát.

Modernizáció és technológiai fejlesztések

Magyarország számára a technológia lehet az egyik kulcs a stratégiai mélység hiányának ellensúlyozásában. A modern haditechnika – például a precíziós rakéták, drónok, kibervédelmi rendszerek, légvédelmi rendszerek és radarrendszerek – lehetővé teszi, hogy az ország hatékonyabb védelmet nyújtson. A modernizáció érdekében Magyarország 2016-ban elindította a *Zrínyi honvédelmi és haderő-fejlesztési programot*, amely magában foglalja a hadsereg modernizálását és felszereltségének javítását. Ezek az eszközök lehetővé teszik, hogy az ország a területének méretéhez viszonyítva megfelelő katonai kapacitással rendelkezzen.

Létfontosságú kérdés, hogy reális és hiteles elrettentő/visszatartó katonai erővel, csapásmérő képességgel, önellátási hadiipari potenciállal, társadalmilag is megtámogatott haderővel rendelkezünk, ami a kor színvonalának megfelelő technikával, kiképzéssel és vezetési rendszerrel és filozófiával, megfelelő személyi és hadfelszerelési készlettel azonnal vagy rövid időn belül bevethető. A hatékony tartalékos rendszer

²⁵ WENDT 1999.

²⁶ ALLISON 2017.

kiépítése, felkészítése és felszerelése nélkülözhetetlen eleme a haderőnek, illetve megkerülhetetlen a lakosságvédelmi feladatok támogatása során is.

Lakosságvédelem tekintetében a földrajzi mélység hiányának következményei jelentősen mérsékelhetők a technológiai innovációval. A modern védelmi technológiák és korai figyelmeztető rendszerek fejlesztésével és alkalmazásával, a stratégiai fontosságú infrastruktúra, mint például kórházak és iskolák megerősítésével és katasztrófaállóságának növelésével, a lakosság rendszeres felkészítésével a veszélyhelyzetekre való reagálásra, például evakuációs gyakorlatokkal és elsősegélyképzésekkel.

Gyors reagálású erők és a mobilitás növelése, csapásmérő képesség kialakítása

Mivel Magyarország kis területű, fontos, hogy a védelmi erők gyorsan tudjanak reagálni és átcsoportosítani, ha szükséges. A nagy mobilitású új haditechnikai eszközök, a gyorsreagálású és különleges erők, valamint a légi szállítási kapacitás növelése segíthet abban, hogy az ország hadereje rugalmasan reagálhasson egy esetleges fenyegetésre, illetve a lakosságvédelmi feladatokban való közreműködésre. A mobil egységek, a helikopterek és drónok hatékony alkalmazása csökkentheti a területi hátrányokat. A csapásmérő képesség fejlesztése biztosítja, hogy az ország képes legyen hatékonyan elrettenteni, vagy megelőző lépéseket tenni fenyegetések esetén, ezáltal időt nyerni a lakosságvédelmi feladatok végrehajtására. A lakosságvédelem integrálása ezekbe a stratégiákba esszenciális. Ez magában foglalhatja a vészhelyzeti kommunikációs rendszerek fejlesztését, a lakosság számára szánt evakuációs terveket és az elsősegélynyújtási képzéseket. A lakosság felkészítése és tájékoztatása az őket érintő veszélyekről, valamint a hatékony evakuációs és mentési eljárások kidolgozása létfontosságú a vészhelyzetek hatékony kezelésében.

Szövetségi rendszerek erősítése (NATO, EU)

Magyarország NATO-tagsága kulcsfontosságú szerepet játszik a stratégiai mélység hiányának kezelésében. A NATO kollektív védelem alapelve szerint, egy ország elleni támadás esetén a szövetség minden tagja válaszlépéseket tehet. Ez azt jelenti, hogy Magyarország nem maradna egyedül egy esetleges támadással szemben. Ugyanígy az Európai Unióval való szoros együttműködés is segít abban, hogy a regionális stabilitás fenntartható legyen, és az ország biztonsági kihívásaira közös válaszokat lehessen találni. Ez a nemzetközi védelmi garancia lehetővé teszi, hogy Magyarország fokozza saját védelmi képességeit, miközben növeli a lakosság biztonságát és csökkenti a kiszolgáltatottságot. Az Európai Unióval való együttműködés tovább erősíti a regionális stabilitást, és lehetővé teszi a közös válaszok kidolgozását Magyarország biztonsági kihívásaira, ami szintén hozzájárul a lakosság átfogó védelméhez és a nemzeti biztonsági stratégia hatékonyságának javításához.

Diplomácia és regionális együttműködés

Magyarország számára a regionális együttműködés, különösen a szomszédos országokkal, alapvető a biztonság szempontjából. A határon túli magyar közösségek támogatása, valamint a velük kapcsolatos diplomáciai kérdések békés rendezése segít elkerülni a feszültségeket és konfliktusokat. Geostratégiai adottságaink szövetségi keretben és regionális szinten történő kihasználása csak úgy célszerű, ha az igazodik az ország törvényes rendjéhez, a nemzeti érdekeinkhez. Ez csak a *saját dinamizmus a nemzetközi dinamizmus befolyásolására* elvek alapján tud érvényesülni. Ez a megközelítés nemcsak a külpolitikai manővereket teszi hatékonyabbá, hanem hozzájárul a lakosság védelméhez is, mivel a külső és belső biztonsági fenyegetések csökkentésével növeli az országban élők biztonságérzetét.

Energiabiztonság és infrastruktúra-diverzifikáció

Magyarország nagymértékben függ az orosz földgáztól és más energiahordozóktól, ami geopolitikai sebezhetőséget jelenthet, különösen, hogy részben egy háború által sújtott országon keresztül érkeznek hozzánk ezek az energiahordozók. Az energiaellátás biztonsága kulcsfontosságú a stratégiai mélység növelésében, mivel egy energiaellátásból fakadó krízis megbéníthatná az ország védekezési képességeit. Az energiadiverzifikáció, különösen a megújuló energiaforrások és alternatív energiaszállítási útvonalak kiépítése (például déli gázvezetékek) csökkentheti ezt a függőséget. Ezek az intézkedések nemcsak hogy csökkentik a külső geopolitikai nyomást, hanem hozzájárulnak a lakosság védelméhez is, mivel biztosítják az energiaellátás folyamatosságát és stabilitását. Egy esetleges energiaellátási krízis esetén az ország képes maradhat a létfontosságú szolgáltatások biztosítására, így védelmezve a lakosság mindennapi életét és biztonságát.

Kritikus infrastruktúra decentralizálása és védelme

A stratégiai mélység hiányát részben azzal lehet ellensúlyozni, hogy az ország kulcsfontosságú infrastruktúráját – például energetikai, közlekedési, ipari és információs rendszereket – decentralizálják és megerősítik azok védelmét. Az infrastruktúra sebezhetőségének csökkentése és a katasztrófaállóság növelése elengedhetetlen, különösen a modern, hibrid hadviselés (például kibertámadások) korszakában.

A decentralizált infrastruktúra lehetővé teszi, hogy a lakosság számára létfontosságú szolgáltatások, mint az energiaellátás, a közlekedés és a kommunikáció, folyamatosan elérhetőek maradjanak még válsághelyzetek esetén is. A megerősített védelem biztosítása pedig közvetlenül hozzájárul a lakosság biztonságához, mivel minimalizálja azokat a kockázatokat, amelyek egy központosított infrastruktúra esetében fennállnak, például, hogy egyetlen támadáspont megbénítja az ország működését. Az ilyen lépések, amelyek az infrastruktúra diverzifikálását és erősítését célozzák,

kulcsfontosságúak a lakosság védelme szempontjából, mivel növelik az ország ellenálló képességét és csökkentik a sebezhetőséget.

Rezilienciaépítés

A stratégiai mélység problémájának kezelése Magyarország számára elsősorban a társadalom bevonásával és a reziliencia építésével érhető el.

A reziliencia Magyarország azon képességét jelenti, amely lehetővé teszi, hogy megőrizze szuverenitását, gazdasági stabilitását, kulturális identitását és közösségeinek kohézióját a globális kihívások és válságok közepette, miközben biztosítja állampolgárainak biztonságát és jólétét.

A reziliencia építése, mint stratégia, azon képesség megerősítését célozza, hogy a társadalom és az ország jobban ellenálljon a különböző kihívásoknak, legyen szó természeti katasztrófákról, katonai fenyegetésekről vagy gazdasági válságokról. Ennek részeként a kritikus infrastruktúra, például az energiahálózatok megerősítése és diverzifikálása, valamint a közösségi ellenálló képesség fejlesztése kulcsfontosságú. Mindezek hozzájárulnak ahhoz, hogy a lakosság mindennapjai biztonságosabbak és stabilabbak legyenek, csökkentve ezzel a sebezhetőséget és növelve a közösségi biztonságérzetet.

A reziliencia építése nemcsak a katonai és biztonsági képességeket erősíti, hanem a lakosság védelmét is közvetlenül segíti, támogatva Magyarország hosszú távú stabilitását és adaptációs képességét a modern világ kihívásaival szemben.

Példaként említhető a haderő társadalmasítása, ami azt jelenti, hogy a civil lakosságot és a katonai szektort szorosabb együttműködésbe kell vonni, ami fokozza a biztonság iránti közös felelősségvállalást és a hazafias elköteleződést. Ez lehetőséget ad a társadalom szélesebb rétegeinek, hogy hozzájáruljanak a nemzet védelméhez, például tartalékos haderő formájában vagy különféle önkéntes programokon keresztül.

Lakosságvédelmi konklúziók összefoglalása

A lakosságvédelmi feladatokat a végrehajtás módszere szerint két részre bonthatjuk: egyéni és csoportos védelemre. A csoportos védelem egy másik elterjedt elnevezése a kollektív védelem.²⁷

Az egyéni védelemben a lakosság személyi védőeszközökkel történő ellátása mellett beleértendők a légzés- és bőrvédelmi felszerelések, a veszélyeztető hatások egyénre gyakorolt terhelésének mérésére szolgáló eszközök alkalmazása, valamint ezek mellett a lakosság azon egészségügyi vakcinális, illetve egyéb beviteli módszerű anyagokkal való ellátása is, amelyekkel a veszélyeztető hatás megelőzhető, az egyén immunitása kialakítható, vagy a maradandó károsodás elhárítható.

A csoportos lakosságvédelmi feladatokat helyi és távolsági védelemre lehet még szétválasztani. Helyi védelem az elzárkóztatás és az óvóhelyi elhelyezés, távolsági

²⁷ NAGY 2019.

védelem a kitelepítés, kimenekítés, kiürítés és az ezekhez kapcsolódó befogadás és visszatelepítés.²⁸ Ez kötődik ahhoz a lakosságvédelmi alapfelvetéshez, hogy vagy a veszélyforrást kell mitigálni, vagy a lakosságot kell távol tartani.

Magyarország, földrajzi és stratégiai helyzete miatt, különleges kihívásokkal szembesül a lakosságvédelem terén, különösen a stratégiai mélység földrajzi hiánya miatt, ami a lakosság veszélyforrásoktól való távoltartását vagy a távolsági védelem megtervezését erősen korlátozza. Példaként említhető, hogy a Nemzetközi Atomenergia Ügynökség Biztonsági Szabványok Sorozata²⁹ az azonnali evakuációs zónán kívüli területek, jellemzően 30–80 kilométeres távolságban, Sugárzási Megfigyelési Zónák lehetnek. Ezeken a területeken sugárzási megfigyelési intézkedéseket és védelmi intézkedéseket, beleértve a lehetséges kitelepítést, kell mérlegelni a fennálló körülmények és a potenciális radiológiai kockázatok alapján. Ennek megfelelően a lakosságot legalább 80 km-es távolságra kell kitelepíteni, ami, ha figyelembe vesszük, hogy az Észak–Dél távolság a Paks vonalon ~220 km, a 80 km-es távolság pedig a körköröségi elven átmérőre számítva 160 km, máris látszik, milyen behatároló tényező a földrajzi paraméter a lakosságvédelem tekintetében.

Az ország védelmi képességének növelése érdekében kulcsfontosságú az infrastruktúra, beleértve a közlekedési, kommunikációs és energiaellátó rendszerek modernizálását és megerősítését, amelyek növelik a gyors reagálás lehetőségét és az ország általános ellenálló képességét válsághelyzetekben. A katasztrófavédelmi és honvédelmi képességek, mint a mentőcsapatok képzése és a válságkezelő központok fejlesztése, szintén fontosak a lakosság védelme, illetve a bekövetkezett események következményeinek csökkentése szempontjából.

A technológiai innovációk, mint a korai figyelmeztető rendszerek és a drónok, javítják a fenyegetések észlelését és kezelését, miközben a nemzetközi együttműködés, különösen a NATO-val való kapcsolatok, biztosítják a kollektív védelmi előnyöket és a technológiai együttműködést. Ezek az intézkedések segítenek Magyarországnak a stratégiai mélység hiányának kompenzálásában általánosságban, illetve ezen keresztül közvetve a lakosságvédelmi tevékenységek hatékonyságának növelésében.

A demográfiai és társadalmi stratégiák, mint a vidéki területek népességmegtartó képességének növelése és az urbanizáció kezelése, szintén fontosak a társadalmi kohézió és ezáltal a lakosság védelmének növelése érdekében. Ezenkívül a lakosság felkészítése, a fiatal nemzedék oktatása és tájékoztatása a veszélyhelyzetek kezelésére vonatkozóan növeli a társadalmi támogatottságot és az általános társadalmi felkészültségi szintet.

A kulturális stratégiai mélység közvetetten, de jelentős módon hat a lakosságvédelemre. A közösség kulturális háttere, hagyományai, szociális kohéziója, helyi tudása és nemzeti identitása mind befolyásolja a lakosság felkészültségét, reakálási képességét és ellenálló képességét vészhelyzetek esetén. A sikeres lakosságvédelemnek figyelembe kell vennie ezeket a kulturális tényezőket, hogy hatékonyan meg tudja védeni az embereket és értékeiket.

²⁸ NAGY 2019.

²⁹ IAEA 2015.

Az összehangolt lakosságvédelmi stratégia, amely magában foglalja ezeket az elemeket, elengedhetetlen Magyarország hosszú távú biztonságának és stabilitásának fenntartása érdekében.

Felhasznált irodalom

- ALLISON, Graham (2017): *Destined for War: Can America and China Escape Thucydides's Trap?* Boston: Houghton Mifflin Harcourt.
- BASSIN, Mark (1987): Imperialism and the Nation State in Friedrich Ratzel's Political Geography. *Progress in Human Geography*, 11(4), 473–495. Online: <https://doi.org/10.1177/030913258701100401>
- BERNEK Ágnes [Rubicon Történelem] (2024): Az eurázsiai fogalom változásai. *YouTube*, 2024. január 12. Online: www.youtube.com/watch?v=jeYEorTQdCw
- BLACK, Jeremy (2009): *Geopolitics and the Quest for Dominance*. [H. n.]: Indiana University Press.
- DAVUTOĞLU, Ahmet (2014): *Stratégiai mélység: Törökország nemzetközi helyzete*. Budapest: Antall József Tudásközpont.
- FRIEDMAN, Thomas L. (1990): *From Beirut to Jerusalem*. New York: Farrar, Straus and Giroux.
- FRIEDMAN, George (2009): *The Next 100 Years: A Forecast for the 21st Century*. New York: Doubleday.
- GADDIS, John Lewis (2005): *The Cold War: A New History*. New York: The Penguin Press. Online: <https://ia803100.us.archive.org/33/items/thecoldwaranewhistory/The%20Cold%20War%20%20a%20new%20history.pdf>
- HERWIG, Holger H. (1999): Geopolitik: Haushofer, Hitler and Lebensraum. *The Journal of Strategic Studies*, 22(2–3), 218–241. Online: <https://doi.org/10.1080/01402399908437762>
- HUNTINGTON, Samuel (1996): *The Clash of Civilizations and the Remaking of World Order*. New York: Simon & Schuster.
- IAEA Safety Standards Series No. GSR Part 7 (2015). Vienna: International Atomic Energy Agency. Online: https://www-pub.iaea.org/MTCD/Publications/PDF/P_1708_web.pdf
- KAPLAN, Robert D. (2012): *The Revenge of Geography*. New York: Random House. Online: <https://archive.org/details/TheRevengeOfGeographyWhatTheMap-TellsUsAboutComingConflictsAndTheBattleAgainstFate>
- KENNEDY, Paul (1987): *The Rise and Fall of The Great Powers: Economic Change and Military Conflict from 1500 to 2000*. New York: Random House. Online: <https://cheirif.files.wordpress.com/2015/08/paul-kennedy-the-rise-and-fall-of-the-great-powers-19891.pdf>
- KISSINGER, Henry (1994): *Diplomacy*. New York: Simon & Schuster.
- MACKINDER, Halford J. (1904): The Geographical Pivot of History. *The Geographical Journal*, 23(4), 421–437. Online: <https://doi.org/10.2307/1775498>
- MAHAN, Alfred Thayer (1890): *The Influence of Sea Power upon History 1660–1783*. Boston: Little, Brown and Co.

- MEARSHEIMER, John (2001): *The Tragedy of Great Power Politics*. New York – London: Norton.
- MITCHELL, Martin D. (2020): Using the Principles of Halford J. Mackinder and Nicholas John Spykman to Reevaluate a Twenty-First-Century Geopolitical Framework for the United States. *Comparative Strategy*, 39(5), 407–424. Online: <https://doi.org/10.1080/01495933.2020.1803709>
- NAGY Sándor (2019): *A lakosságvédelmet érintő kockázatelemzés és kockázatkezelés fejlesztése*. PhD-értekezés. Nemzeti Közszerológati Egyetem. Online: <https://doi.org/10.17625/NKE.2019.030>
- NYE, Joseph S. (2004): *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.
- TOAL, Gerard (1996): *Critical Geopolitics: The Politics of Writing Global Space*. Minneapolis: University of Minnesota Press.
- TSYGANKOV, Andrei P. (2013): *Russia's Foreign Policy: Change and Continuity in National Identity*. Lanham: Rowman & Littlefield. Online: https://archive.org/details/russiasforeignpo0000tsyg_c5y0
- WALTZ, Kenneth N. (1979): *Theory of International Politics*. Reading, MA: Addison-Wesley Publishing Company. Online: https://dl1.cuni.cz/pluginfile.php/486328/mod_resource/content/0/Kenneth%20N.%20Waltz%20Theory%20of%20International%20Politics%20Addison-Wesley%20series%20in%20political%20science%20%20%20%201979.pdf
- WENDT, Alexander (1999): *Social Theory of International Politics*. Cambridge: Cambridge University Press. Online: www.guillaumenicaise.com/wp-content/uploads/2013/10/Wendt-Social-Theory-of-International-Politics.pdf

István Mihály¹

Estimating the Air Leakage Rate of Smoke Control Doors for Calculations Procedures, Part 2

Abstract

The extent of smoke spread during building fires is critical, as it can adversely affect both evacuation and firefighting intervention. Smoke migration can occur through structural gaps, the potential for which should be minimised. One way to exclude smoke is to pressurise the structure, and an important starting parameter for the design of this is to know the leakage areas. The need for knowledge of the size of structural gaps has been high since the inception of design methods. This article aims to identify the potential for improving the calculation procedures by using the results of measurements on existing smoke control doors in pressurised vestibules. In this section, the author compares the results of two different measurement methods with a series of measurements in a pressurised vestibule. Using computational procedures, the air flow coefficient and leakage area of the single-leaf smoke control doors under investigation are estimated. Suggestions are made for possible improvements to the design methods.

Keywords: smoke control door, leakage area, air flow coefficient, stairwell pressurisation, fire safety design

Introduction

The first part of this article highlighted the risk of uncontrolled spread of smoke and toxic combustion gases from fires in buildings, posing a threat to evacuation and the safety of those fleeing. One concept of evacuation in complex buildings is phased evacuation, whereby the complete evacuation of the building is prolonged over time. In some cases, where there are persons who are unable to use the stairs

¹ Certified Fire Protection Specialist, Judicial Expert, CEO, Brandplan Kft.; PhD student, Doctoral School of Military Engineering, Ludovika University of Public Service, e-mail: m.istvan@brandplan.hu

independently, it may be necessary to create temporary protected spaces.² One way of doing this may be to provide a separate room with a fire and smoke barrier of a specified performance.³

Pressurisation is the technical method of supplying a defined amount of fresh air into the space to be protected (e.g. stairwell, vestibule, etc.) to create a relative overpressure. Air is then flowed out of the pressurised space through gaps in the structure, through door gaps, which keeps out smoke and toxic combustion products.⁴ When designing the stairwell pressurisation, the leakage that will occur must be estimated.⁵ Since doors play a particularly important role in leakage losses, it is important to know the gap dimensions as accurately as possible.⁶

Even early research was concerned with estimating the amount of air flowing through door gaps at various pressure differentials. The size of the leakage area is an important input parameter both for manual calculations and for computer programmes. One method is the orifice method, where the gaps are considered in the calculations as a numerical value expressed in terms of surface area. In the descriptive equation for doors, the discharge coefficient is typically 0.65 and the flow exponent is 0.5.⁷ The air leakage coefficient and gap length can be used to characterise the air flow through the gaps in the openings, which is also a traditional parameter for air leakage through windows and doors in Hungary and in Poland, as well.⁸

In one of Tamura's paper about a computer study of smoke movement, the equivalent flow area for stairwell doors was 0.0185 m².⁹ Based on air leakage tests on installed doors, Hobson and Stewart estimate the equivalent flow area to be 0.01–0.02 m² for single-leaf doors.¹⁰ BS 5588-4 also recommends using a leakage area of 0.01–0.02 m² depending on the direction of door opening.¹¹ This recommended value has been retained in EN 12101-6 and EN 12101-13.¹²

Klote et al. gave flow areas of gaps values for single-leaf doors in tabular form, which can be used in the orifice equation with a flow coefficient of 0.65. For doors 2.13 m high, 0.914 m wide and 44.5 mm thick, the typical value is 0.0073–0.0428 m² depending on the thickness of the gaps above and below the door.¹³

The approach in length of the gaps in Hungary is suggested by the Fire Protection Technical Guideline in the field of Protection against Heat and Smoke Spread (TvMI) with an air flow coefficient value of 1.11 and a flow exponent of 0.67.¹⁴ In the literature reviewed in the first part of this article, there is a significant variation with

² National Directorate General for Disaster Management 2024: 38–42.

³ Decree 54/2014 (XII. 5.) of the Ministry of the Interior.

⁴ BUTCHER–PARNELL 1979: 109–111; BÉRCZI–BADONSKZI 2021: 66–96.

⁵ International Code Council and Society of Fire Protection Engineers 2022: 208.

⁶ GROSS 1991: 171–177.

⁷ MARTIN 1970: A4-3.

⁸ LIS–LIS 2021; BAUMANN 2005: 28–30.

⁹ TAMURA 1970.

¹⁰ HOBSON–STEWART 1972: 47–56.

¹¹ British Standards Institution 1978: 145; British Standards Institution 2004: 66.

¹² CEN 2005b: 88–91; CEN 2022: 67.

¹³ KLOTE et al. 2012: 119; KLOTE et al. 2024: 56.

¹⁴ National Directorate General for Disaster Management 2025: 51–52.

air flow coefficient values between 1 and 9 for doors.¹⁵ The problem is that there is little literature data available on the values of air leakage coefficients.¹⁶

The fire prevention solutions presented in this publication provide an opportunity to prevent or reduce the harmful effects of a possible fire on health.¹⁷ The examination of the harmful effects shows similarities with the consequences of toxic combustion products produced in an industrial environment like chemical warehouses.¹⁸ Additional technical solutions can be fire protection signalling systems, the development of which provides many new solutions in the field of property protection and fire protection.¹⁹ Finally, we can learn important practical lessons for the development of fire protection authority activity when dealing with the policing issues of event order security.²⁰

Results

In a recent paper by Mihály et al., the airtightness of single-leaf smoke control doors was investigated by measurements on existing doors.²¹ The findings of these measurements and other conclusions that can be drawn from the measurement results are presented below.

Comparison of measurement methods – Blower door and funnel with vane probe

The measurement methods recommended by the harmonised standard for determining the air permeability of buildings include the Blower Door and air permeability measurement using the building's own ventilation system.²²

Before starting to measure the air permeability of the vestibules and doors with a funnel and a vane probe, the air permeability of the building's own ventilation system was tested to see how it agreed with the measurements made with the Blower Door method. This provides information on how the results of the funnel measurement relate to the measurement results recorded by the Blower Door instrument.

During the tests with the Blower Door, the instrument was installed in a door of the vestibule. For the funnel with vane probe measurements, the Blower Door was removed, the door was closed and the door gaps were taped to ensure conditions were nearly identical. The funnel kit consisted of a measuring funnel with a sealed rim, a flow straightener and a vane probe. The differential pressure was recorded by a tube passed through a gap in the structure under test. A comparison of the measured values is illustrated in Figure 1.

¹⁵ HOBSON-STEWART 1972: 47–56; RECKNAGEL et al. 2000: 882–891; VÁRFALVI s. a.; BARNÁ 2015; GÁBOR-ZÖLD 1981: 130–131; LIDDAMENT 1986: 6.25; ÉSZK 1984: 6–7.

¹⁶ BAUMANN 2011.

¹⁷ ALMÁSI et al. 2022.

¹⁸ BERGER et al. 2024.

¹⁹ KÁTAI-URBÁN 2023.

²⁰ KANYÓ – VÁSÁRHELYI-NAGY 2021.

²¹ MIHÁLY et al. 2025.

²² CEN 2016: 17–18.

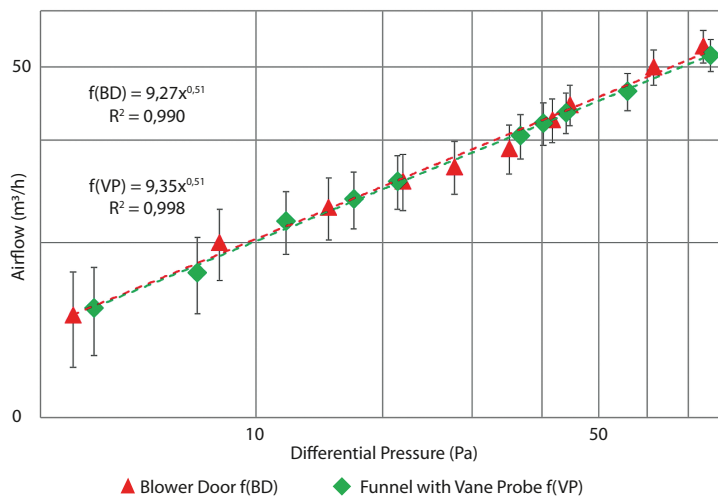


Figure 1: Comparison of measurement results

Source: compiled by the author based on MIHÁLY et al. 2025

Each opening in the building envelope, however, is often described by the power law equation as shown in equation (1).²³

$$= c \times (\Delta p)^n \quad (1)$$

where

- Q – is the airflow through opening (m^3/s)
- c – is the flow coefficient ($\text{m}^3\text{s}^{-1}\text{Pa}^{-n}$)
- n – is the pressure exponent, dimensionless
- Δp – is the pressure difference (Pa)

Applying the energy law equation, the pressure exponent of the two series of measurements was found to be the same, 0.51. This suggests that turbulent flows dominated during the measurements. The value of the flow coefficient is also nearly the same, which suggests good agreement between the two measurements made under identical conditions using two different measurement methods. This indicates that the vestibules' own ventilation system and the funnel kit with vane probe measurement may be adequate for air tightness testing.

Estimation of leakage area

In the first series of measurements, the gaps around the doors opening into the hallway and the doors opening from the hallway were taped. In this case, the amount of air supplied through the disc valve flowed through the structural gaps, assuming that the amount of air leaking through the adhesive tape was negligible.

²³ OWEN 2017: 16.15.

The measurements were carried out at a pressure differential of 10–15–25–50–75 Pa. A manually adjustable disc valve is used to adjust the amount of air required to maintain the specified pressure level. The volume of air supplied, the pressure differential produced and the ambient conditions were then recorded.

From the resulting differential pressure and volume flow pairs, the estimated surface area of the structures surrounding the vestibules can be expressed using the recommendation in Annex A of EN 12101-13. In practice, this means all surfaces of wall structures and floors. Table 1 summarises the structural surfaces calculated for each vestibule.

Table 1: Average effective leakage area of structures

Vestibule	Average effective leakage area of walls + floors (m²)
6 th Floor, Section A	0.001067
6 th Floor, Section B	0.001285
5 th Floor, Section A	0.001084
5 th Floor, Section B	0.001108
4 th Floor, Section A	0.001261
4 th Floor, Section B	0.001151
3 rd Floor, Section A	0.001087
3 rd Floor, Section B	0.001145
2 nd Floor, Section A	0.001123
2 nd Floor, Section B	0.001043
1 st Floor, Section B	0.001055
Mean	0.00113

Source: compiled by the author based on MIHÁLY et al. 2025

The wall area of the examined vestibules was 14.07 m², while the total floor and ceiling area was 5.76 m². By using these values, it is possible to compare how the measured values agree with the values of the leakage areas recommended by EN 12101-13 for walls and floors.²⁴ According to the standard, the leakage area ratio for stairwell walls is 1.1×10^{-4} , while for floors it is 5.2×10^{-5} . Taking these values into account, using the estimation method proposed in the standard, the estimated wall and floor area of the vestibule can be calculated using formulae (2) and (3).

$$A_{LW} + A_{LF} = (A_{LW}/A_{WALL}) \times A_{WALL} + (A_{LF}/A_{FLOOR}) \times A_{FLOOR} \tag{2}$$

$$A_{LW} + A_{LF} = 1.1 \times 10^{-4} \times 14.07 \text{ m}^2 + 5.2 \times 10^{-5} \times 5.76 \text{ m}^2 = 0.00185 \text{ m}^2 \tag{3}$$

where
 A_{LW} – is the total wall leakage area (m²)
 A_{LF} – is the total floor leakage area (m²)

²⁴ CEN 2022: 70–71.

A_{LW}/A_{WALL} – is the leakage area ratio for walls, dimensionless

A_{LF}/A_{FLOOR} – is the leakage area ratio for floors, dimensionless

From the above calculation, it can be seen that the gap area estimated by the standard is in good agreement with the value calculated from the measurements, and lies between the tight and average ranges.

The measurements were then taken on each door. To do this, the adhesive tape had to be removed from the gaps of the door under test. Air was then supplied to the vestibule, which flowed through the walls, floor and through the gaps of the door under test. Under these conditions, the amount of air to be introduced to maintain the given pressure differential and the ambient data were recorded at a pressure differential of 5–10–15–25–50–75 Pa, set by a manually adjustable disc valve. Using the estimation method of the standard, the amount of air flowing through the door gaps at a given pressure differential could be estimated from the difference between the total air introduced and the air flowing through the walls and floors. From the air volume thus determined, the leakage area of the door could be estimated for a given pressure difference. The results of the measurements taken in each of the vestibules are shown in Table 2.

Table 2: Average effective leakage area of doors

Vestibule	Average effective leakage area of doors	
	into pressurised space (m2)	from pressurised space (m2)
6 th Floor, Section A	0.00315	0.00428
6 th Floor, Section B	0.00354	0.00367
5 th Floor, Section A	0.00331	0.00372
5 th Floor, Section B	0.00376	0.00379
4 th Floor, Section A	0.00325	0.00346
4 th Floor, Section B	0.00391	0.00442
3 rd Floor, Section A	0.00326	0.00340
3 rd Floor, Section B	0.00358	0.00373
2 nd Floor, Section A	0.00378	0.00382
2 nd Floor, Section B	0.00523	0.00424
1 st Floor, Section B	0.00400	0.00312
Mean	0.00371	0.00379
	0.00375	

Source: compiled by the author based on MIHÁLY et al. 2025

Based on the measurement results, the air leakage area of the single-leaf smoke control doors was 0.00375 m². The values measured showed no significant difference in whether the doors opened into the pressurised vestibule or from the pressurised vestibule. The leakage area of 95.5% of the tested smoke control doors fell within two standard deviations of the mean value.²⁵

²⁵ MIHÁLY et al. 2025.

Estimation of air leakage coefficient

Using the differential pressure and volume flow values from the series of measurements, the gap length of the doors can be used to determine the air leakage coefficient of a given door. The gap factor describes how much air flows through a gap of 1 metre in length of a window or door due to a unit pressure difference.

The volume of air leaking through the doors was determined using the power law equation. For various differential pressures, the amount of air flowing through the structures of the vestibule is known. The volume of air flowing through the door can be estimated as the difference between the volume of air flowing through the door and the structure as a whole and the volume of air flowing through the structure at a given pressure.

The length of the gap was 6.106 m for the door opening into the vestibule and 5.940 m for the door opening from the vestibule. The surface area of the doors was 2.03 m² for the door opening into the vestibule and 1.89 m² for the door opening from the vestibule.

For all doors, the air leakage coefficient has been determined taking into account the calculation procedure proposed by the TvMI. The calculated values are given in Table 3.

Table 3: Average air leakage coefficient of doors

Vestibule	Average air leakage coefficient of doors m ³ /(hPa ^{0.67})	
	into pressurised space (CV)	from pressurised space (VC)
6 th Floor, Section A	0.99	1.39
6 th Floor, Section B	1.08	1.15
5 th Floor, Section A	1.02	1.18
5 th Floor, Section B	1.19	1.22
4 th Floor, Section A	0.99	1.09
4 th Floor, Section B	1.19	1.38
3 rd Floor, Section A	1.00	1.06
3 rd Floor, Section B	1.05	1.13
2 nd Floor, Section A	1.16	1.21
2 nd Floor, Section B	1.57	1.29
1 st Floor, Section B	1.18	0.95
Mean	1.13	1.19
	1.16	

Source: compiled by the author

The results show that there is no significant difference in the value of *c* for doors opening to the vestibule and doors opening from the vestibule. 95.5% of the values are within two standard deviations of the mean value.

Figure 2 shows the calculated value of *c* per door tested. The orange line in Figure 2 shows the average of the calculated values (1.16) and the *c* value proposed by the TvMI (1.11). It can be seen that some of the measured values are above the

currently proposed value of 1.11, i.e. there was a slightly higher leakage than the one given in the design formula.

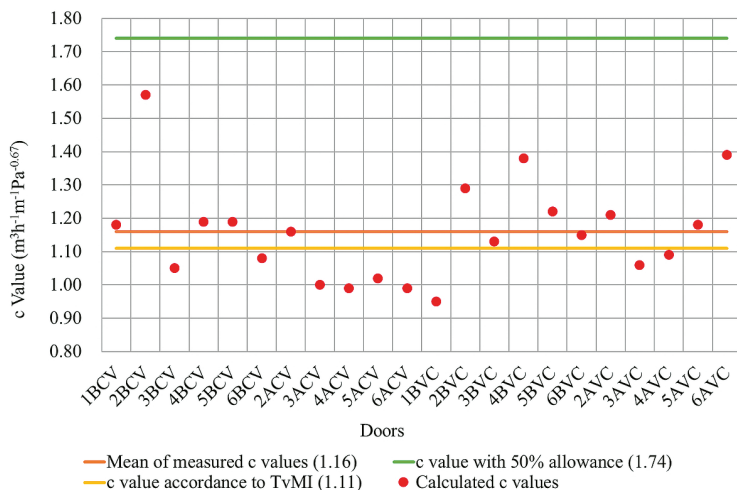


Figure 2: c values according to the TvMI and based on measurement results

Source: compiled by the author

If we increase the measured values of c by an uncertainty factor of 50%, we obtain an air leakage coefficient of 1.74 (green line), which covers all measured values with a high degree of confidence.

For the comparability of the calculated values, the air permeability coefficient was determined by taking into account the exponent $2/3$. Figure 3 illustrates these values.

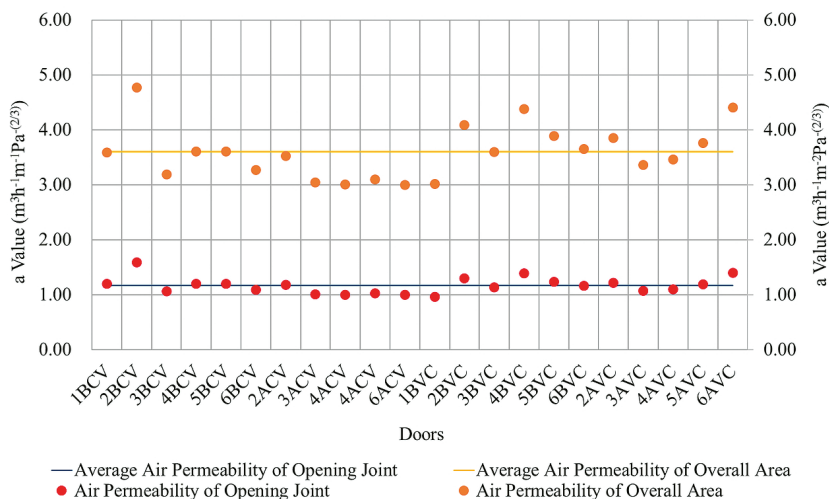


Figure 3: Air leakage coefficients

Source: compiled by the author

On the left axis, the air leakage coefficient is given for the length of opening joint, which is $1.17 \text{ m}^3/(\text{hmPa}^{2/3})$. On the right axis, the air leakage coefficient is given for the total surface area of the doors, which is $3.6 \text{ m}^3/(\text{hm}^2\text{Pa}^{2/3})$.

Discussion

The initial tests compared the results measured by the Blower Door instrument with the results measured by the funnel with vane probe. In the case of the Blower Door instrument, the supply air was provided by the instrument fan. In the case of the funnel with vane probe, the building's own ventilation system provided the air supply. The comparative measurements showed a good agreement, which confirmed the technical solution proposed by EN ISO 9972 that the building air ventilation system can be used to perform the air permeability measurements. Based on these tests, the results of the funnel type volumetric flow metre were considered usable for further measurements.

Once the amount of air flowing through the vestibule doors at a given pressure was measured, the leakage area of the doors could be calculated. The resulting value of 0.005 m^2 is less than the value recommended by the relevant literature, EN 12101-13, EN 12101-6 and BS 9944. It is half the recommended value of 0.01 m^2 for doors opening into a pressurised space and a quarter of the recommended value of 0.02 m^2 for doors opening from a pressurised space. This value is also lower than the values proposed by Hobson and Stewart. The value of 0.005 m^2 was independent of the direction of the opening of the doors, which is in accordance with the standard for the testing and classification of smoke control doors, which requires that smoke control doors meet the air tightness requirement from all sides, regardless of the direction of opening. The air leakage through the doors at a pressure differential of 25 Pa ranged from 48 to $67 \text{ m}^3/\text{h}$, which is well below the $3 \text{ m}^3/\text{h}/\text{m}$ specified by the classification standard for the leakage length at ambient temperature. It is important to note that the test standard ignores leakage under the doors.

The resulting air leakage coefficient value of 1.16 is in good agreement with the current TvMI, but it should be noted that it exceeds the value of 1.11 , which suggests that the TvMI value could be corrected or increased by a safety factor. Values in the relevant literature vary widely, ranging from 1 to $9 \text{ m}^3/(\text{hmPa}^{2/3})$. The air leakage coefficient 1.17 , calculated with a factor of $2/3$, is in good agreement with the proposed air leakage coefficient of the doors with threshold described by Várfalvi, Gábor-Zöld and Barna.²⁶ This value is much more favourable than the value between 4 and 9 considered for doors without threshold and lower than the value proposed in ME-04-132-84.²⁷

Based on the results obtained, it is urged that the leakage area values recommended in Annex A of EN 12101-13 be added. For single-leaf smoke control doors, regardless of their opening direction, a leakage area of 0.005 m^2 can be considered

²⁶ VÁRFALVI S. A.; BARNÁ 2015; GÁBOR-ZÖLD 1981: 130–131.

²⁷ ÉSZK 1984: 6–7.

up to a maximum perimeter of 6.1 m at a pressure differential of 10–50 Pa at ambient temperature.

For the calculation method used in the TvMI, a minimum increase in c is recommended. Based on the measured values, it is recommended to increase the value of the air flow coefficient by a safety factor in the calculations to take into account the uncertainty depending on the quality of the installation.

Given that the tests are carried out on one type of door, it is recommended that several different door designs and geometries be tested in the future. It is necessary to test a wider range of doors, which should include double doors, windows, glazed facades and lift landing doors.

Conclusion

Based on the studies supported by the measurements, the following conclusions can be drawn:

- Based on comparative measurements with the Blower Door instrument, funnel with vane probe measurement with the building's own ventilation system can be a suitable method for measuring air permeability.
- The values proposed by EN 12101-13 for the leakage area for walls and floors were in good agreement with the values measured in the vestibules tested.
- It is proposed to supplement the table of leakage area values for doors in EN 12101-13. For smoke control doors, regardless of whether they open into or out of the pressurised compartment, 0.005 m². This value may be taken into account up to a leakage perimeter of 6.1 m, between 10 and 50 Pa and at ambient temperature margins.
- The value of the air leakage coefficient determined by the TvMI showed good agreement with the measured value. However, it is recommended to increase the coefficient by a safety factor to take into account uncertainties due to installation conditions.
- In accordance with the additional classes S_{a3} and S_{a4} defined in EN 13501-2, it is also proposed to amend the test standard to allow for S_{a3} and S_{a4} tests. A corresponding amendment to the EN 15269-20 standard is also proposed.²⁸

The results of the tests can be used in the design of air supply systems for pressurised smoke-free staircases and pressurised smoke-free vestibules. The recommendations cover both the estimation methods recommended in Annex A of EN 12101-13 and those recommended by the TvMI. The proposal to amend the test standard may help in the future application of the classification standard.

²⁸ CEN 2023: 52–53; CEN 2005a; CEN 2021.

References

- ALMÁSI, Csaba – CIMER, Zsolt – KÁTAI-URBÁN, Lajos – VASS, Gyula (2022): Prevention of Terrorist Attacks during the Transport of Dangerous Goods by Road in Hungary. *American Journal of Research Education and Development*, (2), 2–10.
- BARNA, Lajos (2015): *Tűzelőberendezések égési levegő ellátása*. Előadás. „A szén-monoxid mérgezések hatékony megelőzése” Országos szakmai konferencia, Budapest, 5 March 2015. Online: www.vedelem.hu/files/UserFiles/File/aktualis/20150403/04.pdf
- BAUMANN, Mihály (2005): Tűzelőberendezések légellátása. *Magyar Installateur*, 15(10–11), 28–30.
- BAUMANN, Mihály (2011): *Épületek légforgalma*. 17th “Building Services, Mechanical and Building Industry Days” International Conference, Debrecen, 13–14 October 2011. Online: www.e-gepesz.hu/files/cikk9422_EUG_Baumann.pdf
- BÉRCZI, László – BADONSZKI, Csaba (2021): A tűzvédelmi tervezés fő tartópillérei a tűzvédelmi műszaki irányelvek. *Védelem Tudomány*, 6(2), 66–96. Online: <https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13473>
- BERGER, Ádám – KÁTAI-URBÁN, Lajos – NÉMETH, Zsolt – ZSITNYÁNYI, Attila – KÁTAI-URBÁN, Maxim – CIMER, Zsolt (2024): Applicability of Design Methodology for the Remediation Bund of Flammable Dangerous Liquid Storage Tanks. *Fire*, 7(7). Online: <https://doi.org/10.3390/fire7070246>
- British Standards Institution (1978): *BS 5588-4:1978 Fire Precautions in the Design and Construction of Buildings*. Part 4. Code of Practice for Smoke Control in Protected Escape Routes Using Pressurisation. London: British Standards Institution.
- British Standards Institution (2004): *BS 5588-4:1998 + A2:2004 Fire Precautions in the Design, Construction and Use of Buildings*. Part 4. Code of Practice for Smoke Control Using Pressure Differentials. London: British Standards Institution.
- BUTCHER, Edward G. – PARNELL, Alan C. (1979): *Smoke Control in Fire Safety Design*. London: E. & F. N. Spon Ltd.
- CEN (2005a): *EN 1634-3:2005 Fire Resistance Tests for Door and Shutter Assemblies*. Part 3. Smoke Control Doors and Shutters. Brussels: Technical Committee of the European Committee for Standardisation.
- CEN (2005b): *EN 12101-6:2005 Smoke and Heat Control Systems*. Part 6. Specification for Pressure Differential Systems. Kits. Brussels: Technical Committee of the European Committee for Standardisation.
- CEN (2016): *EN ISO 9972:2016 Thermal Performance of Buildings*. Determination of Air Permeability of Buildings. Fan Pressurization Method (ISO 9972:2015). Brussels: Technical Committee of the European Committee for Standardisation.
- CEN (2021): *EN 15269-20:2021 Extended Application of Test Results for Fire Resistance and/or Smoke Control for Door, Shutter and Openable Window Assemblies, Including Their Elements of Building Hardware*. Part 20. Smoke Control for Doors, Shutters, Operable Fabric Curtains and Openable Windows. Brussels: Technical Committee of the European Committee for Standardisation.
- CEN (2022): *EN 12101-13:2022 Smoke and Heat Control Systems*. Part 13. Pressure Differential Systems (PDS). Design and Calculation Methods, Installation, Accep-

- tance Testing, Routine Testing and Maintenance. Brussels: Technical Committee of the European Committee for Standardisation.
- CEN (2023): *EN 13501-2:2023 Fire Classification of Construction Products and Building Elements*. Part 2. Classification Using Data from Fire Resistance and/or Smoke Control Tests, Excluding Ventilation Services. Brussels: Technical Committee of the European Committee for Standardisation.
- ÉSZK (1984): *ME-04-132-84 Füstmentes lépcsőházak követelményei*. Budapest: Építészeti Szabványosítási Központ.
- GÁBOR, László – ZÖLD, András (1981): *Energiagazdálkodás az építészetben*. Budapest: Akadémiai Kiadó.
- GROSS, Daniel (1991): Estimating Air Leakage Through Doors for Smoke Control. *Fire Safety Journal*, 17(2), 171–177. Online: [https://doi.org/10.1016/0379-7112\(91\)90040-6](https://doi.org/10.1016/0379-7112(91)90040-6)
- HOBSON, P. J. – STEWART, L. J. (1972): *Pressurisation of Escape Routes in Buildings*. Fire Research Note No. 958. Bracknell: Heating and Ventilating Research Association. Online https://publications.iafss.org/publications/frn/958/-1/view/frn_958.pdf
- International Code Council and Society of Fire Protection Engineers (2022): *Fire Safety for Very Tall Buildings. Engineering Guide*. The Society of Fire Protection Engineers Series. Cham: Springer. Online: <https://doi.org/10.1007/978-3-030-79014-1>
- KÁTAI-URBÁN, Maxim (2023): Veszélyes anyagok és áruk tárolásának biztonsága, különös tekintettel a baleseti vízzennyezésre. *Hadmérnök*, 18(1), 29–41. Online: <https://doi.org/10.32567/hm.2023.1.3>
- KANYÓ, Ferenc – VÁSÁRHELYI-NAGY, Ildikó (2021): A beavatkozó tűzoltói állomány kompetencia alapú fizikai állapotfelmérése. *Védelem Tudomány*, 6(1), 204–217.
- KLOTE, John H. – MILKE, James A. – TURNBULL, Paul G. – KASHEF, Ahmed – FERREIRA, Michael J. (2012): *Handbook of Smoke Control Engineering*. Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers.
- KLOTE, John H. – MILKE, James A. – TURNBULL, Paul G. – KASHEF, Ahmed – PHILLIPS, Duncan A. – EVANS, Douglas H. – WEBB, William A. – ROTH, Michael J. (2024): *Handbook of Smoke Control Engineering*. Second Edition. Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers.
- LIDDAMENT, Martin W. (1986): *Air Infiltration Calculation Techniques. An Applications Guide*. Coventry: The Air Infiltration and Ventilation Centre. Online: www.aivc.org/resource/air-infiltration-calculation-techniques-applications-guide
- LIS, Piotr – LIS, Anna (2021): The Required Amount of Ventilation Air for the Classroom and the Possibility of Air Infiltration through the Windows. *Energies*, 14(22). Online: <https://doi.org/10.3390/en14227537>
- MARTIN, P. L. ed. (1970): *IHVE Guide. Book A*. London: The Institution of Heating and Ventilating Engineers.
- MIHÁLY, István – BÉRCZI, László – BOGNÁR, Balázs – KÁTAI-URBÁN, Maxim – TÓTH, Levente – KÁTAI-URBÁN, Lajos – VASS, Gyula – VARGA, Ferenc (2025): Experimental Study to Determine the Leakage Area of Single-Leaf Smoke Control Doors in the Design of Pressure Differential Systems. *Fire*, (8)1. Online: <https://doi.org/10.3390/fire8010005>

- National Directorate General for Disaster Management (2024): *Tűzvédelmi Műszaki Irányelv* [Fire Protection Technical Guideline]. *Kiürítés* [Evacuation]. TvMI 2.6:2024.02.01. Belügyminisztérium, Országos Katasztrófavédelmi Főigazgatóság. Online: www.katasztrofavedelem.hu/application/uploads/documents/2023-12/82903.pdf
- National Directorate General for Disaster Management (2025): *Tűzvédelmi Műszaki Irányelv* [Fire Protection Technical Guideline]. *Hő és füst elleni védelem* [Protection against Heat and Smoke Spread]. TvMI 3.6:2025.02.01. Belügyminisztérium, Országos Katasztrófavédelmi Főigazgatóság. Online: www.katasztrofavedelem.hu/application/uploads/documents/2024-12/84963.pdf
- OWEN, Mark S. ed. (2017): *2017 ASHRAE Handbook. Fundamentals. SI Edition*. Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers.
- RECKNAGEL, Hermann – SPRENGER, Eberhard – SCHRAMEK, Ernst-Rudolf (2000): *Fűtés- és klimatechnika 2000. I. kötet*. Budapest–Pécs: Dialóg Campus.
- TAMURA, George T. (1970): *Computer Analysis of Smoke Movement in Tall Buildings*. Research Paper No. 452. Ottawa: National Research Council of Canada, Division of Building Research. Online: <https://doi.org/10.4224/40000451>
- VÁRFALVI, János [s. a.]: *Ablakszerkezetek légáteresztése*. Online: http://152.66.45.150/EPFIZ/Ablakszerkezetek_legatreresztese.pdf

Legal source

- 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról [Decree 54/2014 (XII. 5.) of the Ministry of the Interior on the Issuance of the National Fire Protection Regulation]. Online: <https://njt.hu/jogszabaly/2014-54-20-0A>

Varró Tekla¹

A katasztrófavédelmi oktatás és tájékoztatás fejlesztési lehetőségei a magyar felnőtt lakosság körében

Development Opportunities for Disaster Management Education and Information among the Hungarian Adult Population

Absztrakt

A modern világban egyre gyakoribbá válnak a természeti és civilizációs katasztrófák, amelyek megelőzéséhez, kezeléséhez és hatásainak enyhítéséhez a hivatásos katasztrófavédelem és a lakosság szoros együttműködése szükséges.

Kutatásom célja annak felmérése volt, hogy a magyar lakosság egy véletlenszerűen kiválasztott részének körében milyen katasztrófavédelmi tájékoztatásra és riasztásra alkalmas eszközök (például okostelefon, rádió, televízió, internetes hírportálok, közösségi média) állnak rendelkezésre, valamint ezen eszközök alkalmazásával egy olyan oktatási rendszert kialakítani, amely online és offline oktatóanyagokkal, tesztekkel és gyakorlati szimulációkkal bővíti a lakosság ismereteit.

A kutatás során a nemzetközi és hazai szakirodalom, hazai jogszabályok, valamint kérdőíves felmérések eredményeinek elemzésével vizsgáltam a tájékoztatás hatékonyságát. Az eredmények alapján egy új, mindenki számára elérhető, a katasztrófavédelem által alkalmazott lakossági tájékoztató és felkészítő rendszer kiegészítéseként létrehozandó katasztrófavédelmi felkészítési rendszer bevezetését javaslom, amely magában foglalná a tűzvédelmi, iparbiztonsági és polgári védelmi modulokat, és hozzájárulna a lakosság alapszintű katasztrófavédelmi felkészítéséhez. Az oktatási rendszer célja,

¹ Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: tekla.varro@yahoo.com

hogy a lakosság felkészült legyen a katasztrófák esetén követendő magatartási szabályok betartására, ezzel csökkentve a katasztrófák káros hatásait.

Kulcsszavak: katasztrófavédelmi alapoktatás, lakossági tájékoztatás és riasztás, e-learning a katasztrófavédelemben, képzés és felkészítés

Abstract

Natural and civil disasters are becoming increasingly common in the modern world, and the prevention, management and mitigation of their effects require close cooperation between professional disaster management and the public.

The aim of my research was to assess what tools (e.g. smartphones, radio, television, online news portals, social media) are available for disaster management information and alerts, and to develop an educational system using these tools that expands the population's knowledge with online and offline educational materials, tests, and practical simulations. In the course of the research, I analysed the effectiveness of information provision by analysing international and national literature, Hungarian legislation and the results of questionnaire surveys. Based on the results, I propose the introduction of a new disaster preparedness training system, accessible to all, to complement the public information and preparedness system used by the disaster management, which would include modules on fire safety, industrial safety and civil protection and would contribute to the basic disaster preparedness of the population. The aim of the training system is to prepare the population to comply with the standards of behaviour and protocols to be followed in the event of disasters, thereby reducing the harmful effects of disasters.

Keywords: basic disaster education, public information and alert, e-learning in disaster management, training and preparedness

Bevezetés

A mai globalizált világban mind a természeti, mind a civilizációs eredetű katasztrófák előfordulása egyre gyakoribbá és súlyosabbá válik.² Hatékony megelőzésük és kezelésük az állampolgárok együttműködését kívánja, ugyanakkor a hivatásos katasztrófavédelem nélkülözhetetlen a feladatok szakszerű koordinálásában és végrehajtásában. A katasztrófavédelmi szervek által alkalmazott technológiák, riasztási rendszerek és módszertani megoldások kulcsszerepet játszanak a felkészülésben, a gyors reagálásban, valamint a társadalom és a szakmai szereplők összehangolt együttműködésében, amely a hatékony védekezés sikerének záloga. Az innovatív megoldások és technológiai fejlesztések garantálják a gyorsabb, pontosabb beavatkozást és védekezést, ami jelentősen hozzájárul a társadalom biztonságához.

² World Meteorological Organization 2021.

Kutatásommal célom felmérni, hogy milyen technikai eszközök állnak a lakosság rendelkezésére, amelyeken keresztül a lakossági tájékoztatás, riasztás folyamata végbe tud menni, illetve a rendelkezésre álló eszközök alkalmazásával célom egy olyan felkészítési rendszer kialakítása, kidolgozása, amely a lakosságnak alapvető katasztrófavédelmi ismereteket biztosít, elősegítve ezzel a lakosság alapszintű katasztrófavédelmi felkészítését.

A katasztrófavédelem nemcsak a szakmai szervek feladata, hanem a társadalom széles körű együttműködését igényli. Ennek jogi alapját a 2011. évi CXCVIII. törvény 1. § (2) bekezdése adja, amely kimondja, hogy minden állampolgárnak joga van megismerni a környezetében lévő kockázatokat, elsajátítani a védekezési szabályokat, valamint kötelessége aktívan részt venni a katasztrófavédelmi tevékenységekben.

A téma aktualitását mutatja, hogy természeti és civilizációs katasztrófák bármikor előfordulhatnak, amelyek kockázatot jelenthetnek a lakosságra és a környezetre nézve. Magyarországnak a nemzeti katasztrófakockázat-értékeléséről szóló 2024-es jelentése 20 féle veszélyt sorol fel, amelyekre szükséges felkészülni lenni.³

„A tűzoltó és polgári védelmi jogelődökből létrehozott új katasztrófavédelmi szervezetnek, mint kihívásokkal, szembe kellett néznie a civilizációs veszélyekkel, a természeti csapásokkal, a humán és ökológiai fenyegetésekkel. A civilizációs veszélyeket a nukleáris-energiarendszerek, nukleárisanyag-szállítások, a határon túli nukleáris balesetek, a veszélyes anyagokkal bekövetkező ipari balesetek, a veszélyes üzemek, és a veszélyes anyagszállítások jelentették. A természeti csapások fenyegetései hidrológiai, geológiai, valamint meteorológiai eredetűekként lettek prognosztizálva. A humán és ökológiai kihívásokat az ökológiai szennyezések, a természetet veszélyeztető tüzek, a lehetséges járványok, a proliferáció, a migráció, a terrorizmus lehetséges előfordulásai jelentették.”⁴

Bár ez a leírás a 2000-es évek kihívásaira fókuszál, fontos megjegyezni, hogy a katasztrófavédelmi rendszer mai feladatai azóta jelentősen bővültek és átalakultak. A jelen kutatás azokat az eszközöket és módszereket vizsgálja, amelyek napjainkban, 2025-ben állnak rendelkezésre a hatékony tájékoztatás és riasztás érdekében, így a hangsúlyt a releváns és aktuális veszélyekre helyezi. Fontos, hogy az érintett lakosság tisztában legyen ezen események veszélyeivel, valamint azzal, hogy az esetlegesen bekövetkező katasztrófa negatív következményeinek csökkentése érdekében milyen intézkedéseket és viselkedési normákat szükséges követni.

Tudományos problémaként fogalmazom meg, hogy a lakosság tájékoztatásával és riasztásával kapcsolatos technikai eszközökkel való ellátottságról és ezek lakossági tájékoztatásra és riasztásra, valamint oktatásra történő használatával eddig kevés kutatás foglalkozott.

A 234/2011. (XI. 10.) Korm. rendelet (Kat. vhr.) 24. pontja VII. fejezetének rendelkezéseiből adódóan kiemelt feladat egy alap katasztrófavédelmi oktatás kidolgozása, amely – a tűzvédelmi és munkavédelmi oktatáshoz hasonlóan – a szükséges

³ Magyarország nemzeti katasztrófakockázat-értékeléséről szóló jelentése 2023.

⁴ MUHORAY 2012: 2.

ismereteket nyújtja a riasztás, veszélyhelyzeti tájékoztatás és a követendő magatartási szabályok terén. Bár a rendelet nem életkorhoz köti az érintetteket, a felnőtt lakosság elsősorban azért került a vizsgálat fókuszába, mert a döntéshozatali, cselekvési felelősség, valamint az önálló reagálás képessége általában náluk a legmeghatározóbb; ugyanakkor mindenkinek, aki érintett lehet veszélyhelyzetben, biztosítani kellene az ilyen jellegű oktatást és tájékoztatást. Ez nem csupán a jogszabályi megfelelés, hanem a társadalom biztonsága szempontjából is indokolt. A jogszabály nemcsak az intézményekre és szervezetekre, hanem közvetetten a lakosságra is előírásokat fogalmaz meg, amelyek között szerepel többek között a riasztás esetén követendő magatartási szabályok betartása, az elhangzó információk helyes értelmezése, valamint a megfelelő reagálás az adott helyzetre. Ezen kötelezettségek csak akkor teljesíthetők hatékonyan, ha az érintettek – így a lakosság is – tisztában vannak a riasztás és tájékoztatás jelentőségével, jelentésével, céljával és a követendő magatartási szabályokkal.

Az alap katasztrófavédelmi oktatás⁵ szükségességét, a tűz- és munkavédelmi oktatás szükségességével kívánom párhuzamba állítani. Ahogyan a tűz- és munkavédelmi szabályok is csak akkor képesek ellátni funkciójukat, ha az érintettek ismerik azokat, ugyanígy a katasztrófavédelmi kötelezettségek⁶ is csak a lakosság megfelelő ismereteinek birtokában valósíthatók meg.

A Kat. vhr. által a lakosság számára előírt konkrét magatartási elvárásokkal kapcsolatos ismeretek megszerzését és az ezekre történő felkészítést az államnak, az önkormányzatoknak, valamint a munkáltatónak szükséges biztosítania oktatás és rendszeres tájékoztatás keretében.

A 62/2011. (XII. 29.) BM rendelet (BM rendelet) 46. § (1) bekezdése meghatározza, hogy „a katasztrófavédelmi felkészítés célja a természeti, civilizációs és egyéb eredetű katasztrófák, veszélyhelyzetek megelőzése, az elhárítása, és a helyreállítás során jelentkező, a Kat. tv. 52. §-ában meghatározott feladatok végrehajtására való felkészülés, továbbá bekövetkezés esetén a káros következmények lehető legkisebbre csökkentése”, ami alapot biztosít a katasztrófavédelmi képzés létrehozásához.

A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (BM OKF) évente felkészítési programokat dolgoz ki, amelyek a kockázatbecslésen és a veszélyelhárítási tervekben meghatározott feladatokon alapulnak, és a BM OKF főigazgatója hagyja jóvá. Bár e programok részletes elemzése és kronologikus összehasonlítása a jelen tanulmány keretein kívül maradt, érdemes lenne a jövőben ezek fejlődési ívét feltárni és a jó gyakorlatokat kiemelni. A tervezett alapszintű katasztrófavédelmi oktatást – amely elsősorban a lakosság széles körének alapismereteit kívánja

⁵ Az „alap katasztrófavédelmi oktatás” alatt a felnőtt lakosság számára szervezett, rendszerezett ismeretanyagot értem, amelynek célja, hogy bemutassa a legfontosabb veszélyhelyzeteket (természeti és civilizációs katasztrófák), a riasztás és tájékoztatás folyamatát, a veszélyhelyzetben követendő magatartási szabályokat. Az oktatás nem hivatásos szakmai képzés, hanem – a tűz- és munkavédelmi oktatáshoz hasonlóan – alapvető ismeretek átadása, amelyek szükség esetén minden érintett számára alkalmazhatók. Az ismeretek átadására alkalmas módszerek lehetnek: e-learning-platformok, interaktív online és offline tananyagok, gyakorlati szimulációk, valamint tesztek, amelyek időszakos vagy eseményalapú formában, például évente vagy veszélyhelyzet előtt szervezetteren biztosíthatók.

⁶ A katasztrófavédelmi kötelezettségek alatt azt az elvárást értem, hogy minden állampolgárnak ismernie kell a veszélyhelyzeti riasztásokkal kapcsolatos eljárásokat, a magatartási szabályokat (tűz, árvíz, veszélyes anyagokkal kapcsolatos balesetek stb. esetén), együtt kell működni a hatóságokkal, valamint alkalmaznia kell a megelőző intézkedéseket és magatartási szabályokat.

bővíteni – a felkészítési programok kivonataként, azok alapelveire és tapasztalataira támaszkodva képzelem el, kiegészítve a legfrissebb, innovatív oktatási módszerekkel és digitális eszközökkel.

Az oktatás alatt ebben az összefüggésben a felnőtt lakosság számára szervezett, átfogó, strukturált tudásátadást értem, míg a felkészítés inkább a katasztrófavédelem szervezeti, szakmai állományára, illetve a speciális helyzetekre való célirányos tréningre, gyakorlatokra utal.

A 2021. évi CXL. törvény (Hvt.) a 45. § (2) bekezdésében meghatározza, hogy a hivatásos katasztrófavédelmi szervezet, valamint a polgári védelmi szervezeteket fel kell készíteni és ki kell képezni a fegyveres összeütközések időszakában végzendő polgári védelmi feladatokra is.

„A katasztrófavédelmi törvény tartalmazza [...] a polgári védelem katasztrófavédelemmel kapcsolatos feladatait, illetve a köteles polgári védelmi szervezetekkel kapcsolatos (a központi, területi, települési, munkahelyi polgári védelmi szervezetekre vonatkozó) rendelkezéseket, míg a honvédelmi törvény a fegyveres összeütközések időszakában végrehajtandó polgári védelmi feladatokra vonatkozó szabályokat.”⁷

Bár a Hvt. és a vonatkozó katasztrófavédelmi jogszabályok kiemelten foglalkoznak a hivatásos katasztrófavédelmi szervek, valamint a polgári védelmi szervezetek felkészítésével – különösen fegyveres összeütközések idejére –, kutatásom fókuszja nem a szakmai állomány képzésére, hanem a lakosság, ezen belül is elsősorban a felnőtt polgári személyek tájékoztatására és alapvető ismereteinek bővítésére irányul. A cél, hogy az oktatási és tájékoztatási modell a jogszabályi elvárásokat figyelembe véve, de kifejezetten a civil érintettek szükségleteire összpontosítson: online és offline elérhető, gyakorlatias tudásanyag, tesztek, szimulációk formájában.

A BM rendelet 66. §-a részletesen szabályozza a BM OKF szervezése alatt megvalósuló lakosságtájékoztatási módokat, felsorolva az aktív (például személyes tájékoztatás, rendezvények, tréningek) és passzív (például kiadványok, plakátok, digitális felületek) információátadási formákat is. Bár jelen kutatásban nem történt átfogó vizsgálat arra vonatkozóan, hogy az egyes vármegyei igazgatóságok, katasztrófavédelmi kirendeltségek vagy hivatásos tűzoltó-parancsnokságok milyen konkrét lakosságtájékoztatási tevékenységeket folytattak, a tapasztalatok azt mutatják, hogy a gyorsan változó technológiai környezetben, valamint a lakosság digitális eszközökkel való ellátottságának növekedésével szükségessé vált az oktatási és tájékoztatási lehetőségek folyamatos modernizálása, bővítése. Kutatásom célja ezért olyan új, korszerű tájékoztatási és oktatási modellek kidolgozása, amelyek hatékonyabban képesek megszólítani a felnőtt lakosságot, alkalmazkodva a digitális kommunikációs szokásokhoz, valamint erősítve a veszélyhelyzeti magatartásformák terjedését.

Hipotézisem a következő:

Feltételezem, hogy létrehozható egy, speciálisan a civil lakosság felnőtt korosztálya számára kifejleszthető oktatási módszer, amely a lakosság tájékozottságát képes fejleszteni a lakossági tájékoztató- és riasztóintézkedések témakörben.

⁷ AMBRUSZ 2025: 23.

A létrehozandó képzés alapját a BM rendelet VI–IX. fejezetében meghatározottak adják: a polgári védelmi szervezetek állományának kiképzését a hivatásos katasztrófavédelmi szervek végzik, míg a munkahelyi polgári védelmi szervezetbe beosztott személyek kiképzéséről a gazdálkodó szerv vezetője által meghatározott időpontban a munkahelyi polgári védelmi parancsnokság gondoskodik. Ez alapján javaslom a polgári védelmi szervezetek bevonását a lakosság képzésébe, valamint jogszabályi változtatást javaslok a Kat. vhr.-ben. A Kat. vhr. 49. § (5) bekezdése kimondja, hogy a hivatásos katasztrófavédelem területi szerve végzi a polgári védelmi szervezetek és a lakosság felkészítését. Ahhoz, hogy lehetőség szerint Magyarország felnőtt lakossága részesülhessen katasztrófavédelmi alapoktatásban, jogszabályi változtatásra van szükség. Ez lehetővé tenné, hogy az arra jogosultsággal rendelkező katasztrófavédelmi előadók is végezzenek oktatási tevékenységet a hazai munkahelyeken, elősegítve ezzel az ismeretanyag minél szélesebb körű elterjedését.

Fontos megjegyezni, hogy jelenleg a Katasztrófavédelmi Oktatási Központ (KOK) szakmai képzési programjai részletesen szabályozzák a katasztrófavédelmi oktatók felkészítését és képzését, amelyeket a KOK Tanulmányi Osztályán meg lehet tekinteni. A szerző az új alapoktatási rendszer kidolgozásánál ezek ismeretére alapozva tervezi az oktatás célcsoportját és módszertanát, hogy valóban hatékony és jogszabályoknak megfelelő képzést kínáljon a felnőtt lakosság részére.⁸

A Központi Statisztikai Hivatal (KSH) adatai szerint a magyar lakosság száma 2025. január 1-jén 9 539 502 fő,⁹ amelyből a 0–18 éves korosztály 1 762 325 fő, a 18 és 65 év közötti korosztály 5 996 205 fő, a 65 év feletti korosztály 1 991 000 fő.¹⁰

2025 májusában a foglalkoztatottak száma 4 669 000 fő volt,¹¹ ami azt jelenti, hogy ha csak a munkahelyeken megvalósulhat a képzés, a lakosság 48,94%-a lenne közvetlenül elérhető. Ez ugyan jelentős bázist biztosíthat egy reziliens társadalom kialakításához, azonban fontos tudni, hogy az oktatás munkahelyi megvalósítása számos kihívást rejt magában. Közgazdasági, jogi és társadalomtudományi szempontból például kérdéses, hogy a munkahelyek milyen mértékben érdekeltek a képzésben, ki finanszírozza és valósítja meg a képzést, illetve milyen módon tehető kötelezővé vagy ajánlóssá. Dr. Endrődi Istvánnal egyetértve fontosnak tartom továbbá a családok, illetve az egyes családtagok felkészítését is. Amennyiben a család legalább egyik tagja pontosan ismeri a veszélyhelyzeti teendőket és a kötelező magatartási szabályokat, képes lesz segítséget nyújtani a család többi tagjának veszélyhelyzet esetén.¹² „A gyorsan cselekvőképessé váló – kognitív leküzdési stratégiát produkálni tudó – lakosok száma növekedhet, ha előzetesen megismerik a veszélyhelyzeteket, a felkészítések alkalmával fejlődik ön- és társmentési képességük, továbbá sikeresen alkalmazni tudják a megfelelő menekülési módozatokat (magatartási szabályokat).”¹³

A gyermekek (0–18 éves korosztály) jelen cikkben nem tartoznak a vizsgált célcsoportba.

⁸ VARRÓ 2024: 132.

⁹ Központi Statisztikai Hivatal 2025a.

¹⁰ Központi Statisztikai Hivatal 2025b.

¹¹ Központi Statisztikai Hivatal 2025c.

¹² ENDRŐDI 2007: 4.

¹³ BOLGÁR-MÓGOR 2015: 4.

Kutatási céljaim megvalósításához részletesen tanulmányoztam a releváns hazai jogszabályokat, valamint a katasztrófavédelmi oktatással és lakossági tájékoztatással kapcsolatos szakmai anyagokat. A nemzetközi szakirodalomból jelenleg egyetlen, a témához közvetlenül kapcsolódó, elemző forrást idézek, amely a katasztrófaesemények gyakoriságának és hatásainak tendenciáit mutatja be globálisan. Emellett önálló kérdőíves kutatást végeztem, amelynek eredményeit diagramokon szemléltettem.

Magyarország lakosságának katasztrófavédelmi tájékoztatáshoz és riasztáshoz szükséges technikai eszközökkel való ellátottsága

A lakosság védelmének és biztonságának alapvető feltétele, hogy a katasztrófavédelmi tájékoztatás és riasztás hatékonyan működjön. Ennek elengedhetetlen feltétele, hogy megfelelő technikai eszközök álljanak rendelkezésre, amelyek az információk gyors és pontos célba juttatását biztosítják veszélyhelyzetek esetén. A lakosság tájékoztatáshoz és riasztáshoz szükséges technikai eszközökkel való ellátottságának vizsgálata képet ad az adott technológiai infrastruktúra alkalmazhatóságáról, valamint a katasztrófavédelmi rendszer hatékonyságának egyik kulcsfontosságú tényezője is lehet a vizsgált célcsoport körében. A továbbiakban részletesen ismertetem a 250 fő részvételével kitöltött kérdőívem kiértékelését, amely a lakossági tájékoztatáshoz és riasztáshoz szükséges technikai eszközök ellátottságával és elterjedtségével kapcsolatban ad betekintést a vizsgált csoport tájékozottságába.

A lakosság katasztrófavédelmi tájékoztatáshoz és riasztáshoz szükséges technikai eszközökkel való ellátottságát felmérő kérdőív

A lakosság katasztrófavédelmi tájékoztatáshoz és riasztáshoz szükséges technikai eszközökkel való ellátottságát egy 250 fő által kitöltött, anonim kérdőív feldolgozásával, valamint a vonatkozó jogszabályok felhasználásával vizsgáltam a 2024. augusztus 1. és 2024. szeptember 15. közötti időszakban. A generációk életkori megoszlását 5 fő kategóriára bontottam: 0–18, 19–35, 36–60, 61–70 és 71 év fölötti kategóriákra. E kategorizálás az életkori jellemzők és a társadalmi szerepek különbözőségei alapján történt, figyelembe véve a magyarországi demográfiai és társadalmi struktúrát. Ugyanakkor fontos megjegyezni, hogy jelen kutatás kizárólag a felnőtt lakosságra fókuszál, ezért az 0–18 év közötti korcsoport eredményeit nem vettem figyelembe az elemzésekben annak érdekében, hogy elkerüljük az adatok torzulását.

Az adatgyűjtéshez és elemzéshez a Google Forms onlinekérdőív-felületét használtam, amely lehetővé tette a demográfiai adatok pontos rögzítését és kategorizálását.

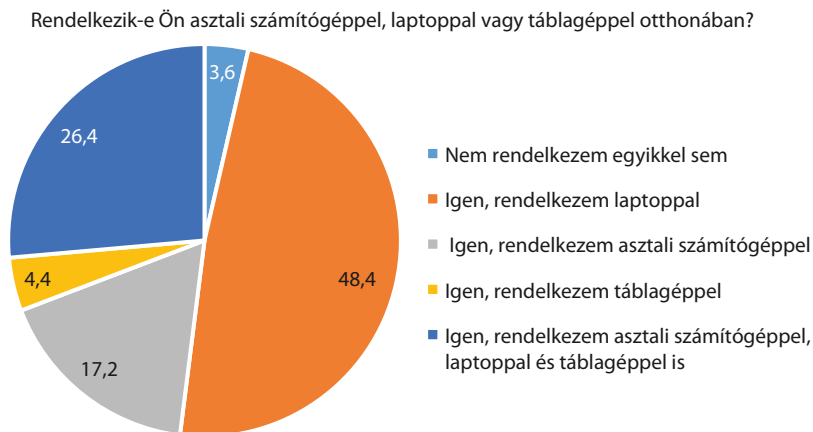
A kérdőívben 14 kérdést kellett megválaszolni a kitöltőknek, amelyből 13 kérdésre kötelező volt válaszolni, 1 kérdésre a válaszadás opcionális volt.

A kérdőívet kitöltők legnagyobb arányban (52%) a 19–35 éves korosztályból került ki, a 2. legnagyobb számú kitöltés (39,6%) a 36–60 éves korosztálytól, ezt követően pedig a 61–70 éves korosztálytól (5,6%), majd a 71 év fölötti korosztálytól (1,6%), végül pedig a 0–18 éves korosztálytól (1,2%) érkezett. A kérdőív megválaszolóit

között a 19 és 60 év közötti korosztály képviseltette magát a legnagyobb arányban. A kitöltők között látható tehát, hogy a katasztrófavédelem munkája iránt leginkább fogékony korosztály a 19 és 60 év közötti lakosság. Fontos azonban hangsúlyozni, hogy ez a megoszlás a minta összetételét tükrözi, és nem feltétlenül jelenti azt, hogy ez a korosztály mutatná a legnagyobb fogékonyságot a katasztrófavédelmi témák iránt. A kérdőívet elsősorban online, de papírfomátumon is terjesztettem, amelyet később az online felületre felvittem, így a minta nem reprezentálja teljes egészében a magyar felnőtt lakosságot. Ezért az eredmények interpretálásakor e korlátozást figyelembe kell venni.

A kérdőívet kitöltők legnagyobb aránya Budapesten (46%), a 2. legnagyobb száma Pest vármegyében (43,6%), 3. legnagyobb száma (2,8%) Zala vármegyében él életvitelszerűen. Heves vármegyéből a kitöltések 1,6%-a érkezett, Baranya és Hajdú-Bihar vármegyéből 1,2%, míg a kitöltések száma 0,8% Borsod-Abaúj-Zemplén és Szabolcs-Szatmár-Bereg vármegyékben. A kitöltők aránya mindenhol 0,4% volt Jász-Nagykun-Szolnok, Komárom-Esztergom, Nógrád, Győr-Moson-Sopron és Somogy vármegyékben. Nem érkezett kitöltés Bács-Kiskun, Békés, Csongrád-Csanád, Fejér, Tolna, Vas és Veszprém vármegyékből.

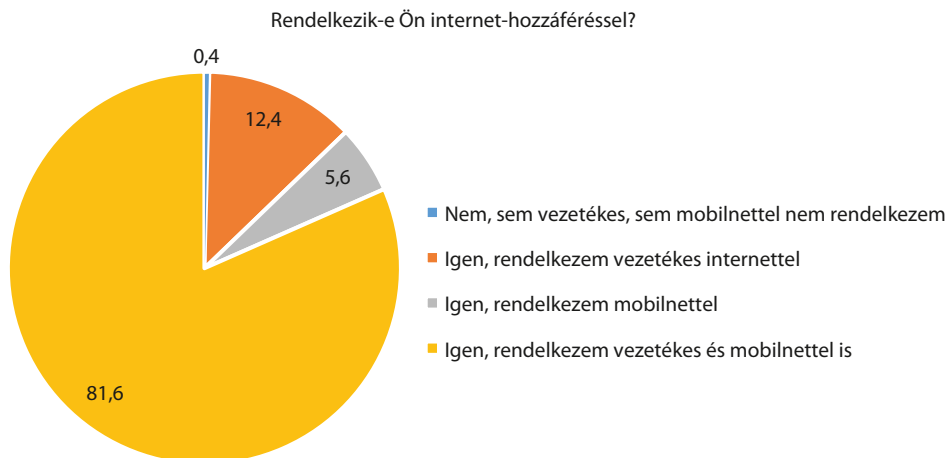
Az 1. ábrán látható adatok a kitöltők számítógéppel, lappal, táblagéppel kapcsolatos ellátottságát hivatottak bemutatni. 48,4% rendelkezik lappal, 26,4% rendelkezik lappal, asztali számítógéppel és táblagéppel is, 17,2% pedig csak asztali számítógéppel. A kitöltők 4,4%-a csak táblagéppel rendelkezik, 3,6% pedig egyik elektronikai eszközt sem birtokolja. Összeségében elmondható, hogy a digitális eszközök jól lefedik a válaszadók körét, azonban a jövőbeni fejlesztések során érdemes figyelmet fordítani az eszközhányban szenvedő, illetve a digitálisan kevésbé felszerelt csoportokra is, hogy mindenki számára biztosított legyen a modern technológiákhoz való hozzáférés.



1. ábra: A kérdőívet kitöltők számítógép-, laptop- és táblagépbirtoklása (%)

Forrás: a szerző szerkesztése

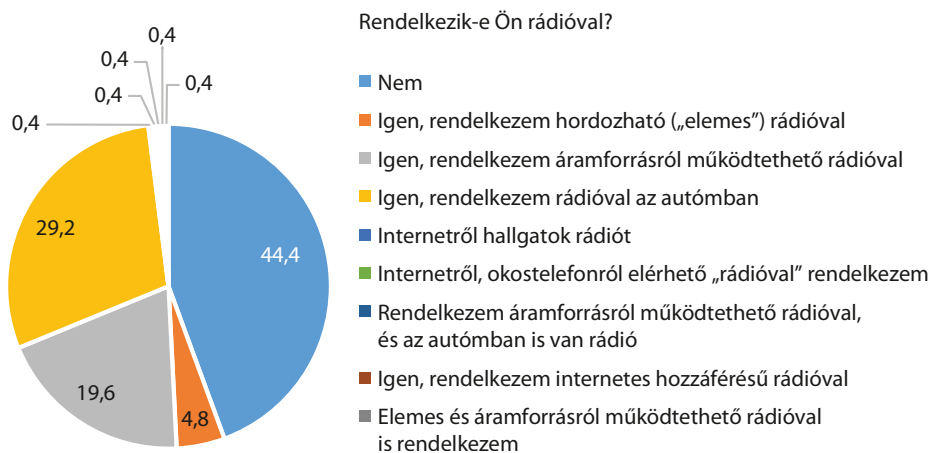
A 2. ábra a kitöltők internet-hozzáféréseinek adatait mutatja be. A kitöltők legnagyobb aránya, 81,6% rendelkezik vezetékes és mobilnettel is, 12,4% csak vezetékes internettel, míg 5,6% csak mobilnettel rendelkezik. A kitöltők között nincs olyan, aki sem vezetékes, sem mobilnettel nem rendelkezik.



2. ábra: A kérdőívet kitöltők internet-hozzáférése (%)

Forrás: a szerző szerkesztése

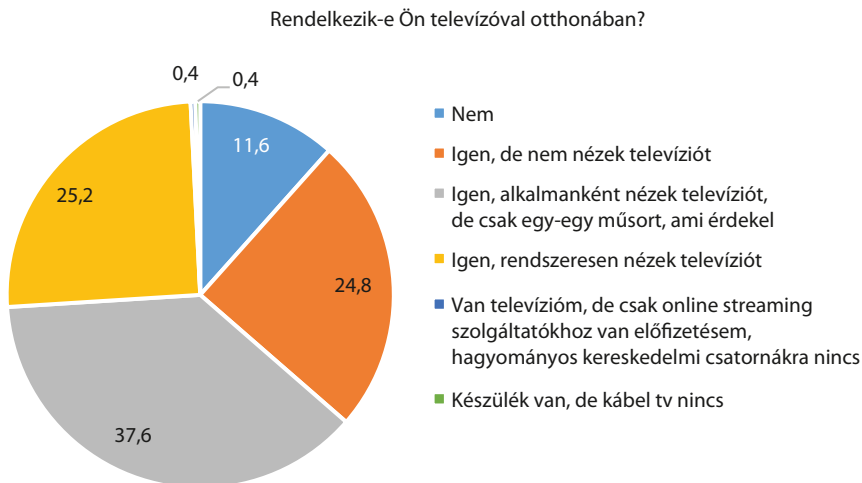
A 3. ábrán látható, hogy a kitöltők legnagyobb aránya, 44,4% nem rendelkezik rádióval. 29,2%-nak autórádiója van, 19,6%-nak áramforrásról működő rádiója van, míg 0,4% internetről hallgat rádiót. Szintén 0,4%-nak van elemes és áramforrásról működtethető rádiója és autórádiója, internetről elérhető rádiója. A válaszokból arra lehet következtetni, hogy a hagyományos rádiós tájékoztatás korlátozott hatékonyságú.



3. ábra: A kérdőívet kitöltők rádióbirtoklása (%)

Forrás: a szerző szerkesztése

A 4. ábra bemutatja, hogy a válaszadók milyen arányban rendelkeznek televízióval otthonukban, illetve milyen televíziónézési szokásaik vannak. A legnagyobb arányban lévő kitöltők (37,6%) rendelkeznek televízióval otthonukban, de csak alkalmanként néznek televíziót és akkor is csak egy-egy műsort, ami felkelti érdeklődésüket. 25,2% rendszeresen néz televíziót, míg 24,8% annak ellenére, hogy rendelkezik televízióval, nem nézi azt. 11,6%-nak nincsen televíziója, 0,4% pedig csak online streamingszolgáltatóknál rendelkezik előfizetéssel, hagyományos kereskedelmi csatornája nincs, valamint szintén 0,4% az, akinek televíziója van, viszont kábeltévéje nincs, tehát csak az ingyenesen elérhető csatornákhöz van hozzáférése.



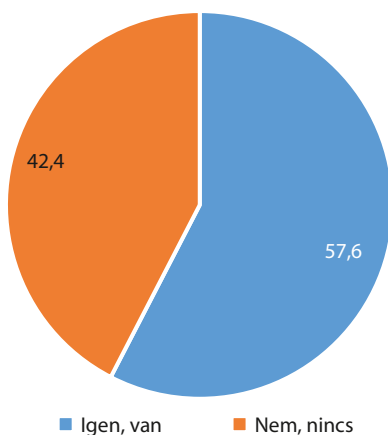
4. ábra: A kérdőívet kitöltők televízió-birtoklása (%)

Forrás: a szerző szerkesztése

Az 5. ábrán szereplő kérdés arra volt kíváncsi, hogy van-e sürgősség-tartaléknak számító akkumulátor- vagy töltőkészüléke (*power bank*) a lakosságnak. 57,6% azt mondta, hogy rendelkezik ilyen eszközzel, míg 42,4%-nak nincs ilyen eszköze. A *power bank* elterjedtsége válság- és katasztrófavédelem, a lakosságtájékoztatás és a mindennapi biztonság szempontjából is döntő. A 42,4%-os ellátatlansági arány mind a hatóságok, mind a közösségek részéről lépéseket indokolhat – például tudatosító kampányokat vagy eszközbeszerzési támogatásokat – a lakosság ellenálló képességének növelése érdekében.

A 6. ábrán látható adatokból kiderül, hogy a kitöltő lakosság 79,6%-a nem rendelkezik vezetékes telefonnal, és csupán 20,4% az, akinek van készüléke, így lakossági tájékoztatásra és riasztásra ezen módszer alkalmazása kizárólagosan nem alkalmas.

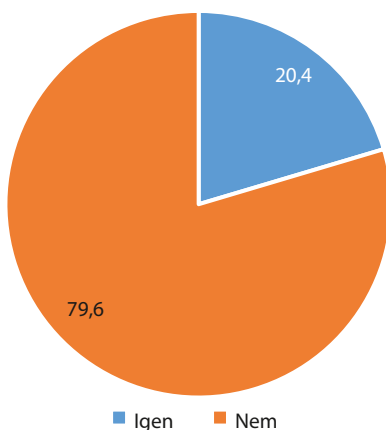
Van-e sürgőstartaléknak számító akkumulátor- vagy töltőkészüléke (power bank)?



5. ábra: A kérdőívet kitöltők ellátottsága sürgőstartaléknak számító akkumulátor- vagy töltőkészülékkel (%)

Forrás: a szerző szerkesztése

Rendelkezik-e Ön működőképes vezetékes telefonnal?

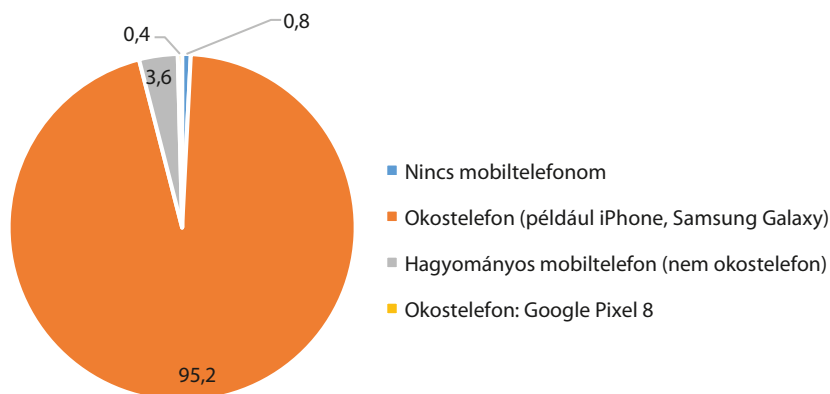


6. ábra: A kérdőívet kitöltők ellátottsága működőképes vezetékes telefonnal (%)

Forrás: a szerző szerkesztése

A 7. ábrán látható adatokból kiderül, hogy a kérdőívet kitöltő lakosság 95,2%-a rendelkezik okostelefonnal, és mindössze 3,6% az, aki hagyományos, nem okostelefont birtokol. 0,8% egyáltalán nem rendelkezik mobiltelefonnal, illetve 0,4% volt, aki a Google Pixel mobiltelefonját nem tekintette okostelefonnak, én viszont ezt mégis az okostelefon-kategóriába sorolom. A mobiltelefonok aránya messze a legmagasabb az elektronikai eszközök birtoklásában, így célszerűnek tartom a mobiltelefonos riasztás, tájékoztatás lehetőségeit fejleszteni akár applikáció, akár a Cell Broadcast rendszer használatával, a jogszabályban meghatározott hagyományos riasztási és tájékoztatási módok mellett.

Rendelkezik-e Ön mobiltelefonnal? Amennyiben igen, milyen típusú mobiltelefonja van?

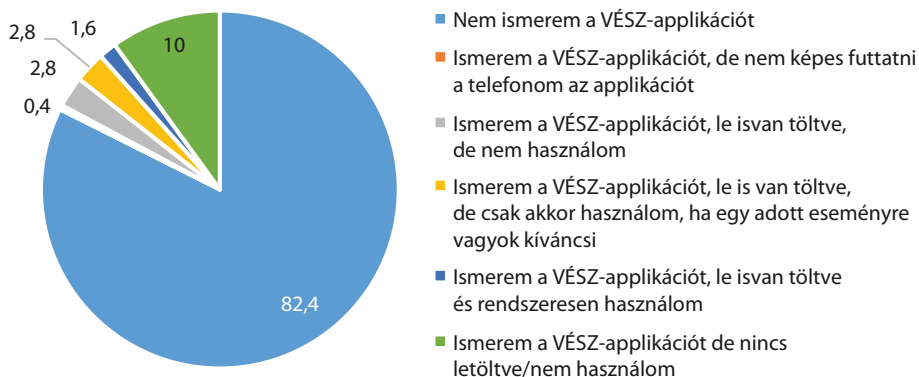


7. ábra: A kérdőívet kitöltők mobiltelefon-birtoklása (%)

Forrás: a szerző szerkesztése

A 8. ábrán látható kérdés arra volt kíváncsi, hogy a kérdőívet kitöltők ismerik-e a VÉSZ-(veszélyhelyzet értesítési szolgáltatás) applikációt. A legnagyobb arány (82,4%) egyáltalán nem ismeri a VÉSZ-applikációt, 10% ismeri, de nem használja, és nincs is letöltve a telefonjára, 2,8% volt, aki ismeri, le is van töltve a telefonjára, de nem használja, valamint szintén 2,8% az, aki ismeri az applikációt, le is van töltve a telefonjára, de csak akkor használja, ha egy adott eseményre kíváncsi. Csupán 1,6% azoknak az aránya, akiknek le van töltve az applikáció, és rendszeresen használják is azt. 0,4% ismeri a VÉSZ-applikációt, azonban az nem képes futni a telefonján.

Ismeri-e Ön a VÉSZ-applikációt (veszélyhelyzeti értesítési szolgáltatás)?
Amennyiben igen, rendelkezik-e Ön olyan mobiltelefonnal, amelyen képes futni a VÉSZ-applikáció?

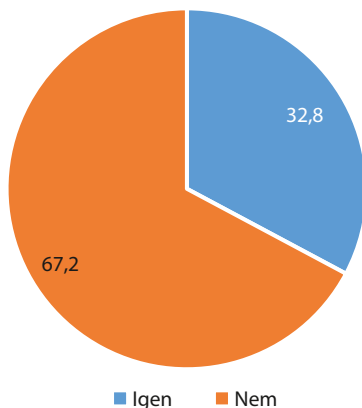


8. ábra: A kérdőívet kitöltők ismerete a VÉSZ-applikációval kapcsolatban, valamint az ellátottság az annak futtatására alkalmas mobiltelefonokkal (%)

Forrás: a szerző szerkesztése

A 9. ábra kérdése arra vonatkozik, hogy a kérdőívet kitöltő lakosság használta-e már a mobiltelefonját a hivatásos katasztrófavédelem által kiadott riasztások fogadására (például a 2013. március 15-i hirtelen leesett nagy mennyiségű hó és markáns hideg miatt a Belügyminisztérium SMS-értesítése az úton tartózkodó lakosságnak). 67,2% válaszolt igennel a kérdésre, 32,8% viszont azt válaszolta, hogy még soha nem kapott riasztást a hivatásos katasztrófavédelemtől.

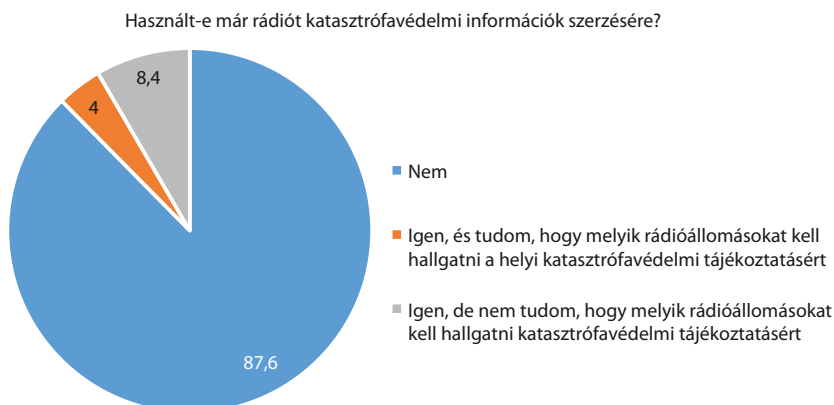
Használta-e már valaha mobiltelefonját a hivatásos katasztrófavédelem által kiadott riasztások fogadására? (Például a 2013. márciusi nagy havazáskor a Belügyminisztérium által elküldött automatikus SMS-értesítés fogadására)



9. ábra: Katasztrófavédelmi SMS-riasztás fogadása a kérdőívet kitöltők között (%)

Forrás: a szerző szerkesztése

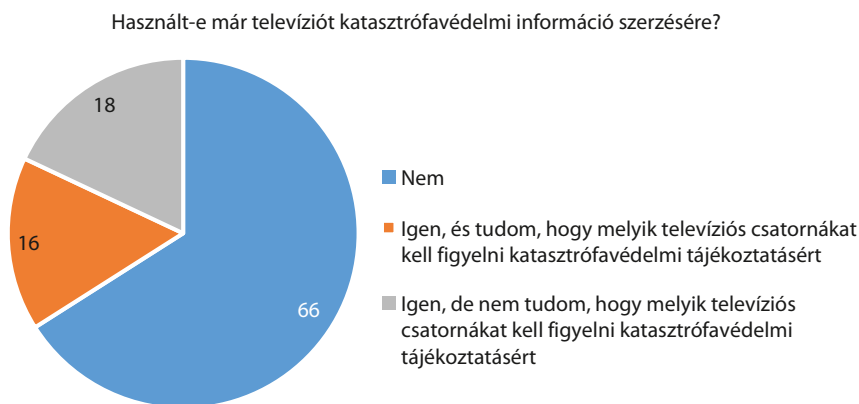
A 10. ábra kérdése arra kíváncsi, hogy a kitöltők használtak-e már valaha rádiót katasztrófavédelmi információk szerzésére. 87,6% még sosem használt rádiót e célra, 8,4% már használt, ugyanakkor nem tudja, hogy melyik rádióállomást kell hallgatnia. Csúpán 4% azoknak az aránya, akik már használtak rádiót katasztrófavédelmi információk szerzésére és tudják is, hogy melyik rádióállomást kell hallgatni.



10. ábra: Katasztrófavédelmi információk szerzése rádión keresztül a kérdőívet kitöltő lakosság körében (%)

Forrás: a szerző szerkesztése

A 11. ábra szintén a katasztrófavédelmi információk szerzésére vonatkozott, csupán annyi különbséggel, hogy itt arra volt kíváncsi a kérdés, hogy televíziót használt-e már a kérdőívet kitöltő lakosság katasztrófavédelmi információk szerzésére. Itt már kevesebb a nemleges válaszok aránya az előző kérdéshez képest: 66% állította azt, hogy még nem használt televíziót katasztrófavédelmi információk szerzésére. 18% már használt e célra televíziót, de nem tudja, hogy melyik televíziós csatornát kell figyelni, 16% pedig azt állítja, hogy már használt e célra televíziót, és tudja is, hogy melyik televíziós csatornát kell figyelni katasztrófavédelmi tájékoztatásért.

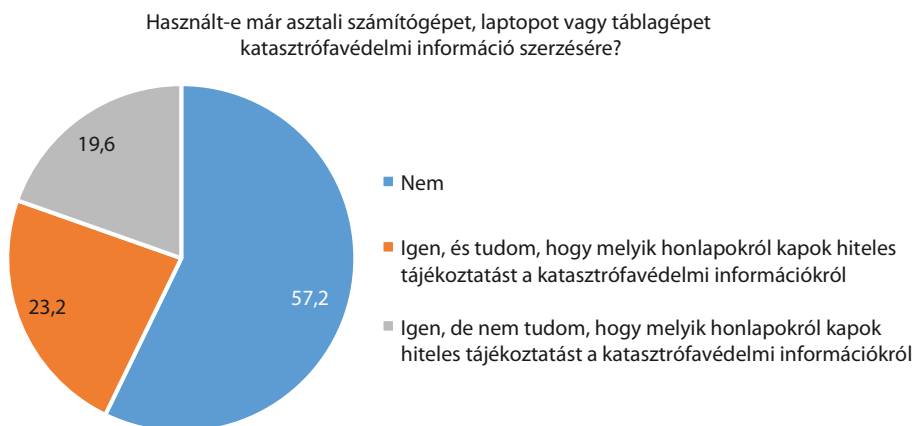


11. ábra: Katasztrófavédelmi információk szerzése televízión keresztül a kérdőívet kitöltő lakosság körében (%)

Forrás: a szerző szerkesztése

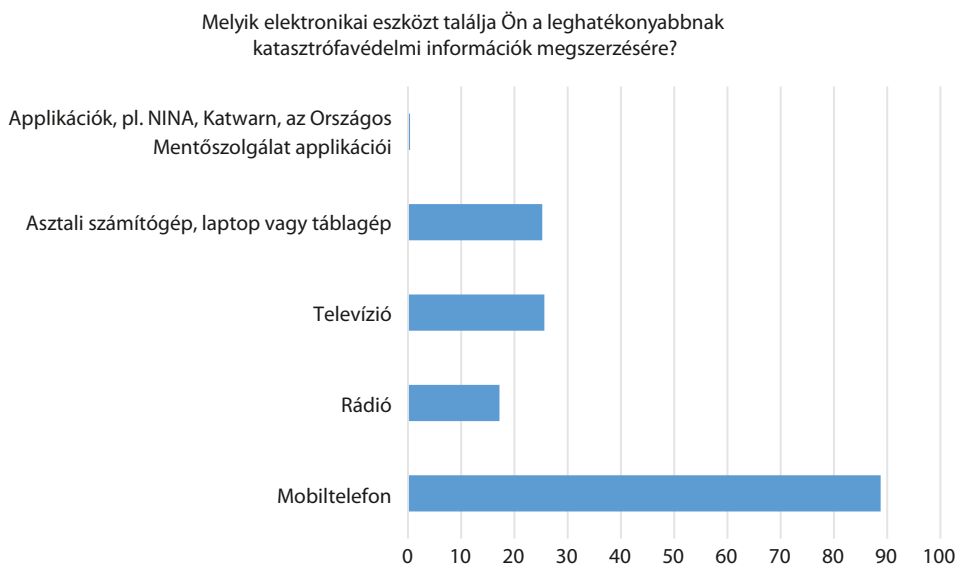
A 12. ábra kérdése is a katasztrófavédelmi információk megszerzésére vonatkozott: arra volt kíváncsi a kérdés, hogy használt-e már laptopot, asztali számítógépet, táblagépet a kitöltő katasztrófavédelmi információk szerzésére. 57,2% még nem használta e célra a felsorolt elektronikai eszközöket. 23,2% már használta e célra a fentebb felsorolt elektronikai eszközöket, és tudja is, hogy melyik honlapokról tud hiteles információhoz jutni a katasztrófavédelmet érintő tájékoztatásokkal kapcsolatban. 19,6% állítja, hogy használta már katasztrófavédelmi információszerzésre a fentebb felsorolt eszközöket, azonban nem tudja, hogy melyik honlapokról kaphat hiteles tájékoztatást katasztrófavédelmi kérdésekben.

A 13. ábra a kérdőívet kitöltő válaszadók véleményére volt kíváncsi, hogy melyik elektronikai eszközt találja a leghatékonyabbnak a katasztrófavédelmi információk megszerzésére. 88,8% a mobiltelefont találja a legalkalmasabbnak, 25,6% a televíziót, 25,2% az asztali számítógépet, laptop vagy táblagép valamelyikét, 17,2% pedig a rádiót. 0,4% említett applikációkat – mint a NINA, Katwarn vagy az Országos Mentőszolgálat applikációit –, azonban ezek inkább szoftvereszköznek tekintendők, mint hardvereszköznek, így nem az elsődlegesen feltett kérdésre ad választ.



12. ábra: Katasztrófavédelmi információk szerzése asztali számítógépen, laptopon, táblagépen keresztül a kérdőívet kitöltő lakosság körében (%)

Forrás: a szerző szerkesztése



13. ábra: A leghatékonyabb eszköz a katasztrófavédelmi információk szerzésére a kitöltő lakosság szerint (%)

Forrás: a szerző szerkesztése

Összességében a kérdőívre adott válaszok alapján elvégzett elemzés eredményeként elmondható, hogy a technikai eszközzel való ellátottság tekintetében a kitöltők túlnyomó többsége rendelkezik valamilyen technikai eszközzel, amelyből a legnagyobb

arány a laptop birtoklására (48,4%) irányul, ennél kisebb százalékban az asztali számítógéppel és táblagéppel együtt (26,4%) rendelkezők vannak. A kitöltők között csupán 3,6% az, aki egyáltalán nem rendelkezik semmilyen elektronikai eszközzel. Internet-hozzáférés tekintetében a kitöltők 99,6%-a vallotta, hogy rendelkezik internet-hozzáféréssel (vezetékes és/vagy mobilnet). Ez az arány biztosítani képes az online tájékoztatás széles körű lehetőségét.

Rádió- és televízióhasználat terén elmondható, hogy a kérdőívet kitöltő lakosság jelentős része (44,4%) nem rendelkezik rádióval. Azon kitöltők közül, akik rendelkeznek rádióval, csupán 4% az, aki használja katasztrófavédelmi információ szerzéséhez, és 87,6% ez idáig még sosem használta a rádióját ilyen célra. Televízióhasználat tekintetében 88,4% az, aki egyáltalán rendelkezik televízióval, de csak 34% az, aki valaha használta már azt katasztrófavédelmi információk szerzésére. Azok közül, akik használták, kevesebb mint a felük (16%) tudja csak, hogy melyik csatornát kell figyelnie ahhoz, hogy katasztrófavédelmi információkhoz juthasson.

Az okostelefonok tekintetében a kérdőívet kitöltő lakosság igen nagy része nagyon jól áll: 95,2%-a rendelkezik okostelefonnal. Jelenleg a leghatékonyabb eszköznek az okostelefon bizonyul a katasztrófavédelmi információk szerzésére a kitöltők szerint (88,8%). A VÉSZ applikáció ismertsége rendkívül alacsony: 82,4% egyáltalán nem ismeri, és csupán 1,6% használja rendszeresen. Ez az adat rávilágít arra, hogy az applikáció népszerűsítése, fejlesztése prioritásként kezelendő.

A mobiltelefonos riasztások fogadásában a válaszadók 67,2%-a részesült már, ami azt mutatja, hogy ez egy jól működő csatorna lehet, azonban 32,8% jelenleg a kérdőívet kitöltő lefedetlen lakosság, ami azt mutatja, hogy ez a riasztási forma nem ad sokféle típusú veszélyről tájékoztatást.

Szükségartalékok tekintetében a válaszadók 57,6%-a rendelkezik akkumulátor vagy egyéb töltőkészülékkel, ami az áramkimaradások esetén hasznos lehet.

Vezetékes telefonja a kitöltők csupán 20,4%-ának van, ami a hagyományos kommunikációs csatornák háttérbe szorulását mutatja.

Nemzetközi kitekintésként Izraelt említem, mert meglátásom szerint az egyik legkiválóbban működő védelmi és biztonsági rendszer ebben az országban működik. Izraelben a Pikud HaOref látja el a lakosság- és hátországvédelmet. Elsődlegesen a fegyveres támadások elleni lakosságvédelmet biztosítja, emellett pedig a természeti katasztrófák, biológiai, kémiai és a veszélyes anyagok elleni védelmi, földrengés elleni lakosságvédelmi intézkedéseket is ellátja. Lakossági tájékoztatás céljából honlapot működtetnek, ahol különböző nyelveken elérhetővé teszik az információkat. A honlap csak Izraelből érhető el biztonsági okok miatt. A Pikud HaOref honlapján minden korosztály számára megfelelő információhoz hozzáférhet az érdeklődő: kisfilmekkel, tájékoztató kiadványokkal és letölthető applikációval, a gyermekek számára több részes rövid mesefilmekkel biztosítja a lakosság felkészítését, a veszélyhelyzeti magatartási szabályok elsajátítását. A honlap többek között tartalmazza a veszélyhelyzeti teendőket földrengés, tűz, veszélyes anyagokkal kapcsolatos események, valamint árvíz esetére. Információkkal szolgál a veszélyhelyzetek felismerésének segítésére, tűz megelőzésére, már bekövetkezett esemény esetén a teendőkre, a betartandó magatartási szabályokra, valamint a biztonságot nyújtó helyek fellelésére (ilyenek például a lakásban és nyilvános helyeken lévő óvóhelyek). A honlap információval

szolgál arra vonatkozólag is, hogy veszélyhelyzetben mit tartsunk otthon, és ha el kell hagyni a lakhelyünket, mi legyen a menekülőcsomag tartalma. Minden Izraelben élő tájékozódhat róla műsorszolgáltatókon, interneten, televízión, mobil- és számítógépes applikáción keresztül, hogy a lakhelye szerinti körzetben van-e veszélyt jelentő esemény.

„Polgári védelmi felügyelőt kell alkalmazni olyan üzemekben, ahol 10, vagy annál több dolgozót foglalkoztatnak, oktatási intézményekben, kórházakban, a 10-nél kevesebb dolgozót foglalkoztató üzemekben akkor, ha a védelmi minisztérium elrendeli számukra, továbbá olyan komplexumokban, ahol legalább két üzem működik és 20 vagy annál több főt foglalkoztatnak [...] Az IDF (Izraeli Védelmi Erők) egységeit kiegészítik a fiatal önkéntesek, akik 16 éves koruktól csatlakozhatnak és vehetnek részt a lakosságvédelmi feladatokban. A helyi önkormányzatok képezik azt az alapkövet, amelyre a helyi közösség védelme épül, képes az ott lakóikról megfelelően gondoskodni, ennek érdekében a HFC (hátszágvédelem) végzi a helyi önkormányzattal együtt a képzést. A felkészítést nem lehet elég korán elkezdni, ezért már az általános iskolákban elkezdődik a tanulók felkészítése, az elsajátított ismeretek gyakorlat keretében történő bemutatása. Így szereznek ismeretet a saját, a családjuk és közösségük védelméről, és 16 éves koruktól az ismeretek birtokában csatlakozhatnak önkéntesként a HFC egységeihez”¹⁴

A lakosság felkészítése, képzése – katasztrófavédelmi alapoktatás

A Kat. vhr. 49. § (5) bekezdése kimondja, hogy a hivatásos katasztrófavédelmi szerv területi szerve végzi a polgári védelmi szervezetek és a lakosság felkészítését. Jelen cikk témáját tekintve, miszerint Magyarország – lehetőség szerint – teljes lakossága részesüljön katasztrófavédelmi alapoktatásban, szükség van jogszabályi változtatásra, amely szerint az arra jogosultsággal rendelkező katasztrófavédelmi előadó is végezhet oktatási tevékenységet – amennyiben az oktatási anyag megfelel a szakmai és jogi követelményeknek – a Magyarországon működő munkahelyeken, ezzel könnyítve a tananyag eljutását minél több emberhez.

„Az ismeretek átadásának lehetséges és rendelkezésre álló módszerei közül a leghatékonyabbat kell kiválasztani a feltételektől függően. Figyelembe kell venni a felkészítendő célcsoport átlagos életkorát, jellemző intellektusát, a már megszerzett ismereteket. Tekintettel kell lenni továbbá a végzettségükre, a családi, mikro- és makrokörnyezetre is. A felkészítés folyamatában az érintettek veszélyhelyzeti magatartásának cselekvési szintű befolyásolása elérhetővé válik.”¹⁵

A lakosságfelkészítés, a polgári védelmi feladatokra történő felkészítés a felnőttoktatás, felnőttképzés területéhez tartozik. Figyelembe véve az előzőekben ismertetett kérdőívre adott válaszokat, valamint azt a tényt, hogy a munkahelyi kötöttségek megnehezítik a hagyományos oktatásban történő részvételt, az e-learning¹⁶

¹⁴ NOVÁKY 2018: 69–70.

¹⁵ AMBRUSZ 2023: 667.

¹⁶ Infokommunikációs és kommunikációs technológiák, eszközök által támogatott tanítás-tanulás.

és az m-learning¹⁷ használatát hatékony megoldásnak találom a felnőttoktatás terén, mivel ezek lehetővé teszik az ismeretek rugalmas, idő- és helyfüggetlen elsajátítását. Ezek a módszerek kényelmes tanulási környezetet biztosítanak, miközben a tanuló folyamatos kapcsolatban áll tanárával, valamint az adott csoport többi tagjával is. Az e-learning és m-learning rendszere napjaink legmodernebb digitális oktatási formái közé tartozik, köszönhetően hatékonyságának, minőségének és költségtakarékosságának. További előnye, hogy a tananyag önálló tanulással is elsajátítható, így a tananyagot saját haladási sebességgel, saját időbeosztással dolgozza fel a tanuló.

A 2021. évi XCIII. törvény (Vbö.) 19. §-ában és a Kat. tv. 42. §-ában meghatározott bejelentések értékelése után katasztrófa veszélye, kiterjedt káresemény és veszélyhelyzet esetén, az emberi élet és a létfenntartáshoz szükséges anyagi javak mentése érdekében a rendelkezésre álló riasztó-, illetve tájékoztató rendszertől függően szóveges közléssel, illetve szirénajelekkel kell jelezni az esemény bekövetkezését vagy annak elmúlását, illetve haladéktalanul közölni kell a lakossággal a követendő magatartási szabályokat..

A *gamification*, vagyis a „játékosítás” (gamifikáció) a felnőttek képzésében az egyik legnépszerűbb megoldás lehet. Az emberekben gyermekkoruktól kezdve él a jutalom és elismerés utáni vágy: jól elvégzett feladatért dicséret jár, ami jó érzéssel tölti el, további feladatok hatékony elvégzésére motiválja őket. Napjaink felnőttjei és gyermekei egyaránt szeretnek játszani, így a megfelelően kialakított gamifikáció jelentős segítséget nyújthat az oktatás területén. A megfelelő jutalmazási módszerek alkalmazásával minden ember ösztönözhető a hatékonyabb munkavégzésre, tanulásra. A gamifikációhoz szorosan kapcsolódnak a mobiltelefonokra és táblagépekre letölthető különböző applikációk, szimulációs játékok. Javasolom tehát egy alap katasztrófavédelmi oktatás játékos formában történő átadását és tesztelését, ahol helyes válaszokért és megoldásokért pontokat, jutalmakat, érmekeket lehet gyűjteni, ezáltal a játékosok egyre magasabb szinteket érhetnek el a játékban.¹⁸

A 14. ábrán egy játékos feladat látható, amely a menekülőcsomag tartalmát hivatott bemutatni. A helyes válaszok esetén az adott tárgy táskába húzásakor zöld pipa jelenik meg, míg helytelen válasz esetén piros x. A táskába húzható tárgyak között szerepelnek személyes iratok, ruhaneműk, alsóneműk, hálósák, szájmaszk, ivóvíz, tartós élelmiszer, készpénz, tisztálkodószerek, gyógyszerek, valamint gyermekeknek játékok. A helytelen válaszok között szerepel játékkonzol, cserepes virág, valamint kenyérpírtó.

¹⁷ A távoktatás és az e-learning fajtája, amely során a tanuló bárhol és bármikor tanulni képes hálózati kötöttségek nélkül laptopon, tableten vagy mobiltelefonon.

¹⁸ KOVÁCS-HORNYACSEK 2019: 123–127.

Mit tartalmazzon a menekülőcsomag?



14. ábra: Mit tartalmazzon a menekülőcsomag? gamification játék. (A táskába behúzva a különböző tárgyakat láthatjuk, hogy helyesen ismerjük-e a menekülőcsomag tartalmát.)

Forrás: Mikes Adél szerkesztése

Az oktatási anyag oktatási segédanyagként is használható, amelyet nyomtatott és online formában is szükséges elérhetővé tenni a lakosság számára. Igény esetén az oktatási anyag „számonkérése” is teszt, játékos feladatok formájában történhet. Ezenfelül javasolt a katasztrófavédelmi és rendvédelmi napokon felnőtteknek szóló előadások megtartása a kidolgozott oktatási anyagból. Az előadások utáni tesztek végén a helyes válaszokat apró katasztrófavédelmi ajándékokkal, például kulcstartóval, bevásárlókocsi-érmével, nyakba akasztóval, tollal, jegyzetfüzettel vagy hűtőmágnessel jutalmaznak. A BM OKF a rendvédelmi napokon a jutalmazás ezen eszközét évek óta sikeresen alkalmazza.

Összegzés

A felmérés adatai azt mutatják, hogy az okostelefonra és az online platformokra alapozott katasztrófavédelmi kommunikáció lehet a leghatékonyabb tájékoztatói és riasztási forma a katasztrófavédelem területén, azonban a hagyományos eszközökre és a lakosság edukációjára is szükség van a sikeres védekezés érdekében. Ennek megoldására javaslatom – a széles körű internet- és okostelefon-használat miatt – a katasztrófavédelmi kommunikáció fő csatornájaként a mobiltelefonos és az online tájékoztatás prioritásként kezelése. Ez alatt nemcsak a hivatásos katasztrófavédelmi szervek (például BM OKF) hagyományos információs csatornáit (weboldal, Facebook, Instagram, YouTube és SMS-riasztások) értem, hanem a komplex, kétirányú

lakossági kommunikáció, interaktív alkalmazások, frissített tájékoztató anyagok és szimulációs modulok kialakítását is. Célom az, hogy a már meglévő technológiai lehetőségek mellett további digitális innovációkat, fejlesztéseket vezessünk be, például:

- egyéni veszélyhelyzeti értesítések és helyzetfüggő tájékoztató üzenetek;
- online tananyagok és tesztek okostelefonos elérésének bővítése;
- visszacsatolás és lakossági aktivitás növelése digitális platformokon.

Az új fejlesztési irányokkal a magyar lakosság minél szélesebb körét tervezem elérni, adaptívabb, felhasználóbarátabb módon. A KSH adatai szerint 2024-ben a háztartások internetkapcsolat-típusainak aránya az alábbiak szerint oszlik meg: 90,5% rendelkezik helyhez kötött széles sávú internetkapcsolattal, 84,8% rendelkezik mobil széles sávú kapcsolattal.¹⁹ Szintén a KSH adatai szerint 2025. I. negyedévében a mobil-előfizetések száma 14 829 000 darab volt.²⁰ Ezen számok tükrében a mobiltelefonos riasztási rendszer kiterjesztése és hatékonyságának növelése érdekében érdemes azokat is elérni, akik eddig még nem használták ezt a riasztási formát. A „mobiltelefonos riasztási rendszer” alatt Magyarországon elsősorban az SMS-alapú, földrajzilag meghatározott területre célzott veszélyhelyzeti értesítési rendszert értjük (Veszélyhelyzeti Értesítési Szolgáltatás, MoLaRi). Ez a rendszer SMS-ben küld riasztó és tájékoztató üzeneteket a veszélyeztetett területen tartózkodó mobil eszközökre, amelyek több ezer hangszórós szirénahálózattal is kiegészülhetnek. A rendszer fejlesztése biztosítja, hogy az üzenetek gyorsan és a lehető leghatékonyabban eljussanak az érintettekhez.

Fontos megjegyezni, hogy a rendszer nemcsak az SMS-üzenetek egyszerű kiküldését jelenti, hanem a lakosság lehetőség szerinti interaktív tájékoztatását is, valamint a modern okostelefonos alkalmazások szerepe egyre növekszik a veszélyhelyzeti kommunikációban. Jövőbeni fejlesztési irányok közé tartozik a helyalapú *cell broadcast* technológia bevezetése, amely az összes mobiltelefont egy adott cellán belül egyszerre tudja elérni, így növelve a hatékonyságot és lefedettséget.

Ezek tükrében a „mobiltelefonos riasztási rendszer kiterjesztése és hatékonyságának növelése” azt jelentené, hogy célzottan elérjünk olyan lakosokat is, akik eddig nem használták vagy nem vették észre a kapott riasztásokat, illetve bővítsük a kapcsolatfelvétel módjait, például okostelefonos alkalmazások, digitális platformok bevonásával.

A rádió és televízió továbbra is nélkülözhetetlen kommunikációs csatornái a katasztrófavédelmi tájékoztatásnak, különösen az idősebb korosztály számára, akik esetleg kevésbé használnak digitális, online platformokat. Célzott oktatással és tájékoztatással elősegíthető, hogy a lakosság tisztában legyen azzal, mely rádió- és televíziócsatornákat érdemes követni katasztrófa helyzetekben.

Ugyanakkor indokolt a veszélyhelyzetek definíciójának és a gyakori károkat okozó, de jogilag nem veszélyhelyzetként besorolt események (például viharok, aszályok, villámárvizek) kiemelt kezelése is, mivel ezek Magyarországon évente ismétlődően jelentős károkat okoznak, és a lakosság rezilienciájának erősítése szempontjából fontosabb kihívást jelentenek.

¹⁹ Központi Statisztikai Hivatal 2025d.

²⁰ Központi Statisztikai Hivatal 2025e.

Érdemes a kommunikációban ezekre a természeti jelenségekre és az ezekhez kapcsolódó közterületi figyelemfelkeltő intézkedésekre (például tavi viharjelzés, parkolási szabályok, népegészségügyi figyelmeztetések hőhullámok esetén) is fókuszálni. Emellett a tájékoztatási csatornák között meg kell említeni az Útinform rendszert is, amely a közlekedők számára alapvető, könnyen elérhető információforrásként szolgál veszélyes időjárás és közlekedési körülmények esetén.

A szükségtartalékok esetében a *power bankok* és egyéb szükségtartalék-eszközök fontosságát hangsúlyozni kell a lakosság körében, különösen olyan területeken, ahol áramkimaradások gyakran előfordulhatnak.

Az oktatás során érdemes hangsúlyozni, hogy hol találhatók hiteles információk (például katasztrófavédelmi honlapok, megbízható híroldalak). Ez csökkentheti az információhiányból eredő kockázatokat. Az anyagból diabemutató készítése ajánlott, amelyet oktatási anyagként lehet használni munkahelyeken, katasztrófavédelmi nyílt napokon.

Összességében megállapítható, hogy a jogi környezet megfelelő alapot nyújt az oktatóanyag és vele a katasztrófavédelmi alapoktatás bevezetéséhez, azonban jogszabályi változtatásra szükség van, amennyiben a rendszert elfogadják.

További javaslatom, hogy az oktatási anyag széles körű eljuttatása e-learning (online tanfolyamok) és m-learning (mobilalkalmazás-alapú tanulás) formájában történjen, valamint játékos oktatóanyagok (gamifikáció) bevonásával is növeljük a lakosság katasztrófákkal szembeni ellenálló képességét.

Az oktatási anyag alatt olyan, a felnőtt lakosság számára kialakított, könnyen érthető és interaktív tananyagot értek, amely bemutatja a katasztrófák fő típusait, a helyes magatartási szabályokat, valamint a riasztási és tájékoztatási módszereket. Az anyag célja, hogy a közvetítendő információk ne csak száraz ismeretek legyenek, hanem a lakosság számára motiváló, személyre szabott és gyakorlatias tudást nyújtson a veszélyhelyzetek kezeléséhez. Az oktatási anyag teljes kidolgozását jövőbeni kutatási célként fogalmazom meg.

Fontos hangsúlyozni, hogy ez nem jelenti azt, hogy minden 18 évesnek azonnal egyetemi szintű katasztrófavédelmi képzésben kellene részt vennie – ilyen átfogó képzés jelenleg elérhető például a Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézetében –, hanem egy könnyen elérhető, tömeges alapoktatási rendszer kidolgozása és bevezetése a cél, amely széles körben és hatékonyan fejleszti a lakosság felkészültségét. Az oktatás kivitelezésében, ismételten fontos hangsúlyozni a munkahelyi katasztrófavédelmi előadók szerepét, illetve a polgári védelmi szervezetek bevonását.

Az elméleti oktatás kiegészítéseként gyakorlati oktatás és szimulációs gyakorlatok szervezését javaslom, amelyek elősegítik a lakosság számára a megszerzett ismeretek hatékony elsajátítását és alkalmazását. A további kutatási irányok között fontos a gyakorlati oktatási módszerek és szimulációs gyakorlatok részletes vizsgálata, amelyek hozzájárulhatnak a lakosság katasztrófavédelmi felkészültségének hatékonyabb fejlesztéséhez. Javasolt, hogy a következő kutatások fókuszában egy kis, jól körülhatárolt mintán végzett, mélyreható vizsgálatok álljanak, amelyek feltárják ezen innovatív képzési formák fejlesztési lehetőségeit és alkalmazhatóságát a gyakorlatban.

Az idősebb generáció esetében a nyomtatott kiadványok, szórólapok, brosúrák, naptárak, valamint a televízió- és rádiócsatornák műsorai maradnak az elsődleges

információforrások, míg a fiatalabb korosztály esetén az interneten megtalálható információk, az oktatóvideók, a podcastok, az okostelefonokra letölthető alkalmazások lehetnek a gyakorlati felkészítés kiegészítő elemei. A lakosság katasztrófavédelmi felkészítésének egyik elsődleges célja a figyelem felkeltése és az alapvető tudás átadása, amely megalapozza a tudatos és felelősségteljes magatartás kialakítását. A hatékony kommunikáció és oktatás érdekében célszerű alkalmazni a modern technológiai eszközökön alapuló módszereket, mint például az online platformokat, közösségimédia-csatornákat, interaktív tananyagokat, valamint hagyományos médiát, mint a rádió és televízió, különösen a különböző korosztályok igényeit figyelembe véve.

A 2023-as és 2024-es adatok tükrében a BM OKF kommunikációs szolgálata több ezer bejegyzést és közleményt tett közzé, amelyek milliós megtekintéssel és jelentős közönségeléréssel bírnak, alátámasztva a meglévő tájékoztatási tevékenység hatékonyságát. A cél azonban nem csupán a széles körű elérés, hanem a közönség aktivizálása, az interakció és az információ tudatos befogadása, amely elősegíti a lakosság felkészültségének növekedését.

Ezen komplex megközelítés révén biztosítható, hogy a lakosság tagjai ne csak értesüljenek a veszélyhelyzetekről, hanem megtanulják a megfelelő magatartási formákat és cselekvési terveket is, így növelve az egyéni és közösségi rezilienciát.²¹

Felhasznált irodalom

- AMBRUSZ József (2025): A polgári védelmi kötelezettségre vonatkozó szabályok változásai és katasztrófavédelmi vonatkozásai a védelmi és biztonsági reform tükrében. *Védelem Tudomány*, Különszám, 20–25. Online: <https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/18920/15510>
- BOLGÁR Judit – MÓGOR Judit (2015): *A lakossági tájékoztatás lélektani kérdései*. Online: <https://vedelem.hu/letoltes/anyagok/257-a-lakossagi-tajekoztatasi-lelektani-kerdesei.pdf>
- Borsod-Abaúj-Zemplén Vármegyei Katasztrófavédelmi Igazgatóság (2020): *Lakossági tájékoztatók – KVT lakossági tájékoztató Miskolc*. Online: <https://baz.katasztrofa-vedelem.hu/16833/lakossagi-tajekoztatok>
- ENDRŐDI István (2007): *A katasztrófa-elhárításra felkészítő ismeretek*. Egyetemi szakanyag. Online: http://dmn29.admin.tagi.rsoe.hu/wp-content/uploads/2023/08/Katasztrorfa-elharitsra_felkeszito_ismeretek.pdf
- HORNYACSEK Júlia – BARTA Ágnes (2020): A lakosság árvízi felkészítésének feladatai és módszerei. *Hadtudományi Szemle*, 13(2), 179–189. Online: <https://doi.org/10.32563/hsz.2020.2.14>
- KOVÁCS Gergely – HORNYACSEK Júlia (2019): Korszerű oktatási eszközök és módszerek alkalmazása a polgári védelmi felkészítésben. *Műszaki Katonai Közlöny*, 29(2), 117–132. Online: <https://doi.org/10.32562/mkk.2019.2.10>
- Központi Statisztikai Hivatal (2025a): 22.1.1.2. *A népesség száma és átlagos életkora nem szerint*. Online: www.ksh.hu/stadat_files/nep/hu/nep0002.html

²¹ HORNYACSEK–BARTA 2020: 181.

- Központi Statisztikai Hivatal (2025b): *Magyarország népességének száma nemek és életkor szerint, január 1.* Online: www.ksh.hu/interaktiv/korfak/orszag.html
- Központi Statisztikai Hivatal (2025c): *4 millió 669 ezer fő volt a foglalkoztatottak száma, a munkanélküliségi ráta 4,3%.* Online: www.ksh.hu/gyorstajekoztatok/fem/fem2505.html
- Központi Statisztikai Hivatal (2025d): *12.1.1.14. A háztartások internetkapcsolat típusainak aránya [%]*.* Online: www.ksh.hu/stadat_files/ikt/hu/ikt0016.html
- Központi Statisztikai Hivatal (2025e): *22.1.1.2. Mobil-előfizetések és hívások száma, mobil adatforgalom negyedévente.* Online: www.ksh.hu/stadat_files/ikt/hu/ikt0032.html
- Magyarország nemzeti katasztrófakockázat-értékeléséről szóló jelentése* (2023). Online: www.katasztrofavedelem.hu/application/uploads/documents/2024-01/83120.pdf
- MUHORAY Árpád (2012): A katasztrófavédelem aktuális feladatai. *Hadtudomány*, 22(E-szám). Online: <https://ojs.mtak.hu/index.php/hadtudomany/article/view/6270/4913>
- NOVÁKY Mónika (2018): Lakosságvédelem – Polgári védelem Izraelben. *Műszaki Katonai Közlöny*, 28(4), 59–79. Online: <https://folyoirat.ludovika.hu/index.php/mkk/article/view/1519/836>
- SZABÓ Csaba – AMBRUSZ József szerk. (2023): *A katasztrófavédelem lakosságfelkészítési feladatai.* Budapest: Pytheas Könyvmanufaktúra.
- VARRÓ Tekla (2024): Új képzési és felkészítési formák, módszerek alkalmazhatósága a hazai katasztrófavédelemben. *Védelem Tudomány*, 9(4), 130–162. Online: <https://doi.org/10.61790/vt.2024.17742>
- World Meteorological Organization (2021): *Weather-Related Disasters Increasing Over Past 50 Years, Causing More Damage but Fewer Deaths.* Online: <https://wmo.int/media/news/weather-related-disasters-increase-over-past-50-years-causing-more-damage-fewer-deaths>

Jogi források

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról. Online: <https://njt.hu/jogszabaly/2011-128-00-00>
2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről. Online: <https://njt.hu/jogszabaly/2021-140-00-00>
2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról. Online: <https://njt.hu/jogszabaly/2021-93-00-00>
- 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról. Online: <https://njt.hu/jogszabaly/2011-234-20-22>
- 62/2011. (XII. 29.) BM rendelet a katasztrófák elleni védekezés egyes szabályairól. Online: <https://njt.hu/jogszabaly/2011-62-20-0A>

Szajkó Gyula¹

Az Összhaderőnemi Logisztikai Felderítő Csoport lehetséges összetételének meghatározása és alkalmazása az MH szervezeti struktúrájában

The Possible Composition of the Joint Logistic
Reconnaissance Team and Its Application in the
Hungarian Defence Forces

Absztrakt

A Magyar Honvédség (MH) – a globális és kontinentális szervezetek tagjaként (NATO, ENSZ, EU) – különböző műveletekben, kiképzéseken és gyakorlatokon vesz részt, hogy teljesítse szövetségesi kötelezettségeit, valamint biztosítsa csapatainak felkészültségét az alaprendeltetési feladatok végrehajtásához. A katonai műveleteknél meghatározó, hogy az erők mozgatása és ellátása az előre meghatározott parancsnoki követelmények figyelembevételével valósuljon meg. Ennek érdekében a haderők átfogó tervet készítenek, amelynek egyik részeleme a műveletek logisztikai támogatásával kapcsolatos elemzések elkészítése. A művelettervezést végző törzsek számára kulcsfontosságú, hogy valós idejű információkkal rendelkezzenek a közlekedési alágazatok igénybevételének lehetőségeiről, a raktár- és javítóbázisok kapacitásadatairól, az ellátási forrásokról, a befogadó nemzeti támogatás (BNT), valamint a harmadik fél által nyújtott szolgáltatásokról. A logisztikai támogatást befolyásoló tényezőkről szóló adatokkal hatékonyan lehet hozzájárulni a parancsnokok törzsének döntés-előkészítési tevékenységéhez, mivel ezek az információk hatással lehetnek az erőforrások mennyiségére, felhasználására és azok optimális elosztására.

¹ Tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Katonai Logisztikai Intézet, Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék, e-mail: szajko.gyula@uni-nke.hu

Az előzetes adatok összegyűjtésében lényeges szerepet tölt be az Összhaderőnemi Logisztikai Felderítő Csoport, amely elsők között települ a műveleti területre, hogy tevékenységével hozzájáruljon a műveletek sikeres tervezéséhez és végrehajtásához. Az MH azonban nem rendelkezik hasonló jellegű csoporttal, és nincs olyan szervezeti eleme, amely logisztikai felderítést végezne, vagy a BNT-vel (szolgáltatások biztosíthatóságával, infrastruktúrák igénybevételeivel) kapcsolatban helyszíni szemrevételezést hajtana végre. Ezért a cikkben a szerző célja, hogy bemutassa a felderítő csoport lehetséges feladatait, hogy ezt követően javaslatot tegyen az összetételére és az MH-ban történő elhelyezkedésére, amelyet alkalmazva növelni lehetne a műveletek tervezésének és végrehajtásának hatékonyságát.

Kulcsszavak: logisztikai felderítés, összhaderőnemi logisztikai felderítő csoport, információ, biztosítás, állománytábla, összetétel

Abstract

The Hungarian Defence Forces (hereinafter: HDF), as a member of global and continental organisations (NATO, UN, EU) takes part in various operations, trainings, and exercises to fulfil its allied obligations and ensure the readiness of its troops for performing their primary mission tasks. In military operations, it is crucial to carry out the movement and supply of forces by considering the predefined command requirements. The armed forces create a comprehensive plan, which involves analyses related to logistical support to operations. It is essential for the staffs to have real-time information about the availability of transportation networks, capacity data of storage and repair bases, supply sources, about the host nation support, and contractor support to operations. Information about the factors influencing logistical support can effectively contribute to the decision-making process of commanders' staffs, these details have an impact for the quantity, utilisation and optimal distribution of resources. The Joint Logistic Reconnaissance Team plays a key role in collecting preliminary data, which will be deployed first at the operational area to contribute to the successful planning and execution of operations. However, the HDF does not possess a similar group, nor does it have any organisational element, which can conduct logistic reconnaissance or carry out site survey about HNS (considering availability of services or use of infrastructure). Therefore, the aim of this article is to show the potential tasks of the reconnaissance team, and then make a proposal for its composition and placement within the Hungarian Defence Forces, which could be used to increase the efficiency of planning and executing operations.

Keywords: logistic reconnaissance, Joint Logistic Reconnaissance Team, information, providing, personal table of organisations, composition

Bevezetés

A katonai műveletek végrehajtásakor rendkívül fontos, hogy az erők mozgatása, szállítása és ellátása a parancsnoki elvárások szerint valósuljon meg. Ennek érdekében a haderők művelettervezést végeznek, amelynek segítségével biztosítani lehet a kitűzött célok elérését. A műveletek hatékony, valamint megbízható tervezéséhez és szervezéséhez

azonban szükséges, hogy a törzsek valós idejű, valamint pontos információkkal rendelkezzenek a logisztikai támogatást befolyásoló tényezőkről, mivel ezek az adatok hatással lehetnek az alkalmazandó erők nagyságára, az erőforrások mennyiségére, felhasználására és azok optimális elosztására. Az előzetes adatok összegyűjtésében, valamint az erők ellátásával kapcsolatos helyzetértékelés kialakításában lényeges szerepet tölt be az Összhaderőnemi Logisztikai Felderítő Csoport (ÖLFCS), amely elsőik között települ a műveleti területre, hogy tevékenységével hozzájáruljon a műveletek sikeres tervezéséhez és végrehajtásához. A jelentőségét jól mutatja, hogy a NATO alkalmazza ezt a csoportot és képez ki hozzá személyi állományt, hogy az általuk teljesített felderítői, összekötői feladatokkal is támogassák a műveletek logisztikai támogatásáért felelős csoportok² munkálatait.

Az MH azonban nem rendelkezik hasonló jellegű csoporttal, és nincs olyan szervezeti eleme, amely logisztikai felderítést végezne vagy műveleti területen a BNT lehetőségeivel kapcsolatban helyszíni szemrevételezést, valamint értékelést végezne.

Felmerülhet a kérdés, hogy a Magyar Honvédség (MH) hogyan tudta akkor biztosítani a művelettervezéshez szükséges kezdeti adatok rendelkezésre állását a szervezeti elemek, törzsek részére, hiszen az elmúlt évtizedekben is részt vett különböző műveletekben. Elmondható, hogy a Honvédelmi Minisztérium és az MH az együttes intézkedéseik, utasításaik kiadásával, valamint szakértő személyek kijelölésével valósítják meg valamely művelet előkészítéséhez és tervezéséhez szükséges adatok begyűjtését, felderítését. A hatékony feladat-végrehajtás érdekében azonban célszerű lehet a minden egyes új küldetésre kiadott parancsok, intézkedések stb. alkalmazása és szakértő személyek (ideiglenes) kijelölése helyett egy olyan logisztikai felderítéssel foglalkozó csoportot alakítani az MH-nak, amely – a NATO eljárásait figyelembe véve – képes a feladat vételét követően rövid időn belül települni a műveleti területre és információkat gyűjteni a szükségleteknek megfelelően. Ehhez érdemes megvizsgálni a csoporthoz kapcsolódó tevékenységeket, majd meghatározni a személyi állomány lehetséges összetételét.

Ennek megfelelően a fő célkitűzésem, hogy – a teljességre törekvés igénye nélkül – bemutassam az ÖLFCS feladatait, majd ezt követően javaslatot fogalmazzak meg az összetételükre és az MH-ba illeszthetőségükre vonatkozóan, amelyet alkalmazva növelni lehetne a logisztikai támogatás tervezésének és végrehajtásának hatékonyságát.

Az Összhaderőnemi Logisztikai Felderítő Csoport feladatai

Az ÖLFCS feladataihoz köthető kutatásokkal, tudományos értekezésekkel és tanulmányokkal ritkán lehet találkozni a magyar és a külföldi (katonai jellegű) szakirodalmakban. A hadszíntér felderítésével és a logisztikai támogatással foglalkozó kutatók eredményei azonban támpontot nyújtanak az elemzési feladatok végrehajtásához. Ezek közé sorolhatók Báthy Sándor, Forray László, Resperger István, Pohl Árpád, Szászi Gábor, Deák Péter, Venekei József publikációi, valamint Luke P. High, William T. Smith, Charles Kurz tanulmányai, cikkei. Az ÖLFCS működésével kapcsolatos

² A NATO által vezetett többnemzeti műveletekben a logisztikai támogatás tervezésért és szervezésért a Joint Logistic Support Group (Összhaderőnemi Logisztikai Támogató Csoport [ÖLTCS]) a felelős. AJP-4.6 2018: 41.

dokumentumokat, szabályzatokat minősített adatokként tartja nyilván a NATO, így csak korlátozott mértékben lehet rájuk utalni és taglalni a bennük foglalt információkat. Ezek közül kiemelkedik a JLSG SOP³ 701.03 utasítás és a nyílt adatforrású AJP-4.6⁴ szabvány, amelyek kitérnek például az ÖLFCS küldetésére is. A dokumentumok alapján a csoport feladatai közé tartozik, hogy az információgyűjtő tevékenységén keresztül eredményesen támogassa az ÖLTCS tervezési munkálatait. Ennek érdekében a logisztikai felderítési és összekötői feladatai kitérnek:

- a lehetséges (például a légi, tengeri, vasúti) kirakó pontok jellemzésére;
- a potenciális bázisok, létesítmények, területek vizsgálatára, amelyek alkalmasak az erők állomásoztatására;
- a vasút- és közúthálózatok értékelésére;
- a körletek szemrevételezésére, amelyek megfelelőek lehetnek a csapatok gyülekeztetésére;
- az ÖLTCS hadszíntéri parancsnokságának lehetséges helyszíneinek feltérképezésére;
- a BNT keretében és a harmadik fél által nyújtható szolgáltatásokra, termékekre, például a hozzájuk kapcsolódó díjakra, vámokra;
- a biztonsági helyzetértékelésre, amely befolyásolhatja az erők átcsoportosítását és továbbmozgását.
- összeköttetés kiépítésére a befogadó nemzet küldött képviselőivel, a biztonsági szolgálatokkal, a hadszíntéren állomásozó katonai erők összekötő tisztjeivel, a nem kormányzati szervezetek közvetítőivel, a polgári cégekkel, amelyek szolgáltatásokat, anyagokat, eszközöket biztosíthatnak a saját csapatok részére.⁵

A felsorolás alapján az ÖLFCS feladatait két nagy csoportra lehet osztani, amelyet az 1. táblázat szemléltet. Az ÖLFCS állománytáblájára és összetételére vonatkozó információk szintén nem nyilvános adatként szerepelnek a korábban említett JLSG SOP 701.03 utasításban. Ennek megfelelően az ÖLFCS személyi összetételével kapcsolatos javaslatomat a logisztikai felderítői és összekötői feladatok részletezésén keresztül fogalmazom meg.

Az összekötői tevékenységeken belül a helyi kormányzati és nem kormányzati, valamint nemzetközi (például humanitárius, jogi, vallási vagy gazdasági) szervezetekkel kialakított kapcsolatokon keresztül adatokat lehet gyűjteni a politikai pártok tevékenységéről, az általuk gyakorolt befolyás mértékéről (az ország vagy az érdekeltségi terület vezetésére, gazdaságára vonatkozóan), a hadszíntéren állomásozó katonai, rendfenntartó erők állapotáról, valamint azokról a vállalkozásokról, amelyek alkalmasak lehetnek a szolgáltatások nyújtására és a termékek biztosítására. Az információgyűjtő feladatok sikeres végrehajtása érdekében célszerű (felderítő, CIMIC,⁶ hadműveleti és a logisztikai támogatásban tapasztalatokkal rendelkező) tiszteket kijelölni, akik mélyrehatóan tudják elemezni katonai szempontból a hadszíntéren fennálló helyzetet (például a fegyveres csapatok érdekeit, a diverzáns csapatok lehetséges céljait, a politikai pártok befolyását vagy a helyi vállalkozások megbízhatóságát stb.).

³ *Standard operating procedure, SOP.*

⁴ *Allied Joint Publication, AJP.*

⁵ *Joint Logistics Support Group 2011: 5.*

⁶ *Civil-military cooperation – civil-katonai együttműködés.*

1. táblázat: Az ÖLFCS tevékenysége a hadszíntéri kitelepülésekor

ÖLFCS	
Összekötői feladatok	Felderítői feladatok
1. Kapcsolat kiépítése a helyi kormányzati szervezetekkel	6. Hadszíntéri kikötők felderítése
2. Összeköttetés létesítése a helyi nem kormányzati szervezetekkel, vállalkozásokkal	7. Hadszíntéri repülőterek felderítése
3. Kapcsolat kiépítése a nemzetközi szervezetekkel	8. Közúthálózatok értékelése
4. Összeköttetés a hadszíntéren állomásozó katonai erők képviselőivel	9. Vasúthálózatok értékelése
5. Kapcsolat kiépítése a befogadó nemzet küldött képviselőivel	10. Hadszíntéri Logisztikai Bázis felderítése
	11. A műveleti területre települő parancsnokság lehetséges helyszíneinek felderítése
	12. Az erők állomásoztatására, valamint gyűleltetésére alkalmas területek feltérképezése
	13. Információk gyűjtése az infrastruktúrák, szolgáltatások után fizetendő díjakról, vámokról stb.

Forrás: a szerző szerkesztése a Joint Logistics Support Group 2011 alapján

A katonai képviselőkkel folytatott tárgyalások, értekezletek fontosak lehetnek abból a szempontból, hogy a felderítő csoport információkat szerezzen a műveleti területen állomásozó erőkről, azok elhelyezkedéséről, képességeiről és szándékáról. A sikeres adatgyűjtéshez széles körű biztonságpolitikai szakértelemmel rendelkező szakértők szükségesek, akik képesek stratégiai szinten értelmezni a kialakult helyzetet, és a megfelelő módszerek alkalmazásával tudják elemezni a megszerzett információkat.⁷

A befogadó nemzet képviselőivel kialakított kapcsolatokon keresztül az ÖLFCS kulcsfontosságú adatokat szerezhet a BNT keretében nyújtott, valamint harmadik fél által elérhető szolgáltatásokról és a rendelkezésre álló hadszíntéren található katonai és rendfenntartó erők állapotáról. Ezekkel az információkkal hozzá lehet járulni a logisztikai támogatás tervezési folyamataihoz. Jelentősen segítheti műveleti területen az ellátás megszervezését, ha például technikai megállapodások alapján igénybe lehet venni a közlekedési alágazatok infrastruktúráit, vagy szolgáltatásokat, anyagokat és eszközöket lehet rendelni az állami szervezetektől, civil vállalkozásoktól (például műveleti bázisok ellátáshoz közüzemi vagy egyéb szolgáltatásokat). A sikeres együttműködés kiépítéséhez, valamint a megállapodások előkészítéséhez a BNT-hez kapcsolódó eljárások lefolytatásában tapasztalattal rendelkező logisztikai, pénzügyi, jogi és összekötő tiszteket célszerű delegálni.

⁷ Válságreakáló műveletekben például, amikor ENSZ-felhatalmazás alapján szövetséges csapatokat vezényelnek a béke megőrzése, helyreállítása érdekében egy konfliktusövezetbe, ott a szomszédos, valamint az érintett országok katonai képviselőivel folytatott tárgyalásoknál az ÖLFCS-nek szüksége lesz olyan szakmailag felkészült tisztekre, személyekre, akik (biztonság)politikai tapasztalattal, ismeretekkel is rendelkeznek.

A felderítéshez köthető tevékenységek közül a tengeri kikötők értékelésére akkor lehet szükség, ha kontinenseken átívelő (honi bázistól távoli) műveletet kell végrehajtani, és a haditechnikai eszközöket gazdaságosabb, előnyösebb vízi közlekedésen keresztül szállítani. Az infrastruktúra-elem felderítésekor ki kell térni a kikötői vízterület (például a bekötőcsatornák, vízi utak szélességének, hosszának, mélységének), a létesítmények (horgonyzóhelyek, hajóállások elhelyezkedésének), a működést biztosító infrastruktúrák, a szolgáltatások és a vasúti, közúti csatlakozási pontjainak jellemzésére, valamint a fejlesztési lehetőségekre. Az értékelési folyamathoz hozzátartozik, hogy a felelős logisztikai szervezetek a megszerzett adatok alapján megvizsgálják, milyen mértékben felelnek meg az infrastruktúra-elemek a csapatok szállítási szükségleteinek kielégítésére. Ezzel kapcsolatosan a NATO meghatároz képességekre vonatkozó követelményeket is, amelyeket szükséges figyelembe venni az átcsoportosítások megkezdése előtt. Az infrastruktúra-elemmel szemben alapvető elvárás például, hogy rendelkezzen Ro-Ro⁸ komp kikötőhellyel, amely legalább 300 méter hosszú, 40 méter széles, 12 méter mély, valamint legyen alkalmas naponta 1 db 6. generációs konténerhajó, ezen belül 750 db haditechnikai eszköz, valamint 4000 db 20 lábas konténer fogadására és minimum 250 fő ellátására (elhelyezés, étkeztetés).⁹ Mindezeket figyelembe véve véleményem szerint az adatok begyűjtésére célszerű műszaki, mérnöki tiszteket, valamint olyan közlekedési szakembereket alkalmazni, akik a vízi szállításban tapasztalattal rendelkeznek.

Az ÖLFCS feladatai közé tartozik a repülőterek részletes értékelése is. A felderítő csoportoknak érdemes megvizsgálni a repülőgépek le- és felszállását biztosító futópályák méretét, hosszát, lejtését, a futópályaküszöb elhelyezkedését és a gurulóutak tulajdonságait, valamint a forgalmi előterek kapacitásait, a fénytechnikai leszállító rendszerek üzemeltetését. Külön ki kell térni a légi forgalmi szolgáltatások (például a bevezető és a repülőtéri irányító szolgálat) működésének, valamint a légikikötő biztonságát garantáló erőforrásoknak (például a személyi feltételek, eszközellátottság) jellemzésére is. Ezenkívül érdemes felmérni a repülőtér közelében a személyi állomány pihentetésére és az eszközök tárolására, karbantartására alkalmas létesítményeket, objektumokat is. A jellemzésüknél célszerű tekintettel lenni arra a követelményre, hogy a katonai alkalmazhatóságánál (stratégiai szintű légi átcsoportosítások végrehajtásakor) a repülőtér rendelkezzen legalább 3048 méter hosszú és 60 méter széles futópályával, legyen alkalmas naponta 8 db C-17-es típusú repülőgép fogadására, valamint 1500 fő ellátására (elhelyezés, étkeztetés).¹⁰ Az ÖLFCS állományába ennek megfelelően szükséges delegálni légi szállításban tapasztalattal rendelkező közlekedési szakállományt, valamint elhelyezési, infrastrukturális tiszteket is.

A közúthálózatok felderítéséből származó adatok jelentős segítséget nyújtanak a szállítási feladatok sikeres tervezéséhez és szervezéséhez. Az utak osztályozásakor meg kell határozni például az útpálya szélességét, teherbírását, átbocsátó képességét, vagy a rajta elhelyezkedő csomópontok, műtárgyak méretét, valamint azokat

⁸ *Roll-on – roll-off* egy hajótípus, amelynél a közúti járművek be tudnak gördülni a hajótérbe, majd kirakáskor kihajtani, elkerülve a költséges és rendkívül időigényes rakodási feladatokat, például a daruzást. *Super International Shipping* [é. n.].

⁹ NATO SHAPE 2024: 25.

¹⁰ NATO SHAPE 2024: 22.

a fejlesztési feladatokat, amelyeket célszerű elvégezni (például a földutak járhatóvá tételét) a biztonságos közlekedés érdekében. Az értékeléskor érdemes figyelembe venni a közutakkal szemben támasztott katonai követelményeket is, amelyek egyrészt vonatkoznak a közlekedő járművekre, másrészt a hidak MLC¹¹ besorolására. Például ezzel összhangban olyan ellátási útvonalakat célszerű kijelölni a haditechnikai eszközök közlekedtetésére, amelyek minimum 4,5 méter sávszélességgel, 4,5 méter szabad magassággal (az adott útszakaszon nincs ennél alacsonyabb magasságkorlátozás), maximum 6%-os lejtési szöggel és 600 méteres hosszanti dőléssel rendelkeznek.¹² Összeségében a begyűjtött információk alapján már meg lehet tervezni a személyek és eszközök közötti szállítást. Ennek érdekében érdemes közlekedési és műszaki tiszteket kijelölni a felderítési feladatok végrehajtására.

A vasúti szállítás különösen fontos a szárazföldi hadászati és hadművelleti mozgékonyság biztosításában. Az infrastruktúra-elem feltérképezésekor ki kell térni a vonalak villamosítottságára, a pályák nyomtávolságára, teherbírására, az űr- és rakszelvényméretekre, valamint a vasútállomások kapacitásadataira és a gördülő állomány jellemzésére. Ezek a tényezők jelentősen korlátozhatják a katonai szerelvények leközlekedtetését, ami hatással lehet a műveletek logisztikai támogatására. Itt is megjelenik (NATO) katonai követelmény, amelyre célszerű figyelmet fordítani a felderítéskor. Alapvető elvárás például, hogy egy vasútállomás legyen képes legalább 125 jármű, valamint 625 tonna raklapos vagy konténeres rakomány, illetve ezek kombinációjának kirakodására a hét nap 24 órájában, valamint rendelkezzen olyan szilárd burkolatú területtel, ahol minimum 60 jármű elhelyezhető a konvojképzéshez.¹³ A kapacitásadatok begyűjtéséhez és értékeléséhez az ÖLFCS állományába véleményem szerint indokolt vasúti szállításban tapasztalattal rendelkező személyeket vezényelni.

A hadszíntéri logisztikai bázisok, létesítmények elhelyezkedése, kapacitásadatai, az igénybevételének szabályai, önmagában a rendelkezésre állásuk rendkívül fontos tényezők, mivel általuk valósítható meg hadművelleti területen az anyagok, eszközök tárolása és elosztása. A hadszíntéren egy elosztóközvet vagy raktárbázis kialakításakor – egy zászlóaljharccsoport szintű kötelék fogadása, ellátása érdekében – például az alábbi képességeket szükséges biztosítani:

- minimum 1000 fő részére ételmezési ellátást, szállást, egészségügyi szolgáltatást;
- minimum 200 db 20 lábas konténer tárolását, rakodását, kezelését;
- minimum 500 db haditechnikai eszköz tárolására, üzemanyag feltöltésére alkalmas létesítményt, telephelyet;
- megfelelő kommunikációs és információs rendszereket, amelyek lehetővé teszik a bázis üzemeltetését, valamint az adatok, jelentések fogadását és továbbítását;
- a vezetés és irányításhoz kapcsolódó feladatok végzésére alkalmas védett objektumot, létesítményt.¹⁴

¹¹ Military Load Classification: Katonai Járműteherbírási Osztályok. A NATO Stanag 2021 szabvány szerint az MLC-besorolás vonatkozik egyrészt a katonai járművek osztályba sorolására, másrészt a hidak, kompok, tutajok teherbíró képességére. HAJÓS 2024: 5–20.

¹² NATO SHAPE 2024: 28.

¹³ NATO SHAPE 2024: 28–30.

¹⁴ NATO Standardization Agency 2016: 39.

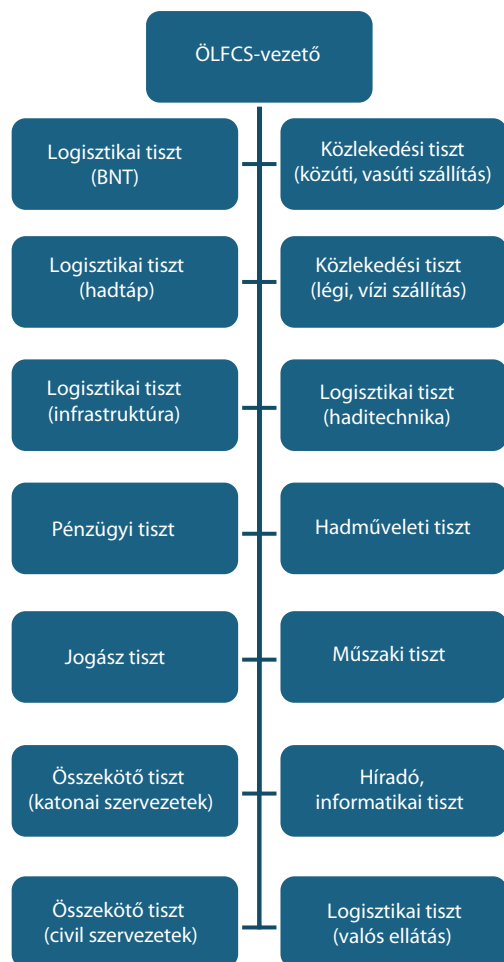
A felderítéskor tehát érdemes megvizsgálni minden olyan lehetséges létesítményt, logisztikai központot, amelyek megfelelőek lehetnek az anyagok, eszközök tárolására, fogadására, valamint elosztására. A feladatok végrehajtására véleményem szerint célszerű elhelyezési, infrastrukturális, valamint műszaki szaktisztákat kijelölni az adatok begyűjtésére és a megszerzett információk elemzésére.

Az ÖLFCS feladatai közé tartozhat továbbá az erők állomásoztatásához, telepítéséhez, a műveletek irányításáért felelős parancsnokság elhelyezéséhez szükséges területek, létesítmények, objektumok, katonai bázisok felderítése is. A részletes felméréshez meg kell vizsgálni, hogyan lehet kialakítani például egy műveleti bázis funkcionális elemeit (a parancsoki övezetet, a technikai területet, tartalmazva a telephely, javítópont, üzemanyag-ellátó pontot, az ellátási körleteket, beleértve a raktárakat, az étellemezési ellátó pontot, az elhelyezési övezetet), valamint az őr- és biztosító tevékenységek ellátáshoz a feltételeket. Ez egy összetett feladatként jelentkezik az ÖLFCS számára, és a végrehajtására több szakértő személyt, köztük hadtáp, haditechnikai, infrastrukturális, hadműveleti, pénzügyi, híradó és informatikai tiszteket érdemes kijelölni.

Az egyes szolgáltatások, termékek, közlekedési infrastruktúrák igénybevétele után fizetendő díjakról, adókról, vámokról is indokolt tájékozódni, információt gyűjteni a fogadó ország területén a felderítő csoportoknak. Ez a feladat az összekötői tevékenységekkel együtt jelentkezik, mivel a kormányzati szervezetekkel és vállalkozásokkal szükséges tárgyalásokat lefolytatni. Összességében az ÖLFCS lehetséges tevékenységeihez rendelt szakértő személyek meghatározásán keresztül összeállítható a csoport állománya, amelynek alkalmazásával hozzá lehet járulni a logisztikai támogatás tervezésekor és szervezésekor jelentkező információs igények kielégítéséhez. Az ÖLFCS általam javasolt összetételét az 1. ábra mutatja be.

Az előzőekben részletezett tevékenységekkel összhangban az ÖLFCS struktúrájában szerepelnek összekötő tisztek is. Létszámát tekintve (a vezetővel együtt) 15 főből áll, amely a várható feladatok függvényében kiegészülhet további tanácsadókkal, tisztekkel, például közlekedési szakemberekkel (külön a légi, vízi, közúti és vasúti szállításban tapasztalattal rendelkező személyekkel). A létszámnövelésre, a csoport megerősítésére akkor lehet szükség, ha a műveletek logisztikai támogatását tervező szervezetek részéről többlet információs igény jelentkezik, vagy a logisztikai felderítési feladatok végrehajtására minimális idő áll rendelkezésre. Az ÖLFCS állománytábláját tehát célszerű mindig igazítani a várható feladatokhoz. Amennyiben nincs szükség például a kikötők vagy repülőterek felderítésére (mivel használatuk nem tervezett), úgy érdemes a csoport létszámát ez alapján csökkenteni is.

Az ÖLFCS állományába elsődlegesen indokolt a BNT, a hadtáp, a haditechnikai, a közlekedési, az infrastrukturális vagy az elhelyezési területen szaktudással rendelkező tiszteket, műszaki, hadműveleti, híradó, informatikai, pénzügyi, jogi szakértőket, valamint összekötő tanácsadókat kijelölni, delegálni. Az 1. ábrán szerepel valós ellátásért felelős tiszt is. Az ő dolga, hogy megfelelő feltételeket teremtsen (például a szállítások szervezésén, valamint az étellemezési és elhelyezési stb. biztosításon keresztül) annak érdekében, hogy a csoport sikeresen el tudja látni feladatait.



1. ábra: Az ÖLFCS lehetséges összetétele

Forrás: SZAJKÓ 2025: 182

Véleményem szerint a 15 főből álló ÖLFCS képessé válhat – a hadszíntérre érkezve – információkat gyűjteni és feladatait sikeresen elvégezni.

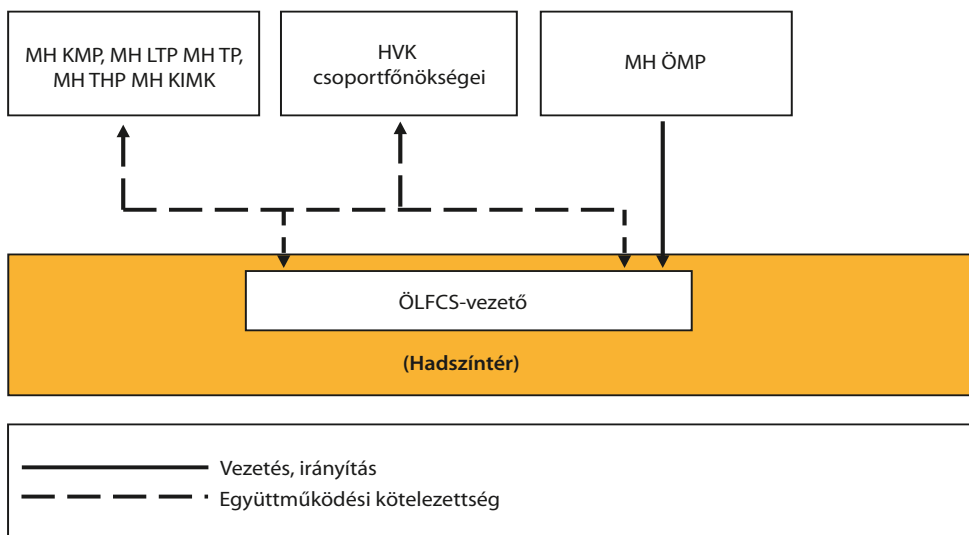
A logisztikai felderítést végző csoport illeszkedése az MH szervezeti struktúrájába

Az MH stratégiai szintű szervezeti átalakítása 2019-ben vette kezdetét, amely jelenleg is tart. A Honvéd Vezérkar (HVK) – mint legfelső szintű stratégiai szervezet – felelős az ország katonai védelemre való felkészítéséért, valamint az MH katonai

tevékenységeinek irányításáért. Fő feladata, hogy biztosítsa Magyarország szuverenitásának, határainak – ezen belül területe, légtere és kibertere – védelméhez, valamint a szövetségi rendszerekben vállalt kötelezettségek ellátásához szükséges katonai képességek kialakítását és fenntartását, továbbá az ezekhez szükséges feltételrendszert.¹⁵ Az újonnan kialakított rendszerben tehát a stratégiai szintű vezetésért, irányításért és tervezésért a HVK és közvetlen szervezeti elemei (csoportfőnökségei), míg a hadműveleti szintű feladatok végrehajtásáért – a HVK vezetése alatt működő – az alábbi szervezeti egységek felelősek:

- az MH Összhaderőnemi Műveleti Parancsnokság (MH ÖMP);
- az MH Különleges Műveleti Parancsnokság (MH KMP);
- az MH Logisztikai Támogató Parancsnokság (MH LTP);
- az MH Transzformációs Parancsnokság (MH TP);
- az MH Területvédelmi és Hadkiegészítő Parancsnokság (MH THP);
- az MH Kiber- és Információs Műveleti Központ (MH KIMK).

Ebben a struktúrában elsődlegesen meg kell határozni a felderítő csoport vezetés, irányítási rendszerét. Véleményem szerint az ÖLFCS-t az MH ÖMP alárendeltségébe érdemes utalni, mivel ez a katonai szervezet végzi a különböző („folyó”, valamint háborús) műveletek hadműveleti szintű tervezését, szervezését. Az általam javasolt vezetés, irányítási rendszert a 2. ábra szemlélteti.



2. ábra: Az ÖLFCS vezetés, irányítási rendszere műveletben

Forrás: a szerző szerkesztése SZAJKÓ 2025: 184 alapján

¹⁵ Honvéd Vezérkar 2025.

Az általam javasolt struktúrában az MH ÖMP parancsnoka mint a műveletek tervezéséért és szervezéséért felelős személy megszabhatja a felderítő csoport számára, mely feladatokat, adatokat kell kiemelten kezelni, hogy a művelettervezési folyamatok végrehajtása a kitűzött célokat elérve valósuljon meg. A csoport együttműködik a szakmai szervezetekkel, amelyektől iránymutatást (segítséget) kérhet, illetve pontosításokat adhatnak az ÖLFCS számára a begyűjtött információkkal, adatokkal kapcsolatban. A csoport állománytábláját úgy alakítottam ki, hogy önállóan is végre tudja hajtani feladatait. Ugyanakkor megerősítésére szükség lehet, amennyiben az elérendő célok ezt megkövetelik, például az ÖLTCS-be érdemes az általános katonai felderítésben szaktudással rendelkező tisztet és további összekötő tanácsadókat delegálni az információgyűjtés és az azt követő elemzés hatékonyságának növelése érdekében.

Az ÖLFCS összetételének és küldetésének meghatározásakor további vizsgálandó tényezőként jelenik meg, hogy milyen feltételekkel működtethető hatékonyan. A csoport alkalmazására többféle módszer áll rendelkezésre. Az egyik lehetőség az állandó, míg a másik az ideiglenes, vagy készenléti ÖLFCS-ként történő létrehozása. Véleményem szerint mindkét szervezeti kialakítás hordozhat magában előnyöket és hátrányokat is egyben. Az összehasonlításukhoz olyan tényezőket vettem figyelembe, amelyek egy műveleti alegység működtetésekor felmerülhetnek vizsgálandó szempontként. Ezek a következők:

- a csoport vezetése és irányítása;
- az állomány kiképzése;
- a humán erőforrásokkal és eszközökkel történő gazdálkodás;
- a csoport működési rendje.

A vezetési és irányítási rendszer kialakítása elsőrendű prioritás egy műveleti csoport megalakításakor annak érdekében, hogy az aktiválásuk, valamint alkalmazásuk a megfelelő időben és módon valósuljon meg. A kiképzések és gyakorlatok végrehajtása azért fontos tényező, mert biztosítja, hogy a műveleti feladatra kijelölt erők felkészüljenek a küldetéseik sikeres teljesítésére. Az erőforrásokkal történő hatékony gazdálkodás továbbá követelményként jelenik meg a katonai szervezetek működtetésekor, ennek megfelelően a csoportok kialakításakor is szükséges figyelembe venni. A működési rend befolyásolhatja (rövidítheti vagy növelheti a készenléti idő meghatározásával) a csoportok aktiválási és bevetési idejét. Ezek a tényezők tehát hatással lehetnek egy ideiglenes vagy állandó csoport alkalmazására. A 3. ábrán egy nem túl részletes SWOT- (*strengths, weaknesses, opportunities, threats*) analízissel vizsgáltam meg elsőként az állandó alkalmazással jelentkező várható hatásokat.

Erősségek • Az állomány kiértékelésének ideje gyorsabb és egyszerűbb • Folyamatosan rendelkezésre áll az állomány • Az állomány továbbképzésének tervezése és szervezése egyszerűbb	Gyengeségek • Rutinszerű feladatellátás, ami hibák előfordulásához vezethet • A tapasztalt és kiképzett állomány más feladatra nehezebben bevonható, ami akkor jelent nem hatékony humán erőforrásokkal történő gazdálkodást, ha csoport nincs alkalmazásban
Lehetőségek • A tapasztalatfeldolgozásból származó infomációk, eljárások könnyebben átülthetővé válnak részükre • Az előjáró számára elérhetővé válik a rövid idejű bevetetőségi képesség	Veszélyek • Az állandó alkalmazás költségnövekedést okozhat az MH számára • A rendszeresített beosztások betöltésével rugalmatlanabbá válik a személyek frissítése, cseréje • A folyamatos munkavégzéshez infrastruktúra- és eszközberuházásra van szükség

3. ábra: Az ÖLFCS állandó alkalmazásának SWOT-analízise

Forrás: a szerző szerkesztése

A csoport vezetését és irányítását az állandó alkalmazáskor egyszerűbben, gyorsabban meg lehet valósítani a parancs kiadásától a működés kezdetéig terjedő időszakban. Ez az előny és erősség azért jelentkezik, mert az állandó csoport katonái egy helyőrségben, egy szervezeti elemnél teljesítik szolgálati kötelezettségeiket szemben a készenléti csoport állományával, akik külön helyőrségben, más és más katonai szervezeteknél szolgálhatnak. Ebben a helyzetben a készenléti állomány kiértékelése és beérkezése – a felkészítés helyszínére – több időt vesz igénybe, mint akkor, ha a riasztást egy helyőrségben, egy szervezeti elemnek kell kiadni.

A felkészítéséről elmondható, hogy a kiképzett állomány folyamatos rendelkezésre állásával biztosítani lehet a csoport állandó működtetését mind békeidőszakban, mind különleges jogrendi időszakban egyaránt. Ráadásul a továbbképzések tervezésének és szervezésének feladatai is egyszerűbbé válhatnak, mivel az ÖLFCS parancsnoka könnyebben dönthet az állomány kirendelésének, vezénylésének engedélyeztetéséről, mint az ideiglenesen összeállított állomány vezetője, aki főként csak a szakemberek berendelését követően rendelkezik majd – hasonló jellegű kérdésekben – parancsnoki jogkörrel.

A gyengeségeket tekintve hátrányként említhető, hogy a képzett „tanácsadókat” nehezebben lehet az eredeti beosztásuktól független feladatokkal megbízni és vezényelni más alegységekhez, egységekhez, amennyiben a csoport nincs alkalmazásban. Ráadásul az állandó működés egyik velejárója, hogy a hosszú időn keresztül ugyanazt a beosztást betöltő személyeknél kockázati tényezőként jelenhetnek meg a régi rutinszerű feladatellátásokból eredő hibák, ami érintheti a katonákat is.¹⁶

Ugyanakkor lehetőségként értékelhető, hogy a tapasztalatfeldolgozásból származó fejlesztő javaslatok gyakorlatba történő átültetése gyorsabban megvalósítható, hiszen

¹⁶ BELÉNYESI 2014.

az állomány rövid időn belül tud reagálni a változtatásokra, tudja módosítani, átalakítani az eljárásrendeket és a kapcsolódó dokumentumokat. A csoport képessé válhat továbbá az elrendeléstől számított azonnali bevetettség biztosítására. Az ideiglenes alkalmazásnál ez csak készenléti erőként tartható fent, ráadásul ebben a helyzetben is a szakembereket „csak” bizonyos feladatok végzésére lehet bevonni, amelyek nem befolyásolják a riasztást követő beérkezések időintervallumát.

Veszélyként lehet értelmezni azt, hogy az állandó alkalmazást figyelembe véve a bérrel, beosztásokkal vagy a dologi költségvetéssel történő gazdálkodás szűkebb lehetőségeket biztosít a magasabb szintű parancsnokoknak, mivel új beosztásokat szükséges megalakítani, azokat szakemberekkel kell feltölteni, és hozzá illetményt is indokolt szolgáltatni a csoportnak. A rendszeresített állandó állomány frissítése és cseréje is rugalmatlanabbá válhat az ideiglenes működéssel megalakított csoporthoz képest, ahol bővebb lehetőség kínálkozik a személyek kiválasztására és szükség szerinti rotálására. Ez egyben azt is jelenti, hogy állandó alkalmazásnál a keretlétszámot is úgy érdemes kialakítani, hogy elegendő (felkészülő, felderítési, összekötői feladatot végrehajtó és regeneráló) váltás álljon rendelkezésre, amennyiben szükséges, hogy a felderítő csoportok a főerők megérkezését követően is tovább végezzék információgyűjtő tevékenységüket. Az állomány részére állandóan biztosítani kell megfelelő felszerelést, eszközöket, munkavégzésre alkalmas helyiségeket, amelyek további költségeket jelentenek az MH számára. Ezzel összefüggésben humán- és eszközkapacitás-felesleg keletkezik akkor, ha a két csoport nincs műveleti alkalmazásban.

A készenléti vagy más néven ideiglenes ÖLFCS megalakítása is rejt magában előnyöket és hátrányokat, amit a 4. ábra szemléltet.

Erősségek

- A tapasztalt és kiképzett állomány funkcionálisan több feladatba is bevonható, amikor a csoport nincs alkalmazásban
- A személyi állomány frissítése, cseréje könnyebben végrehajtható
- Csökkenhet a rutinszerű feladatellátásokból eredő hibák bekövetkezésének valószínűsége

Gyengeségek

- Az állomány kiértékelésének ideje hosszabbá és bonyolultabbá válhat
- Az állomány összeszokottságához több idő szükséges
- Hosszabb idejű bevetettség képesség

Lehetőségek

- A kiképzéseken és képzéseken keresztül bővíthet a kiválasztható szakemberek száma
- A készenléti alkalmazás kevesebb bérköltséget jelenthet az MH-nak
- Az infrastruktúra- és eszközberuházásból származó költségek kisebbek
- A rendelkezésre álló humán és eszközkapacitások felhasználhatók, ha csoport nincs alkalmazásban

Veszélyek

- A kiképzések, továbbképzések tervezése, szervezése és ütemezése nehezebben megvalósítható
- A tapasztalatfeldolgozásból származó információk, eljárások lassabban adaptálhatók

4. ábra: Az ÖLFCS állandó alkalmazásának SWOT-analízise

Forrás: a szerző szerkesztése

Az erősségeket figyelembe véve elmondható, hogy az állomány folyamatos cseréjével és az új „rutin” beépítésével csökkenthető a hibák bekövetkezése, ami a készenléti kialakításnál érhető el leginkább.¹⁷ Ez annak köszönhető, hogy az ideiglenes kialakítással (kiképzések és felkészítések megtartásán keresztül) növelhető a felderítő csoportok állománytáblájában szereplő beosztások betöltésére alkalmas személyek köre, ezáltal a rotálási lehetőségek is. Az állomány folyamatos cseréje és a rövidebb (az állandó csoporthoz képest) szolgálati idő miatt kevésbé jelentkezhetnek a rutinszerű feladatellátásból származó hibák. Ráadásul a szakértő személyek funkcionálisan több, vagy más feladatokba is bevonhatók eredeti beosztásukban, mivel készenléti erőként nem állnak folyamatos alkalmazásban.

Ugyanakkor a készenléti kialakítás gyenge „pontja” lehet, hogy a katonák összezokottságához, „összekovácsolásához” több idő szükséges, mivel a csoportparancsnok és a beosztottak nem a napi rendszerességgű munkavégzés, feladatvégrehajtás által ismerik meg egymás készségeit és képességeit, hanem az időszakos begyakorlásokon, felkészítéseken és kiképzéseken keresztül. Továbbá a készenléti csoport (alapesetben) hosszabb idejű bevetetőségi képességgel is rendelkezik, amelyhez párosulhat a kiértesítések végrehajtásának bonyolultsága is. Ez azzal magyarázható, hogy az állomány az eredeti beosztásában látja el feladatait, így a kiértesítéseket személyenként vagy katonai szervezetenként tudja megvalósítani az előljáró, majd a készenléti kategóriáknak megfelelően csak bizonyos idő elteltével válik majd képessé a csoport a hadszíntéri információgyűjtő folyamatok végzésére.

A készenléti alkalmazás számos lehetőséget is tartalmazhat. Például a folyamatos kiképzéseken és képzéseken keresztül – amelyeket a korábban a felderítő csoportban szolgáló tanácsadók bevonásával tartanak – növelni lehetne a kiválasztható szakemberek számát, így a rotációs lehetőségek „tárházát”. Ezzel összefüggésben a tartalékos rendszernek köszönhetően az Önkéntes Műveleti Tartalékosok (ÖMT) vagy az Önkéntes Területvédelmi Tartalékosok (ÖTT) különböző katonai feladatokba (gyakorlatokba, kiképzésekbe, missziókba) is bevonhatók,¹⁸ ennek megfelelően véleményem szerint a csoport részére tartandó képzéseken is részt vehetnek. Itt azonban fontosnak tartom megjegyezni, hogy alkalmazásuknál célszerű megvizsgálni az ÖMT- és ÖTT-állomány honvédséggel kötött szerződésének hosszát, biztosítva, hogy a kiképzett katonák bármikor képesek legyenek az ÖLFCS küldetésének végrehajtására, és a „sikert” nem befolyásolja a szerződések lejáratának közelsége. További lehetőségként lehet értelmezni, hogy kevesebb költségárfordítás jelentkezhet az MH részéről, mivel ennél a „megoldásnál” a csoportokat a felelős szervezetek ideiglenesen állítanák össze a műveletek időszakáig, majd a küldetés befejezésekor (a felderítési és műveleti összekötői feladatok teljesítését követően) az erők és eszközök az eredeti rendeltetés szerinti helyükre térnének vissza. Ráadásul az infrastruktúra- és eszközberuházásból származó költségek kisebbek az állandó csoportnál felmerülő kiadásokhoz képest. Az állomány részére nem kell folyamatosan biztosítani munkavégzésre alkalmas helyiségeket, felszereléseket és azokat fenntartani, üzemeltetni, nincs szükség csak és kizárólag a csoport működése érdekében beruházásokat végrehajtani (például

¹⁷ BELÉNYESI 2014: 50.

¹⁸ ŐZE 2021: 127–139.

infokommunikációs eszközöket, gépjárműveket beszerezni). A kijelölt eszközök átadása (a csoport részére) a már meglévő, letárolt vagy rendszerben lévő más katonai szervezetek által használt készletekből is megvalósítható, amelyek működőképesek, karbantartottak és átcsoportosításuk nem okoz gondot a feladatok ellátásában. Ez természetesen megoldható az állandó csoport működtetésekor is, azonban fontos tényező, hogy a készletléti állomány alkalmazásakor ezeket az eszközöket más katonai szervezetek más tevékenységekre is használhatják az ÖLFCS aktiválásáig.

Ugyanakkor veszélyként lehet értelmezni, hogy a kiképzések, továbbképzések tervezése, szervezése és ütemezése nehezebben megvalósítható, mivel a készletben lévő szakértő állományt minden egyes felkészítésre külön ki kell rendelni az egységétől. Ráadásul a tapasztalatfeldolgozásból származó információk, eljárások is lassabban adaptálhatók, ha azt a tényt vesszük figyelembe, hogy az előre betervezett időszakos kiképzések, felkészítések megtartásával, valamint azokat módosítva lehet a fejlesztő javaslatokat integrálni a csoport működési rendjébe, míg az állandó ÖLFCS-nél (a folyamatos elérhetőség és célirányos munkavégzés miatt) ez a folyamat rövidebb időt vesz igénybe.

Összességében kijelenthető, hogy az ÖLFCS-t készletléti erőként célszerű létrehozni (a költségátfordítások és az állomány feladatmegosztása, terhelése miatt). A NATO, az Amerikai Egyesült Államok és az Egyesült Királyság is hasonló módszerrel alkalmazza a csoportot. A NATO például úgynevezett *double-hatted* beosztásokat rendszeresít az összhaderőnemi parancsokságokon, valamint az ÖLTCS-nél, amelynek lényege, hogy a beosztásokat betöltő felkészült állomány alaprendeltetési feladatait hajtja végre a törzsben, majd az ÖLFCS aktiválásakor csatlakoznak a csoporthoz, és a továbbiakban a hadszíntéri információk gyűjtésére (folyamatok tervezésére, szervezésére, a kitelepülésre és a feladatellátásra) fókuszálnak.

Mindezeket figyelembe véve elmondható, hogy a csoport működését tekintve több alternatíva közül is lehet választani. Azonban fontosnak tartom megjegyezni, hogy az ÖLFCS megalakítását és az MH struktúrájába történő beillesztését mindenképp indokoltnak tartom megvalósítani, hogy ezáltal is növelni lehessen a műveletek, valamint a logisztikai támogatás tervezésének, szervezésének és végrehajtásának hatékonyságát.

Összegzés

A műveleti területre elsőként érkező ÖLFCS tevékenységét vizsgálva megállapítható, hogy az általa végzett logisztikai felderítési feladatok teljesítésén keresztül eredményesen járulhat hozzá a katonai műveletek logisztikai támogatásának sikeres tervezéséhez és végrehajtásához. A cikkben kitértem rá, hogy az MH-ban jelenleg nincs hasonló jellegű csoport, amelynek az lenne a feladata, hogy a hadszíntérre elsőként érkezve összeköttetést építsen ki a civil kormányzati és nem kormányzati nemzeti, nemzetközi szervezetekkel, majd információkat gyűjtsön a közlekedési infrastruktúrák (a lehetséges vasúti, tengeri, légi kirakópontokról, a közúthálózatokról stb.), a logisztikai, raktár-, valamint javítóbázisokról, vagy a BNT keretében nyújtható szolgáltatásokról. Jelentőségét alátámasztja az a tény, hogy több ország (például az Amerikai Egyesült

Államok, Franciaország, Egyesült Királyság) és a NATO is alkalmaz hasonló jellegű csoportot, és hozzá képeznek ki állományt, majd tartanak részükre folyamatos felkészítéseket.¹⁹ Sokoldalúságára jó példa, hogy az ÖLFCS részt vett egyhetes kiképzésen a Művelti Összekötő és Felderítő Csoporttal (amelynek jelentőségét korábbi tanulmányomban már vizsgáltam²⁰), valamint a Magyarországra telepített NATO Erőket Integráló Elemmel (NFIU²¹). A kiképzés célja az volt, hogy a felderítői és összekötői feladatok végrehajtásán keresztül elősegítsék a NATO gyorsreagálású erők mozgékony telepítését.²² Természetesen kérdésként merülhet fel, hogy ha a NATO már rendelkezik ilyen csoporttal, miért van szüksége az MH-nak is ilyen jellegű szervezeti elemre?

A NATO alárendeltségében működő ÖLFCS mindig a szövetség és a JLSG érdekében fog csak logisztikai felderítési feladatokat végrehajtani a hadszíntéren, ebből adódóan több ország is saját ÖLFCS-t alkalmaz, hogy ezáltal segítse (akár többnemzeti környezetben, a kijelölt felelősségi terület vizsgálatával) a műveletek logisztikai támogatásának tervezési és szervezési folyamatait. Ráadásul az ÖLFCS-t nemcsak válságreagáló műveletekben, hanem országvédelmi feladatoknál is lehetne alkalmazni, amikor szükség lehet előzetes vagy reagáló logisztikai felderítést elvégezni (a lehetséges felvonulási, utánpótlási útvonalak kijelöléséhez), valamint együttműködni a polgári kormányzati és nem kormányzati szervezetekkel.

Az ÖLFCS összetételét tekintve elmondható, hogy az általam javasolt 15 fős állomány képessé válhat a logisztikai felderítési feladatok végrehajtására, amelyet érdemes készenléti erőként alkalmazni. Az alá- és fölérendeltségi viszonyát vizsgálva továbbá kijelenthető, hogy a csoportot célszerű az összhaderőnemi műveletek tervezéséért és szervezéséért felelős parancsnok, az MH ÖMP alárendeltségébe utalni, hogy az ÖLFCS minden körülmények között hatékonyan tudja segíteni a parancsnok és törzsének döntés-előkészítő tevékenységét, valamint a műveletek logisztikai támogatásának tervezési feladatait.

Felhasznált irodalom

- AJP-4.6 *Allied Joint Doctrine for Joint Logistic Support Group Edition C Version 1 (draft)* (2018). NATO Standardization Office. Online: https://www.coemed.org/files/stanags/01_AJP/AJP-4.6_EDC_V1_E_2230.pdf
- BELÉNYESI Emese (2014): *Változásmenedzsment a közgazdaságban* [ePub]. Budapest: Nemzeti Közszerológati és Tankönyv Kiadó Zrt. Online: https://real.mtak.hu/82340/1/Valtozasmenedzsment_a_kozgazdasagban_u.pdf
- Hajós Bence (2024): A STANAG 2021 szerinti katonai járműteherosztályok a polgári hídszabályzatok tükrében. *Hadmérnök*, 19(1), 5–20. Online: <https://doi.org/10.32567/hm.2024.1.1>
- Honvéd Vezérkar (2025): *Rendeltetés*. Online: <https://honvedelem.hu/alakulat/honved-vezerkar.html>

¹⁹ KLAAUW 2024: 74–79.

²⁰ SZAJKÓ 2022: 19–31.

²¹ NATO Force Integration Unit.

²² NATO 2018.

- Joint Logistics Support Group (2011): *Standard Operating Procedure, 701.03 Joint Logistic Reconnaissance Team*. Brussels: NATO.
- KLAAUW, Cornelis van der (2024): How to Prepare and Deploy Operational Liaison and Reconnaissance Teams. *The Three Swords Magazine*, 40, 74–79. Online: www.jwc.nato.int/wp-content/uploads/2025/03/OLRT_2024.pdf
- NATO (2018): *OLRT Deployment*. Online: <https://mncne.nato.int/newsroom/news/2018/olrt-deployment>
- NATO Standardization Agency (2016): *Bi-SC Capability Codes and Capability Statements*. Brussels. Online: www.armadnioviny.cz/domains/0001/userfiles/files/toaz_info-capability-codes-and-capability-statements-2016-bi-sc-nu0083-pr_39b656a9da6698fa2d44b0b85ae4de07.pdf
- NATO SHAPE (2024): *ACO Directive. Criteria and Standards for the Zones of the Reinforcement and Sustainment Network*. Belgium.
- ŐZE Zoltán (2021): Az Önkéntes Területvédelmi Tartalékosok ABV-mentesítőképeségének kialakítása. *Hadmérnök*, 16(2), 127–139. Online: <https://doi.org/10.32567/hm.2021.2.9>
- Super International Shipping [é. n.]: *Roll-on/roll-off (RoRo) hajók magyarázata: típusok, költségek és előnyök*. Online: <https://super-internationalshipping.com/hu/roll-on-roll-off-ships/>
- SZAJKÓ Gyula (2022): A Műveleti Összekötő és Felderítő Csoport lehetséges összetételének meghatározása és illeszkedése az MH szervezetébe. *Honvédségi Szemle*, 150(6), 19–31. Online: <https://doi.org/10.35926/HSZ.2022.6.2>
- SZAJKÓ Gyula (2025): *A logisztikai felderítés rendszerének továbbfejlesztési lehetőségei a Magyar Honvédség műveleteinek előkészítésében*. PhD-disszertáció (benyújtva). Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola. Online: <https://doi.org/10.17625/NKE.2025.033>

Tartalom

HADITECHNIKA

PAPP ISTVÁN: <i>Rakétairányítási és célbefogási folyamatok a modern kor hadviselésében</i>	5
--	---

VÉDELEMINFORMATIKA

BENKE BÁLINT PÉTER: <i>A kriptovaluták kettős arca</i>	25
--	----

BOTTYÁN SÁNDOR: <i>Nagy nyelvi modellek az internetes nyílt forrású információgyűjtésben</i>	49
--	----

ATTILA HAMMAS: <i>More Data, More Problems?</i>	71
---	----

SZABOLCS JOBBÁGY: <i>The Convergence of the Digital Virtual World and Artificial Intelligence – Or What the Future Symbiosis Brings in the Synergy of the Metaverse and AI</i>	85
--	----

PÁL KÁROLY LASKA: <i>Empirical Analysis of the Impact of Personality Traits on Cybersecurity Awareness</i>	101
--	-----

PATAKI JÁNOS IMRE, SULÁNYI PÉTER: <i>Az autóipari vállalatok és beszállítók integrált biztonsági és védelmi stratégiája</i>	113
---	-----

SZABÓ GERGŐ: <i>A generatív mesterséges intelligencia használata a kibertudatosítási képzésekben, 2. rész</i>	135
---	-----

FÓRUM

SOMOGYI JÁNOS JÓZSEF, NAGY SÁNDOR: <i>A geopolitika és a lakosságvédelem kapcsolata</i>	157
---	-----

Környezetbiztonság

ISTVÁN MIHÁLY: <i>Estimating the Air Leakage Rate of Smoke Control Doors for Calculations Procedures, Part 2</i>	175
--	-----

VARRÓ TEKLA: <i>A katasztrófavédelmi oktatás és tájékoztatás fejlesztési lehetőségei a magyar felnőtt lakosság körében</i>	189
--	-----

KATONAI LOGISZTIKA ÉS KÖZLEKEDÉS

SZAJKÓ GYULA: <i>Az Összhaderőnemi Logisztikai Felderítő Csoport lehetséges összetételének meghatározása és alkalmazása az MH szervezeti struktúrájában</i>	213
---	-----