HADMÉRNÖK

Kiemelt közlemények

16. évf. (2021)
3. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

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

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

Kiadó
Nemzeti Közszolgálati Egyetem, Ludovika Egyetemi Kiadó
Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
A kiadásért felel: Koltay András rektor
Olvasószerkesztők: Gergely Zsuzsánna, Resofszki Ágnes, Zsávolya Zoltán

Tartalom

Fórum

HADMÉRNÖK
BIZTONSÁGTECHNIKA

16. évfolyam (2021) 3. szám 5–16.
DOI: 10.32567/hm.2021.3.1

Borsos Döníz[1]

A LoRaWAN-technológia szerepe az elektronikai védelem területén, az építőipari beruházások vonatkozásában

The Role of LoRaWAN Technology in Electronic Protection Concerning Construction Investments

Az ipari nagyberuházásokban, az építőiparban folyamatosan változó környezettel, feladatokkal és kihívásokkal kell szembenézni a vagyonvédelem területén. Ezért megfelelő, komplex vagyonvédelmi rendszer kialakítása elengedhetetlen, amelynek folyamatosan igazodnia kell az adott építkezés sajátosságaihoz. Mivel a munkaszakaszok során különböző értékű és mennyiségű anyagok, eszközök és gépek védelméről is beszélünk, ezért kiemelten fontos funkciót tölt be az elektronikai védelem egy komplex rendszer részeként. A tanulmány azt vizsgálja, hogy milyen szerepe van az építőipari beruházások során az elektronikai jelzőrendszernek, az alkalmazott technológiáknak, különös tekintettel a LoRaWAN-technológiára.

Kulcsszavak: építőipari beruházás, komplex védelem, elektronikai védelem, LoRaWAN-technológia

With large-scale industrial investments, we have to face continually changing environments, tasks and challenges in property protection in the construction industry. Therefore, an appropriate, complex property protection system, which must be continuously adapted to the given construction's specifics, is essential. In terms of protecting materials, devices and machines of different values and quantities during the work phases, electronic protection plays a significant role in a complex system. The study examines the role of electronic signalling systems and applied technologies, especially LoRaWAN technology, in construction investments.

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola, doktori hallgató, e-mail: borsos.doniz@uni-obuda.hu

Keywords: **construction investment, complex protection, electronic protection, LoRaWAN technology**

1. Bevezetés

Egy építőipari kivitelezés során akár óránként változó környezettel, lehetőségekkel és értékekkel kell számolni. Vagyonvédelmi szempontból ez jelentős kihívást jelent a szakemberek számára. A komplex vagyonvédelem alappillérei a megelőző intézkedések, a mechanikai védelem, az elektronikai védelem, az élőerős védelem, a biztosítás és a fennmaradó saját kockázat.[2] Egy építőipari kivitelezés során a megelőző intézkedéseknek nemcsak vagyonvédelem szempontból van jelentősége, hanem életvédelmi szerepük is van. A megfelelő mechanikai védelem kialakításával megakadályozhatók vagy késleltethetők az illetéktelen behatolások, időt biztosítva az élőerős személyzet részére. Az élőerős feladatok ellátása nagy szervezettséget, felügyeletet kíván, és folyamatos, magas költségekkel jár. Ennek kiküszöbölésére egyre jelentősebb szerepet kap az elektronikai jelzőrendszer, eszközök felhasználása az élőerős védelem kiváltására, kiegészítésére, de akár ellenőrzésére is.[3] Ismert, hogy tökéletes biztonság nem alakítható ki, erre nyújt megoldást a biztosítás. Amire pedig az sem, azt saját kockázatként kell elkönyvelni.

A tanulmány elektronikai jelzőrendszerekkel, azon belül is olyan megoldásokkal foglalkozik, amelyek építőipari kivitelezések során alkalmazhatók és LoRaWAN-technológiát használnak a kommunikációra, a jelzések küldésére. A technológiát és az építőipari beruházások sajátosságait, szakaszait a későbbiekben ismertetem. Általánosságban elmondható, hogy az ilyen jellegű kivitelezések során a következő kihívásokkal kell szembenézni. Olyan környezetről beszélhetünk, ahol az elektronikai jelzőrendszer eszközeinek hálózati tápellátása nem minden esetben biztosítható. Az eszközök vezetékezése fizikai akadályba, esztétikai problémába ütközhet, vagy anyagi megfontolások nem teszik lehetővé. Megállapítható, hogy nagy mennyiségű, változó jellegű és értékű eszközök, anyagok védelméről kell gondoskodni. Továbbá a környezeti feltételek sajátosságai technológiai korlátokat is szabhatnak bizonyos megoldások alkalmazhatóságának.

Mindezek figyelembevételével, szükséges ismerni a kivitelezések egyes szakaszait, folyamatait és azok vagyonvédelmi kockázatait. Továbbá, az említett LoRaWAN-technológia paramétereinek tisztázása elengedhetetlen az alkalmazási területek behatárolásához. Megfelelő mérések elvégzésével pedig igazolhatók a felvetett alkalmazási lehetőségek.

Tehát olyan, komplex védelmet kell kialakítani, amely folyamatosan igazodik az építőipari beruházások sajátosságaihoz, rugalmas és moduláris.

[2] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései. Doktori (PhD) értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2009. 13.

[3] Bodrácska Gyula – Berek Tamás: Megelőző intézkedések szerepe a komplex vagyonvédelem területén, építőipari beruházások biztosítása során. *Hadmérnök,* 5. (2010), 1. 17–23.

2. Építőipari beruházások jellegzetességei

Az építési kivitelezési munkálatok főbb szakaszai a munka jellege szerint a következőképpen alakulnak:

- bontási munkák;
- terep- és környezetrendezési munkák, alapozás;
- szerkezetépítési munkák;
- befejező kiviteli munkák;
- ideiglenes közműellátási, -létesítési munkák.[4]

Számos esetben az építési feladatok bontási munkálatokkal kezdődnek. Bontás során az emberi, fizikai munkavégzés mellett legtöbbször földmunkagépekkel, emelőgépekkel, rakodógépekkel dolgoznak. Az ilyen munkagépek ára elérheti a százmillió forintos nagyságrendet, de használt állapotukban is tízmillió forintos árat képviselhetnek. Ezeknek a gépeknek a bérlési költsége is igen magas, néhány tízezer forinttól akár a több százezer forintig is terjedhet naponta. Nem is a bérlési költségen van a hangsúly egy nem saját gép esetében, hanem a kaució mértékén. Építési munkagépek esetében a letét mértéke több százezer, akár milliós nagyságrend is lehet. Ezért kiemelten fontos e gépek illetéktelenektől való védelme.

A következő lépés a tereprendezés, ahol főleg földmunkával kapcsolatos feladatokat kell elvégezni, előkészíteni az alapozást. Ebben az esetben is, hasonlóan a bontási feladatokhoz, igen nagy értékű munkagépekkel végzik a folyamatokat. A munkagéplopások és -rongálások mellett kritikus probléma az üzemanyaglopás[5] is. Emellett olyan munkagépekről beszélünk, amelyek használata csak szigorú munkavédelmi szabályok betartása mellett megengedett és akár külön engedélyhez is kötött. Ezért az illetéktelenek által való hozzáférés az anyagi károk mellett emberi életeket is veszélyeztethet.

Az építés során a legnagyobb volumenű szakasz a szerkezetépítés. Idetartoznak a betonozási munkák, a zsaluzási munkák, a falazatok kivitelezésével kapcsolatos munkák, az ácsmunkák, a tetőfedéssel kapcsolatos munkálatok és egyéb szerkezetépítési munkák.[6] Minden felsorolt munkafolyamat sajátossága, hogy jelentős mennyiségű és értékű anyagot építenek be. Ezen agyagok felügyelete és védelme komoly feladat, sokszor teljes mértékben nem megoldott. Természetesen ebben a szakaszban is használatosak munkagépek, értékes szerszámok, segédeszközök, de jellemzően kisebb értéket képviselnek a nagy munkagépekhez viszonyítva.

A szerkezetépítés után a befejező kiviteli munkák következnek. Itt szintén olyan alfolyamatokról beszélünk, ahol a felhasznált anyagok és berendezések jelentős értéket képviselnek. Ilyen munkák a következők lehetnek: a nyílászárók beépítése, a festéssel, burkolással, vakolással kapcsolatos munkálatok.[7] Ezeken kívül gépészettel és elektromossággal kapcsolatos szerelési feladatok. Előfordulhat olyan helyzet

[4] Lámer Géza – Szűcs Edit: *Építési folyamatok szervezése.* Budapest, TERC Kft., 2013; Épülettervezés és építés: Az építésről, kivitelezésről – az építés folyamata. (é. n.)
[5] Bodrácska–Berek (2010): i. m. 19.
[6] Lámer–Szűcs (2013): i. m.; Épülettervezés és építés (é. n.): i. m.
[7] Lámer–Szűcs (2013): i. m.; Épülettervezés és építés (é. n.): i. m.

is, hogy még a nyílászárókat nem szerelik be, de az épületgépészeti berendezések már megérkeztek. Ekkor azok felügyeletéről szintén gondoskodni kell, hiszen szintén jelentős értéket képviselnek és gyakori célpontnak tekinthetők.

Mindezek mellett előfordulnak ideiglenes jellegű feladatok is, amelyek főleg a létesítés és a közműellátás köré csoportosulnak. Ezek olyan feladatok, amelyek az építés egyes folyamatait és az ott dolgozókat segítik, lehet szó egy ideiglenes tárolóról, pihenőhelyről vagy az ahhoz kapcsolódó víz- és energiaellátásról. Itt többnyire az objektumok védelmét kell figyelembe venni, és a (közmű)fogyasztási értékek monitorozását.

Az imént ismertetettekből látszik, hogy egy építkezés során folyamatosan változó környezetről, jelentős értékekről és számos felügyelendő anyagról, eszközről, gépről beszélhetünk. A folyamatos változás magával hozza azt, hogy nem alkalmazhatók azonos védelmi eszközök és módszerek egy építkezés minden szakaszában. Elengedhetetlen a komplex védelem kialakítása, amelynek folyamatosan igazodnia kell az aktuális körülményekhez.

A komplex vagyonvédelem egyik összetevője az elektronikai védelem, amelynek területén számos megoldással találkozhatunk. Elektronikai berendezésekről, eszközökről beszélve, a közös pont az elektromos tápellátás. Egy építési kivitelezés folyamán nem ritka, hogy a védendő tárgy vagy objektum környezetében nem áll rendelkezésre elektromos áram. Ebből következik, hogy szükségessé válik olyan eszközök használata, amelyek támogatják a telepes tápellátást. Emellett kiemelhető, hogy a vezetékes összeköttetés számos esetben nem megoldható vagy költséges. Erre megoldás lehet olyan elektronikai jelzőrendszer telepítése, amely vezeték nélküli kommunikációt használ. Egy másik kritikus pont a kivitelezési munkák során az épületek jellegéből adódik. Az épületek különböző anyagokból és kiterjedésben készülhetnek, amelyek nagyban befolyásolhatják a vezeték nélküli kommunikációt. A legtöbb vezeték nélküli kommunikáció nem alkalmazható föld alatti építményekben, vasbetonszerkezetű épületekben vagy nagy adatátviteli távolság esetén. A vasbeton épületek és az épületek alatti mélygarázsok egyre népszerűbbek az ipari nagyberuházások folyamán. Ezekre a problémákra nyújthat megoldást a LoRaWAN-technológia, amelynek összefoglaló technológiai ismertetését a következő fejezet tartalmazza.

3. Technológiai háttér

A LoRaWAN-technológia alapja a LoRa-technológia, amely az angol long-range (nagy hatótávolság) szavak rövidítése.[8] A LoRa egy vezetéknélküli kommunikációs technológia, amelynek alapvető jellemzője a kis energiafogyasztás, a nagy adatátviteli távolság és a jelentős zavarimmunitás. A LoRa önmagában egy pont–pont kommunikáció, amely alapjául szolgált a LoRaWAN hálózati kommunikációnak.

A LoRaWAN lehetővé teszi az eszközök nagy területet lefedő összekapcsolását és az általuk szolgáltatott adatok gyűjtését. A LoRaWAN-specifikációk kidolgozásával

[8] Semtech: What is LoRa®? (é. n.).

a LoRa Alliance (LoRa Szövetség) foglalkozik, amely az eszközök tanúsításáért is felel.[9] A specifikációknak megfelelve egy LoRaWAN-hálózat a következő elemekből tevődik össze: végberendezések, átjáró(k), hálózati szerver és alkalmazásszerver(ek).[10] A végberendezések az átjárók vagy más néven gateway-ek felé továbbítják az üzeneteket. Az átjárók a hálózati szerverekkel állnak összeköttetésben, amelyek az alkalmazásszerveren keresztül tartják a kapcsolatot a felhasználókkal. Az alkalmazásszervereken különböző megjelenítési és feldolgozási feladatok történhetnek. A hálózati topológia tehát összetett csillag elrendezésben alakul. A végberendezések közvetlenül nem állnak kapcsolatban egymással. A technológia lehetővé teszi a privát hálózatok kialakítását is, nem szükséges szolgáltatói közreműködés a használatához.

LoRaWAN esetében a kommunikáció kétirányú, azaz a végberendezések tudnak üzeneteket küldeni és fogadni is, bár többnyire a küldés a hangsúlyos. Ennek az oka az, hogy főleg olyan készülékekről beszélünk, amelyek a környezetükből gyűjtenek adatokat, mérnek meghatározott paramétereket. Ezenfelül két típusú üzenetet különböztethetünk meg, a nyugtázást váró üzenetet és a nyugtázást nem váró üzenetet.[11] Ennek a tartalom fontosságának megkülönböztetésénél van jelentősége. Vannak olyan tartalmak, amikor nem szükséges nyugtázás. Ilyen lehet egy folyamatosan küldött hőmérsékletadat, hiszen nincs kritikus jelentősége, ha egy üzenet kimarad. Ellenpélda erre az „életjel" üzenet küldése, hiszen ott kiemelt fontosságú annak megérkezése.

1. táblázat

A LoRaWAN technológiai paraméterei

Forrás: a szerző szerkesztése Semtech (é. n.): i. m.; LoRa Alliance (2018): i. m. alapján

Moduláció	Chirp Spread Spectrum (CSS) – Frekvenciasöpréses szórt spektrumú frekvenciamoduláció
Frekvencia	433 MHz, 868 MHz (Európában)
Sáv	ISM, szabad felhasználású
Sávszélesség	250 kHz, 125 kHz
Csatornaszám	3 (minimum 3, tipikusan 8 + 1)
Adatátviteli sebesség	50 Kbit/s (maximum)
Hasznos adat mérete	243 byte (maximum)
Duplexitás	Half-duplex
Titkosítás	AES128
Adatátviteli távolság	15 km (maximum)
Interferenciaimmunitás	Nagyon magas

Egy technológia alkalmazásakor nemcsak a tulajdonságainak ismerete a lényeges, hanem a korlátok tisztázása is. A LoRaWAN-technológia jellemzőit az 1. táblázat foglalja össze. Látható, hogy a kommunikáció Európában a 433 MHz-es és a 868 MHz-es ISM-sávot használja, ebből következik, hogy (bár a küldés-fogadás technológiailag

[9] LoRa Alliance: *About LoRa Alliance:* https://lora-alliance.org/about-lora-alliance
[10] LoRa Alliance: *LoRaWAN Specification* V1.0.3. 2018.
[11] LoRa Alliance: *LoRaWAN Specification* V1.0.3. 2018.

nem korlátozott) egy végberendezés az idő 1%-át használhatja kommunikációra. Továbbá az üzenetek mérete is korlátozott, ami befolyásolja az alkalmazhatóság területét, maximálisan 243 byte hasznos adat küldhető egy üzenetben. Ez azt jelenti, hogy a technológia nem alkalmas olyan esetekben, amikor nagy adatok folyamatos továbbítására van szükség. Ilyen lehet élőkép vagy hang átvitele.

A végberendezéseknek három működési osztálya ismert A, B és C jelöléssel.[12] Az A osztályú végberendezések alkalmazása a legáltalánosabb, mivel energiafogyasztás tekintetében ez a működés a legkedvezőbb. Hátránya, hogy a végberendezés az üzenetküldést követően képes csak a fogadásra, ekkor nyit két vételi ablakot. Ez azt eredményezi, hogy a végberendezéseknek küldött üzenetek megérkezése nem azonnal történik.

Mindezek mellett meg kell említeni, hogy melyek azok a tulajdonságok, amelyek miatt a technológiának jelentősége van az elektronikai védelem területén, az építőipari beruházások vonatkozásában. Kiemelhető a nagy adatátviteli távolság, amely városias területen néhány km körül alakul, beépítettség függvényében; vidéki, kevésbé beépített, lakott területen akár 10 km is lehet. Ezenfelül az alkalmazott speciális modulációnak köszönhetően kevésbé érzékeny a környezeti tényezőkre, legyen az időjárás, domborzat vagy épített környezet. A végberendezések A osztályú működés mellett, telepes tápellátással akár 10 évig is működőképesek lehetnek. Másik nagy előnye a technológiának a privát hálózat kialakításának lehetősége és a távoli felügyelhetőség. Egy gateway telepítésé akár több négyzetkilométernyi területet is lefedhet. Több építési terület esetén pedig ezek az átjárók összekapcsolhatók, így egy hálózatban kezelhető minden érintett helyszín. Természetesen szolgáltatói hálózatot is igénybe lehet venni, amely Magyarország területén 70-80%-os lefedettséget[13] jelent jelenleg. A technológia további előnye, hogy a kommunikáció AES128 titkosítást használ.[14]

A felsorolt tulajdonságokból látszik, hogy a LoRaWAN-technológia számos olyan problémára megoldást nyújthat, amely az építőipari beruházások sajátosságaiból adódik. A következő fejezet tárgyalja azokat az alkalmazási területeket és környezeteket, ahol a LoRaWAN-technológia használata előnyös az elektronikai védelem aspektusában.

4. Alkalmazhatóság területei

A LoRaWAN-technológia kifejezetten alkalmas olyan eszközök esetén, ahol ideiglenes telepítés történik, így egy folyamatosan változó építési területen, vagyonvédelmi feladatok ellátására mint az elektronikai védelem része. Az eszközök alacsony fogyasztásuknak és a vezeték nélküli kommunikációnak köszönhetően könnyen és rugalmasan telepíthetők. A LoRaWAN-eszközök képesek stabil kommunikációt biztosítani épületen kívül és belül is, amelynek helyszíne lehet föld alatti vagy földfelszín feletti egyaránt. A korábban említettek tükrében kiemelve, a technológia nem alkalmas folyamatos

[12] LoRa Alliance (2018): i. m.
[13] Az Antenna Hungária Zrt., a hazai LoRaWAN-szolgáltató, 2019. évben megrendezett LoRaWAN fejlesztői napján tartott beszámoló adatai alapján.
[14] LoRa Alliance (2018): i. m.

hang- és videóanyag átvitelére, így olyan megoldásokat ismertetek, amelyekben többnyire kis méretű szenzoradatok átvitele valósul meg.

Az építési kivitelezés ismertetett sajátosságai alapján a következő alkalmazhatósági területek határozhatók meg:

- *munkagépek védelmével kapcsolatos alkalmazások:* munkagépek nyomkövetése, üzemanyaglopás figyelése;
- *építési, szerelési anyagok védelmével kapcsolatos alkalmazások:* raklapkövetés, elmozdítás érzékelése;
- *ideiglenes objektumok védelmével kapcsolatos alkalmazások:* nyitás érzékelése, mozgás detektálása;
- *közműellátások monitorozásával kapcsolatos alkalmazások:* fogyasztásmérés, szivárgásdetektálás;
- *további, általános behatolásjelzéshez kapcsolódó alkalmazások.*

A munkagépek nyomkövetése tipikusan GPS-helymeghatározáson alapul, esetlegesen gyorsulásérzékelővel vagy egyéb szenzoros megoldással kiegészítve.[15] A nyomkövető eszköz szerelése egy jármű esetén lehet rejtett a szenzoregységek kis méretének és a technológia interferenciaimmunitásának köszönhetően. A rejtett szerelés megakadályozza, hogy illetéktelenek eltávolíthassák a nyomkövető egységet. A helyadatok küldése lehet periodikus vagy eseményvezérelt.[16] A periodikus küldés esetén a helyadatokat előre meghatározott időközönként küldi el. Eseményvezérelt működés esetén különböző külső hatások bekövetkezésekor vagy megváltozásakor történik az adatküldés. Ilyen esemény lehet akár egy elmozdulás. A kettő kombinációja, amikor csak mozgás során történnek periodikusan az adatok küldései. Felmerül a kérdés, hogy mi van abban az esetben, ha a GPS-koordináták nem állnak rendelkezésre, ilyen eset lehet a gép épületen belülre kerülése. Ebben az esetben a kiegészítő szenzorokon van a fő hangsúly. Az előbb említett gyorsulásérzékelő használatával detektálható a munkagép beindítása, elmozdítása. Meg kell jegyezni, hogy épületen belül a GPS-koordináták ismerete irrelevánssá is válik. Nyomkövetés alkalmazásával a gépek telephelyek közötti mozgása is monitorozható.

Nagyon gyakori probléma az üzemanyaglopás egy építési kivitelezés során. Ez történhet közvetlenül a járműből vagy a tárolóedényekből. Az üzemanyaglopási kísérlet detektálható a tárolóegység sapkája, kupakja, fedele elmozdításának érzékelésével, ezenkívül folyadékszint érzékelésével. A folyadékszint érzékelése[17] jobb megoldásnak tekinthető, mivel elképzelhető olyan helyzet, ahol az üzemanyagtároló falazatát bontják meg, ekkor a fedélelmozdulás érzékelése nem bizonyul jó megoldásnak. A folyadékszint-érzékelő egységet lehetőség van rejtve is szerelni, ez tovább növeli a felügyelhetőség hatékonyságát.

Említettem, hogy az építési, szerelési anyagok védelme szintén kiemelt feladat, hiszen nagy értéket képviselnek. Ezek az anyagok lehetnek csomagolt vagy ömlesztett formában. Az ömlesztett anyagok felügyelete többnyire csak közvetve valósítható

[15] LoRa Alliance: Oyster Battery Powered GPS Asset Tracker. (é. n.); LoRa Alliance: FFLYTRACK MyriaPlus. (é. n.).
[16] Pajzs gépjárművédelem: Pajzs- radar Kommunikátor LoRaWAN technológiával. (é. n.).
[17] IoT Factory: Fuel-Water Level lorawan Sensor (ultrasonic). (é. n.); smart parks: Tank Level Probe – Petrol. (é. n.).

meg. A csomagolt anyagok tárolása a legtöbb esetben raklapon történik. Egy „raklapnyi" anyag képviselhet már akkora értéket, hogy kifizetődő legyen a felügyelet. Itt szintén megvalósítható nyomkövetés, ha kültéren helyezik el, illetve elmozdítás érzékelése beltéri tárolás esetén.[18] Természetesen a kettő kombinációja tekinthető a lejobb megoldásnak, mivel az elmozdulás érzékelésével a cselekmény a korai szakaszban érzékelhető és beltéren tárolt anyagok később kültérre kerülnek. Elmozdulás érzékelésével egy raklap tartalmának megbontása is detektálható, ez a szenzor érzékenységbeállításának kérdése csupán.

Ideiglenesen létesített épületek esetén az általános behatolásjelzésen van a hangsúly. Ezek az épületek szolgálhatnak ideiglenes raktárként, ekkor a tárolt anyagok, eszközök, gépek védelme a fontos. Természetesen itt is alkalmazható az előzőekben ismertetett nyomkövetés és elmozdulásérzékelés, de az elődleges cél a behatolás érzékelése. Nem szabad megfeledkezni arról, hogy a fő cél az építési területre való bejutás megakadályozása, hiszen komplex védelemről beszélünk, de ez a tanulmány az elektronikus jelzőrendszer vonatkozásait vizsgálja. A behatolásjelzés eszközkészlete számos megoldást foglal magában védelmi körök alapján csoportosítva. Egy olyan helyszínen, ahol folyamatos a változás és főként ideiglenes eszközökre van szükség, a legegyszerűbb megoldásra szokott esni a választás a költséghatékonyság fényében. A legegyszerűbb ilyen érzékelők a nyitásérzékelők és a mozgásérzékelők. Ideiglenes tárolóként általában konténereket alkalmaznak, amelyek többnyire egy, esetleg kettő nyílászáróval vannak ellátva. A konténerek tipikus mérete 6096 mm × 2438 mm × 2590 mm – 13 716 mm × 2438 mm × 2895 mm között alakul.[19] Mindez azt feltételezi, hogy akár egy mozgásérzékelővel[20] és egy nyitásérzékelővel[21] lefedhető egy konténer. Az acélváz és falazat a LoRaWAN-kommunikációt jelentős mértékben nem befolyásolja.

A közműellátások monitorozása az esetleges meghibásodások vagy rongálások végett fontos. Számos olyan eszköz elérhető a piacon, amelyek komplett fogyasztásmérő órák vagy LoRaWAN-kommunikációjú kiegészítők fogyasztásmérő órákhoz.[22] Ezenkívül vannak speciálisan szivárgásdetektálásra alkalmas eszközök is.[23] A kiépített villamos hálózatra való illetéktelen rácsatlakozás anyagi károkat okoz. A víz- vagy gázhálózat szivárgása az anyagi károk mellett emberéleteteket is veszélyeztethet.

Mindezek mellett ki kell emelni általánosságban a behatolásjelzést. Természetesen ez nem egy mellékes opció, fontos feladat megakadályozni az illetéktelenek belépését az építési területre, vagy ha az nem lehetséges, akkor jelzést küldeni az eseményről. A behatolásjelzés vonatkozhat a teljes építési területre, az épületre, vagy az épület egyes helyiségeire is. A vezeték nélküli, telepes tápellátással rendelkező érzékelők az építési kivitelezés bármelyik szakaszában alkalmazhatók.

Az ismertetett megoldások, a komplex vagyonvédelem részeként, szerves részét képezhetik az építőipari beruházások vagyonvédelmi koncepciójának. Több szó esett a technológia zavar iránti erős érzéketlenségéről, de tudjuk, hogy az elmélet

[18] Government Technology: Wichita, Kan., Deploys IoT Sensors to Prevent Copper Theft. 2019.
[19] Konténer Hungária Kft.: Konténer méretek és adatok. (é. n.).
[20] IoT Factory: LoRaWAN Presence/Motion Detection Sensor. (é. n.).
[21] IoT Factory: LoRaWAN Door – Window opening and closing Detection Sensor. (é. n.).
[22] LoRa Alliance: Meters (LoRaWAN) certified devices search. (é. n.).
[23] LoRa Alliance: Noah Multifunction Leak Sensor. (é. n.); LoRa Allaince: ArrowWan. (é. n.).

és a gyakorlat nem minden esetben találkozik. A következő fejezet az ezzel kapcsolatos mérések eredményét vizsgálja.

5. Mérések és eredmények

Az ismertetendő mérés elsődleges célja az volt, hogy olyan környezeti tényezők mellett vizsgálja a LoRaWAN-kommunikációt adatátviteli szempontból, amelyek egy építési kivitelezés során előfordulnak. Ennek legtipikusabb példája a többszintes vasbeton épületekből történő kommunikáció. Ebből is a legkritikusabb rész a vasbeton mélygarázs vagy pincerendszer. A mérés során azt vizsgáltam, hogy egy vasbeton szerkezetű mélygarázsból az elküldött és fogadott üzenetek aránya hogyan alakul különböző adatátviteli sebességek és hasznos adathosszúságok mellett.

A mérés során felhasznált eszközök: Kerlink Wirnet iFemtoCell IoT beltéri LoRaWAN gateway,[24] Micromite GPS LoRa MOTE,[25] Loriot hálózati szolgáltatás.[26] *A mérés helyszíne, körülményei:* belváros, vasbeton szerkezetű épület: mélygarázs, végberendezés és átjáró közötti távolság 300 m.

A mérés során a végberendezés szerepét egy Micromite GPS LoRa MOTE készülék töltötte be, amelyet elhelyeztem egy vasbeton szerkezetű mélygarázsban, a belépési ponttól legtávolabb eső helyre. A készülékre periodikus adatküldést állítottam be, amely nagyban megkönnyíti a mérés folyamatát. A mérés során minden tesztesetben 100 darab üzenetet küldtem el 30 másodperces időközönként. Az átjáró szerepét egy Kerlink Wirnet iFemtoCell IoT beltéri LoRaWAN gateway töltötte be, amelyet a végberendezéshez képest 300 m távolságban, egy téglaépítésű épület első emeletén telepítettem. Az adatok monitorozása a loriot LoRaWAN hálózati szolgáltatás felhasználásával valósult meg. A kiértékelés az ott beérkezett és az elküldött üzenetek alapján zajlott. Az előzőekben ismertetett mérési elrendezés az 1. ábrán látható.

1. ábra
Méréshez használt hálózati összeállítás
Forrás: a szerző szerkesztése

[24] kerlink: Wirnet iFemtoCell. (é. n.)
[25] chipCAD: Micromite GPS LoRa MOTE. (é. n.).
[26] loriot: *Connecting the Internet of Things*: www.loriot.io

A 2. táblázatban, amely a mérés eredményeit foglalja össze, látszik, hogy a mérés során a legnagyobb adatátviteli sebesség megengedése mellett is 6 byte-os hasznos adattal, az elküldött és megérkezett üzenetek aránya 80% körül alakul, azaz az üzenetek 80%-a érkezik meg sikeresen. Ez az adatátviteli sebesség csökkentésével tovább növelhető. Hozzá kell tenni, hogy a helyszínen mobiltelefonos szolgáltatás használhatatlan, nem elérhető. A mérés során alkalmazott gateway egy beltéri kivitelű, kis teljesítményű eszköz, ennek a kültéri, nagy teljesítményű változatával sokkal jobb eredmények célozhatók meg.

2. táblázat

Mérési eredmények

Forrás: a szerző szerkesztése

Adat megnevezése	**teszteset**	**teszteset**	**teszteset**	**teszteset**
Adatátviteli korlát	290–5470 bit/s Nincs limit	290–5470 bit/s Nincs limit	290–440 bit/s	290–440 bit/s
Hasznos adat hossza	16 byte	6 byte	16 byte	6 byte
Az elküldött és megérkezett üzenetek aránya	56%	80%	82%	90%

A mérési eredmények bizonyítják, hogy valóban nagy a technológia interferenciaimmunitása, és alkalmazható építési területeken, akár vasbeton épületek pince- vagy mélygarázsrészében is.

6. Konklúzió

A tanulmány a LoRaWAN-technológia szerepével foglalkozik az elektronikai védelem részeként az építőipari beruházások folyamán. Az elektronikai jelzőrendszerek alrendszerei a következők:[27] kültéri védelmi rendszer, behatolásjelző rendszer, beléptető rendszer, videófelügyeleti (CCTV-) rendszer, áruvédelmi rendszer, járőrkövető rendszer, távfelügyeleti rendszer, tűzjelző rendszer.[28] A lehetséges alkalmazások megállapításánál a következő területek köré csoportosulnak a megoldások: nyomkövetés, behatolásjelzés. Külön területként lehetne említeni a fogyasztásmérés–szivárgásdetektálást, az elmozdítás érzékelését és az üzemanyaglopás jelzését. Ha figyelembe vesszük a behatolásjelzés eszközkészletét, akkor megállapítható, hogy az elmozdításérzékelők a tárgyvédelem érzékelői közé sorolhatók, ez igaz lehet a fogyasztásmérés–szivárgásdetektálásra és az üzemanyaglopás jelzésére alkalmas eszközökre is. A munkagépek védelmével kapcsolatos közvetlen megoldások, a nyomkövetés és az elmozdításérzékelés, szintén beletartozhatnak ebbe a kategóriába. Tehát összességében megállapítható, hogy a LoRaWAN-technológia alkalmazása a behatolásjelzés területén ideális

[27] Többféle csoportosítás is lehetséges.
[28] Utassy (2009) i. m. 14.; Berek Lajos: Biztonságtechnika. Budapest, Nemzeti Közszolgálati Egyetem, 2014. 15.

megoldást jelenthet építőipari kivitelezések folyamán. Felmerül a kérdés, hogy a többi alrendszer esetében alkalmazható-e a technológia.

A kültéri védelem megoldásai és érzékelői hasonlatosak a behatolás jelzéséhez, így természetesen alkalmazható a LoRaWAN-technológia. Kifejezetten olyan eseteket kell itt érteni, ahol kis fogyasztású szenzorokkal kell dolgozni és az elküldendő adat mennyisége nem haladja meg a technológia korlátját.

CCTV-rendszerek szinte teljesen kizárják a technológia alkalmazását. A tanulmány elején tisztáztam, hogy a LoRaWAN-technológia nem alkalmas folyamatos kép- és hanganyag továbbítására. Olyan megoldás lehetséges, amikor a kamerarendszer intelligens funkciókkal rendelkezik (például objektumeltűnés detektálása, vonalátlépés érzékelése), akkor a riasztási események elküldésére alkalmas lehet. Ez viszont egy egészen speciális kiegészítő megoldás lenne.

Online járőrkövető rendszerek esetében használható a LoRaWAN-technológia, kiegészítve valamilyen nyomkövetésre alkalmas megoldással. Ilyen kiegészítés lehet a GPS vagy kihelyezett olvasó terminálok.

A távfelügyeleti rendszerek esetén sajnos még mindig a GSM-technológia használata a leggyakoribb. Számos hátránya emelhető ki, a legkritikusabb ezek közül a zavarhatóságuk. LoRaWAN-technológiával ez a probléma kiküszöbölhető, de fő átjelzésre nem javasolt, viszont másodlagos rendszernek ajánlatos.

A beléptetőrendszerek esetében már más a helyzet, ezekre a feladatokra nem, vagy nagy kompromisszumokkal, megkötésekkel alkalmazható csak a technológia. Az árvédelmi rendszerek nem tartoznak a tématerülethez, így ilyen szempontból nincs jelentősége az ott alkalmazható eszközöknek. A tűzjelző rendszerek területe az előzőkhöz képest egy sokkal speciálisabb, érzékenyebb terület, így azt nem tárgyaltuk.

Megállapítható, hogy a LoRaWAN-technológia számos területen alkalmazható az építőipari beruházások során, a vagyonvédelem területén, az elektronikai védelem aspektusában, de a behatolásjelzésben kifejezetten. Az elvégzett mérések igazolják, hogy a kommunikáció olyan speciális körülmények között is működőképes, mint az ismertetett építőipari kivitelezési munkálatok. A LoRaWAN-technológia alkalmazása a kialakított komplex vagyonvédelem részeként megoldást nyújthat azokra a sajátosságokra, amelyek kritikusak egy építőipari kivitelezés folyamán.

Felhasznált irodalom

Berek Lajos: *Biztonságtechnika.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. Online: http://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf

Bodrácska Gyula – Berek Tamás: Megelőző intézkedések szerepe a komplex vagyonvédelem területén, építőipari beruházások biztosítása során. *Hadmérnök,* 5. (2010), 1. 17–23. Online: http://hadmernok.hu/2010_1_bodracska_berekt.pdf

chipCAD: *Micromite GPS LoRa MOTE*. (é. n.). Online: www.chipcad.hu/hu/product/development-tools-atmel-microchip-micromite/micromite-gps-lora-mote–LOR055

Épülettervezés és építés: *Az építésről, kivitelezésről – az építés folyamata.* (é. n.). Online: https://tervezes-epites.hu/epitesrol-kivitelezesrol-epites-folyamata/

Government Technology: *Wichita, Kan., Deploys IoT Sensors to Prevent Copper Theft.* 2019. Online: www.govtech.com/biz/wichita-kansas-deploys-iot-sensors-to-prevent-copper-theft.html
IoT Factory: *LoRaWAN Door – Window opening and closing Detection Sensor.* (é. n.). Online: https://iotfactory.eu/products/iot-sensors/lora-door-window-opening-and-closing-detection-sensor/
IoT Factory: *LoRaWAN Presence/Motion Detection Sensor.* (é. n.). Online: https://iotfactory.eu/products/iot-sensors/lorawan-presence-motion-detection-sensor/
IoT Factory: *Fuel-Water Level lorawan Sensor (ultrasonic).* (é. n.). Online: http://iotfactory.eu/products/iot-sensors/fuel-level-measurement-lora-sensor/
kerlink: *Wirnet iFemtoCell.* (é. n.). Online: www.kerlink.com/product/wirnet-ifemtocell/
Konténer Hungária Kft.: *Konténer méretek és adatok.* (é. n.). Online: www.kontener.hu/kontener-kisokos/kontener-meretek
Lámer Géza – Szűcs Edit: *Építési folyamatok szervezése.* Budapest, TERC Kft., 2013.
LoRa Alliance: *ArrowWan.* (é. n.). Online: https://lora-alliance.org/lora_products/arrowwan/
LoRa Alliance: *About LoRa Alliance.* (é. n.). Online: https://lora-alliance.org/about-lora-alliance
LoRa Alliance: *FFLYTRACK MyriaPlus.* Online: https://lora-alliance.org/lora_products/fflytrack-myriaplus/
LoRa Alliance: *LoRaWAN Specification V1.0.3.* 2018.
LoRa Alliance: *Meters (LoRaWAN) certified devices search.* (é. n.). Online: https://lora-alliance.org/showcase/search/?_sf_s=meter&_sfm_lorawan_certified_device=certified
LoRa Alliance: *Noah Multifunction Leak Sensor.* Online: https://lora-alliance.org/lora_products/noah-multifunction-leak-sensor/
LoRa Alliance: *Oyster Battery Powered GPS Asset Tracker.* Online: https://lora-alliance.org/lora_products/oyster-battery-powered-gps-asset-tracker/
Pajzs gépjárművédelem: *Pajzs- radar Kommunikátor LoRaWAN technológiával.* Online: www.pajzs.hu/pajzs-radar-termek
Semtech: *What is LoRa®?* (é. n.). Online: www.semtech.com/lora/what-is-lora
smart parks: *Tank Level Probe – Petrol.* Online: www.smartparks.org/product/tank-level-probe-petrol/
Utassy Sándor: *Komplex villamos rendszerek biztonságtechnikai kérdései*. Doktori (PhD) értekezés. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2009. Online: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/9723/Teljes%20sz%c3%b6veg%21?sequence=1&isAllowed=y

HADMÉRNÖK
BIZTONSÁGTECHNIKA

16. évfolyam (2021) 3. szám 17–40.
DOI: 10.32567/hm.2021.3.2

Jasztrab Péter János,[1] Meglécz Katalin[2]

A világítás katonai vonatkozásai

3. rész: Körletvilágítás

Part III. The Military Aspects of Light

The Lighting of Military Bases

A cikksorozat első és második részében bemutattuk a katonai világítás követelményeit és jogszabályi aspektusait, illetve a műveleti felhasználásának, alkalmazásának körülményeit és azok specifikus eszközeit. Kitekintést tettünk a vizuális teljesítmény fokozása érdekében folyó fejlesztési irányok felé, valamint röviden összefoglaltuk a fénynek és fénybiztosításnak a hadtörténeti szerepét. Ebben a fejezetben a körletvilágításról, a katonai szabályozás szerinti felosztás következő alcsoportjáról esik szó. Körbejárjuk a vonatkozó követelményeket, a terület specifikumait, hogy nyomatékosítsuk a korábbiakban már említett témakör aktualitását és fontosságát. A cikkben elsősorban a munkahelyi világításra helyezzük a hangsúlyt, amelyben kitérünk a modern katonai világítás értelmezésére, a szakági követelményekre, annak ellenőrzésére és a lehetséges megoldásokra, ajánlásokra.

Kulcsszavak: **körletvilágítás, infrastruktúra megvilágítása, őrzésvédelmi világítás, világítási kritériumok, kontroll, átalakítás, okos katonai bázisok, CAD, akkreditáció, vizsgálat**

The third article of this series presenting the military aspects of the light and visibility continues the previous topic. In the first and second parts, we presented the legal and requirements of lighting in the military area, as well as the issues of military operations, the conditions and means of their application. We have taken a look at trends in development to enhance visual performance and briefly summarised the military history of the role of light and lighting support. In this article we go around the relevant requirements of military bases to point out the specifics of the area and emphasise the importance of the topic. We focus on workplace lighting, in which we

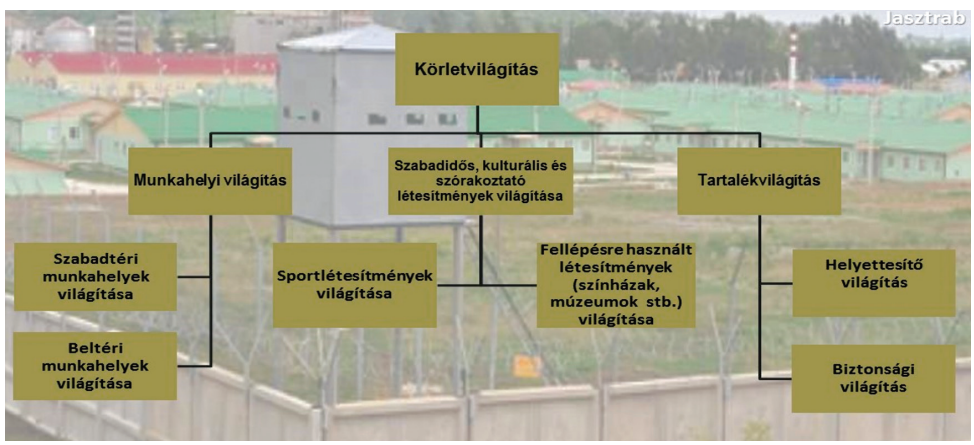
[1] Óbudai Egyetem, EHS, gépészmérnök, munkavédelmi szakmérnök, egészségügyi szakértő, e-mail: jasztrabp@yahoo.com
[2] MHP Egészségügyi Csoportfőnökség, Haderővédelmi és Gyógyító Főnökség, intézetvezető főorvos, e-mail: meglecz.katalin@hm.gov.hu

cover the interpretation of modern military lighting requirements and its control. We show technical parameters and possible solutions and recommendations for design.

Keywords: **lighting of military bases, infrastructure lighting, security lighting, lighting criteria, control, alteration, redesign, smart military bases, CAD, accreditation, testing**

1. Bevezetés

A körletvilágítás[3] (a közlekedési, reptéri világítás, illetve harctéri világítás mellett) a katonai világítás egyik főcsoportja, és beletartozik „a közlekedő, kantin, konyha, egészségügyi és sportlétesítmények, közösségi helyiségek, irodák, hálók, de még a vészvilágítás[4] is".[5] Alapvetően három területre osztható fel, „a munkahelyi világításra, szabadidős, kulturális és szórakoztató létesítmények [...] világítására és tartalékvilágításra".[6] A terület részletesen szabályozott és egyben „a munkavédelem legeklatánsabb"[7] része, amely munkaegészségügyi mérésekkel jól kontrollálható. Itt előtérbe kerül a komfort, illetve a metrológia kérdése is,[8] de a szolgálati feladatokra tekintettel érdemes a vizuális teljesítményre is figyelmet fordítani. (Lásd a körletvilágítás felosztását az 1. ábrán.) A terjedelmi korlátok miatt a szabadidős, kulturális és szórakoztató résszel nem foglalkozunk.[9]



1. ábra

Körletvilágítás felosztása

Forrás: Jasztrab–Gúth (2015): i. m. 13.

[3] Lásd Jasztrab Péter János – Istók Róbert: Fény és világítás katonai aspektusai. In XXXV. Jubileumi Kandó Konferencia. Budapest, 2019. 147.

[4] Ezt a MSZ EN 1838 szabvány tartalékvilágításnak nevezi, de a külföldi irodalom ettől eltér. Vö. Jasztrab Péter János: Minimális látási követelmények vészhelyzetekben, avagy a biztonsági világítás. *Hadmérnök,* 10. (2015), 2. 5–21.

[5] Jasztrab Péter János – Istók Róbert: A világítás katonai vonatkozásai: 1. rész: Navigálás a látási és láthatósági követelmények, világítási előírások katonai aspektusai között. *Hadmérnök,* 14. (2019), 4. 20.

[6] Jasztrab–Istók (2019): i. m. 20.

[7] Jasztrab Péter János – Gúth Gábor: A minimális látási követelmények és eszközeiknek katonai szemlélete II. rész. *Hadmérnök,* 10. (2015), 4. 12.

[8] Méréstudomány (méréstan). Itt értjük a mérési pontosság és a megismételhetőség, akkreditáció szerepét.

[9] Illetve elmarad az egészségügyi szakág és hitelet, oktatási intézmények tárgyalása.

A körletvilágításra jellemző, hogy a területen használatos világítás jól illeszkedik az európai szabályozáshoz,[10] ahol a termékek alkalmazása lényegében egy megfelelőségi minősítéssel lehetséges, azonban ennek fontos eleme a felhasználás körülményének és módjának ismerete. Az elvárandó követelmények helyes ismeretével elkerülhetők a tervezői félreértések és a megbízói hanyagság, amelynek eredménye a nem megfelelő kivitelezés. Az írásunkkal ösztönözni szeretnénk a mérnöki felelősségvállalást, és célunk a területen az egyediségek megőrzése mellett a tudatosság növelése. A honvédség az egyik legfontosabb munkáltató az intézményeivel, alakulataival, nem is beszélve a beszállítói és alvállalkozói hálózatáról. Szerepe egyedülálló, mértékadó és szabályteremtő a piacon. Ezért a korlátozó körülmények lebontásával, a mérnöki kreativitás és lehetőségek irányába kell fordulnunk. A katonai specifikumok hangsúlyozása a végfelhasználók, megrendelők, tervezők, gyártók érdekeit szolgálja, és elősegíti a normák hézagainak kitöltését és az ellentmondások kiküszöbölését. A megfelelő körletvilágítás kialakításával bizonyítottan magasabb vizuális teljesítmény érhető el, nem utolsósorban hatékonnyá tehető a felhasználás. Ezenfelül ne feledjük, a műveleti területen az erőforrások korlátozottan vannak jelen, ezért prioritást kell, hogy élvezzen a tudatos tervezés.

A cikkben szó esik a katonai világítás modern értelmezéséről, a szakági feladatokról, a műszaki szempontokról, és azok értelmezéséről, illetve az ellenőrzés lehetőségéről a katonaságon belül, valamint általunk meghatározott követelményekről, javaslatokról.

2. A modern katonai világítás értelmezése

Elkerülhetetlen a fejlődés és az új technológiák implementálása, ezért előremutató az elterjedést figyelembe vevő követelmények beépítése az előírásokba. Az egyik ilyen irányzat az automatizálás, amely könnyebbé teszi az életünket. Számos kialakítása létezik. A szakirodalomban okos jelzővel[11] emlegetik őket.

Az épületek hatékonyságának és ellenállóképességének javítása érdekében a létesítményeket át kell alakítani, hogy nyomon lehessen követni az energiafelhasználást és a kialakult trendet. A szenzorokkal hatékonyan elemezhető a kihasználtság, ami segít az erőforrások átcsoportosításában. A kontroll kiterjedhet az épületek közeli és távoli környezetére, illetve veszélyeztetett fajok jelenlétére és külső hatások, expozíciók figyelemmel kísérésére.[12] (Lásd az amerikai okos bázist a 2. ábrán.)

[10] A minőség nem egyenlő a mennyiséggel. A nagy választék közül a felhasználáshoz az optimálist kell választani.
[11] Itt értsd smart (automatizált).
[12] „2017-ben a Maxwell Légierő Bázisa nyilvánosság elé tárt egy vezeték nélküli intelligens kerületet, amely infravörös érzékelőket és arcfelismerést használt a behatolók és a bázis személyzetének észlelésére és azonosítására." Susan Miller: Army plans industry day for IoT and 'smart bases'. *Defense Systems,* 2019. március 8.

2. ábra
USA, Alabama, Maxwell Légierő Bázis
Forrás: Google Earth

A katonai bázisok épületek, építmények, szabadterek együtteséből állnak, melyek működéséhez a mesterséges megvilágítás elengedhetetlen. A világítás szerves része a létesítésnek és használatnak egyaránt, amire oda kell figyelni.

A komplexitásnak köszönhetően a modern mérnöki munka nem nélkülözheti a számítógépes tervezést. Segítségével megteremthető a létesítmény teljes élettartamára a rendszeres, tervszerű karbantartás. A tervezőknek meg kell felelniük a világítási teljesítményre, vezérlésre vonatkozó követelményeknek,[13] amiben a virtuális tér segítséget nyújt.

Az ötlet alapján generált digitalizált fotometriai tervekkel verifikálni lehet a kiválasztott fényforrásokat, hogy azok kialakítása és elhelyezése megfelel-e az előírt teljesítménykritériumoknak.[14] A számítógép segítségével történő tervezés során fontos paraméterek:[15]

- vízszintes megvilágítási értékek munkasíkon vagy más meghatározott magasságban;
- minimális és maximális fényerő és fokozatok;
- megvilágítási átlagos minimális karbantartási érték;[16]

[13] Melyeknek a végleges kialakítást kell tükrözniük az összes korlátozó, befolyásoló tényezővel, mint a növényzet, berendezés, környező épületek, természetes fényforrások.
[14] A katonai világítást tárgyaló cikksorozatunkban a számítógépes tervezőrendszerekkel az 5. részben fogunk foglalkozni.
[15] A világítási környezetet meghatározó fő jellemző a láthatósággal (információval) és zavarmentességgel kapcsolatos igények: fénysűrűség-eloszlás, megvilágítás, káprázás, fényszín és színvisszaadás, fény iránya, villogás.
[16] A megvilágítás időbeli egyenletességét is mérlegelni kell a fényforrásadatlap alapján.

- egyenletesség, azaz a vízszintes megvilágítás átlagos maximális és minimális aránya;
- világítás teljesítménysűrűsége; [17]
- fényhasznosítás és élettartam.

3. Szakági feladatok a katonai bázisokon

A katonai világítás aspektusainak tárgyalása közül a körletvilágítás mutat rá a legjobban a honvédelmi ágazat egyedi követelményeinek szükségességére és aktualitására, amely érdemessé teszi annak polgári élettől eltérő tárgyalását. A teljesség igénye nélkül bemutatjuk az élőerős őrzés-védelem fő területeit és egy koncepcionális világítás-tervezés megoldását. Szó lesz a fegyverraktárakról, kikötőkről és szigorúan őrzött területekről, illetve a pihenőkörletekről, kültéri közlekedőkről, speciális és egyéb helyiségekről. Ez a felosztás szándékos egyszerűsítést tükröz, amire a terjedelmi korlát miatt van szükség.[18]

3.1. Őrzés-védelem, kontroll, átvizsgálás

Kiemelten fontos szempont a katonai feladatok között az épített környezet, létesítmény, objektum élőerős védelme, ami kulcsszerepet tölt be a fenyegetés időben történő észlelésében és az agresszió, szabotázs, kémkedés elhárításában, valamint a lopás megelőzésében, és az illetéktelen behatolás megakadályozásában. Ehhez nélkülözhetetlen a jó látási körülmények, illetve este a megfelelő megvilágítás biztosítása. A rendszer fizikai elemeit kiegészítve a védelemnek elő kell segítenie a biztonságos eszközhasználathoz foganatosított intézkedéseket, melyek lehetnek az őrzött terület határán, kiemelt létesítménynél vagy ellenőrzőpontokon.[19] A kiépített rendszernek képesnek kell lennie a fenyegetés észlelésére, felmérésére, majd annak semlegesítésére. Cél az átlátható és a vizuálisan jól felismerhető terület biztosítása,[20] amely javíthatja a biztonság megítélését és a szolgálatot teljesítők munkakörülményeit.[21]

A világítást össze kell hangolni az őrutasítással vagy a védelmi (biztonsági) tervvel. A világítás lehet telepített, folyamatos fényt biztosító lámpasor, amit készenléti és hordozható (mobilis) világítások egészíthetnek ki. A kiegészítő rendszerek rendkívüli vagy váratlan események hatására aktivizálódnak. Elsősorban elrettentő szerepük van, de energia-megtakarítás is elérhető az időszakos működésüknek köszönhetően. A hordozható eszközök a rendszer tökéletlenségeit egészíthetik ki, és fokozzák az egyének vizuális teljesítményét.

[17] Itt watt/négyzetméter.

[18] Szofisztikált és részletesebb leírás lehetséges. Bizonyos területek összevonásával, egyszerűsítésével éltünk.

[19] Legyen ez élőerővel vagy kamerával megfigyelt terület.

[20] A fény növeli az észlelés, azaz a lebukás valószínűségét, és arra késztetheti a behatolást végrehajtó agresszorokat, hogy könnyebb célpontot keressenek. Korreláció a fény minősége és a bűncselekmények száma között nincsen. Rebecca Steinbach et al.: The Effect of Reduced Street Lighting on Road Casualties and Crime in England and Wales. Controlled Interrupted Time Series Analysis. *Journal of Epidemiology & Community Health,* 69. (2015), 11. 1118–1124.

[21] Lorenzo Munar Suard: *Munkahelyi veszélyek és ártalmak megelőzése a magánbiztonsági iparágban.* Bruxelles, Centre de Sociologie de la Santé, Université Libre de Bruxelles, 2004. 47.

3.1.1. Épületek be- és kijárata és épületek külső területe, belépési pontok

Az épületek be- és kijáratait meg kell világítani. Fényforrása lehet rejtett, teljesen árnyékolt, illetve fényszennyezés- és káprázásmentes. Az épület bejáratánál a fényerő növelésével a látogatókat és más személyzetet irányítsa a megfelelő épületbejárathoz. Vészkijárati világításként is szolgálhat. Veszély esetén az embereket vezesse ki az épületből. Ezeken a helyeken a világítás véd az illetéktelen behatolástól, és elegendő fényt biztosít a fenyegetés felméréséhez. Az épület vagy a szomszédos terület egyaránt megvilágítható falra szerelhető vagy a földbe süllyesztett lámpatestek használatával. A homlokzati telepítés és a fény ernyőzése növeli a fényerőt és csökkenti a fényszennyezést. Mindemellett őrzés-védelem szempontjából érdemes különbséget tenni az alacsony, közepes vagy magas szintű védelmet igénylő zónák között.[22] Besorolástól függően kell megvilágítani a bejáratot, az épületet vagy az épület környékét (lásd a 3. ábrát).

3. ábra

Kültéri ajtó és épületek külső területei

Forrás: a szerzők szerkesztése

3.1.2. Ellenőrző létesítmények, őrhelyek, átvizsgálási pontok, járművizsgálat

Az ellenőrző létesítményeknek több fajtája létezik. Idetartoznak az állandó gyalogos- és gépjárműellenőrzési pontok, őrhelyek, tornyok, ellenőrző-áteresztő pontok, gépkocsi-átvizsgálási helyek.[23] A belépést ellenőrző létesítmények több fő zónára oszthatók fel: megközelítési, belépési és reagálási területre (lásd a 4. ábrát).[24]

[22] Illetve függ a környező megvilágítási értéktől is.
[23] Itt értjük a mobil ellenőrző-áteresztő pontot (EÁP) is.
[24] A felállítási hely a körülményektől függ.

A megközelítési zóna szolgál arra, hogy a közeledőket biztonságosan a belépési zónába vezesse. A tükröződés minimalizálása érdekében használjon teljesen árnyékolt vagy felfelé ernyőzött, vízszintesen szerelt lámpatesteket. A szem akkomodációjára figyelve fokozatosan kell növelni az átmeneti megvilágítás segítségével a megvilágítási szintet, amelyhez akár néhány másodperc is szükséges.[25] A zónához közeledve a szolgálati személyzet vizuális teljesítményének megőrzéséért utasítsák jelzések a fényerő (itt a fényszórók) csökkentésére (vagy kikapcsolására).

A megvilágítás a belépési és ellenőrzési zónában a legmagasabb. Itt figyelembe kell venni a vizuális azonosítási és dokumentumellenőrzési feladatokat. Nagyobb részében teljesen árnyékolt vagy felfelé fényt ki nem bocsátó lámpatestek biztosítsák a megfelelő világítást. A függőleges megvilágítás segíti az arcfelismerést. Használjunk alacsony fényerejű fényforrásokat (< 3500 lumen), illetve a személyzet mögé, a falra szerelt lámpatesteket. A folyamatos fényerőváltozáshoz történő alkalmazkodás fárasztja a szemet és kimerültséghez vezet.

A reagálási zónában szintén egyenletességre kell törekedni, és fokozatosan csökkenjen meg a világítás értéke a területen. A káprázás legyen minimális az áthaladók, illetve a személyzet számára egyaránt. Teljesen árnyékolt vagy felfelé korlátozott fénykibocsátású és vízszintes síkba szerelt lámpatesteket használjunk, minimális káprázási értékkel. Ezenkívül jelzések hívják fel a figyelmet a fényforrás- (fényszóró-) korlátozás végére, hogy ne felejtsék el azt visszakapcsolni. Az úttest megvilágítása legyen előírás szerinti.

A gyalogosoknak tisztán látniuk kell a kaput, a kártyaolvasót, illetve az áteresztő ponthoz közeledő gyalogosokat tegyék azonosíthatóvá.

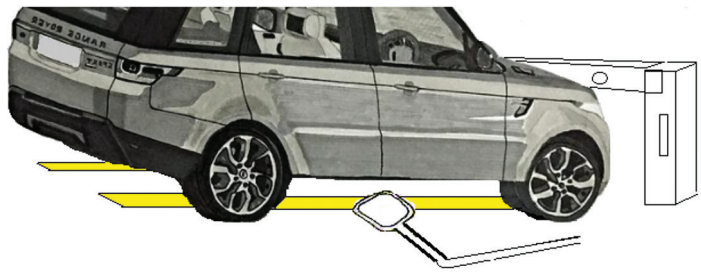
4. ábra

Ellenőrző létesítmények, megközelítési, belépési és reagálási területek

Forrás: a szerzők szerkesztése

[25] Lásd még az *IES RP-22-11 Tunnel Lighting* írásban, illetve Mark Stanley Rea (szerk.): *The IESNA Lighting Handbook*. Illuminating Engineering Society of North America, 2000.

Az ellenőrzés egyik fontos eleme a járművizsgálat. Miközben a járművek ellenőrzés céljából megállnak, az alváz átnézését is lehetővé kell tenni. Itt az egyenletesség fontos tényező, illetve az, hogy az alkalmazott tükör által árnyék ne keletkezzen (lásd az 5. ábrát).



5. ábra
Gépjármű-átvizsgálás
Forrás: a szerzők szerkesztése

Az őrszolgálati helyiségekben (bódékban, tornyokban) világítást kell biztosítani az azonosításhoz, a papírmunkához[26] és esetleg a képernyő előtt végzett feladatokhoz. A belső fényforrást alacsonyabb szinten kell tartani, mert kívülről a belátást el kell kerülni. A belső világítás árnyékolásának minimalizálnia kell az üvegről való visszaverődést, amely korlátozhatja a látást kifelé. A munkaállomás egyes feladatainak világítása magasabb szintre emelhető. Valamennyi világítótestnek szabályozhatónak kell lennie a belső világítási szint beállításához. Ahol (fegyveres) őr áll, ott a személyzet megvilágítását kerüljük el. A vörös színű fény segíti a szem sötét alkalmazkodásának megőrzését, de ne használjon ilyen fényt a feladat megvilágításához, ahol a színlátás (színérzékelés) a tevékenységhez elengedhetetlen (lásd a 6. ábrát).

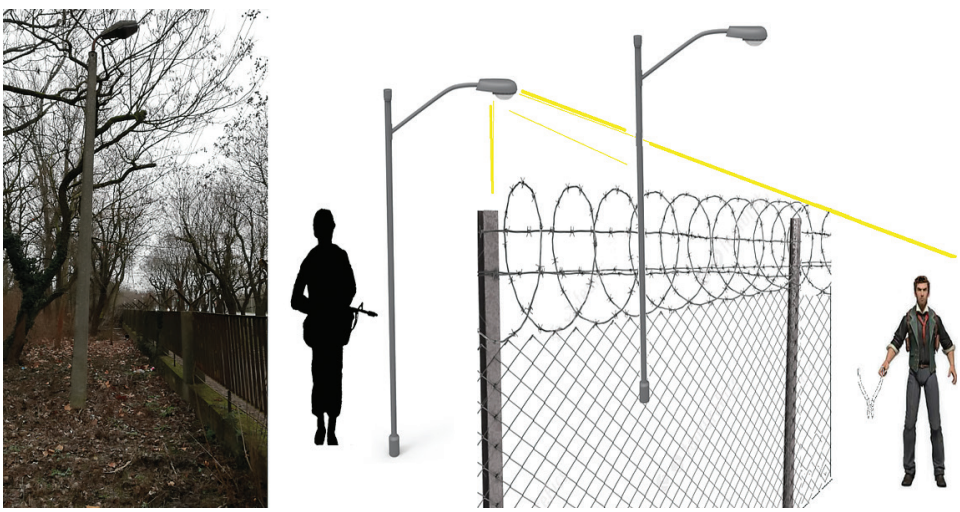
6. ábra
Őrhelyek
Forrás: a szerzők szerkesztése

[26] Itt lehet 300 lux vagy ennél magasabb követelmény is.

3.1.3. Külső területek ellenőrzése, héjvédelem, járőrútvonal

A külső területek biztosítása, azaz a héjvédelem sokszor az ellenőrzött terület határán túl magában foglalja a kerítéssel szomszédos külső és belső szabad zónákat, vagy bizonyos esetekben a kettős kerítés vonalának (izolációs zóna) részét. A világítás lehet folyamatos vagy készenléti, vezérelt, továbbá a fenyegetés mértékétől függően a vakítás céljára fényszórókkal bővített.

A műszaki paramétereket tekintve biztosítani kell tartóoszlopokat, áramellátást és transzformátort. A fényforrások lokalizációját egyeztetni kell, hogy a kiürítés előírásain és a vagyonvédelem szempontjain ne essen csorba. Ha lehetséges, az oszlopok távolsága átlátható kerítés esetén annak vonalától nem lehet kevesebb, mint 1,5 méter, dupla kerítés esetén 0,5 méter (lásd a 7. ábrát).[27]



7. ábra
Héjvédelem, járőrútvonal a külső területen
Forrás: a szerzők szerkesztése

3.1.4. Helyettesítő- és tartalékvilágítás

A helyettesítő- és tartalékvilágításra jellemző, hogy a szabályozása és a műszaki kialakítása elkülönül a hagyományostól, és a feltételrendszere is ehhez idomul. Az irodalomban is sok esetben elkülönítik, azonban érdemes integrálni a modern értelmezés alapján a körletvilágítás követelményrendszerébe. A kialakításnak elő kell segítenie a menekülést és az életmentést, valamint a veszélyhelyzet megelőzését. A minimális látási körülményeket figyelembe véve nem szabad, hogy az az őrzés-védelem szerepét

[27] Optikai szálat vagy infrasorompót is figyelembe kell venni.

csökkentse. Egy korábbi publikációban olvashatók ajánlások a követelményekre,[28] ezért itt ennek részletezésére nem térünk ki.

Összességében elmondható, hogy a vizuális információk kulcsszerepet töltenek be a biztonságérzet növelésében, a kiürítés és a pánik kezelésében. Az előírás vonatkozik a tömegtartózkodású helyekre,[29] a menekülési útvonalakra, a füstmentes lépcsőházakra, illetve minden irányváltoztatási pontra, kijárati ajtóra, biztonsági liftre, előtérre, továbbá tűzoltási, beavatkozási helyiségre, pontra. A minimumszint meghatározásánál mindenhol figyelembe kell venni a fényforrás öregedését, szennyeződését és az energiatáplálásban elképzelhető változásokat.

3.1.5. Műszaki szempontok és követelmények

Itt essen pár szó a műszaki paraméterekről is, de közben ne feledkezzünk meg az olyan alkalmazott eszközökről, mint az éjjellátó kamerák, érzékelők.

Számos kameratípus létezik. Elmondható róluk, hogy a megfigyelés kiterjesztésének eszközei. Jellemző rájuk, hogy működésük eltér az emberi szemétől. A színes kamerák általánosságban magasabb fényszintet igényelhetnek,[30] mint monokróm társaik. A CCTV[31] színes vagy monokróm típusaihoz megfelelő és egyenletes megvilágítást kell biztosítani. A kamerákat általában magasban telepítik, és környezettől függően a vertikális megvilágítási érték fontosabb, mint a horizontális irányú. A függőleges megvilágítás legyen 2–5 lux a talaj felett másfél méterrel mérve a látás irányában, az egyenletesség aránya pedig 4 : 1.

Az infravörös kamerák érzékelik a kibocsátott hullámok visszaverődését a területen lévő tárgyakról. Használatához egy infravörös adóra van szükség. A hőtechnikát alkalmazó eszközök működése nem igényel fényforrást (adót). A képeket az emberek, a járművek, a talaj és a lombok közötti hőkülönbségek alapján hozzák létre. Más kameratechnológiákkal ellentétben a hőfényképeket nem befolyásolja a fényszórók vagy a fényforrások tükröződése. Ez a technológia látja az embereket és tárgyakat teljes sötétségben, de nem biztosít részletes képet. Csak az említett technológiák integrálása nyújt megoldást.

Az érzékelők a működés és vezérlés kontrollálásának elengedhetetlen eszközei, a kézi és az időzítő típusok mellett. A jelenlétérzékelők infravörös, ultrahang-, esetleg hangszenzorosak vagy ezek ötvözetei. Lényeges a késleltetés,[32] nem úgy, mint az adaptív technológiánál. Ezenfelül fontos kérdés az érzékelők érzékenysége, amely egyben függ az aktivitástól a helyiségben.

További kritikus tényező a biztonsági világítórendszerek működésének folytonossága. Többféle módszer létezik, amelyek tartalék áramellátást biztosítanak áramkimaradás esetén. Mindegyiknek van előnye és hátránya. Fő differenciálási

[28] A követelményeket lásd Jasztrab Péter János: Minimális látási követelmények vészhelyzetekben, avagy a biztonsági világítás. *Hadmérnök,* 10. (2015), 2. 5–21.
[29] 100 fő befogadóképességű helyiség.
[30] ≥ 80 CRI.
[31] Closed-circuit television.
[32] A fényforrás élettartalmát figyelembe véve 10-15 percnek kell lennie.

lehetőségek az energiaellátás időtartama, valamint az áramkimaradás és a tartalék energia bekapcsolása között eltelt idő, illetve működési költségeik. A tartalék áramellátó rendszernek figyelembe kell vennie néhány fényforrás újbóli bemelegedési idejét is. A fémhalogenideknek és a nagy nyomású nátrium-fényforrásoknak bizonyos időre van szükségük a lehűléshez, mielőtt újra meggyulladhatnak. Ez az idő akár 15 percet is elérhet. Ha ezeket a forrásokat használják, akkor szükség lehet kiegészítő fényforrásra. A LED-es és indukciós fényforrásrendszerek szinte azonnal bekapcsolhatók. A szünetmentes tápegység (UPS, angolul Uninterruptible Power Supply) egy akkumulátorforrás, amely áramellátás esetén azonnali energiát biztosít, de a bekerülési költsége magas és a karbantartása drága.

A másik módszer a lendkerék használata, amely pillanatnyi teljesítményt biztosít rövid ideig. Ez az energia áramkimaradás esetén azonnal hasznosítható és felhasználható a kritikus megvilágítás áramellátására. Ehhez képest a generátorok bekapcsolási ideje hosszú.

A vezérlés módja lehet automatikus vagy manuális, esetleg félautomata, amely aktiválódhat sötétség hatására, vagy amikor a láthatóság csökken, továbbá, ha jelenlétet vagy mozgást érzékel. Ezenkívül számos más szenzor is telepíthető.[33] A kézi működtetésnél lényeges, hogy ellenőrzött helyen legyen annak ki- és bekapcsolási lehetősége. (Lásd részletesen később a 2. táblázatban.)

Szeretnénk kihangsúlyozni, hogy a kialakítástól és adottságtól függően egyedi megvilágítási kritériumok válhatnak szükségessé. Az egyes tevékenységekhez kapcsolódó javaslatok az utolsó fejezetben találhatók. Az elektromos részek követelményei önálló részt érdemelnének, de ezen szempontok tárgyalására itt nem térünk ki.

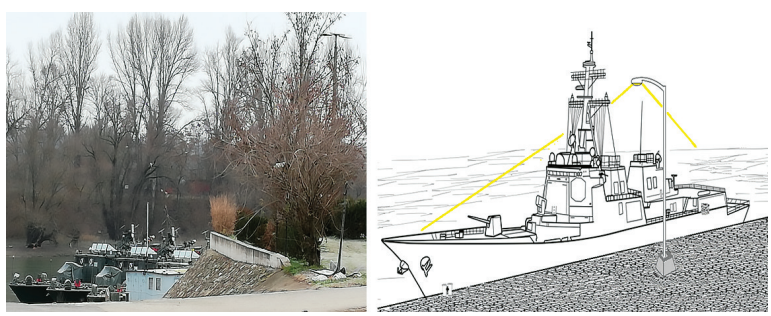
3.2. Fegyverraktárak, kikötők és szigorúan őrzött területek

A körletvilágítás egy része a védett terület, amely szintén objektumok vagy köztes szabadterek együttese. Jellemzően oszlopon találhatók a világítótestek, de ha lehetséges, telepítsünk fali lámpatesteket a költségek minimalizálása érdekében. Biztosítsanak egyenletes megvilágítást úgy, hogy minimalizálják az árnyékokat. Tűz- és robbanásveszélyes környezetben a tűzvédelmi és ATEX követelményeket figyelembe kell venni. Teljesen árnyékolt és káprázásmentes lámpatesteket használjunk. A fényvisszaverődés és a fényszennyezés minimalizálása érdekében alacsony fényteljesítményű, de jobb eloszlású lámpa telepíthető. Itt is gondolni kell a kereső és vészhelyzeti világításra, illetve tartalékenergia rendelkezésre állására (lásd a 8. ábrát).

[33] Fotószenzoron kívül ultrahangos, rádiófrekvenciás, optikai, infravörös, hang- vagy mozgásérzékelő szenzorokat is használnak, de az időzítőknek is nagy szerepük van.

8. ábra
Raktár, hangár, depó
Forrás: a szerzők szerkesztése

A hajózható vízparton és kikötőkben ajánlott a magasra helyezett világítás kialakítása az oszlopok számának és így a vízparti akadályok csökkentése érdekében. A tartók és a hozzájuk tartozó betontalapzatok típusainak és elhelyezkedésének a működési és hajózási szempontokat figyelembe kell vennie. Kikötőknél kézi működtetésű reflektorokra van szükség, hogy segítsék az esetleges vízparti fenyegetések felkutatását és felmérését. A világítás vezérlését közvetlen kontroll alatt kell tartani. A víz alatti megvilágításra általában nincs szükség a felszín alatti veszélyek felderítéséhez, és nem javasolt korlátozott előnyök és magas telepítési költségek, továbbá karbantartási problémák miatt. A móló alatt elhelyezett lámpatestek szintén nem ajánlottak, de több szint esetén biztosítani kell a közmű- és munkaterületek megvilágítását. A lámpatestek vezérlésének a kézi és automatika között állíthatónak vagy integráltnak kell lenniük. (Lásd a kikötői világítást a 9. ábrán.)



9. ábra
Hadi kikötő
Forrás: a szerzők szerkesztése

3.3. Pihenőkörletek, kültéri közlekedők

Az állomány számára a munkavégzést tekintve az irodáknak, konferenciatermeknek, a tantermeknek, a karbantartási területeknek és tárgyalóknak, közösségi helyiségeknek domináns szerepük van. A nappali fény árnyékolása növeli a komfortot és elégedettséget. A fokozatos állítási lehetőség preferált a hirtelen be- és kikapcsolással szemben. Ideális esetekben a kézi tompítást a nappali felső határértékkel jó biztosítani. A köztes, átmeneti területek a folyosók, előcsarnokok, mosókonyhák, étkezők, mellékhelyiségek és tárolóhelyek szintén nem elhanyagolhatók. Itt jobban figyelembe vehető a hangulat- és a közvetett, rejtett kialakítás. Lehet automatikus, esetleg két- vagy többszintű kapcsolás. A jelenlétérzékelőkkel a közösségi helyiségekben az energia megtakarítható, de nem telepíthető korlátlanul. A fotószenzoros vezérlésadaptáláshoz szükséges a helyiség jellegzetességeinek felmérése és zónák kialakítása épületen, épületegyüttesen belül. Ezzel megelőzhető a fáradékonyság kialakulása. Előnyös, ha az elsődleges és a másodlagos zónában lévő lámpatestek a nappali fényre kikapcsolnak vagy halványulnak. A mesterséges világításnak akkor kell csökkennie, amikor a nap fénye meghaladja a meghatározott megvilágítás értékét a feladatsíkon. Fokozatmentes (és folyamatos) beállítás javasolt a szakaszos helyett.

A zónák kiválasztásakor az ablakok közelsége és tájolása mellett figyelembe kell venni a külső környezetet is. Más épületek vagy lombkoronák blokkolhatják a napfényt, illetve annak mértéke a földszinten és az emeleten emeletenként is különbözhet, valamint lényeges, hogy a nappali időszakban a fényszint legalább kétszer nagyobb.

3.4. Speciális és egyéb területek, helyiségek

A „Speciális és egyéb területek, helyiségek" bekezdésbe igyekeztük belesűríteni a még nem tárgyalt részeket. Előbbiekben a biztonsággal és védelemmel kapcsolatos témákat emeltük ki, de nem mehetünk el szó nélkül az irodalomban fellelhető ténymegállapítások mellett, melyek rámutatnak „a fény fontosságára a műveletben résztvevők körletben eltöltött ideje alatt. […] A különböző szín hőmérsékletű megvilágítások a közösségi életre, térképolvasásra, és egyéb tevékenységeikre befolyással vannak, és a világítás alatt a sátrakban ülő katonákra az egyik világítási fajta pozitív hangulatot, fokozott éberséget és gyorsabb teljesítményt eredményez a vizuális észlelési és kognitív feladatok során".[34] Érdemes telepítés során a táborokban az állomány feladataira és a személyzet pihenőkörleteire figyelmet fordítani. Azonban idáig, konzekvensen a megkezdett témához, a létesített objektumok fontos részeire koncentrálunk, és itt is csak a legfontosabbakat emeljük ki.

[34] Jasztrab–Istók (2019): i. m. 147.

10. ábra
Különböző színhőmérsékletű fényforrásokra példa
Forrás: a szerzők szerkesztése

A nem ideiglenes létesítményekhez tartoznak és azok fontos részei a műút, a behajtók, a gépkocsibeállók és a parkolók. Ezeknél oszlopra szerelt, teljesen árnyékolt típusok előnyösek, de a behajtóhoz mindenféleképpen szükséges telepíteni. A gyalogosoknak fenntartott útvonalak lámpái és tartószerkezetei illeszkedjenek a szomszédos épületek esztétikájához. Nagy kockázati helyek, mint a kereszteződések, legyenek hangsúlyosak. A lámpatestnek árnyékoltnak kell lennie és a káprázást, fényszennyezést el kell kerülni. (Lásd a 10. ábrát a nem előnyös telepítésre, illetve a terek kialakítására a 11. ábrát.)

11. ábra
Épületek közötti terek
Forrás: a szerzők szerkesztése

4. Mérés és ellenőrzés

A mérési és ellenőrzési feladatok a honvédségen belül is fontosak. Ebben a részben röviden szó lesz az ellenőrző szervezetről és működési feltételéről, illetve a betöltött szerepéről, képességéről.

4.1. Akkreditálás

Az akkreditáló testületeket a bizalom és a megbízhatóság egységes elveire épülő elismerés hozta létre. Feladatuk, hogy bizonyítsák, ha egy szervezet vagy egy természetes személy alkalmas bizonyos tevékenységek (vizsgálat, kalibrálás, mintavétel, tanúsítás, ellenőrzés stb.) elvégzésére. Az Európai Unió tagállamainak hatóságai kötelesek elfogadni az akkreditált szervezetek eredményeit, és ez garanciát jelent a piaci szereplők, állampolgárok számára.

A működés megkezdése és a követelmények fenntartása érdekében fontos a kontroll, amiről egy hiteles ellenőrzés nyújt megfelelő információt. Segítségével a problémák megelőzhetők, és így felszínre kerülnek a nem megfelelőségek.[35] Azonban fontos hangsúlyozni, hogy nem lámpa kihelyezésére, hanem komplett rendszer kialakítására kell gondolni ebben az esetben, és a kötelező ellenőrzést nem szabad a karbantartási feladattal összekeverni.

4.2. Munka- és Sugáregészségügyi Laboratórium

A honvédelmi ágazatot illetően az ellenőrző laboratórium a MH Egészségügyi Központhoz tartozik, és a Védelem-egészségügyi Igazgatóság, a Tudományos Kutató- és Laboratóriumi Intézet, illetve a Katonai, Mikróbiológiai és Környezet-egészségügyi Osztály irányítása alatt végzi a munkáját. A mérés és az ellenőrzés az alakulatok igénye szerint és munkahelyi világítási szabványok alkalmazásával zajlik.[36] A működés feltételeit kézikönyvben rögzítik. A katonai és harctéri specifikumoknak nem jut szerep, ezek működését automatikus felhasználás jellemzi. Egyéni ajánlás nélkül mérlegelésre nincs mód, ezért fontos azok hangsúlyozása és leírása iránymutatásokban.

5. Javaslatok, ajánlások

A jövőt az okos, intelligens épületek jelentik. Az építőanyagok és módszerek továbbra is hasonlóak az évszázad előttivel, de a hadsereg missziójával összefüggő területeket gyors változás jellemzi, ahol a katonaság ingatlanvagyona és -kezelése fokozatosan fejlődik. Az elmúlt évtizedek racionalizálási folyamatai jelentős hatást gyakoroltak az ágazat létesítményeinek állapotára, és bizonyosra vehető, hogy a jelenlegi

[35] Jasztrab (2015): i. m.
[36] Jelenleg nincs akkreditációjuk (2021).

döntéseknek is hosszú távú hatásai lesznek. Ez indokolja a gondos és rugalmas tervezés szükségességét. A tervezési szakaszban már érdemes figyelembe venni a modern kor követelményeit és előnyeit. A létesítmények napjainkban nagyon kifinomultak és személyre szabottak.[37] Automatikus működéssel megkönnyítik a használók, üzemeltetők munkáját, és növelik a komfortérzetet, egyúttal biztosítják az energiahatékonyságot és fenntarthatóságot. A felújítások és átalakítások, korszerűsítések követhetik ezt az elvet, amely költséghatékonysági számításra épül. Ahhoz, hogy optimális legyen, tervezői csoportot kell létrehozni, fel kell mérni a környezeti világítási zónákat, ki kell alakítani a vezérlési és működtetési energiakontroll-stratégiákat.

A tervezőcsoport konkrét tagságát a helyi szempontokra alapozzuk, de általában a következő funkciók legyenek képviselve: a létesítményhasználók, a terrorizmusellenes szolgálat, a műveletek résztvevői, a biztonság és logisztika, a mérnöki tervezői munka képviselői, munkabiztonság- és egészségvédelem és más szakágak emberei szükség szerint. Nekik kell meghatározni azokat a tervezési kritériumokat, amelyek magukban foglalják a védendő eszközöket, a fenyegető veszélyeket és az eszközök védelmének szintjét, az üzemeltetési szempontokat, a munkaerőigényt vagy a korlátozásokat, az energiatakarékossági pontokat és a fenntartási költségeket. A biztonsági világítási rendszernek elő kell segítenie az agresszorok felderítését, és segítenie kell a személyzetet a potenciális fenyegetések felmérésében és azok kezelésében. Minden biztonsági világítási tervet össze kell hangolni minden más tervvel. A helyszínen biztosított világítási rendszer típusa függ a telepítési környezettől és a tervezett felhasználástól. A könnyebb kezelés, érthetőség érdekében lényeges felmérni és zónákba sorolni a területet és épületeket, épületrészeket, szinteket.

A megvilágítási zónák tükrözzék a bázison előírt és a környezeti fényszintet, és vegyék figyelembe a helyi értéket is, hogy a telepítés ne tűnjön ki a szomszédhoz képest. Itt érdemes visszatérni a korábban, a pihenőkörleteknél említett épület részeinek értékelésére és kategorizálásának szükségességére. A döntésekben a modernebb és fenntartható objektumok elbírálásánál szerepet játszik az energiatakarékosság és fenntarthatóság. A gazdasági számításokkal a cikksorozat utolsó írásában foglalkozunk majd.

A vezérelhetőséget illetően több stratégia képzelhető el. A manuális működtetés csak akkor ajánlott, ha más nem lehetséges vagy nem valósítható meg. Egyik megoldás, ha kibővítjük jelenlétérzékelővel, ami a tér kiüresedése után 50%-ra csökkenti vagy teljesen kikapcsolja a megvilágítást, illetve a jelenlét esetén feloltja a lámpák 50%-át vagy a teljes hálózatot aktiválja. Egyes részeken a napfény változásával is kottázható a működés, illetve dimmelhető. Ennek eldöntéséhez a lehetséges jelenlevők és használók számát, valamint a végzett tevékenység jellegét ismerni kell. Minél precízebb vagy inkább odafigyelést igénylő feladatról van szó, annál fontosabb a működtetés feletti kontroll. Arról nem is beszélve, hogy energiamegtakarítással jár. Elképzelhető a hálózat vagy az egész épület automatizálása és a hűtés-fűtési rendszerrel való összehangolása.[38] (Az energiakontroll-stratégiát lásd a 1. táblázatban.)

[37] US Army: Army Installations 2025. 2016.
[38] Erre csak az épületautomatizálás ad lehetőséget.

1. táblázat

Az energiakontroll lehetőségei

Forrás: a szerzők szerkesztése

Belső terület megnevezése	Jelenlét-érzékelő	Többszintű kapcsolás	Idő-kapcsoló	Fotó-kapcsoló	Dimmer	Üresedés-érzékelés
Előadó	x	(x)	–	x	–	(x)
Oktatóterem	x	x	–	x	x	x
Konferenciaterem	x	(x)	–	x	x	x
Előcsarnok	x	(x)	(x)	x	–	–
Előszoba	(x)	(x)	x	–	–	–
Szertár/Irattár	x	–	x	–		x
Nyitott iroda	(x)	x	x	x	(x)	-
Privát iroda	x	x	x	x	x	x
Öltöző	x	(x)	–	–	–	–
WC	x	–	–	(x)	–	–
Raktár	–	x	(x)	(x)	–	–
Külső világítás	(x)	(x)	x	x	–	–
x – jól alkalmazható; (x) – korlátozottan alkalmazható; – alkalmazása nem javasolt.						

A körletvilágítás követelményeinek értékelésére és ellenőrzésére meg kell határozni a minimumértéket, amelyre a fényforrás élettartama előtti karbantartási szintet szokták megadni. Itt érdemes az egyenletességet és a megvilágítási horizontális értéket, a szerelést és az automatizálás érdekében a vezérlés módját megadni. Az általunk javasolt és betartandó előírásokat a 2. táblázatban gyűjtöttük össze.

2. táblázat

A körletvilágítás minimális kritériumai

Forrás: a szerzők szerkesztése

Terület/Feladat			Megvilágítás (*Ē*av)		Egyenletesség (U_o)	További követelmény	Szerelés	Vezérlés, működés
			Vertikális (*Ē*v)	Horizontális (*Ē*h)				
Épület, bejárat	Ajtó felett	Előtető van	6 lux (környező világítás van és alacsony, akkor 10 lux, ha magas, akkor 15 lux.	10 lux (környező világítás van és alacsony, akkor 20 lux, ha magas, akkor 30 lux.	Horizontális: 2 : 1 Vertikális: 4 : 1	Az épület esztétikai szerepét vegye figyelembe a világítás. Az árnyékok keletkezését el kell kerülni a bejáratoknál.	Süllyesztett világítás: Forrás: LED, fluoreszcens	Takarodó után vagy záróra, éjfél után a fényerő 30%-kal csökken. Érzékelő esetén, 15 perc után csökken a fényerősség. Napfényre kikapcsol.
		Előtető nélkül	6 lux (környező világítás van és alacsony, akkor 10 lux, ha magas, akkor 15 lux)	10 lux (környező világítás van, akkor is 10 lux)	Horizontális: 2 : 1 Vertikális: 4 : 1	Az épület esztétikai szerepét vegye figyelembe a világítás. Az árnyékok keletkezését el kell kerülni a bejáratoknál.	Forrás: LED, fluoreszcens	Takarodó után vagy záróra, éjfél után a fényerő 30%-kal csökken. Érzékelő esetén, 15 perc után csökken a fényerősség. Napfényre kikapcsol.

Terület/Feladat			Megvilágítás (*E*av)		Egyenletesség (U_0)	További követelmény	Szerelés	Vezérlés, működés
			Vertikális (*E*v)	Horizontális (*E*h)				
Épület, bejárat	Falon		–	7 lux	NA	Az épület esztétikai szerepét vegye figyelembe a világítás. Ne okozzon káprázást. Színvisszaadás: ≥ 80	Forrás: LED, fluoreszcens	Takarodó után vagy záróra, éjfél után a fényerő 30%-kal csökken. Napfényre kikapcsol.
	Információ felett		–	50–300 lux a felületen az igénytől függően	A kívánt felületen legyen a lehető legegyenletesebb, nem tükröződhet, ha igen, akkor a megvilágítási értéket csökkenteni kell.	Tükröződést minimálisra kell csökkenteni. Színvisszaadás: ≥ 80	Forrás: LED, fluoreszcens	Takarodó után vagy záróra, éjfél után a fényerő 30%-kal csökken. Napfényre kikapcsol.
Épület, kijárata és kiürítési útvonala	Ajtó		–	5 lux	≤ 40 : 1	Elsősorban falra szerelt változat. Ha a környező megvilágítás magas, akkor az ajtó feletti sort kell betartani.	Forrás: LED	Napfényre kikapcsol.
	Kiürítési útvonal	Út közepe	–	1 lux	≤ 40 : 1	Színvisszaadás: ≥ 40	Forrás: LED	Nem kapcsolható le, más jogszabályban meghatározott tűzállósággal kell rendelkeznie.
		Út negyede	–	0,5 lux	≤ 40 : 1	úthossz negyedében lévő sávban Színvisszaadás: ≥ 40	Forrás: LED	Nem kapcsolható le, más jogszabályban meghatározott tűzállósággal kell rendelkeznie.
Épület, biztonsági világítás	Menekülési útvonalon		–	5 lux	≤ 40 : 1	üzemi világítás > 50 lux	Forrás: LED	Nem kapcsolható le, más jogszabályban meghatározott tűzállósággal kell rendelkeznie.
	Biztonsági felvonó előtere		–	5 lux	≤ 40 : 1	üzemi világítás > 50 lux	Forrás: LED, fluoreszcens	Nem kapcsolható le, más jogszabályban meghatározott tűzállósággal kell rendelkeznie.
	Átmeneti védett tér		–	5 lux	≤ 40 : 1	üzemi világítás > 50 lux	Forrás: LED, fluoreszcens	Nem kapcsolható le, más jogszabályban meghatározott tűzállósággal kell rendelkeznie.
	Tömegtartózkodásra szolgáló helyiség, pánik		–	≥ 0,5 lux	≤ 40 : 1	üzemi világítás > 50 lux Színvisszaadás: ≥ 40	Forrás: LED, fluoreszcens	Nem kapcsolható le, más jogszabályban meghatározott tűzállósággal kell rendelkeznie.

Terület/Feladat		Megvilágítás (*E*av)		Egyenletesség (U_0)	További követelmény	Szerelés	Vezérlés, működés
		Vertikális (*E*v)	Horizontális (*E*h)				
Épület, biztonsági világítás	Tűzoltósági helyiségek[39]	–	5 lux	≤ 40 : 1	üzemi világítás > 50 lux Színvisszaadás: ≥ 40	Forrás: LED, fluoreszcens	Nem kapcsolható le, más jogszabályban meghatározott tűzállósággal kell rendelkeznie.
	Tűzoltóság által használatos helyiségek megközelítési útvonala	–	5 lux	≤ 40 : 1	üzemi világítás > 50 lux	Forrás: LED, fluoreszcens	Nem kapcsolható le, más jogszabályban meghatározott tűzállósággal kell rendelkeznie.
Épület, veszélyes munkahelyek helyiségében, tereiben			≥ *E*av · 0,1 de minimum 15 lux	≤ 10 : 1	0,5 m-es peremzónája figyelmen kívül hagyható. Színvisszaadás: ≥ 40	Forrás: LED, fluoreszcens	Nem kapcsolható le, más jogszabályban meghatározott tűzállósággal kell rendelkeznie.
Épületek környezete	Lakóhely	6 lux (környező világítás van és alacsony, akkor 10 lux, ha magas, akkor 15 lux.)	10 lux (környező világítás van, akkor is 10 lux.)	≤ 2 : 1 (horizontális) ≤ 4 : 1 (vertikális)	Lehet falra vagy oszlopra szerelt. Indikátor legyen oszlopok helyett.	Forrás: LED, fluoreszcens	A falra szerelt típusok, amelyek balkonok, erkélyek fényforrásai, manuálisan állíthatók. Sötétedéskor bekapcsol. Automatikusan csökken 30%-kal a fényerő aktivitás megszűnése után 15 perccel. Hajnalban kikapcsol.
	Kocsibejárók	Alacsony környezeti megvilágításnál: 1 lux, közepesnél: 3 lux, magasnál: 8 lux	Alacsony környezeti megvilágításnál: 2 lux, közepesnél: 6 lux, magasnál 10 lux	≤ 10 : 1 (horizontális)	Oszlopra szerelt javasolt a fényforrások csökkentése érdekében. Legyen a gyalogos közlekedési lehetőségek közelébe telepítve és a gócpontok környékére. Színvisszaadás: ≥ 40	Forrás: LED, indukciós, fémhalogén	Sötétedéskor bekapcsol. Automatikusan csökken 30%-kal a fényerő aktivitás megszűnése után 15 perccel. Hajnalban kikapcsol.
	Parkolók (személygépjármű)	1 lux, és 2,5 lux (emelt szintű védelem)	2 lux, és 5 lux (emelt szintű védelem)	≤ 20 : 1, és ≤ 15 : 1 (emelt szintű védelem)	Oszlopra szerelt javasolt a fényforrások csökkentése érdekében. Teljesen árnyékolt felfelé. Káprázás nem lehet. Színvisszaadás: ≥ 40	Forrás: LED, indukciós, fémhalogén	Sötétedéskor bekapcsol. Automatikusan csökken 30%-kal a fényerő, záráskor, tevékenység befejezésének észlelése után 15 perccel vagy éjfélkor, egészen napfelkeltéig vagy nyitásig, de legkésőbb 6 óráig.

[39] Beavatkozási központ, beépített tűzoltó berendezést elzáró helyiség, tűzeseti főkapcsolót tartalmazó helyiség.

Terület/Feladat		Megvilágítás (Eav)		Egyenletesség (U_o)	További követelmény	Szerelés	Vezérlés, működés
		Vertikális (Ev)	Horizontális (Eh)				
Épületek környezete	Gyalogos útvonalak	Alacsony környezeti megvilágításnál: 1 lux, közepesnél: 2 lux, magasnál: 6 lux	Alacsony környezeti megvilágításnál: 2 lux, közepesnél: 6 lux, magasnál: 10 lux	≤ 4 : 1 (horizontális) ≤ 10 : 1 (vertikális)	Minden kereszteződésbe vagy lehetséges, potenciálisan veszélyes helyekre (gócpontokra) lámpaoszlopot kell telepíteni. Indikátor legyen oszlopok helyett.	Forrás: LED, fluoreszcens indukciós (jelzőoszlopok kivételével)	Sötétedéskor bekapcsol. Automatikusan csökken 30%-kal a fényerő aktivitás megszűnése után 15 perccel. Hajnalban kikapcsol.
	Köztes terek, plázák	Alacsony környezeti megvilágításnál: 0 lux, közepesnél: 2 lux, magasnál: 4 lux	Alacsony környezeti megvilágításnál:1 lux, közepesnél: 4 lux, magasnál: 8 lux	≤ 4 : 1 (horizontális) ≤ 10 : 1 (vertikális)	A közteréknél össze kell hangolni az épületek külső világítását, ami a biztonságérzetre hatással van. A gyalogos útvonalaknak fényerőssége az idevonatkozó sor szerint változzon.	Forrás: LED, fluoreszcens indukciós (jelzőoszlopok kivételével)	Sötétedéskor bekapcsol. Automatikusan csökken 30%-kal a fényerő aktivitás megszűnése után 15 perccel. Hajnalban kikapcsol.
Ellenőrző pontok	Megközelítési terület	–	10 lux	≤ 4 : 1	A káprázást meg kell akadályozni. Ki kell tenni a figyelmeztető táblát a menetirányi fény csökkentésére, kikapcsolására.	Forrás: LED, indukciós, fémhalogén	Sötétedéskor bekapcsol. 15 perccel a napfelkelte előtt kikapcsol, illetve záráskor.
	Belépési terület	–	10 lux	≤ 4 : 1	A jelzések háttérvilágítása zavaró lehet, A kontraszt csökkentheti. Lehetőleg süllyesztett vagy tető felületére szerelt típus. Ellenőrző személyzet mögötti világítás.	Forrás: LED, fluoreszcens, felületre szerelt fémhalogén nem ajánlott	Sötétedéskor bekapcsol. 15 perccel a napfelkelte előtt kikapcsol, illetve záráskor.
	Reagálási terület	–	100 lux	≤ 3 : 1	A fényforrást az ellenőrző személyzet háta mögött kell elhelyezni, és az árnyékoltságot minimális szintre kell csökkenteni.	Forrás: LED, fluoreszcens	Csak manuális le- és felkapcsolási lehetőség.
	Gyalogosátkelési helyek	–	20 lux	≤ 3 : 1	Egy horizontális és egy vertikális világításnak kell lennie.[40] A vertikális legyen a kártyaolvasó vagy a belépő ellenőrzési pontjának közelében.	Forrás: LED, fluoreszcens	Csak manuális le- és felkapcsolási lehetőség.

[40] Közúton a gyalogos átkelőhelyeket lásd vonatkozó szabvány szerint.

Terület/Feladat		Megvilágítás (*Eav*)		Egyenletesség (U_0)	További követelmény	Szerelés	Vezérlés, működés
		Vertikális (*Ev*)	Horizontális (*Eh*)				
Ellenőrző pontok	Megfigyelőpont	–	200 lux (munkafelületen) és 30 lux (a megközelítési úton)	NA	A munkafelületen, ne világítson a személyzet szemébe. A külső terület fényforrása lehet fémhalogén. A fény színét meg kell választani.	Forrás: LED, fluoreszcens	Csak manuális le- és felkapcsolási lehetőség.
	Gépjármű-vizsgálási pont	–	100 lux	≤ 3 : 1	Az egyenletességet a gépjármű alvázán kell mérni. Hosszanti mérete 30 cm-nél nem lehet kisebb.	Forrás: LED	Csak manuális le- és felkapcsolási lehetőség, de legyen dimmelhető.
Külső (ellenőrzött) terület		–	40 lux	≤ 10 : 1	Fényforrások csökkentsék a beláthatóságot kívülről. Fényvetőket, azok hatékonyságát ellenőrizni kell. Tartalék-áramforrást biztosítani kell.	Forrás: LED, indukciós, fémhalogén	Automatikus felkapcsolás sötétedéskor. Meghatározott időben történhet a kikapcsolás.
Kikötő	Dokk	–	Aktív zónák: 50 lux, egyéb 5 lux	–	Állatvilágra figyelemmel kell lenni. (Monokromatikus LED)	Forrás: LED, fémhalogén	Automatikus felkapcsolás sötétedéskor. Meghatározott időben történhet a kikapcsolás.
	Móló	–	5 lux	Járófelületen ≤ 20 : 1	Oszlopra szerelt változat a preferált. Állatvilágra figyelemmel kell lenni. (Monokromatikus LED)	Forrás: LED, indukciós, fémhalogén, alacsony nyomású nátriumlámpa	Sötétedéskor bekapcsol. Automatikusan csökken 30%-kal a fényerő aktivitás megszűnése után 15 perccel. Hajnalban kikapcsol.
Katonai raktár		–	50 lux	≤ 20 : 1	Oszlopra szerelt javasolt a fényforrások csökkentése érdekében. De a falra szerelt változatok csökkentik a beruházási költségeket.	Forrás: LED, indukciós, fluoreszcens fémhalogén	Automatikus felkapcsolás sötétedéskor.

Terület/Feladat	Megvilágítás (*Ē*av)		Egyenletesség (U_0)	További követelmény	Szerelés	Vezérlés, működés
	Vertikális (*Ē*v)	Horizontális (*Ē*h)				
Védett nyílt területek	–	50 lux	≤ 15 : 1	Oszlopra szerelt javasolt a fényforrások csökkentése érdekében. De a falra szerelt változatok csökkentik a beruházási költségeket. Legyenek fény növelésére fényszórók felszerelve.	Forrás: LED, indukciós, fluoreszcens fém-halogén	Automatikus felkapcsolás sötétedéskor. Csak manuális le- és felkapcsolási lehetőség.

6. Összefoglalás

Rátekintettünk a munkahelyi beltéri és kültéri körletvilágítás széles körű területére, felvázoltuk a szakági, azaz az egyedi értelmezés szükségességének okait. Bemutattuk a modern világítás értelmezését és ennek megfelelően leírtuk az általunk javasolt követelményeket, amelyek figyelembe veszik a fenntarthatósági, energiahatékonysági, illetve fejlesztési és korszerűsítési irányokat. Ebben a részben szó esett a kontrollt és ellenőrzést gyakorló szervről és működési feltételeiről, hogy megértsük annak a keretrendszerét és a lehetséges javító folyamatokat, valamint az egységes szakági szabályozás szükségességét. A körletvilágítás több mint őrvilágítás. Fontosnak tartjuk egy útmutató készítését, amely eligazító a megrendelők és kivitelezők számára a katonai beruházásoknál, ezenfelül javasoljuk a szoftveres tervezéstámogatás vizsgálatát és a témában a költségelemzés-kutatás elvégzését. A következő részekben foglalkozunk a katonai világítás további, még nem tárgyalt alcsoportjaival.

Felhasznált irodalom

Jasztrab Péter János – Istók Róbert: Fény és világítás katonai aspektusai. In *XXXV. Jubileumi Kandó Konferencia.* Budapest, (é. n.) 138–149. Online: http://kttk.kvk.uni-obuda.hu/sites/default/files/csatolmany/xxxv-jubileumi-kando-konferencia-kiadvanya-v1.pdf

Jasztrab Péter János: Minimális látási követelmények vészhelyzetekben, avagy a biztonsági világítás. *Hadmérnök,* 10. (2015), 2. 5–21. Online: http://hadmernok.hu/152_01_jasztrabpj.pdf

Jasztrab Péter János – Gúth Gábor: A minimális látási követelmények és eszközeiknek katonai szemlélete II. rész. *Hadmérnök,* 10. (2015), 4. 5–15. Online: http://hadmernok.hu/154_01_jasztrabpj_gg.pdf

Jasztrab Péter János – Istók Róbert: A világítás katonai vonatkozásai: 1. rész: Navigálás a látási és láthatósági követelmények, világítási előírások katonai aspektusai között. *Hadmérnök,* 14 (2019), 4. 5–34. Online: https://doi.org/10.32567/hm.2019.4.1

Munar Suard, Lorenzo: *Munkahelyi veszélyek és ártalmak megelőzése a magánbiztonsági iparágban.* Európai képzési kézikönyv. Centre de Sociologie de la Santé, Université Libre de Bruxelles, 2004.

Rea, Mark Stanley (szerk.): *The IESNA Lighting Handbook.* 9th Edition, Illuminating Engineering Society of North America, 2000.
Steinbach, Rebecca – Chloe Perkins – Lisa Thompson – Shane Johnson – Ben Armstrong – Judith Green – Chris Grundy – Paul Wilkinson – Phil Edwards: The Effect of Reduced Street Lighting on Road Casualties and Crime in England and Wales: Controlled Interrupted Time Series Analysis. *Journal of Epidemiology & Community Health,* 69. (2015), 11. 1118–1124. Online: https://doi.org/10.1136/jech-2015-206012

Internetes források

US Army: *Army Installations 2025.* (2016. augusztus 11.). Online: https://api.army.mil/e2/c/downloads/454188.pdf
Miller, Susan: Army plans industry day for IoT and 'smart bases'. *Defense Systems,* 2019. március 8. Online: https://defensesystems.com/articles/2019/03/08/army-installations-of-the-future.aspx

Jogi források

3/2002. (II. 8.) SzCsM-EüM együttes rendelet A munkahelyek munkavédelmi követelményeinek minimális szintjéről
4/2002. (II. 20.) SzCsM-EüM együttes rendelet Az építési munkahelyeken és az építési folyamatok során megvalósítandó minimális munkavédelmi követelményekről

Szabványok

MSZ EN 1838:2000 szabvány Alkalmazott világítástechnika. Tartalékvilágítás
MSZ EN 12464-1:2012 Fény és világítás. Munkahelyi világítás. 1. rész: Belső téri munkahelyek
MSZ EN 12464-2:2014 Fény és világítás. Munkahelyi világítás. 2. rész: Szabadtéri munkahelyek
MSZ CEN/TR 13201-1:2015 Útvilágítás. 1. rész: Irányelvek a világítási osztályok kiválasztásához
MSZ EN 13201-2:2016 Útvilágítás. 2. rész: A világítási jellemzők követelményei
MSZ EN 13201-4:2016 Útvilágítás. 4. rész: A világítási jellemzők mérési módszerei
NFPA 101®. Life Safety Code®. 2021
UFC 3-530-01 Unified Facilities Criteria (UFC) Interior And Exterior Lighting Systems And Controls
UFC 4-020-01 Unified Facilities Criteria (UFC) DoD Security Engineering Facilities Planning Manual 11 September 2008
Joint IDA-IESNA Model Outdoor Lighting Ordinance (MLO) – User's Guide June 15, 2011
IES RP-22, 2011 Edition, February 12, 2011 - Tunnel Lighting

MSZ EN 60598-2-22:2015 Lámpatestek. 2–22. rész: Egyedi követelmények. Tartalékvilágítási lámpatestek (IEC 60598-2-22:2014)
MSZ ISO 16069:2009 Grafikai jelképek. Biztonsági jelek. Menekülési útirányt jelző rendszerek (SWGS-ek)
TvMI 2.3:2020.01.22., Kiürítés, 2019. december 4.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
16. évfolyam (2021) 3. szám 41–54.
DOI: 10.32567/hm.2021.3.3

Zoltán Antal[1]

Severe Accident Management Systems and Procedures

A nuclear power plant's safe operation involves the planning for non-standard operational emergencies, where pre-determined safety measures and damage control interventions must be taken into consideration depending on the developed event. The definition of the severe accident management cannot be explained in a single concept, it needs to be examined in detail. As a result of this it becomes necessary to specify the procedure guidelines appropriate to the nature of the event, which can be used with optimal efficiency under hierarchical organisational control. The experience of nuclear accidents in the world and the precognition of future events, the knowledge of existing guidelines for severe accident management needs to be deepened continuously, but at the same time it can be parallelly upgraded with the application of new technologies.

Keywords: **nuclear power plant, reactor, severe accident, extreme circumstances, safety basis**

1. Introduction

The safety policy of Nuclear Power Plants (NPP) fulfils the highest level of safety planning, with the development of protection systems and procedures that include mobile solutions in addition to multi-level redundant systems to minimise damage to human life, property and the environment, furthermore reduce the irreversible damage that has occurred. The Nuclear Emergency Response Organization (NERO) of NPPs has trained personnel and equipment capable of performing its task in all possible emergencies.

Following the serious accident at the Fukushima Dai-ichi NPP, the world's safety councils came to the conclusion that a targeted safety review is needed in the light of what has happened. The European Union Council has asked the European Nuclear Safety Regulators Group (ENSREG) and the European Commission to redefine the

[1] MVM Paksi Atomerőmű Zrt., Atomix Kft., Létesítményi Tűzoltóság, szerparancsnok; e-mail: antalzmax@gmail.com

contents and methods of comprehensive risk and safety procedures in the framework of the so-called 'stress test' for NPPs in the Union.[2]

2. The serious accident concepts

The state-dependent operator's procedure instructions of the NPP, which are important for system management, have been developed primarily to avoid zone damage. If these interventions are unsuccessful, the system instructions can no longer be effectively applied to actual or former zone damage accidents, as they do not include operations designed to maintain the integrity of the physical barriers in order to be able to fulfil their basic purpose of preventing the release of radioactive materials. As soon as significant fuel-cover damage and zone geometry loss occurs, maintaining a stable state of the hermetic space becomes a primary goal, thereby emissions can still be controlled. In light of this, in some major accident situations, preserving the safety of the hermetic space or preventing the escape of fission products may take precedence over zone cooling. In a case like this, it is necessary to perform the pre-designed operations specified for the incident, which are included in the Severe Accident Management (SAM) Guidelines. According to the provisions of the Nuclear Safety Standards (NSS), a serious accident is:

'An accident condition with significant damage to the reactor zone, associated with zone melting, with more severe external effects than design- and post-design basis failures.'[3]

In case of well-planned and detailed nuclear facilities built on the basis of safety experience, major accidents are most likely to be caused by events for which sufficient information was not available at the time of design. In these special cases, faulty processes lead to an event that the NPP's security systems cannot deal with and can lead to a possible zone melting.[4]

3. Managing severe accidents

The management of serious accidents is a complex, special task the management and objective implementation of which is performed by a predetermined structural organisation temporarily formed to deal with the situation. In the event of a major disruption, the organisation must be formed and operate according to the pre-defined operational management structure until the situation requires the application of the

[2] National Report, *Targeted safety review of the Paks Nulcear Power Plant* (Budapest: National Atomic Energy Agency, 2011), 6–7.

[3] 118/2011. (VII. 11.) Korm. rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről [Government Decree 118/2011 (VII.11.) on the nuclear safety requirements of nuclear facilities and on related regulatory activities], Appendix 10, Nuclear Safety Regulation Definitions, 145.

[4] Severe Accident Management Guidelines, *Atomerőművi reaktor és primerköri rendszerek operátori üzemeltetése* [Operation of nuclear power plant reactors and primary circuit systems] (MVM Paksi Atomerőmű Zrt, Verzió-szám: 2.0, 2013), 5; International Atomic Energy Agency, *Severe Accident Management.*

SAM Guidelines or a stable operating condition is established. If necessary, the managing organisation coordinates the work from a protected base of operations, from which it has a continuous view on the status of the events and the performed tasks. The mission of the management organisation and their sequence are an integrated part of the SAM guidelines, which are implementation instructions fitted in a specific hierarchical regulatory system.

The performance of the SAM assignment is based on the development of situation-specific procedures supported by preliminary survey and praxis to prove that if the organisation in charge performs the tasks according to the SAM guidelines, it will result in an appropriate outcome. This also includes the need to keep any mobile device listed in the regulations with proper maintenance ready for operation. There is a need to build up a sufficient quantity and quality of backup of the existing equipment, such as measuring instruments, communication and IT equipment. In addition, an increased number of participants in the intervention must be ensured.

A consequence of serious accident treatment is that besides properly informing the plant's operational personnel, it is also a basic requirement to inform the surrounding population. The safety of people, who must be evacuated or are confined within the operating area has to be guaranteed, regardless of how many units of the plant are involved in the emergency. According to the SAM guidelines, the evacuation should be finished even before the harmful release.

Important aspects of severe accident management measures in the event of zone cooling function loss:[5]

- Function loss assessment to initiate a prioritised action
  - external cooling of the reactor vessel by flooding the reactor shaft
  - feedback of severe accident management measurement systems
  - commissioning of the unique diesel generators for the operation of the SAM equipment
  - severe accident hydrogen treatment with passive autocatalytic recombiners
  - prevention of cooling water loss due to spent fuel pool pipe breakage
- Probability of fuel damage inside the tank and measures to deal with it
- Injury assessment after reactor damage and prevention of base-plate melting
- Maintain containment integrity, developed pressure and hydrogen treatment
- SAM differences and additional tasks on parallel blocks
- Prevention of radioactive releases after containment integrity loss or drying out of fuel stored in the spent fuel pool[6]

[5] Atomerőmű Tűzoltóság, *Primary circuit knowledge*. ATOMIX Kft., Tűzoltási és Kárelhárítási Szakágazat, Szakmai Ismeretek Oktatási anyag, ATOMIX at-me-6.2.2.-1-v2, 2013.

[6] National Report, *Targeted safety review,* 87–103; MVM Paksi Atomerőmű Zrt., *Átfogó Veszélyhelyzet-kezelési és Intézkedési Terv.* I. modul: Általános kötet [Comprehensive Emergency Management and Action Plan. Modul I: General Volume], Verziószám: 9.3, 2016, 28.

4. Sources of danger at an NPP site

In the aspect of NPPs, it cannot be said that the entire establishment is a source of nuclear danger, but it has systems and system-components that are sources of radioactive material and so they require high safety measures. In the following list, there are the main nuclear hazards of NPPs, the safety of which requires the presence of an accurate design criterion.

- Reactors: escape prevention of fissures from the reactor during heat dissipation of radioactive decay
- Spent fuel pool: cooling of stored irradiated fuels and monitoring of fuel hermeticity
- Systems that contain radioactive material: auxiliary and radioactive waste management systems located outside the hermetic space which are required for the main operation
- Spent fuel transport within the site of an NPP: irradiated fuel element transport between blocks or to the Spent Fuel Temporary Storage Facility – safety of material handling and transport route during transportation
- Hazardous radiation sources: the utilisation and storing of instruments using radiating cells applied in technological processes
- Hazardous substances that can cause a major accident: the quantity and properties of hazardous materials used for the technology in the NPP and the application of the rules both for the safe storage and handling of the materials[7]

5. Prevention and accident management

Accident management aims to prevent damage and core melting by all possible methods which can reduce even the occurrence of major accidents beyond planning. The relationships between preventive and consequence mitigation measures can be summarised in the table below.

Table 1

Accident management

Source: Severe Accident Management Guidelines, 6.

Event	**Within design basis**	**Beyond design basis**	
Goal	Zone-melting prohibition, activity retention in hermetic space		Reducing the consequences of zone-melting
Systems	Application of operational and safety systems within design limits	Usage of all available systems within their design performance values	
Form of accident management	Prevention		Consequence reduction
Instruction/ manual	Optimal recovery instructions	Function restoration instructions	Severe accident manuals

[7] MVM Paksi Atomerőmű Zrt., *Átfogó Veszélyhelyzet-kezelési és Intézkedési Terv*. I. modul: Általános kötet [Comprehensive Emergency Management and Action Plan. Modul I: General Volume], Verziószám: 9.3, 2016, 14.

During accident management, the prevention and consequence-reducing requirements are separated depending on how far the design bases extend; however, severe accident management also has operational parts that can be found in one of the prevention-related operating instructions. It can also be seen that some incident management is possible beyond the design basis according to the guidelines until the situation reaches significant damage or zone melting, from which point the tasks, which are specially designed to reduce and deal with consequences of the serious accident, are required.

Primary consequence reduction to be implemented during severe accident management:

- Restoring a controlled and stable Zone
- Restoring and maintaining a controlled and stable Hermetic space
- Avoid damage to the reactor vessel at high pressure
- Reduction or elimination of radioactive release

Operating manual procedures assume that zone damage can be prevented by performing the tasks contained in it, and therefore includes recurring task sets for zone damages that cannot be fully performed until the zone is restored or stabilised. Consequently, the forecasts of the expected effectiveness of interventions will no longer be applicable. Operator instructions focus tightly on avoiding zone damage by performing operations that are also able to prevent fission material escaping from the hermetic space. At the same time, for each task in the instructions, the risk of the event must be recognised, so the possibility of zone damage must be assessed depending on the effectiveness of the preventive tasks already performed. It should be noted that by using the tasks of the manuals, zone damage can be successfully prevented in the majority of the analysed cases. In recognition of predictable failure of the preventive measures, the change to the SAM procedures should begin in parallel with the suspension of the tasks set out in the prevention manual. After that, it is no longer possible to return to the procedures of the operational treatment assignments, as the SAM guidelines are implemented as fully self-contained, separate complex units, covering all areas needed to prevent an accident and stabilise the zone.[8]

6. Severe accident management manuals

The complex accident management procedures for critical damage and zone-melting are containing guidelines unlike the mandatory actions of the sorted preventive procedures. That is the reason why during the specific steps of the manual, the entire accident management process must be interpreted and analysed and, depending on its current state, a decision must be made to implement the steps of the comprehensive processes to properly manage the accident situation. During the processes, the primary importance is to preserve the integrity of the hermetic space and prevent the escape of fission products, even against the implementation of zone cooling, because

[8] Severe Accident Management Guidelines, 6–7.

at this point the condition of the blocks is beyond the original safety levels that are included in the design bases. The SAM Guidelines are built of several separate sections that include parallel procedures and enforcement steps for each involved technician crew. To justify and support decisions, it is necessary to track them continuously, for which the so-called Diagnostic Flowchart of the systems and the event-formed Accident Status Tree can provide the necessary supporting information. These are accompanied by the instructions for the professional crew that is involved in the accident management. A support centre with professional staff should be set up to analyse the data and make the decisions. In the diagnostic flowchart, all the aspects of the serious accident must be taken into account that endanger the integrity of the physical barriers and the prevention of the release of radioactive materials.

Diagnostic flowchart parameters:

- Reactor condition and primary circuit pressure
- Hermetic space water supply and flooding parameters of the reactor shaft based on the water level
- Supply to the main water circuit system based on zone temperature
- Radioactive release reducing procedures
- Steam generator supply based on water level and inner pressure
- Condition control of the hermetic space depending on its pressure
- Hydrogen reduction inside the annulus
- Level and stability of the spent fuel pool

Based on the results of the performed implementations of the parameters, the increase or decrease of the zone stability can be determined. The condition assessment includes the actual water levels, pressures, radiation levels and information about the open state of the reactor. The results of the flowchart can be used to determine whether there is a major, direct danger parameter that can be classified into the Severe Accident Status Tree model and inheres the need to implement guidelines for the immediate emergency. According to this, the reduction of radioactive material release, decreasing pressure in hermetic space, evaluation of hydrogen control (autocatalytic hydrogen burning via recombiners) and the related appropriate procedures are performed. The Diagnostic Flowchart and Severe Accident Status Tree assessment should be monitored and evaluated in parallel, prioritising the necessary implementation of the status tree guidelines either to achieve or to maintain a stable state.[9]

7. Severe accident management systems

7.1. Accident situations related to the cooling water

To run the technology by the operating nuclear units, the feed-water system implements continuous refrigerant supply. In the case of a malfunction of the service

[9] Severe Accident Management Guidelines, 9–16; Atomerőmű Tűzoltóság, *Primary circuit knowledge*.

feed-water system, its role is taken over by the emergency water-supply system. Their power supply is provided by diesel generators even by the loss of normal power supply. In accordance with the multi-level protection design used in the NPP, the feed-water system was built from such a safety point of view that it was designed for the possible failure of the supply and emergency feed-water system. Therefore, in accordance with the parameters of the emergency water-supply system, an additional emergency water-supply system has been built to ensure the feed of water to the steam generators.

7.2. Reactor shaft flooding

Due the technical design, it is possible to cool the reactor vessel externally so that the melted material is kept inside the tank preserving the structural integrity of the reactor vessel, thereby preventing the reaction of the concrete and the corium. The system provides an adequate amount of water for the hermetic space and the reactor's concrete shaft where it maintains sufficient cooling for the reactor vessel's external surface. In this case, by the conservative assumption the Zone emergency cooling systems are also out of order.

7.3. Combustion of hydrogen accumulated in the hermetic space

According to the analysed processes, during the zone melting, a significant amount of hydrogen is evolved from the reaction of the concrete and the corium, which threatens with an explosion, endangering the hermetic space integrity. To ward this off, passive hydrogen recombiners have been installed to provide catalytic combustion of hydrogen accumulated in the hermetic space.

7.4. Spent fuel pool water depleting and preventing the failure cooling circuit

A special procedure elaboration has become necessary to prevent an accident of the spent fuel pool's cooling failure and due to the damage of the used fuel rods. It has been identified that the damage of the non-excluded parts of the spent fuel pool's pipelines can result a loss in the refrigerant, which can lead to a spent fuel injury without the adequate alternate cooling water.

7.5. External refrigeration supply

The nuclear power plant's heat absorption safety function maintenance systems were designed to monitor and prevent the cessation of heat dissipation. During the external refrigerant supply, alternative water sources are exploited, from which the

amount of cooling water can be provided by mobile devices through the constructional connection points to the steam generators.

The management of an extraordinary event is based on the fact that the power plant's safety heat absorbing systems cannot provide heat dissipation, so an alternative supply is required. That is implemented through a connection point on the pre-determined supply line to achieve long-term heat dissipation indirectly through the steam generators.

For the supply of external refrigerant, it is important to determine the primary water extraction point, because it must be selected depending on which installation's connection point the equipment is connected to and operated by. Relevant aspects of consideration are distance, accessibility, water quality and quantity. The experts of the response team need to have exact information within critical time to begin the preparation of the feed and the building of the mobile supply system on the pre-determined route. The dismantling of the pumps and the hose system takes time, and by an event of a factual nuclear emergency, relocating it to another water source would take much longer than the first installation of the system.

7.6. Power supply accident situations

7.6.1. Assumed electrical failures in a severe accident situation

- Complete voltage loss
- Power sources for emergency power-supply systems become inoperable (both diesel generators and battery packs)
- Lack of external electrical network supply

7.6.2. Independent power supply

Safety systems must have an alternative power source beyond the normal operating intake that can maintain the following systems:

- The electrical fittings for reactor shaft flooding
- Operation of the severe accidents' measurement systems
- Operation of the volume compensator safety and pressure relief valves to avoid zone melting
- Power intake of the Spent fuel pool's drain protection fittings

7.6.3. Elements of the SAM's independent power supply system

- Mobile diesel generator:
  - Power support: one mobile diesel aggregator applied to a trailer for each installation

  - Output: 96 kW
  - Maximum operational time: 40 hours (≈ 900 l fuel)
  - Connection to the electricity network: box constructed outdoor connection
  - Firefighters deliver the diesel aggregators to the chosen point
  - Operation and connectivity: performed by maintenance and electrician specialists
- Outdoor electrical connectors
- Network switch cabinets and the associated connecting cable network
- Uninterruptible power supply for the accident measurement system[10]

8. Extraordinary circumstances causing and affecting a serious accident

8.1. Earthquake

The installation of an NPP follows the industrial custom practice of the given age. During the technical design, the establishment sites were classified on the basis of the current seismological and geological characteristics of the last decades. With today's technological solutions, there are more options for site inspections and the recorded history also helps the qualification. As a result of the test, the expected value of the maximum free-surface horizontal and vertical acceleration force during a possible earthquake is determined, taking into account the vibration transmission of the loose sediment layer covering the surface. The analysis is supplemented by the examination of possible soil liquification, which is the permanent displacement on the surface. The creation of a geological-structural model contains geological, geomechanical, geophysical, tectonic, stratigraphic, hydrogeological, evolutionary and zone divided seismological studies. In case of some particular earthquakes, the tasks of plant operators must be regulated by special preventive emergency instructions. The nuclear power plant is able to withstand seismic activity that does not reach the level of the so-called safety earthquake, which means a level of the planned earthquake that does not exceed a tolerated amount by the units, without significant radioactive release. However, additional damage, fires and other failures may occur in unconfirmed parts or service areas. Indirect effects due to earthquakes may also occur, which do not directly cause the failure in system components that ensure nuclear safety, but it can happen, that other parts of the installation are damaged, which may affect the parts that perform effective safety functions. The possibility of additional refrigerant or electrical supply loss due to an earthquake should be considered by the SAM Guidelines and in every case there must be an alternative source of mobile intake that can guarantee nuclear safety.[11]

[10] Severe Accident Management Systems, *Operation of the primary circuit systems.* MVM Paksi Atomerőmű Zrt., Verziószám: 1.0, 2018.
[11] National Report, *Targeted safety review,* 34–52.

8.2. Flooding, external overflow

Flood protection is the process of the weather, where the properties of the water area and the factors influencing them can be considered parts of the whole, which can be broken down into protection levels. The flooding protective structures established on hazardous water sections are preventive interventions that are designed to be sufficient to protect the specific areas close to water. This is complemented by procedures that provide additional temporary defence walls and mobile response. The location, length and height of the defending structures, as well as their structural properties, are established depending on the water ditch, floodplain and water movements.

Flood protection does not end with the presence of defence. Continuous inspection and control is required depending on the actual level of flood protection. When the flooding water reaches a specified water level on the watercourse meter, flood protection preparedness takes effect, which lasts until this water height is reduced to a safe level and the restoration work of any damaged primary defensive structure is completed. In the event of a flood, rivers leave their riverbed, which can threaten with the inundation of potentially useful areas. Therefore, these useful areas must be artificially separated from the specified water areas and such special designs must be done that further interventions can be taken if necessary, to strengthen the defence. The primary defence-structures should be upgraded, if necessary, with procedures to be applied depending on the current situation. The availability of mobile resources and an adequate size of operational staff is essential to execute an effective defensive implementation. In addition to this, the field experts should take appropriate preventive action so that the defence walls do not weaken the existing primary or pre-built defensive constructions. Reducing the faster course of a flood, dividing it, reducing the amount of water that flows away, or applying a reduction in the area at risk of flooding are the ways in which flood management can intervene effectively. One of the methods based on the area reduction includes the application of protective embankments on the coastline at variable distances. The mobile equipment of the exemption requires the accumulation of adequate quantities and the regularisation of such transport vehicles that are suitable both for carrying and for use in the appropriate terrain.[12]

8.3. Extraordinary weather situations

Extreme weather conditions affecting nuclear safety under the NSS may be the following:

- Powerful wind blasts
- Extreme amount of rainfall

[12] National Report, *Targeted safety review,* 53–56; J Nagy, *Az árvízvédekezés folyamata, feladatai az MVM Paksi Atomerőmű üzemi területén* [The process and tasks of flood protection in the operating area of MVM Paks Nuclear Power Plant] (Oktatási jegyzet [Teaching material], 2019).

- Accumulated ice and snow barriers
- Lightning
- Extreme high/low temperature
- Drought

Drought, as an extremely persistent dryness, affects the NPP through a critical reduction in the primary refrigerant source. The design basis of an NPP shall include each category of event and its effects for nuclear safety and we have to calculate with them in terms of their frequency and magnitude. However, low frequency does not mean that the effects of a certain event can be ignored. In order to make a meaningful reference to design basis, it is necessary to have information about the local natural hazards together with vulnerability data, given effects relevant to load specifications and associated occurrence frequencies.

To define the occurrence and extent of extreme weather events, that are usually estimated by the internationally accepted Gumble approximation, mainly because extreme weather observation consists only of the data collection of limited duration, which results in a pattern loaded with uncertainties. Based on these 10,000 year-periodical-return time events, the values of the wind blasts, daily precipitation, snow thickness and extreme temperatures are determined.

The effect of the persistently low water level of the cooling water supply source must also be taken into account even if the NPP is operating with offline units during a drought period as the cooling water shortage or its extreme fluctuations cannot be tolerated permanently in any operating condition.

In case of lightning strikes, a different method should be used from other meteorological event models, because this phenomenon cannot be described by a single value. Therefore, lightning protection can be justified by compliance with the relevant standards in the design basis. Therefore, the lightning strikes are part of the design basis for safety-class buildings and outdoor technological equipment in an NPP, while the electromagnetic effects of lightning must be taken into account in accordance with the control equipment design basis.

Extreme wind-blows can have an impact on nuclear safety by a disruption of the outdoor power grid cables, and it is necessary to count with additional effects such as the mass of sand and dust stirred up by the wind, which can endanger electrical devices. To avoid this, critical system protection and safety system elements are protected against dust. In case of damage to any classified dust-protection, it is necessary to proceed in accordance with the relevant enforcement instructions.

The important system protection units including the power supply interiors are also air-conditioned. If the cooling of these rooms was left out, significantly high temperatures could develop. The magnetic-switches and circuit breakers in these rooms are able to fulfil their intended function for some time even at elevated temperature, and the battery packs are capable of upholding their discharge capacity. However, this status cannot be maintained for a long time without the failure of electrical systems. But you can prepare for the effects of the extreme high temperature with mobile controllers. Heating the functional areas, which are performing safety roles can also be planned to offset the effects of extreme low temperatures. Attention must be

paid to management measures to be implemented for the temperature protection of all critical systems.

For treatment of the effect of extreme quantity and duration rainfall, the design basis must count with an adequate quality and permeability of drainage, based on the site-specific increased rainfall efficiency model, including the identification and emergency measures for critical overflow areas.[13]

9. Losing electrical supply and final heat absorption

For the operation of the safety systems an NPP adequate cooling water is needed, which is provided by electrically powered pumps. So, the two types of security sources are closely connected to each other and the loss of any function of one of the systems cannot cause a loss of security operation on the other side. According to this, the cooling water sources and the transmitting electrical supply pumps can be ensured by establishing several redundant systems.

By the event of an electricity supply loss, it is an important aspect which category of the NPP's consumers must be supplied with electricity and for how long the primary reserves can maintain this. Depending on the power demand, if necessary, power supplies that can maintain electrical replacement properly for longer periods should also be put into operation. To operate alternative sources, planned safety criteria for earthquakes, floods and extraordinary weather must also be calculated with. In addition to the establishment of safety systems, mobile power supplies must be provided as part of the severe-accident prevention strategy so that additional alternative units can be used in the event of the safety power loss of the supply systems.

In case of final heat absorption loss, all heat removal systems from the reactor shall fail, which means that due to the failure and dropout of the redundant safety heat absorption function providing systems, the heat removal performance will be unsatisfactory. Examining the roles of the systems, their operational structure, performance, the resistance of technical barriers as a function depending on the elapsed time, their electrical supply implementation, fuel and lubricant limits, a well-established additional safety procedure is required to achieve the heat subtraction of the reactor in an alternative way as soon as possible. In an extreme case, such as the heat abstraction from the primary circuit and the containment cannot be ensured through the secondary circuit systems, the water supplied from the external source can also be injected into the hermetic space through the special feed-water side purge valves of the secondary circuit steam generator. Safety-critical cooling water and electrical systems include realisations that can independently provide the necessary replenishment on an alternative route without function loss. In addition to these, there are other mobile replenishments that can be found in the SAM guidelines.[14]

[13] National Report, *Targeted safety review,* 57–62.
[14] National Report, *Targeted safety review,* 63–86.

10. Summary

One of the most basic aspects of the efficiency and development in the SAM guideline is the comprehensive knowledge of preparedness and prior professional science. In addition to the technological and safety parameters of NPPs, an accurate knowledge of the existing equipment and the possibilities of intervention in the necessary situation can provide the basis on which nuclear safety can be built. This requires professionals who meet all the mentioned criteria. To meet this standard, the transfer of expertise is needed for the staff involved in remediation at any level. The flow of information in an emergency situation must have a real-time communication channel, the availability and content of which cannot be limited by any external or technical circumstance. This means, that the operating management team and the technological control systems must be in accordance with the current status of information and must use real time communication channels.

The personnel performing tasks under the authority of the organisation responsible for the Severe Accident Management of an NPP are obliged to meet the requirements not only in terms of their preparedness, but also in terms in their quantitative factor. Safety bases should also be designed for the occurrence of another serious accident developing in parallel or arising from an existing nuclear accident, since the resources deployed for one incident cannot discharge the global nuclear resources in such an extent that they cannot manage a corresponding event.

It can be seen that Severe Accident Management is a complex and elaborate task that requires careful planning to manage with it effectively. To this purpose, in addition to all possible hazards for NPPs and their emergency management, a bastion of protection must be provided, which besides the known dangers, has such an additional source that can be used at any time to strengthen the defence or even stand in their place completely instead of the original protection protocols.

References

National Report, *Targeted safety review of the Paks Nulcear Power Plant.* Budapest: National Atomic Energy Agency, 2011.

Severe Accident Management Guidelines, *Atomerőművi reaktor és primerköri rendszerek operátori üzemeltetése* [Operation of nuclear power plant reactors and primary circuit systems]. MVM Paksi Atomerőmű Zrt., Verziószám: 2.0, 2013.

MVM Paksi Atomerőmű Zrt., *Átfogó Veszélyhelyzet-kezelési és Intézkedési Terv*. I. modul: Általános kötet [Comprehensive Emergency Management and Action Plan. Modul I: General Volume], Verziószám: 9.3, 2016.

Nagy, J, *Az árvízvédekezés folyamata, feladatai az MVM Paksi Atomerőmű üzemi területén* [The process and tasks of flood protection in the operating area of MVM Paks Nuclear Power Plant]. Oktatási jegyzet [Teaching material], 2019.

Atomerőmű Tűzoltóság, *Primary circuit knowledge.* ATOMIX Kft., Tűzoltási és Károlhárítási Szakágazat, Szakmai Ismeretek Oktatási anyag, ATOMIX at-me-6.2.2.-1-v2, 2013.

Severe Accident Management Systems, *Operation of the primary circuit systems.* MVM Paksi Atomerőmű Zrt., Verziószám: 1.0, 2018.
International Atomic Energy Agency, *Severe Accident Management Programmes for Nuclear Power Plants.* Safety Standards Series No. NS-G-2.15, IAEA, Austria, 2009.

Legal source

118/2011. (VII. 11.) Korm. rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről [Government Decree 118/2011 (VII.11.) on the nuclear safety requirements of nuclear facilities and on related regulatory activities].

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
16. évfolyam (2021) 3. szám 55–79.
DOI: 10.32567/hm.2021.3.4

Antal Papp[1]

The Place and Role of HAZMAT Units with Respect to Increasing Public Safety in Hungary

The basis of public safety is dependent on the assessment of risk of potential disasters. Furthermore, the term involves protecting and safeguarding people from disasters and other potential dangers or threats. The increasing importance of a nation's preparedness is becoming more obvious in case of disasters, in order to protect the health and safety of citizens, properties, material assets, industrial facilities and the environment. This paper offers an outline review of hazardous materials related emergency response units' (HAZMAT Units) role in the fields of prevention, control, communication, identification of hazard impacts, decontamination and recovery activities.

Keywords: **public safety, disaster, crisis management, dangerous substances, equipment, training of intervention units**

1. A brief overview of the Hungarian and international systems of hazardous material safety

Major accidents are becoming more frequent with the development of industry, consequently affecting our environment or, more broadly, the earth's biosphere, which includes humanity.

Nowadays, it is an observable and growing phenomenon that natural disasters and further circumstances in the same manner with global climate change are causing more and more industrial disasters and vice versa. Recognising these problems for decades, developed industrial countries have created a system of special devices, mobile laboratories, which are able to detect, indicate, evaluate these phenomena and designate the danger zone.

In Hungary, disaster management authorities have been involved in the official control of the transport of dangerous goods by road (ADR) since 2001, according to the amendment of Government Decree No. 122/1989 (XII.5.). Accidents occurring

[1] PhD, Director, Professor, Disaster Management Training Centre, Hungary, e-mail: antal.papp@katved.gov.hu

during the transport of dangerous goods (be it ADR, ADN, RID, and so on) are investigated by the HAZMAT Units.[2]

The purpose of this short article is to present the possibilities that characterise the world of HAZMAT Units in order to determine how well they cope in today's world. Therefore, I primarily present the tools and forces currently operating in the world, then I present the Hungarian possibilities by highlighting one or two features, for instance training technique, instrumentation and field practice.

However, it is important to note that the factual, accurate description is also justified by the fact that this document is intended to represent the current state in 2021. In several years, decades, there will be a basis of comparison in which we will be able to determine how far we have reached and where we have come from.

Therefore, I dedicate the research method to describe, compare and evaluate the existing foreign literature, manuals, descriptions, as well as the experience gained during the domestic operation in order to suggest directions for possible further developments.

1.1. Main sources of disasters in Hungary

Similarly to most European countries, there are two main sources of disasters in Hungary. One of these is flood, which has been proved to be predictable due to monitoring the indicative factors. Another outstandingly significant cause of harm happens to be related to the transport of dangerous goods, which definitely seems to be less foreseen. The development of science and industry has created the opportunity of new sources of danger. Producing of hazardous chemicals has never faced similar heights before. This actively demonstrates the simultaneously increasing result in the volume of road transport of hazardous substances, contributing to the boost in the chances of accidents. Besides, a notable indicator of contemporary society is that industrial and natural disasters can occur simultaneously with social dissatisfaction, mass riots, arson and violent activities. Therefore, the importance of CBRN preparedness is undeniable and the participation of HAZMAT Units is essential.

1.2. International overview – Europe

In the event of an accident, not only the population, the environment, but also the interveners are at particular risk (poisoning, acid corrosion, and so on). As normal protective gear does not protect against all hazardous materials, special protective clothing is required. Primarily, larger fire departments can afford acquiring and maintaining these special equipment.

[2] Act No. CXXVIII of 2011 concerning disaster management and amending certain related acts.

1.2.1. Germany

In Germany, transport of dangerous goods is regulated by act. In case of hazardous material related accidents, the Gemeinsames Melde- und Lagezentrum coordinates nationwide as an intervention centre. The interveners use the ERI-Cards[3] and the TUIS system for collecting information. Fire brigades,[4] TUIS firefighters, environmental authorities, the Technische Hilfswerk and the Disaster Management units are capable of providing intervention, varying from province to province. The CBRN reconnaissance car used by the Fire Department's Analytische Task Force may seem to be similar to Hungary's HAZMAT Units. The tasks of the CBRN reconnaissance car involve detection of radiological and chemical radiation, the identification of hazardous and tactical materials, the measurement of radioactive contamination, the demarcation of the contaminated area, support of disaster management and sampling (air, soil, vegetation, water). The devices can also measure while driving at a maximum speed of 20 km/hour, furthermore, they can be removed from the vehicle and installed at a particular location. Devices are constantly updated, equipped with the latest software, they are adapted to the latest trends in radiation measurement, and the sampling procedure is also renewed regularly. Civil Defence provides tools for fire departments, as well as manages the training of personnel. The crew does not hold field practice, they prepare by simulation.[5]

1.2.2. Cyprus

The Cyprus Fire Service does not have a special vehicle used only for hazardous detection purposes. Each District area has its own fully equipped hazardous substances vehicle, capable of managing any incident involving leakage of hazardous materials. The storage, inspection and control of any hazardous materials are in the duties of the competent and relevant departments of the state such as the Labour and Inspection Department, local authorities and the appropriate department of the Ministry of Energy Commerce and Industry, and the Environmental Department. The personnel working in the field and all the relevant departments corporate and coordinate jointly in such cases within the framework of their duties.

1.2.3. The Netherlands

In the Netherlands, the responsibilities regarding hazardous materials are divided between different organisations. Safety regions are responsible for the mitigation of CBRN incidents. For nuclear incidents there is a special law, and one of the safety regions is in charge of procedures, regulations, inspection and organisation of expertise. Fire service is not in

[3] *Eri-Cards – Ausgabe 2008: Emergency Response Intervention Cards* (1st German Edition, Kohlhammer, 2008).
[4] Ulrich Kortt, Rolf Schmid, Hermann Schröder and Walter Hamilton, *Hamilton. Handbuch für den Feuerwehrmann* (Boorberg, 2003).
[5] Oliver Meisenberg and Stefan Sellmeier, *ABC-Einsatz: Realistische Übungen mit der "Erkunder-Simulation"* (BRANDSchutz, 2013), 957–959.

charge when a nuclear incident should occur. Apart from that, the military has special experts and equipment. In case of a CBRN related terrorist attack, forces take over with the assistance of the fire service. Each station (950) is equipped with explosion sensors, sensors for radioactivity and CO_2. The regional expert has the same gear as we have in Hungary, but also all kinds of indicator tubes and sensor cells, and more sophisticated sensors like IR detection equipment, and also more sophisticated sensors for radioactivity. There are also reconnaissance teams all over the country, composed of firefighters, who have a box of indicator tubes and they are commanded to the field to make measurements. The regional expert receives special education with a chemical background. The coordinator has a special education to calculate and predict the spread of hazardous materials and to coordinate measurements. Reconnaissance and HAZMAT teams are educated at regional educational offices by instructors who are educated by IFV.

1.2.4. Ireland

Fire services in Ireland carry detection equipment on emergency vehicles, as well as a range of rescue equipment.[6] Response to hazardous materials incidents is led by fire services, with support from ambulance, police and other local authority services, such as environmental protection. For large-scale incidents at industrial installations which attract the requirements of the Seveso Directive, the response includes activation of on-site emergency plans by the operator of the installation, along with off-site emergency plans of the principal response agencies (police, health service and local authority including fire service). This response provides for mobilisation of the necessary resources, and co-ordination between the principal response agencies and the operator of the installation. There are 27 fire services providing training for their firefighters.[7] Training for officers is provided centrally by the National Directorate for Fire and Emergency Management.[8]

1.2.5. Turkey

The institution affiliated to the Ministry of Internal Affairs, namely AFAD, is responsible for coordinating the events from the chemical, biological, radiological and nuclear materials that occur within the country. The first diagnosis and detection is made by AFAD teams. They have a vehicle equipped with various measuring devices to detect CBRN agents scattered around as a result of any industrial accident. In addition, people affected by the CBRN agent in the incident area are also referred to hospitals being decontaminated by AFAD teams. Theoretical training related to CBRN issues are given to the personnel on a regular basis and applied field exercises are carried out.[9]

6 'CBRNe World Convergence – All Hazards Response 2013', Dublin, Department of Defence, 16 April 2013.
7 'Training and development in the Reserve Defence Forces', Defence Forces Ireland, 2016; 'Annual Report of An Garda Síochána 2009', An Garda Síochána.
8 Darren Boyle, 'Gardai get 'dirty bomb' protection', *The Mirror,* 29 March 2007.
9 L Malerova, K Chmelikova and M Zajic, 'The Safety Situation within the Context of Simulations of Crisis Management Processes', *Wit Transactions on the Built Environment* 150 (2015), 209–218.

1.3. International overview – USA

The official website of the Federal Emergency Management Agency provides guidance on hazardous materials for primary interveners, which contains a basic knowledge of HAZMAT events in the United States.[10] The HAZMAT Response Team, as defined in the Hazardous Materials Response Special Teams Capabilities and Contact Handbook is 'an organized group of individuals who are trained and equipped to perform work to control actual or potential leaks, spills, discharges or releases of hazardous materials, requiring possible close approach to the material. The team/equipment may include external or contracted resources'.[11] The teams are subdivided into three categories. HAZMAT teams must meet all of the minimum criteria to qualify for Type I, II, or III. In terms of differences, Type I equipment for field measurement to test for known chemicals, unknown chemicals, known or suspected weapons of mass destruction, chemical/biological agents, and to ensure their decontamination. Type I and II are equipped with measurement tools suitable for known and unknown chemicals, while Type III HAZMAT unit is only for testing known materials as well as ensuring the removal of contaminants. In case of radiation measurement, the first two types of units are suitable for Alpha, Beta, Gamma detection and the third type is suitable for Beta, Gamma detection; while Type I has 7 personnel, the others have 5 personnel. The primary goal of the Type I team is to respond to a large-scale, complex and long-lasting event that involves multiple hazards and/or contains unknown chemical/biological hazardous substances. Deployment time should be within four hours. Type II is a hazardous materials response team that requires sustained effort in the event of a known and unknown hazardous materials incident. Deployment time is two hours. Type III response teams can be deployed in case of specific/known hazardous substances within one hour. The list of standardised equipment prepared by FEMA (AEL 19) is available on the official website. The AEL illustrates the types of equipment approved in FEMA's preparedness programs, and consists of 21 equipment categories, which are divided into further subcategories and individual equipment items.

1.3.1. International overview – Russia

In Russia, the Ministry of the Russian Federation for Civil Defence, Emergencies and Elimination of the Consequences of Natural Disasters is responsible for coordinating disaster related activities and emergency management. Also known as EMERCOM of Russia, involving six regional territories, like the Volga–Ural Regional Center, the Siberian Regional Center, the Central Regional Center, the Northwestern Regional Center, the Southern Regional Center and the Far Eastern Regional Center. Furthermore, it includes the subdivision of several departments, such as the Department for Protection of the Population and Territories; the Department for Disaster Prevention; the Department

[10] United States Fire Administration, *Hazardous Materials Guide for First Responders* (Emmitsburg: USFA, 1999).
[11] *Hazardous Materials Response Special Teams Capabilities and Contact Handbook* (Washington, D.C.: U.S. Coast Guard, 2003).

of Forces; the Department for International Cooperation; the Department for the Elimination of Consequences of Radiological and other Disasters; the Department for Science and Technology; and the Management Department.[12] Although, there is not a large amount of data available in English language on the Russian critical infrastructure policy,[13] the fact is known that technological disasters are accountable for the death of more than 1,000 people on a yearly basis, and further affecting numerous others,[14] as the list providing data on emergencies used to be available on the official EMERCOM website until 2017.[15] Hazardous materials related transport accidents, emissions, explosions and fires, plant accidents pose the highest percentages of threats. Classification of HAZMAT differs from the method used in the EU, mainly regarding the current lack of environmental hazards regulation in Russia.[16]

This brief international overview underlines the fact that industrial development is accompanied by the occurrence of major accidents. The reduction and prevention of emergencies have become important factors regarding the population and environment in all European and other developed countries. The mobile laboratories of HAZMAT Units are becoming more and more differentiated, with chemical, atomic, biological and water quality units specialising in certain cases. In Hungary, all ranges of tools are adapted into one unit, consequently narrowing the measurement capacities, boundaries and possibilities of devices.

2. Skills and duties of HAZMAT Units

The systematisation is based on the need of having a primary deployable unit at territorial level, which is able to identify hazardous substances released into the environment in case of an accident or disaster. A unit which is able to monitor the changing situation by providing continuous measurements and their analysis; present data and proposals to protect the health and safety of individuals. Furthermore, is able to reduce the impact of incidents by means of active responses. If necessary, in case of complex events, the response team is able to cooperate with other emergency response organisations, as Police, Ambulance Service, Environmental Protection or Water Management Authority, to manage and support emergency response duties through mutual cooperation.[17] There are currently 22 equipped units operating in Hungary. One for each county, one for the capital and one for the Liszt Ferenc International Airport. In addition to these, the Disaster Management Training Centre also has one

[12] John Pike, *Military,* s. a.
[13] Roger Roffey, Russia's EMERCOM: Managing Emergencies and Political Credibility (Swedish Defence Research Agency [FOI], 2016).
[14] Christer Pursiainen, 'Russia's Critical Infrastructure Policy: What do we Know About it?', *European Journal for Security Research* 6 (2021), 21–38.
[15] Antonia Reihlen, Juhan Ruut, Philipp Engewald, Heidrun Fammler and Elvira Moukhametshina, *The Russian system of chemicals management* (Baltic Environmental Forum Group, June 2010).
[16] Elena Petrova, 'Natural Hazards and Technological Risk in Russia: The Relation Assessment', *Natural Hazards and Earth System Sciences* 5, no 4 (2005), 459–464.
[17] Katasztrófavédelmi Mobil labor (KML), s. a.

unit for their own special tasks in aspects of vocational training. In the capital and in Borsod County, the vehicles possess a full set of superstructure and supplies. There are two types of vehicles[18] adapted in Hungary, as depicted in the following pictures.

Picture 1
Fully equipped HAZMAT vehicle
Source: Molnár, Fully equipped HAZMAT vehicle.

2.1. Primary duties

Just as public safety is a complex, multi-layered activity, the duties of the team are diverse. Their basic priority is related to emergency response activities: the cleanup of hazardous substances released into the environment in the event of an incident; the protection of the operational personnel, the population and material assets in the case of natural and civilisational disasters. This includes detection, data collection and measurement-evaluation tasks, in addition to risk assessment with reference to the vulnerability of the intervention team, the population and material assets. Furthermore, making proposals to assist the commander in decision-making and in the field of public protection measures. The unit can also participate in warning the population, even in case of a necessary evacuation. It performs planning and organising activities, contributes to the implementation of discharge duties, cooperates with the interveners of the emergency, provides professional assistance to cooperating agencies, contributes to vulnerability assessment and provides data for the Defence Committee. In case of an incident, it maintains contact and co-operates with other organisations dealing with emergency detection, damage prevention and environmental protection.

[18] KEHOP-1.0.6-15-2016-00008 SEQ ID project, "Advanced industrial safety interventions and capacity development" HAZMAT Unit vehicle procurement.

Picture 2
Fully equipped HAZMAT vehicle
Source: Molnár, Fully equipped HAZMAT vehicle.

2.2. Secondary duties

From time to time, the unit plays a crucial role in ensuring the protection of delegations and major sport events in the aspects of public safety. When there is no alert, it also performs official duties according to a defined plan; participates in the control of hazardous material transportation including on-site checkups; as well as investigates accidents and incidents related to the transport of hazardous materials in order to stabilise public safety in a broader sense. Additionally, it also carries out periodic official supervision of hazardous plants, reviews and certifies the practices of internal protection plans; investigates the circumstances of accidents and breakdowns in factories.

The development of HAZMAT Units in Hungary was largely determined by what is called public safety in a broader sense. A significant part of this new task is provided by the compliance with the new expectations, which are intended for the security and the economy of the population.

3. HAZMAT equipment

The equipment of currently operating teams can be grouped in various categories, such as chemical detection devices; biological detection devices, radiation measuring

devices; water analysis devices; personal protective gear; meteorological detection devices; sampling devices; first aid kit; rescue gear, electrical and lighting tools; info-communication tools; ADR equipment for transporting hazardous goods and others. The abbreviation 'ADR' refers to the European Agreement concerning the International Carriage of Dangerous Goods by Road. The reason behind the necessity of biological detection tools can be attributed to the anthrax panic in Hungary, causing serious financial losses and the fact what terrorists are preparing for at present still remains unforeseen. Special tools of chemical detection: hand-held spectrometers, action detection tubes, MHA detection tubes and motor pump, universal indicator (pH) papers, digital pH meter.

3.1. Grouping

These tools and devices can be grouped according to the state of the hazardous substance or the perceived unknown substance.

3.1.1. Gas measuring equipment

Certainly, measurement monitoring with gas detectors is almost without exception one of the basic tasks, as the level of individual protection and safety depends on the oxygen and carbon dioxide content of the air, the presence of explosive gas vapours, possible dangerous gases and vapours. There are several options available for analysing gaseous samples. One possible option would be the determination with a set of detection tubes, mainly for qualitative determination, but under appropriate conditions for quantitative, as well. The gas sample to be analysed is passed through the detection tubes by means of a motorised gas pump. The detectable gases can be divided into several groups, these are separated according to test sets. Detectable gases include inorganic gases: acid gases (hydrochloric acid), hydrogen cyanide, carbon monoxide, alkaline gases (ammonia), nitrous gas (nitrogen dioxide), sulfur dioxide, chlorine, hydrogen sulfide, phosphine, phosgene, organic gases, ketones (acetone), aromatics (toluene), alcohols (methanol), aliphatics, chlorinated hydrocarbons (perchlorethylene) and toxic warfare agents: thioether/sulfur mustard, hydrogen cyanide, arsenic hydrogen and organic arsenic compounds, organic nitrogen compounds, chloro cyanide, thioether, phosphoric acid esters, and so on. Gas measuring equipment also includes a gas detector, containing various sensors for measuring explosive gas mixture, oxygen content, carbon monoxide, carbon dioxide, methane, hydrogen sulfide, ammonia, chlorine, hydrogen cyanide and phosphine.

3.1.2. Solid or liquid substances

Nearly 12 to 13,000 compounds can be identified with tools capable of detecting unknown substances in solid or liquid form. Each measurement can be performed in

a few minutes, making them suitable for fingerprint-like, non-destructive analysis of compounds or mixtures. In connection with chemical detection, a portable GC-MS has also been installed at two different locations to implement analysis of gaseous, liquid or solid samples after the appropriate sample preparation. This extremely sensitive tool has been developed specifically for field usage; however, it requires special professional qualities, for which the operator is specially trained. The device can be used for detection or analysis, although it would be suitable for quantitative analysis as well, but mostly applied for qualitative analysis, for the particular reason that quantitative analysis also demands special competence and in the case of most interventions this type of analysis is not required.

3.1.3. Biohazard detection

A biohazard detection device has been installed for biological detection on the mobile laboratory vehicles, providing the sampling for 8 infectious agents. With this rapid test, a liquid or solid sample can be detected in a relatively short time frame of 10–15 minutes. Agents that can be uncovered by the series of tests: anthrax, ricin, botulism, staphylococcus, plague, tularemia, filoviruses (ebola), smallpox, Q fever, salmonella, dysentery, coli, alphaviruses. Water analysis tools include items for sampling and sample preparation, as well as the digital pH meter and the spectrophotometer with a series of measurements tests (free chlorine, ozone, chloride ions, nitrite ions, nitrate, cyanide ions, sulfate ions, iron, manganese, ammonia, phenol, water hardness) and a measuring tool for determining the dissolved oxygen content and measuring conductivity.

3.2. Meteorological reconnaissance gear

Systematic meteorological reconnaissance devices and instruments are an integral part of the Environmental Monitoring Station. The mobilisable micrometeorological measuring system is suitable for scanning wind speed, wind direction, temperature at 2 points to determine the vertical stability of the air, relative humidity, air pressure, plus it is able to measure radioactive radiation along with a gas detection part for monitoring 12 different gases, and further applicable for modelling and propagation calculations. The data scanned by the measuring device installed on the on-board computer is managed and evaluated by a software developed for this particular purpose. Certainly, an alarm system also belongs to the unit, providing signs when the gas detector or the radiation measuring apparatus reaches a specified value. The surveying unit is suitable for field installation, either set on the vehicle or attached to a separate stand, besides being able to on-the-go monitoring and executing scanning procedures while the vehicle is on the move at reduced speed. The meteorological reconnaissance gear contains an additional item, a hand-held meteorological appliance to define wind speed, wind direction, relative humidity, air pressure values.

3.3. Additional tools

The fully equipped hazardous material response unit vehicle contains the following accessories: mobile and handheld radios, binoculars, night vision binoculars, safety rope and seat harness, cordless lamp, torch, handheld search lamp, LED reflector, several types of power generator extensions, damage marking devices (cordless cone and chemical protection signal kit), textbooks, databases, maps, on-board computer communication module, laptops, multifunction printers, disinfectants, toiletries, special first aid equipment, thermal imager, video recording system, folding ladder GPS, hand tools (axe, pick, shovel), blanket, seat belt-cutter, plastic bag, handheld powder fire extinguisher, handheld foam extinguisher and first aid kit. Besides, there are ADR gears including telescopic mirror/camera, number plate with arrows, laser range finding telemeter with a laser reflective plate, tape measure, plastic seals, 70–50–30 speed limit traffic signs, sign for vehicles transporting dangerous goods to proceed in the direction indicated by the arrow, additional road sign depicting 'ADR control', portable traffic sign stands and life jacket with lamp. Mandatory material requirements for the control of the transport of dangerous goods are defined by the measures of the National Directorate General for Disaster Management. The vast majority of the appliances includes compulsory standby appliances, but some can be optionally detached and only carried when needed.

3.3.1. Protective gear

The hazardous material response unit is also armed with personal protective equipment, as the type "A" heavy gas protective suit, supplied-air respirators and spare composite bottle, gas mask, filter inserts, filter type protective suit, light protective suit, protective gloves, protective hood, safety helmet, rubber boots and protective trousers with boots. With these personal protective equipment, type A and C protection can be provided.

3.3.2. Decontamination kit

For decontamination, there is a decontamination kit available on vehicles including water, CBRN decontamination substance, decontamination ring, decontamination tray, cold season decontamination solution. Besides, a portable shelter and shower system containing a hot water module with pumps, hoses and a flexible 1 m^3 waste tank to capture contaminated water generated during discharge. With the mentioned equipment, only a partial removal of dangerous substances can be executed, before the next deployment, some apparatus needs to be sent to a specialist for a complete neutralisation.

Listing the options has a purpose to show what these units are currently capable of. Their procedure and applicability are largely determined by the professionalism of the devices and their operators. This is the key to the future, for the reason that it provides a foundation and a vision to move towards new challenges.

4. Vocational training of HAZMAT Unit personnel

The training of personnel is extremely important, as the rapid response unit has to be prepared for unforeseen situations, and in addition to the special set of apparatus, they need to acquire in-depth theoretical competence and a wide range of practical preparation. In Hungary, the Civil Protection and Industrial Safety Section of the Disaster Management Training Centre is responsible for the training of the personnel.[19] The currently operating units have been gradually introduced into the system since 2012. The tools and responsibilities that had formerly belonged to the authority of the former Emergency Response Team, were subsequently further developed and modified, taking into account past years' experiences, the possible emergence of new risk factors and the technological development related to the equipment. The first interveners are able to identify various chemical compounds and their hazardous properties, also in case of gaseous, liquid and solid samples, as well as to detect certain infectious – biohazardous – agents and radioactive substances.

4.1. The development of the HAZMAT training

The training of Hungarian HAZMAT Units was carried out in a multi-step process from 2012–2013 by transforming the previous programs. The training is carried out by the Civil Protection and Industrial Safety Department of the Disaster Management Training Centre, under the supervision of the Education Department and Disaster Management Examination Centre of the National Directorate General for Disaster Management and the Nuclear Emergency Response Department. Considering the new deployment unit, the transformation of the training program began with the preparation of teachers. Then, after a smaller transition cycle, today's structure has been gradually developed, during which, the necessary theoretical and practical knowledge is acquired in almost five weeks. The extensive professional experience of our educators, their insight and approach to the field, helps our students to master the equipment of such a complex deployment unit, the specialties of their usage and the tactical features of subsequent reconnaissance at the highest possible level. During the development of the program, our teachers also took into account the previous field experiences and the feedback related to the training. Furthermore, the experience of professional competitions, the newly obtained equipment and additional needs were also taken into consideration.

4.2. The current form of the HAZMAT training program

The current form can also be divided into several parts, as the colleagues who previously intervened with the predecessor Emergency Response Team, had already

[19] 9/2015 (III/25) Decree of the Ministry of the Interior on the professional qualification requirements and vocational training of those employed in professional disaster protection bodies, municipal and facility fire brigades, voluntary fire brigade associations, and related fields.

acquired the necessary basic skills. Therefore, in the context of the transformation, they participated in supplementary training. However, professional firefighters who attended a course for the first time will receive education from the most fundamental.

4.2.1. The structure of the modules

The current training program[20] consists of 3 modules, as follows: Module I – Basics of Emergencies; made up of 30 theoretical and 12 practical lessons. During the lessons, the necessary theoretical basics can be acquired by the participants (mobile laboratory vehicle construction, equipment; basics of radiology; basics of chemistry; basics of navigation; basics of epidemiology; decontamination; water analysis).[21] Module II is based on Technical Asset Management (21 theoretical lessons, 45 practical lessons). Students get acquainted with the instruments, devices and superstructure of the vehicle, their usage, the relevant occupational safety and health rules and the maintenance of the devices. Module III aims to practice the use of technical equipment within the framework of 5 theoretical lessons and 33 practical sessions. During this module, students can practice the use of instruments, protective gears, and various accessories, as well as experienced colleagues provide presentations on deployments to have an impression of real life activities. In addition, two teachers of the Section also participate regularly as directors at the biennial professional HAZMAT competitions. As the best of the counties' units compete here, the gained special experience also greatly contributes to the shaping of the training material now and again, in order to be as complete as possible.

Picture 3
Professional HAZMAT competition
Source: Molnár, Professional HAZMAT competition.

Picture 4
Professional HAZMAT competition
Source: Molnár, Professional HAZMAT competition.

[20] Disaster Management HAZMAT Unit training program (approved by Dr. Zoltán Góra Ff. Major General, Director General of NDGDM, 16 April 2019, registration no. 35001/874/2019).
[21] DMTC Civil Protection and Industrial Safety Section, 'Megújult KML képzés a Katasztrófavédelmi Oktatási Központban', *KOK Híradó* 16, no 1 (2020), 22–23.

Table 1

Table of the program structure

Source: Compiled by the author.

	Course title	Number of Classes			
		Theoretical	Theoretical Practice	Field Experience	Total
	I. Basics of Emergencies				
1.	The Role and Operation of HAZMAT Unit	2			2
2.	Construction and Equipment of the Vehicle	1	1		2
3.	Occupational Safety	1			1
4.	Management Skills	2			2
5.	Introduction to Psychology	1			1
6.	First Aid Knowledge	2		4	6
7.	Basics of News System		2	2	4
8.	Basics of Fire Protection	3			3
9.	Radiological Knowledge	4			4
10.	Basics of Chemistry	8			8
11.	Epidemiological Knowledge and Biological Detection	3	1		4
12.	Navigational Knowledge	2	2		4
13.	Hazardous Material Databases	1			1
	Total:	**30**	**6**	**6**	**42**
	II. Technical Asset Management				
14.	Chemical Detection and Equipment	3	1	4	8
15.	Radiological Detection, Radiation Measuring Devices	3		5	8
16.	Water Analytical Knowledge and Instruments	3		5	8
17.	Sampling and Sampling Equipment	1	1		2
18.	Meteorological Knowledge and Equipment	2	1	5	8
19.	Decontamination, Disinfection and Equipment	2		2	4
20.	Personal Protection	2	1	5	8
21.	ADR and Accessories	1	1		2
22.	Power Generation Operator Training	2		2	4
23.	Practice in parts	1	1	6	8
24.	Complex Practice (control session)	1		4	5
25.	Evaluation of complex practice		1		1
	Total:	**21**	**7**	**38**	**66**
	III. Practice in Handling Technical Equipment				
26.	Vulnerability of the Capital/County and Local Characteristics	2	4		6
27.	Power Generation Operator Training			8	8
28.	Use of Electrical, ADR and other Devices			2	2
29.	Use of Personal Protective Equipment			4	4
30.	Use of HAZMAT Equipment in Practice			12	12
31.	Intervention Experiences and Documents	3	3		6
	Total:	5	7	26	38
	Sum Total:	**56**	**21**	**69**	**146**

4.3. Table of the program structure

Table 1 above also represents the current structure of HAZMAT Units' vocational training in Hungary. There is a great emphasis on the practice-oriented approach, as well as on the fact that new trainees may have the chance to get familiar with the intervention experiences of the professional staff. External lecturers are also involved in aspects of guaranteeing certain special education, for example Radiological Knowledge is taught by Nuclear Emergency Response specialists. The practice mobile laboratory vehicle, which had been designed for educational purposes containing reduced equipment, also plays a major role in the preparation of the personnel. In addition to this, for the practical lessons of the module, the County Disaster Management Directorates also provide additional mobile laboratory vehicles. Hence, a sufficient number of machinery and other tools are available for the students to acquire knowledge and to carry out various partial or complete reconnaissance exercises. Part of the training is composed of complex practice involving a situational exercise similar to real deployments. In doing so, students have to solve a complex task in teams of 3. While accomplishing the task, the activities of the team are constantly controlled – helping them if necessary, and afterwards the evaluation is performed together. The aim is to provide both teachers and students with feedback on whether they have successfully mastered the skills, and explore those parts where practice is still needed. The complex practicing process also helps to prepare for the theoretical and practical parts of the final exam.

4.4. The structure of the final exam

The final exam, in the renewed curriculum also, consists of 3 main parts (written, oral and practical), which are carried out on two following days. On the first day, trainees fulfil the requirements of the theoretical part in written and oral forms. Students who successfully complete the requirements may take a practical exam on the second day. The practical exam involves a complex exercise by solving a situational task in groups of 3. Although individuals find solutions in groups, the committee judges the performance individually. For instance, the driver is responsible for installing the micro meteorological station, keeping in touch with the on-scene commander and county news services. Meanwhile, the commander directs reconnaissance, partially evaluates measurement data and advises the on-scene commander on possible civil protection measures. Certain chemicals cannot be extinguished with water or toxic gases may be formed during the extinguishing. The optional number of students participating in the training is no more than 15. The following photos were taken during the training.

Picture 5
HAZMAT training
Source: Molnár, HAZMAT training.

Picture 6
HAZMAT training
Source: Molnár, HAZMAT training.

Picture 7
HAZMAT training
Source: Molnár, HAZMAT training.

Picture 8
HAZMAT training
Source: Molnár, HAZMAT training.

As it has been pointed out in the evaluation of the previous section, instrumentation and mobility are worthless, if there are no masterfully trained handlers. Clearly, the structure of training becomes more complicated in parallel with the increasing opportunities and expectations set for HAZMAT Units. In addition, the vast majority of these individuals can only respond to a task with a delayed alert. Consequently, this does not form part of their primary tasks, therefore, multiple repeats of training are required. Furthermore, participants need to get to know the best field practice method via different competitions, considering that even after all these years the same tasks are implemented differently across the country. It may be affirmed that a well-trained management personnel is the key to success.

5. Certain examples of HAZMAT Unit deployments

The mobile laboratory can be alerted in case there is a circumstance indicating the presence or threat of a hazardous substance or suspected to be hazardous substance at the scene of the disaster; identification of unknown substances or taking protective measures for the population become necessary. MO, in the case of requiring the unit's special apparatus on the site. Standby service operates with territorial jurisdiction and authority. Nationwide, HAZMAT Units are alerted in 1,200–1,500 cases per year. The following diagram represents the distribution of each deployment type during the last 3 years (2018, 2019 and 2020).

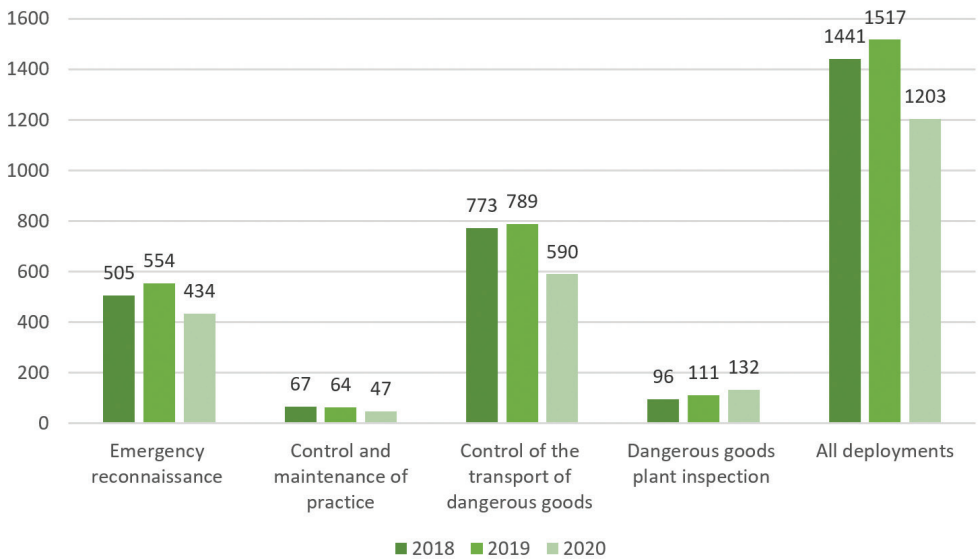


Figure 1

Deployment of HAZMAT Units in recent years

Source: Barbara Korbély Ff. Captain; data source: "Disaster Management Yearbook 2019" and data provision of the Department of Nuclear Accident Prevention NDGDM.

As the graph illustrates, emergency detections preferably account for only about a third of all interventions in a year. Every once in a while, there are a series of significant events or incidents in Hungary, at which the crucial importance of the professional work and assistance of HAZMAT Units is indispensable.

5.1. White Powder Packages

Following the terror attack in New York on 11 September 2001, suspicious packages containing white powder being sent in a package or envelope to famous people

happened to be frequently reported. This powder could have been the carrier of Bacillus anthracis, the bacteria that causes anthrax, as it happened before.[22] The number of 'white powder' cases in Hungary increased before the 2002 elections. Fortunately, there were no positive cases in Hungary, but the hundreds of cases per day significantly increased the number of ERT interventions (predecessor of today's HAZMAT Unit). For that reason all ERT colleagues were on duty (back then all counties, including the capital, were on standby), provided with engine and protective gear needed (gas mask, dust mask, disposable protective clothing, protective gloves, footwear protector, lockable smooth-locked bag, boxes). They were responsible for delivering the suspicious packages under safe conditions to the testing laboratories (Epidemiological Center). Due to the increased number of cases, rapid tests capable of identifying the pathogen of anthrax were procured, with which 'negative packages' could be filtered out in a short time. During the 2006 elections, 'white dust' cases also occurred, but fortunately in fewer numbers. Nowadays, in such 'white powder' or 'white dust' suspicious cases, the interveners work in cooperation with other defence bodies and organisations. Such cases must be handled according to special procedure order and professional briefings.[23]

5.2. The red sludge disaster

Hungary's most severe industrial ecological disaster occurred on 4 October 2010, when the western dyke of cassette X of the sludge reservoir on the site of the Hungarian Aluminium Production and Sales Plc (MAL) breached. Consequently, the mixture of approximately one million cubic meters of red sludge and alkaline water inundated, through the Torna Creek, the lower parts of the settlements Kolontár, Devecser and Somlóvásárhely. Ten people were killed during and after the sludge flow, 286 persons were hospitalised. The disaster in Devecser, Kolontár and Somlóvásárhely affected 358 residential properties, over a thousand hectares of arable land were contaminated. Even on 5 October, in the morning of the day following the disaster, red sludge was standing one meter high in Devecser. Schools, family care services and cultural centres were transformed into temporary shelters, so evacuees could be lodged. On 9 October complete evacuation was ordered in Kolontár, also the Government declared state of emergency in the areas of Veszprém, Győr-Moson-Sopron and Vas Counties. Following the disaster, a total of 106 firefighters and 24 fire engines and 6 Emergency Response Teams (ERT) from the immediately deployable disaster management and firefighter forces were alerted under the territorial Emergency and Rescue Plan. Later, measures were taken to merge 8 ERT into the area, their main task was the continuous sampling, monitoring and informing the population. The basic strategic goal of the water quality control efforts was to stop the pollution reaching the Danube River, since threatening the water source would have caused long-lasting damages. During the rescue duties, the removal of the contaminated sludge and its discharge at the landfill was continuously ensured by the response team.

[22] NDGDM National Industrial Safety Inspectorate press conference no. 1/2013 on the tasks of the HAZMAT Units related to the handling of 'white powder' packages, 12.09.2013.
[23] NDGDM supplementary guide no. 35000/2544/2018 to investigate 'white powder' events, 06.03.2018.

On 1 November, the serving ERT reported that the threads measuring the gap had broken. According to the surveyor assigned to the site in order to assess the situation, the dam rupture could have occurred at any time, so the monitoring of the dam movement with a measuring thread was discontinued and only visual observation was happening. The following day, the possibility of installing a 'building motion and vibration' monitoring system to permanently observe the possible movement was considered. Next week, the possibility of partial withdrawal of the emergency Response Team directed to Devecser was reviewed. The supervision of the damaged dam section was provided by the remaining 5 ERT until the installation of the prism monitoring system, which was put into operation on 1 December. Subsequently, the ERT was withdrawn. The following photographs were taken during the post-disaster work.

Picture 9
Monitoring of dam rupture
Source: Unknown author, 2010.

Picture 10
Red sludge disaster
Source: Unknown author, 2010.

Picture 11
Red sludge disaster
Source: Unknown author, 2010.

5.3. Hazardous waste disposal and storage facility fire in Királyszentistván

2019, in the afternoon of 10 August, a fire broke out at the regional waste management facility in Királyszentistván. The bale storage area behind the biological room, where a total of 9,966 bales (approximately 6,000 tons) were stored, was completely affected. The fire was accompanied by a strong smoke formation. The local response unit provided 52 hours of continuous service in two shifts. Complicating circumstances of firefighting and intervention were the prolonged usage and the long distances between the populated areas. The concentration of hazardous substances in the vicinity of the plant, as measured by the crew was above MAK value in several cases, which refers to the highest permitted rate. However, based on the values measured in populated areas, it was not justified to alert an additional HAZMAT unit to the site and the values measured outside the plant area also did not justify the introduction of population protection measures. The fire attracted considerable interest in the media and several public information requests were also received, therefore the measurement results were made available by the Veszprém County Disaster Management Directorate on its website. Duties and capabilities of the mobile laboratory vehicle were presented at the Veszprém County Disaster Management Directorate press conference. The following photographs were taken at the scene of the fire.

Picture 12
Monitoring of HAZMAT Unit
Source: Unknown author, 2019.

Picture 13
Fire in Királyszentistván
Source: Unknown author, 2019.

The field practice also shows the versatile requirements that have to be met by the operating personnel of the Hungarian HAZMAT Units. Generally, coping with the given challenge is due to the ingenuity of the engineers, which represents the importance of training.

6. Future directions

1. In the case of questions beyond the capabilities, measurement accuracy or technical capabilities of HAZMAT–ADR units, it may be necessary to develop a sampling capability that allows the group to collect environmental or chemical samples for analysis and identification under time-varying circumstances as a first intervention unit, or their contaminant content will be determined in a more sophisticated, specialised laboratory environment.

2. Several elements are already available to ensure the adequacy and closure of the entire sampling chain, for instance the built-in refrigerated sample storage system and certain manual sampling devices.

3. Providing the unit with sampling and storage devices capable of guaranteeing cross-contamination and closed, protected storability that allow the collection, safe storage, appropriate labelling and documentation of liquid or solid samples containing organic compounds, heavy metals or biological contaminants.

4. Implementation of this development program has already begun. The equipment is awaiting allocation. In addition, it is necessary to further train the personnel and develop sampling methodological recommendations for unplanned, risky or unknown sites.

After the study of operator training, it may be stated:

One of the key players in preventing major industrial accidents and mitigating potential damage is the fire department as the primary intervener, but at least as important would be another HAZMAT Unit capable of fast and efficient atomic, chemical, biological detection and reliable data provision.

The word 'would be' has a great significance because the current alarm system does not mean immediate alert in all places.

These organisations, with their current forces and tools, are able to carry out their related reconnaissance tasks in a fundamental way. Nevertheless, – based on my research, experience, consultations and practical training – in the near future, it will be necessary to develop them and prepare their personnel for industrial accidents in the interest of a more operative response.

The areas of development, from my standpoint, could be:

1. Coordination of means of communication with the cooperating and own forces, ensuring the adequacy of the information received in the event of an alert, both in terms of quantity and content.

2. It is recommended to assess the applicability of procedures and technical capabilities, the training and suitability of personnel, and to make practiced all segments of the human and technical sides for specific intervention.

3. As this has not been fully done so far, it is expedient to examine the impact of accident factors (heat and toxic effects, explosions, and so on) on the physical and mental coping capacity of the intervener personnel due to the risk of an accident.

4. It is necessary to analyse the efficiency of the application of HAZMAT Units in the event of an industrial accident, to adapt the adequacy of its existing equipment and its quantitative and qualitative addition to the outflow potential of the hazardous substance that can be predicted in the given plant, switch to the principle of local

and territorial protection, thus to provide them with fewer but more specialised instruments.

5. In parallel, it would be worthwhile to examine, as a possible model, the feasibility of micro-regional rescue stations based on municipal associations, which could provide the material, technical and human conditions for rapid intervention, just like the German, Austrian, Danish examples.

6. In any case, the personnel of existing civil protection organisations planned to contribute to the prevention of chemical accidents shall be reviewed in terms of their organisation, number, training and equipment. Furthermore, following the review, the designated personnel shall be made suitable for continuous work in the damaged area with appropriate training and personal protective equipment, as one of the lessons of the red mud disaster.

7. Conclusion

In conclusion, this research provides an overview of HAZMAT Units, in terms of applicability provided by technical tools. HAZMAT–ADR Units are able to perform detection and public protection functions in extremely hazardous environments. Their instrumentation supports the continuous monitoring of environmental conditions either in installed or mobile mode. Gas sensors in the vehicle can be used to monitor the extent and changes of environmental load by determining gas concentration in the vehicle's environment. They are able to set up a propagation model using their own measured weather and air movement data. Based on the data collected, the personnel makes a proposal to the rescue management team to take the necessary measures to protect the population, and to support the decisions made on possible containment or eviction with measurement data. They are able to determine unknown organic and inorganic gaseous, liquid or solid substances by manual or mobile measuring instruments. The units have acquired proficiency in the determination and identification of Raman active compounds, in the recognition and identification of up to three components of unknown liquids and solids, chemical products. Their water testing kit supports the recording of typical variable parameters of a given environment, the colorimetric and spectrophotometric determination of pH, conductivity, dissolved oxygen and various ions facilitating the rapid detection of water pollution phenomena. By reason of its manual and built-in elements and radiological equipment, the unit is capable of performing complex reconnaissance and is able to monitor continuously even on the move. An important part of the equipment is a rapid immunochromatographic test for the detection of the most characteristic biological agents in bio-terrorism, which is used for detecting the presence of microbes released into the environment in a short time frame. The range of personal protective equipment provides the suitability for secure detection, independent data collection and communication in locations exposed to biological hazards along with chemical risks. The three-person team are able to perform various types of hazardous material and danger detection tasks with appropriate cooperation in industrial and civilian environments, at the scene of an accident, or in unknown built-up and outdoor conditions. Following the interventions,

a HAZMAT Unit is able to provide decontamination for two reconnaissance personnel on site, to remove biological, chemical and radiological contamination, and to safely change protective clothing. The on-board devices allow digital, protected radio broadcasting, besides internet access, as an information base for the involvement of external experts providing on-site advice via video.

References

9/2015 (III/25) Decree of the Ministry of the Interior on the professional qualification requirements and vocational training of those employed in professional disaster protection bodies, municipal and facility fire brigades, voluntary fire brigade associations, and related fields.

Act No. CXXVIII of 2011 concerning disaster management and amending certain related acts.

Disaster Management HAZMAT Unit training program (approved by Dr. Zoltán Góra, Ff. Major General, Director General of NDGDM, April 16, 2019, registration no. 35001/874/2019).

KEHOP-1.0.6-15-2016-00008 SEQ ID project, "Advanced industrial safety interventions and capacity development" HAZMAT Unit vehicle procurement.

A KML–ADR gépjárművek állományának újabb továbbképző tanfolyama, 30 September 2013. Online: https://kok.katasztrofavedelem.hu/32405/hirek/208962/a-kml-adr-gepjarmuvek-allomanyanak-ujabb-tovabbkepzo-tanfolyama

'Annual Report of An Garda Síochána 2009', An Garda Síochána.

Boyle, Darren, 'Gardai get 'dirty bomb' protection', *The Mirror,* 29 March 2007.

'CBRNe World Convergence – All Hazards Response 2013', Dublin, Department of Defence, 16 April 2013.

DMTC Civil Protection and Industrial Safety Section, 'Megújult KML képzés a Katasztrófavédelmi Oktatási Központban'. *KOK Híradó* 16, no 1 (2020), 22–23.

Eri-Cards – Ausgabe 2008: Emergency Response Intervention Cards. 1st German Edition. Kohlhammer, 2008.

Ff. Lieutenant Colonel Tibor Körössy, part of the material incorporated in 2011, for the 'Summary Report on the period from 4 October 2010 to 31 December 2010' entitled *Red Mud.*

Folytatódott a KML alaptanfolyam Pécelen, 14 April 2015. Online: https://kok.katasztrofavedelem.hu/32405/hirek/209130/folytatodott-a-kml-alaptanfolyam-pecelen

Hazardous Materials Response Special Teams Capabilities and Contact Handbook. Washington, D.C.: U.S. Coast Guard, 2003.

Katasztrófavédelmi Mobil Labor (KML), s. a. Online: https://katasztrofavedelem.hu/86/katasztrofavedelmi-mobil-labor-kml

Katasztrófavédelmi Mobil Labor képzés, 12 December 2012. Online: https://kok.katasztrofavedelem.hu/32405/hirek/208891/katasztrofavedelmi-mobil-labor-kepzes

KML mentorok felkészítése, 05 February 2013. Online: https://kok.katasztrofavedelem.hu/32405/hirek/208848/kml-mentorok-felkeszitese

KML szakmai nap Pécelen, 13 February 2017. Online: https://kok.katasztrofavedelem.hu/32405/hirek/209294/kml-szakmai-nap-pecelen
KML vizsga Szolnokon, 04 April 2013. Online: https://kok.katasztrofavedelem.hu/32405/hirek/208906/kml-vizsga-szolnokon
KML–ADR továbbképzés, 30 April 2013. Online: https://kok.katasztrofavedelem.hu/32405/hirek/208926/kml-adr-tovabbkepzes
Korbély, Barbara Ff. Captain; data source: "Disaster Management Yearbook 2019" and data provision of the Department of Nuclear Accident Prevention NDGDM.
Kortt, Ulrich, Rolf Schmid, Hermann Schröder and Walter Hamilton, *Hamilton. Handbuch für den Feuerwehrmann.* Boorberg, 2003.
Lezárultak a KML–ADR továbbképző tanfolyamok, 30 January 2015. Online: https://kok.katasztrofavedelem.hu/32405/hirek/209109/lezarultak-a-kml-adr-tovabbkepzo-tanfolyamok
Meisenberg, Oliver and Stefan Sellmeier, *ABC-Einsatz: Realistische Übungen mit der "Erkunder-Simulation".* BRANDSchutz, 2013, 957–959.
Malerova, L, K Chmelikova and M Zajic, 'The Safety Situation within the Context of Simulations of Crisis Management Processes'. *Wit Transactions on the Built Environment* 150 (2015), 209–218. Online: https://doi.org/10.2495/DMAN150191
Mérföldkőhöz érkeztek a KML képzések, 23 November 2016. Online: https://kok.katasztrofavedelem.hu/32405/hirek/209275/merfoldkohoz-erkeztek-a-kml-kepzesek
Molnár, M, *Fully equipped HAZMAT vehicle.* Disaster Management Training Centre, Civil Protection and Industrial Safety Section, 2020.
Molnár, M, *Professional HAZMAT competition.* Disaster Management Training Centre, Civil Protection and Industrial Safety Section, 2020.
Molnár, M, *HAZMAT training.* Disaster Management Training Centre, Civil Protection and Industrial Safety Section, 2020.
NDGDM National Industrial Safety Inspectorate press conference no. 1/2013 on the tasks of the HAZMAT Units related to the handling of 'white powder' packages, 12.09.2013.
NDGDM supplementary guide no. 35000/2544/2018 to investigate 'white powder' events, 06.03.2018.
NKE–KML Gyakorlat, 03 April 2014. Online: https://kok.katasztrofavedelem.hu/32405/hirek/209035/nke-kml-gyakorlat-2014-aprilis-03
Petrova, Elena, 'Natural Hazards and Technological Risk in Russia: The Relation Assessment'. *Natural Hazards and Earth System Sciences* 5, no 4 (2005), 459–464. Online: https://doi.org/10.5194/nhess-5-459-2005
Pike, John, *Military,* s. a. Online: www.globalsecurity.org/military/world/russia/emercom.htm
Pursiainen, Christer, 'Russia's Critical Infrastructure Policy: What do we Know About it?' *European Journal for Security Research* 6 (2021), 21–38. Online: https://doi.org/10.1007/s41125-020-00070-0
Reihlen, Antonia, Juhan Ruut, Philipp Engewald, Heidrun Fammler and Elvira Moukhametshina, *The Russian system of chemicals management.* Baltic Environmental Forum Group, June 2010.

Roffey, Roger, *Russia's EMERCOM: Managing Emergencies and Political Credibility*. Swedish Defence Research Agency (FOI), 2016.
Sikeres KML alaptanfolyam és vizsga, 16 May 2014. Online: https://kok.katasztrofavedelem.hu/32405/hirek/209050/sikeres-kml-alaptanfolyam-es-vizsga
Sikeres vizsgákkal zárultak a 2014/15-ös tanévre tervezett KML képzések, 15 June 2015. Online: https://kok.katasztrofavedelem.hu/32405/hirek/209153/sikeres-vizsgakkal-zarultak-a-2014-15-os-tanevre-tervezett-kml-kepzesek
'Training and development in the Reserve Defence Forces', Defence Forces Ireland, 2016.
United States Fire Administration, *Hazardous Materials Guide for First Responders*. Emmitsburg: USFA, 1999.
Újabb KML vizsgák Veszprém és Békés megyében, 16 May 2013. Online: https://kok.katasztrofavedelem.hu/32405/hirek/208927/ujabb-kml-vizsgak-veszprem-es-bekes-megyeben
Újabb sikeres KML alaptanfolyam és vizsga, 28 October 2014. Online: https://kok.katasztrofavedelem.hu/32405/hirek/209090/ujabb-sikeres-kml-alaptanfolyam-es-vizsga

Abbreviations

HAZMAT: hazardous materials and substances that may pose risk to health, property, or the environment
CBRN: Chemical, Biological, Radiological and Nuclear
IR detector: a sensing device that reacts to infrared radiation
IFV: the institute for disaster relief and public crisis management in the Netherlands (Instituut Fysieke Veiligheid)
AFAD: Ministry of the Interior, Disaster and Emergency Management Authority of Turkey (Afet ve Acil Durum Yönetimi Başkanlığı)
EMERCOM: Ministry of Russian Federation for Civil Defence, Emergencies and Elimination of Consequences of Natural Disasters
ADR: an international term referring to the European Agreement concerning the International Carriage of Dangerous Goods by Road
RID: an international term referring to the European Agreements Concerning the International Carriage of Dangerous Goods by Rail
ADN: an international term referring to the European Agreement concerning the international carriage of dangerous goods by inland waterway
MAK: maximum concentration of a chemical substance
ERT: Emergency Response Team

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

16. évfolyam (2021) 3. szám 81–96.
DOI: 10.32567/hm.2021.3.5

Berger Ádám[1]

A veszélyesanyag-tárolótartályok tervezésének iparbiztonsági aspektusai

Industrial Safety Aspects of Hazardous Material Tank Design

Az elmúlt tíz évben több veszélyes anyaggal kapcsolatos baleset is bekövetkezett mind a világban, mind az Európai Unió területén. Ezen káresemények jellemzően két okra vezethetők vissza: műszaki meghibásodás vagy emberi mulasztás. A társadalmi, gazdasági növekedés és technológiai fejlődés velejárója, hogy bővül a veszélyes anyagok száma, valamint a velük foglalkozó üzemek köre is. Az üzemek veszélyes anyagnak minősülő alapanyagok iránti megnövekedett igényüket két módon tudják biztosítani, vagy a beszállítások gyakoriságát növelik, vagy új alapanyag-tárolót létesítenek. Jelen publikáció célja a veszélyes folyadékok tárolótartályainak létesítésével kapcsolatos főbb műszaki információk bemutatása, valamint technológiai ajánlások megtétele.

Kulcsszavak: **veszélyes anyag, tárolótartály, tartálysérülés, kármentő medence, védőgyűrű**

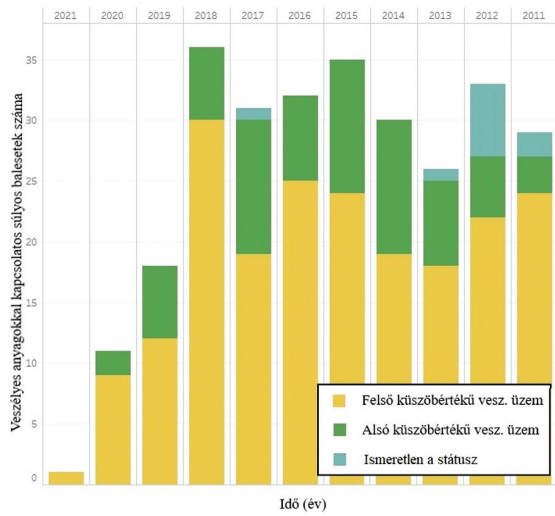
There were several accidents involving dangerous substances in the last 10 years, both in the world and in the European Union. These damage events are typically due to two reasons: technical failure and human negligence. Social, economic growth and technological development are accompanied by an increase in the number of dangerous substances and the range of plants that deal with them. Plants can meet their increased demand for raw materials that are dangerous materials in two ways, either by increasing the frequency of deliveries or by setting up a new raw material storage facility. The purpose of this publication is to present the main technical information related to the construction of storage tanks for dangerous liquids and to make technological recommendations.

Keywords: **dangerous substance, storage tank, tank damage, remediation board, protective ring**

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

1. Bevezetés

Az Európai Unióban a veszélyes anyagokkal kapcsolatos tevékenység szigorú követelményekhez kötött. Ennek ellenére évente több veszélyes anyaggal kapcsolatos súlyos baleset is bekövetkezik. A 2019-es évben világszerte mintegy 11 ezer ember vesztette életét vagy tűnt el a természeti és a civilizációs katasztrófák következtében.[2] Az Európai Bizottság Közös Kutatóközpontja *(Joint Research Centre)* által üzemeltetett Súlyos Baleseti Jelentési Rendszer *(Major Accident Reporting System)* statisztikai adatai alapján megállapítható, hogy az Európai Unió területén az elmúlt 10 évben jelentős számú veszélyes anyagokkal kapcsolatos súlyos baleset történt (1. ábra).



1. ábra

Veszélyes anyagokkal kapcsolatos súlyos balesetek

Forrás: European Comission: *JRC Science Hub, MINERVA Portal* (é. n.)

A veszélyes anyagokkal kapcsolatosan bekövetkezett balesetek alapvetően két okra vezethetők vissza: műszaki meghibásodásokra és/vagy emberi hibára.

A veszélyes anyagokkal kapcsolatos balesetek megelőzése érdekében az Európai Bizottság a veszélyes tevékenység végzését szigorú előírásokhoz köti, amit a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK tanácsi irányelv módosításáról és későbbi hatályon kívül helyezéséről szóló 2012/18/EU Irányelv (Seveso III. Irányelv) tartalmaz. A Seveso III. Irányelv előírásait a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvénybe (Kat. törvény), valamint végrehajtási rendeletébe a veszélyes

[2] Cimer Zsolt – Kátai-Urbán Lajos – Vass Gyula: Katasztrófakockázatok: a településrendezési tervezés szerepe a megelőzésben. In Hábermayer Tamás (szerk.): Katasztrófák, kockázatok, önkéntesek. Szekszárd, Tolna Megyei Katasztrófavédelmi Igazgatóság, 2020. 56–63.

anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X. 20.) Korm. rendeletbe (Rendelet) ültették át.

A veszélyes anyagokkal kapcsolatos balesetekkel szemben az elsődleges cél a prevenció, ennek érdekében a Kat. törvény 25. §-a kétkörös engedélyezési eljárást határoz meg:

„Veszélyes anyagokkal foglalkozó üzemre, veszélyes anyagokkal foglalkozó létesítményre építési engedély csak a hivatásos katasztrófavédelmi szerv katasztrófavédelmi engedélye alapján adható. Veszélyes tevékenység kizárólag az iparbiztonsági hatóság katasztrófavédelmi engedélyével végezhető. Az építési engedélyezéshez és a veszélyes tevékenység végzéséhez szükséges katasztrófavédelmi engedély iránti kérelemhez az üzemeltetőnek csatolni kell a biztonsági jelentést vagy biztonsági elemzést."[3]

A gyártóüzemek termelési volumenének növekedése – amely a gazdasági fejlődés, társadalmi jólét egyik természetes eredménye – a termelési kapacitások bővítését, feloldását, optimalizálását követően magával hozza az alapanyag mennyiségének növelését. A számos esetben veszélyes anyagnak minősülő alapanyag iránti megnövekedett igény két módszerrel biztosítható: a beszállítások gyakoriságának növelésével, vagy új alapanyagtároló építésével. Az elmúlt évek kihívásai azt mutatják, hogy a beszállítások gyakoriságának növelése és az úgynevezett „just in time" gyártásszervezési és készletgazdálkodási leltárstratégia folytatása jelentős kockázatokat hordoz magában, egyrészt az alapanyagok piaci árának hektikus változásai, másrészt a szállítási bizonytalanságok miatt. Ezért egyre jobban előtérbe kerül az alapanyagtárolók („puffer tárolókapacitás") építése, amely a folyékony halmazállapotú anyagok esetében elsősorban tartály létesítését jelenti.

Írásunkban a veszélyesanyag-tárolótartály (elsősorban éghető folyadék) létesítésének javasolt folyamatát mutatjuk be, megfogalmazva technikai, műszaki ajánlásokat.

2. Tárolótartály létesítésének első lépése, tervkoncepció elkészítése

Tárolótartály létesítését megelőzően tisztázni kell, hogy a benne tárolt alapanyag a Kat. törvény szerint veszélyes anyagnak minősül-e vagy sem. A veszélyes anyag fogalmat a kémiai biztonságról szóló 2000. évi XXV. törvény és a kapcsolódó jogszabályok, valamint a Kat. törvény is alkalmazza, de eltérő tartalommal. A Kat. törvény szerinti veszélyes anyag a 2000. évi XXV. törvény szerinti veszélyes anyag részhalmazának tekintendő.

Amennyiben a tárolótartályban Kat. törvény szerinti veszélyes anyag tárolására kerül sor, már a tervezés fázisában tisztázni kell, hogy a megnövekvő veszélyes anyag mennyisége befolyásolja-e az érintett üzem státuszát. Amennyiben az üzem alsó vagy felső küszöbértékű veszélyes anyagokkal foglalkozó üzem, vagy azzá válik, akkor a már a fentiekben hivatkozott Kat. törvény 25. §-a alapján az építési eljáráshoz szükséges a katasztrófavédelmi engedély megszerzése.[4] A küszöbérték alatti üzemek és a kiemelten kezelendő létesítmények vonatkozásában a veszélyes anyagokkal

[3] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról.

[4] Cimer Zsolt et al.: *Iparbiztonsági szakismeretek. Módszertani kézikönyv a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezéssel foglalkozó gyakorló szakemberek részére.* Hungária Veszélyesáru Mérnöki Iroda Kft., 2020. 43–51.

foglalkozó létesítmény építéséhez nem kell katasztrófavédelmi engedély, csak a veszélyes tevékenység megkezdéséhez.[5]

Megjegyzendő, hogy a veszélyes folyadékok vagy olvadékok tárolótartályainak, tároló-létesítményeinek műszaki-biztonsági hatósági felügyeletéről szóló 216/2019. (IX. 5.) Korm. rendelet (216/2019. (IX. 5.) Korm. rendelet) nem az „építés", hanem a „létesítés" definíciót alkalmazza az alábbi tartalommal: „a tárolótartály, tároló-létesítmény adott helyre történő telepítése, beleértve a meglévő létesítmény bővítését is".[6] Így elméletileg az alsó vagy felső küszöbértékű veszélyes anyagokkal foglalkozó üzem esetében sem kell a tartálylétesítéshez katasztrófavédelmi engedély, csak akkor, ha olyan technológiai rész – például épületszerkezet – is kapcsolódik hozzá, amely esetében építési engedélyezési eljárást kell lefolytatni.

A tervezés megkezdése előtt a tárolótartály létesítésénél az alábbi kérdések tisztázása szükséges:

- Hol optimális a tervezett tartály elhelyezése?
- Mekkora legyen a tartály?
- Milyen típusú – védőgyűrűben, kármentőben elhelyezett, vagy esetleg duplafalú – tartályt létesítsenek?

A fenti kérdések megválaszolásánál a logisztikai és a gazdasági számítások mellett a Rendelet 7. mellékletében foglalt katasztrófavédelmi-iparbiztonsági kritériumoknak való megfelelés is elsődleges szerepet játszik.

A veszélyes folyadékok tárolására eltérő méretű, alakú és elhelyezésű tartályok létesíthetők. Az atmoszferikus tartályok esetében a másodlagos védelem szempontjából az alábbi tartálytípusokat különböztethetjük meg:

- Egyszerű atmoszferikus tárolótartály: Az egyszerű atmoszferikus tartály folyadék tárolására alkalmas elsődleges tartályból áll.
- Külső védelemmel ellátott atmoszferikus tartály: A külső védelemmel ellátott atmoszferikus tartály folyadék tárolására alkalmas elsődleges tartályból és egy külső védőrétegből áll. Az elsődleges tartály meghibásodása esetén a külső védőréteg hivatott a folyadékot tárolni, azonban gőz tárolására nem alkalmas. A külső védőréteg nem képes ellenállni bárminemű terhelésnek, vagyis robbanásnak (0,3 bar statikus nyomáshullám 300 másodpercen keresztül), befúródó szilánkoknak és hideg okozta (termikus) terhelésnek.
- Dupla falú atmoszferikus tartály: A dupla falú atmoszferikus tartály folyadék tárolására alkalmas elsődleges tartályból és egy másodlagos tartályból áll. Az elsődleges tartály meghibásodása esetén a másodlagos tartály hivatott a folyadékot tárolni és ellenállni a különféle terheléseknek, vagyis robbanásnak (0,3 bar statikus nyomáshullám 300 másodpercen keresztül), befúródó szilánkoknak és hideg okozta (termikus) terhelésnek. A másodlagos tartály nem alkalmas semmiféle gőz felfogására.

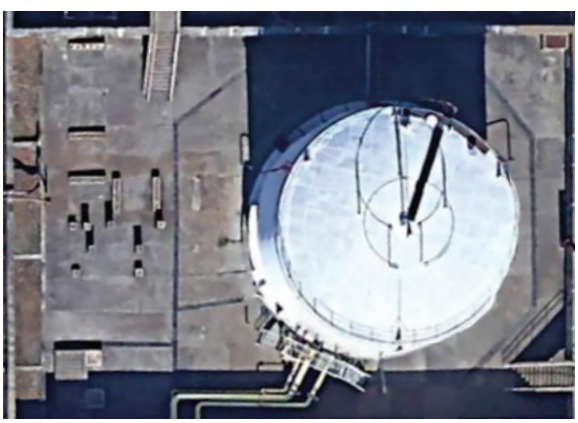
[5] 2011. évi CXXVIII. törvény.

[6] 216/2019. (IX. 5.) Korm. rendelet a veszélyes folyadékok vagy olvadékok tárolótartályainak, tároló-létesítményeinek műszaki-biztonsági hatósági felügyeletéről.

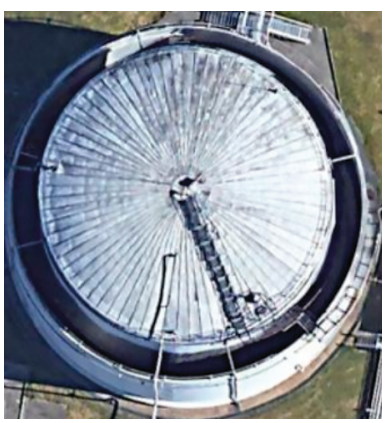
- Teljes védelemmel ellátott atmoszferikus tartály: A teljes védelemmel ellátott tartály folyadék tárolására alkalmas elsődleges tartályból és egy másodlagos tartályból áll. Az elsődleges tartály meghibásodása esetén a másodlagos tartály hivatott mind a folyadékot, mind a gőzt tárolni, és ellenállni bárminemű terhelésnek, vagyis robbanásnak (0,3 bar statikus nyomáshullám 300 másodpercen keresztül), befúródó szilánkoknak és hidegnek. A külső fedél a másodlagos tartály által biztosított és arra tervezték, hogy ellenálló legyen, például a robbanással szemben.
- Föld alatti atmoszferikus tartály: A föld alatti atmoszferikus tartály egy olyan tárolótartály, amelyben a folyadék szintje a föld szintjével egy vonalban vagy alatta van.
- Körbesáncolt atmoszferikus tartály: A körbesáncolt atmoszferikus tartály egy olyan tárolótartály, amelyet a talajréteg teljesen befed és amelyben a folyadék szintje a föld szintje fölött van.[7]

A másodlagos védelem feladata az elsődleges tartály sérülésekor a teljes anyagmennyiség felfogása. A nagy térfogatú (térfogat > 1000 m^3) tartályok vonatkozásában a gyakorlatban két védelemtípus alkalmazása terjedt el:

- egyszerű atmoszférikus tartály elhelyezése kármentőben (2. ábra), amelynek általánosan elterjedt alapanyaga a vasbeton;
- védőgyűrűben (3. ábra) elhelyezett tartály, amelynél az acéllemez alkalmazása terjedt el.



2. ábra
Vasbeton kármentő medence

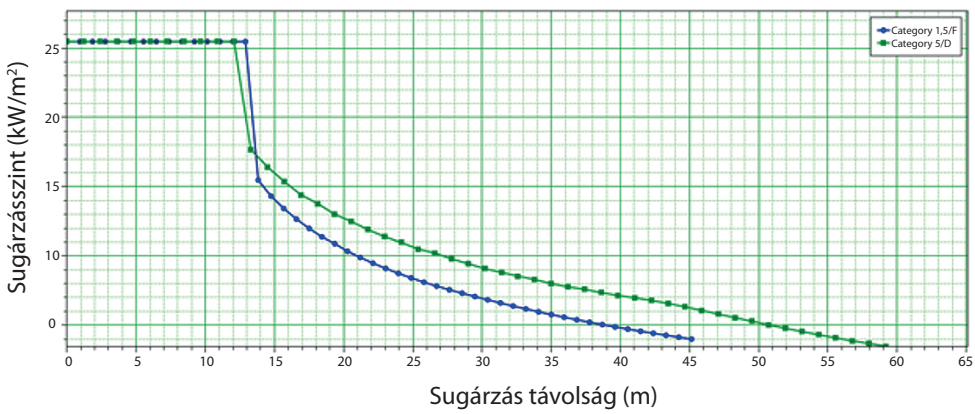


3. ábra
Acéllemezes védőgyűrű

Forrás: Képek © CNES / Airbus, Landsat / Copernicus, Maxar Technologies, 2021.

[7] Committee for the Prevention of Disasters – TNO (Purple Book): *Guidelines for Quantitative Risk Assessment.* CPR 18E. The Director-General of Labour, The Netherlands. 1999.

A tartálytípus kiválasztásánál meghatározó szempont a szabad terület nagysága. Ahogy a 2. és 3. ábrán is látható, a két felfogótér területigénye nagyban eltér egymástól. A kármentő alapterülete jelentősen nagyobb a védőgyűrűhöz képest, így a védőgyűrűs tartály látszólag kedvezőbbnek tűnik, hiszen a létesítése kisebb „értékes" üzemi területet igényel. A kisebb alapterület további előnye, hogy egy esetleges elsődleges tartálysérülés során a párolgó tócsafelület kisebb lesz, így a lehetséges következmények is enyhébbek. Az állítás következményelemzéssel igazolható: a modellezése során (tartálytérfogat: 2000 m^3; veszélyes folyadék: 1900 m^3 n-hexán; tartály átmérője: 16 m; tartály magassága: 10,5 m; kármentő mérete: 27 × 37 × 2,5 m; védőgyűrű mérete: 21 × 8,5 m) a tartály 1 cm-es lyukadásából fakadó szivárgást vizsgáltam, amelynél a tartály teljes tartalma leürül. A 4. ábra a védőgyűrűvel ellátott tartály esetében az esetlegesen bekövetkező tócsatűz során a hősugárzás változását mutatja be a távolság függvényében. Az 5. ábra ugyancsak védőgyűrűvel ellátott tartály esetében az esetlegesen bekövetkező robbanás során kialakuló túlnyomás változását mutatja be, a távolság függvényében. A 6. és 7. ábra a kármentővel ellátott tartályra vonatkozó modellezést mutatja be.[8]



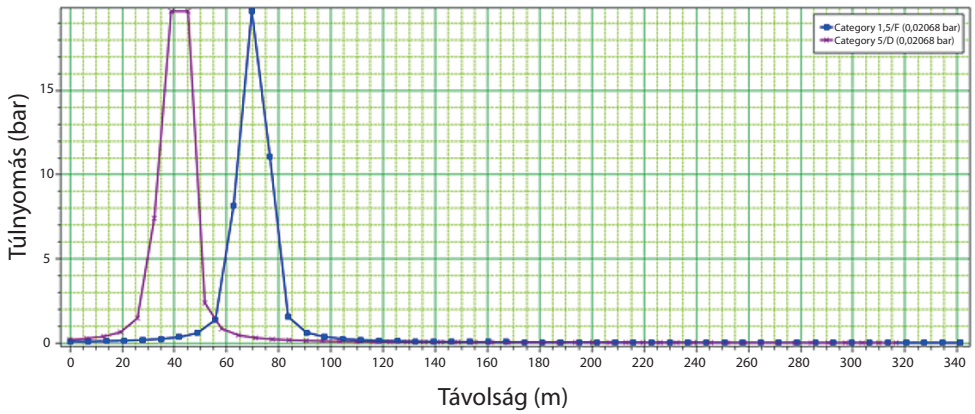
4. ábra

A hősugárzás alakulása a távolság függvényében védőgyűrű esetén

Forrás: Kátai-Urbán – Cimer – Berger (2021): i. m.

A 4. ábrán látható, hogy védőgyűrűvel ellátott tartály esetén (1,5 m/s szélerősség) körülbelül 13 m-ig 25,5 kW/m^2 a hősugárzás mértéke, amely további egy méteren gyors, majd lassú csökkenésbe kezd.

[8] Lajos Kátai-Urbán – Zsolt Cimer – Ádám Berger: Remediation board versus protective ring. Fire Engineering & Disaster Management Prerecorded International Scientific Conference, 2021.

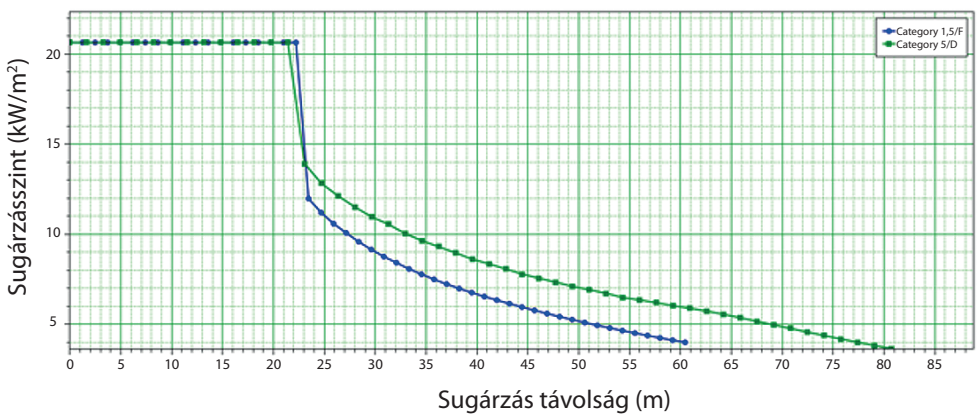


5. ábra

A túlnyomás alakulása a távolság függvényében védőgyűrű esetén

Forrás: a szerző szerkesztése

Az 5. ábra alapján elmondható, hogy védőgyűrű esetén (1,5 m/s szélerősség) 70 m-es távolságban 19,9 bar a túlnyomás értéke. Továbbá látható, hogy 55–70 m-ig intenzív növekedés, majd 70–84 m-ig intenzív csökkenés figyelhető meg.

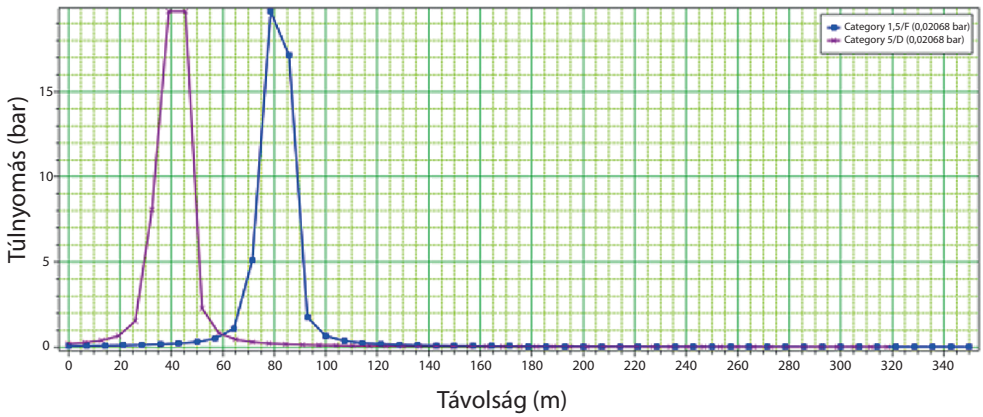


6. ábra

A hősugárzás alakulása a távolság függvényében kármentő medence esetén

Forrás: Kátai-Urbán – Cimer – Berger (2021): i. m.

Kármentő medencével ellátott tartály esetén a következőképpen alakul a hősugárzás nagysága a távolság függvényében (1,5 m/s szélerősség). Körülbelül 22,2 m-ig 20,9 kW/m^2, ezt követően a hősugárzás további egy méteren gyors, majd lassú csökkenésbe kezd.



7. ábra

A túlnyomás alakulása a távolság függvényében kármentő medence esetén

Forrás: a szerző szerkesztése

A túlnyomás vonatkozásában lényeges különbség látható a kármentő medencével ellátott tartály esetében. Ekkor 79 m-en van a túlnyomás maximuma (19,9 bar), tehát 9 m-rel távolabb, mint védőgyűrű esetében. Lényeges különbség, hogy a túlnyomás intenzív növekedése és csökkenése is tolódott, valamint azokban szakaszosság figyelhető meg. Ugyanakkor fontos megjegyezni, hogy a vasbeton szerkezet és az acél hőállósága eltér egymástól, katasztrófavédelmi szempontból a vasbeton tulajdonságai kedvezőbbek.

A három, egymással is összefüggő kérdés – mekkora, milyen típusú tartály, hol legyen – megválaszolása katasztrófavédelmi-iparbiztonsági szempontból iterációs folyamat eredménye, ahol figyelembe kell venni az üzem által okozott, már meglévő veszélyeztetést, a tartálylétesítés következtében a belső és külső dominóhatások megváltozását, valamint a tartálylétesítéssel a veszélyeztetés növekedését.

A tervezés megkezdése előtti iterációs folyamat kihagyása miatt könnyen előfordulhat, hogy a tárolótartályt olyan helyre helyezik el vagy olyan térfogattal tervezik meg, aminek eredményeként az üzem már nem fog megfelelni a 219/2011. (X. 20.) Korm. rendelet 7. mellékletében foglalt kritériumoknak, így a veszélyes tevékenység nem lesz folytatható. Az iterációs folyamat során a mennyiségi kockázatelemzést a tárolótartály specifikumainak ismerete nélkül, általános adatok alapján kell elvégezni.

Magyarország iparbiztonsági szabályozása nagymértékben épül a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló jog-, intézmény- és feladatrendszerre. A Kat. törvény alapján megalakuló egységes iparbiztonsági hatóság szigorú hatósági felügyeletet lát el a preventív munka keretében.[9] Az iterációs folyamat eredményeit ezért javasolt a katasztrófavédelmi-iparbiztonsági hatóság

[9] Vass Gyula – Kátai-Urbán Lajos: Küszöbérték alatti üzemek felügyeletének műszaki előírásai II. rész. *Védelem Tudomány,* 1. (2016), 4. 100–117.

részére bemutatni. A tárolótartály-létesítési koncepció alapján a tervező meg tudja kezdeni a tartály tervezését.

3. A tárolótartály engedélyeztetése

Budapest Főváros Kormányhivatalának egyes ipari és kereskedelmi ügyekben eljáró hatóságként történő kijelöléséről, valamint a területi mérésügyi és műszaki biztonsági hatóságokról szóló 365/2016. (XI. 29.) Korm. rendeletben foglaltak alapján a veszélyes folyadékok és olvadékok – nyomástartó berendezésnek nem minősülő – tárolótartályai és tárolólétesítményei létesítésének engedélyezését hatóságként a fővárosi és a Pest megyei kormányhivatal végzi.

A tárolótartály létesítésének műszaki biztonsági szabályaira a veszélyes folyadékok vagy olvadékok tárolótartályainak, tároló-létesítményeinek műszaki biztonsági követelményeiről, hatósági felügyeletéről az 1/2016. (I. 5.) NGM rendelet ad iránymutatást. A rendelet hatálya kiterjed a veszélyes folyadékok vagy olvadékok tárolótartályainak, tárolólétesítményeinek műszaki-biztonsági hatósági felügyeletéről szóló 216/2019. (IX. 5.) Korm. rendeletben meghatározott tárolótartályok és tárolólétesítmények műszaki biztonságára.

A 216/2019. (IX. 5.) Korm. rendelet 4. pontja vonatkozik a létesítési engedélyezési eljárásra. Ennek alapján az üzemeltetőnek kérelmet kell benyújtania a tárolótartály, tároló-létesítmény létesítésére. A kérelemnek az alábbi fő elemeket kell tartalmaznia:

- általános elrendezési terv a tervezett létesítmény 100 m-es körzetéről;
- műszaki leírás és tervrajzok;
- tervezői nyilatkozat(ok);
- nyilatkozat a mezőgazdasági rendeltetésű földterület termelésből való kivonásáról;
- tervfejezetek, amelyek a vonatkozó szakhatóságok állásfoglalásának kialakításához szükségesek;
- nyilatkozat a létesítés jogosultságáról;
- *a nukleáris létesítmény és a radioaktívhulladék-tároló biztonsági övezetéről szóló 246/2011. (XI. 24.) Korm. rendelet* 7. § (5) bekezdésében meghatározott dokumentum.[10]

A fenti jogszabály rendelkezik arról is, hogy a tárolótartály, tárolólétesítmény létesítését, illetőleg átalakítását követően az üzembe helyezés engedélyköteles, amelynek részleteit külön publikációban tárgyaljuk.

4. Tárólótartály létesítésének második lépése, tervezés

A tervkoncepció elkészültét követően kezdődhet meg a tárolótartály tervezése, amely során a lehetséges legjobb megoldásokkal építjük fel a bekövetkező cselekvéssorozatot.

[10] 216/2019. (IX. 5.) Korm. rendelet.

Ekkor számos befolyásoló, alakító tényezőt kell figyelembe venni. Ilyenek például az emberi tapasztalatok, lehetőségek; a külső környezet, a törvények, szabályok, a közvélemény; illetve a szervezeti kultúra és kapcsolatok.

5. A tervezésre vonatkozó általános előírások

A tárolótartály, tárolólétesítmény műszaki biztonsági követelményeit (tervezés, létesítés, telepítés, üzembe helyezés, karbantartás) illetően az 1/2016. (I. 5.) NGM rendeletben foglaltaknak megfelelően, a Műszaki Biztonsági Szabályzat alapján kell eljárni. Egyenértékű műszaki biztonsági megoldás alkalmazása esetén nyilatkozatok szükségesek a tervezőtől, a kivitelezőtől, a tárolótartály üzemeltetőjétől/tárolólétesítménnyel rendelkezni jogosulttól, hogy az alkalmazott megoldással elérhető és fenntartható a mértékadó műszaki biztonsági szint. Ha a tervezett műszaki megoldásra nemzeti szabvány vagy szakági műszaki előírás hivatkozik és az előírás követelménye teljesül, akkor a rendelet által meghatározott műszaki biztonsági követelményeket teljesítettnek kell venni.

Általános előírásnak vehető, hogy a tárolótartályt, tárolólétesítményt úgy kell megtervezni, kivitelezni és üzemeltetni, hogy az üzemszerű működés esetén sem a kezelő személyzetre, sem a környezetre nem jelenthet veszélyt. Továbbá a biztonságos üzemeltetést a környezeti körülmények nem gátolhatják. Ennek alapja, hogy a berendezés szerkezeti anyagát úgy kell megválasztani, a méretezését úgy kell elvégezni, hogy működése során feleljen meg a tartály, létesítmény feladatának, a normál üzemre jellemző mechanikai, kémiai és hőmérsékleti igénybevételnek, valamint a biztonsági követelményeknek. A tervezés biztonsági követelménye, hogy a tartályt, létesítményt védeni kell az illetéktelen beavatkozástól, illetve a rendszer egészéből származó minden veszélyforrás hatását és azok kölcsönhatásait is figyelembe kell venni. Ha a létesítés megfelel a vonatkozó szabványban vagy szakági műszaki leírásban foglaltaknak, akkor a létesítési előírást teljesítettnek kell tekinteni.

Annak érdekében, hogy az egyes tagországok közötti kereskedelmi akadályokat felszámolhassák, az Európai Közösség Bizottsága 1975-ben akciótervet dolgozott ki, amelynek az Európai Közösséget Alapító Szerződés 95. cikke volt az alapja. Ennek érdekében célul tűzték ki, hogy egységesítik a tartószerkezetek méretezésére vonatkozó műszaki előírásokat. Az Európai Szabványügyi Bizottság (CEN), a tagállamok, valamint az Európai Bizottság között 1989-ben megállapodás született arra vonatkozóan, hogy az Eurocode-ok kidolgozása és közzététele a CEN feladata lesz. Az előírások az 1992–1998 közötti időszakban 64 európai előszabványként, majd ezt követően (2003-tól) európai szabványként, „csomagban" jelentek meg. Azonban a szabványként megjelent Eurocode-ok a tervezéshez, illetve a vizsgálatokhoz szükséges paramétereket sok esetben csak tartalmukban határozzák meg, vagy egy általános értékkel adják meg. Ennek oka, hogy a pontos értékeket az egyes nemzeti hatóságoknak kell megállapítaniuk a rájuk jellemző (például ipari háttér, klimatikus viszonyok, földrajzi helyzet) sajátosságok alapján. Az így meghatározott nemzeti paramétereket, továbbá az Eurocode-ok használatához szükséges magyarázatokat

a Nemzeti Mellékletek tartalmazzák. Ezek a mellékletek a magyar nyelvre lefordított szabványok szerves részét képezik.[11]

A betonszerkezetek használhatósági, tartóssági és tűzállósági követelményeivel kapcsolatban az Eurocode 2 tartalmaz alapelveket és követelményeket. Az Eurocode 2 három részből tevődik össze, az első rész az általános és az épületekre vonatkozó szabályokra, a második rész a szerkezetek tűzhatásra való tervezésére, a harmadik rész pedig a folyadéktartályokra és tárolószerkezetekre vonatkozik. Az Eurocode 3 az acélszerkezetek tervezésére tartalmaz előírásokat, amelyek magukban foglalják az általános szabályokat, a tűzterhelésre való tervezést, a lemezszerkezetek tervezését, a csomópontok tervezését és az anyagok szívósságot és vastagságot illető jellemzőit. Az acél és beton kompozit szerkezetek tervezését illetően az általános szabályokat és a tűzterhelésre való tervezést az Eurocode 4 tartalmazza. A tartályok tervezésénél figyelembe kell venni továbbá az Eurocode 7 (Geotechnikai tervezés) és az Eurocode 8 (Tartószerkezetek tervezése földrengésre) szabványok előírásait is.

Az MSZ 4798:2016 (Beton. Műszaki követelmények, tulajdonságok, készítés és megfelelőség, valamint az EN 206 alkalmazási feltételei Magyarországon) szabványt kell alkalmazni a magas- és mélyépítési, helyszínen készült szerkezetekhez, előregyártott szerkezetekhez és az előregyártott szerkezeti elemekhez gyártott betonokhoz. A szabvány követelményeket határoz meg és ajánlásokat fogalmaz meg az alkotóanyagokra, a beton tulajdonságaira, a tulajdonságok igazolására, az összetétel határértékeire, a friss beton átadására, gyártásellenőrzési eljárásokra, illetve a megfelelőségi feltételekre és azok értékelésére vonatkozólag.[12] A szabvány alapján a beton olyan építőanyag, amelynek tulajdonságai folyamatos változáson mennek keresztül a keverés befejezésétől számítva a beépítés utáni kötésig, szilárdulásig. A beton minőségét befolyásoló tényezők közé tartozik az emberi munka (például a munka minősége) és a környezeti körülmények (például időjárás, talajmechanika) milyensége, amelyek meghatározzák a beton tervezett tulajdonságainak elérését és a rendeltetésszerű használatra érvényes tartósságát a tervezett élettartamára vonatkozóan. A szabványok a beton összetételével kapcsolatos tulajdonságok követelményként való megfogalmazásával (például testsűrűség, cementtartalom, víz–cement tényező), valamint a vasbeton- és feszített vasbetonszerkezetek esetén a betonfedéssel veszik figyelembe a környezeti hatásokat. A megfelelő betonfedés kialakítható a környezeti és a szerkezeti osztály együttes alkalmazása esetén, ekkor a szabványokban előírt követelmények és ajánlások betartásával biztosítható a beton(szerkezet) határértékeknek és tartóssági elvárásoknak való megfeleltetése.[13]

A hegesztett tartályok esetében az API 650-es szabvány követelményeket fogalmaz meg az anyagra, tervezésre, gyártásra, felállításra vonatkozóan az állóhengeres, föld feletti, zárt és nyitott tetejű, különböző méretű, kapacitású és belső nyomású tárolótartályok tekintetében. (További követelmények teljesülése esetén magasabb belső nyomási értékek mellett is.) A szabvány azokra a tartályokra vonatkozik,

[11] Z.E.H. Energetikai és Építőipari Kft.: Eurocode ismertető. (é. n.).

[12] MSZ 4798:2016 Beton. Műszaki követelmények, tulajdonságok, készítés és megfelelőség, valamint az EN 206 alkalmazási feltételei Magyarországon.

[13] Csorba Gábor: *Alkalmazott Betontechnológia – A beton élete a szabványoktól a szerkezetek átadásáig.* Budapest, Forum Média Kiadó Kft., 2018.

amelyeknek az aljzata/fenéklemeze teljes és egyenletes alátámasztással rendelkezik, valamint a maximális hőmérséklete 93 °C. A szabvány célja, hogy az ipar számára megfelelő biztonságú és gazdaságos üzemeltetési tulajdonságokkal rendelkező tartályokat biztosítson a folyékony anyagok tárolásához.[14] A tartályra vonatkozó tervezési és gyártási követelmény, hogy az megfeleljen az MSZ EN 14015:2005 (Folyadékot környezeti és magasabb hőmérsékleten tároló, a helyszínen gyártott, föld feletti, álló, hengeres, sík fenekű, hegesztett acéltartályok tervezési és gyártási előírásai) szabványban, valamint az MSZ EN 1090-es (Acél- és alumíniumszerkezetek kivitelezése. Szerkezeti elemek megfelelőség értékelésének követelményei és Hidegen hajlított szerkezeti acélelemek, valamint tető-, mennyezet-, padló- és falrendszerek hidegen hajlított acélszerkezeteinek műszaki követelményei) szabványcsaládban foglaltaknak.

Abban az esetben, ha a fentiekben ismertetett előírások között ellentmondás van, akkor az alábbi prioritási rendszer szerint kell meghatározni az elsődleges követelményt:

1. Törvények, jogszabályok, valamint a velük harmonizált szabványok.
2. Tervezési dokumentáció.
3. Műszaki leírás követelményei.
4. Projektspecifikáció.
5. Ágazati szakmai szabványok.
6. 6. Ipari gyakorlat

Amennyiben a követelmény nem egyértelmű, vagy az ellentmondás fel nem oldható, akkor a beruházóval és a tervezővel való további egyeztetés eredménye az irányadó.

6. A tervezés során jelentkező iparbiztonsági feladatok

A veszélyes anyagokkal foglalkozó üzem vagy a veszélyes anyagokkal foglalkozó létesítmény építési engedélyezési eljárásával (beleértve a bővítést is) egy időben a hatósághoz benyújtandó biztonsági jelentés/elemzés építési fázisra vonatkozó speciális tartalmi követelményeit a 219/2011. (X. 20.) Korm. rendelet 3., illetve 4. melléklete tartalmazza. Az Üzemeltetőnek be kell mutatnia az alábbi tartalmi elemeket:

- a technológiában alkalmazott biztonsági megoldások (kémiai technológiai, gépészeti és iránytechnikai) értékelése;
- a tervezési filozófia bemutatása: a felhasznált szerkezeti anyag kiválasztása, az alapozás tervezése, nagy nyomáson és magas hőmérsékleten üzemelő berendezések tervezése, a méretezés, a statikai megfontolások, a külső behatás elleni védelem.[15]

A fentiek alapján a katasztrófavédelmi-iparbiztonsági szakértő(k)nek és a tervező(k)nek a tervezés fázisában együtt kell működni, a veszélyes anyag szabadba kerülésének lehetőségeire az ellenintézkedéseket meg kell találni katasztrófavédelmi-iparbiztonsági szempontból a tervezés fázisában javasolt a „What If… (Mi történik, ha…)",

[14] American Petroleum Institute: API Standard 650, Welded Tanks for Oil Storage.
[15] 219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről.

vagy a HAZOP-eljárás alkalmazása. A tartály tervezésére vonatkozó műszaki előírások, szabványok, egyéb ajánlások – mint azt az előző fejezet is bemutatta – számos védelmi szempontot rögzítenek, így elegendő ezek figyelembevételét ellenőrizni, indokolt esetben redundáns feltételrendszert kialakítani. A teljesség igénye nélkül néhány szempont, amelyek a tartály tervezése során figyelembe veendők, valamint ellenőrzendők:

- Tárolandó anyag fizikai, kémiai tulajdonságai. A tartálytervezés alapfeltétele a tárolandó folyadék fizikai, kémiai tulajdonságainak pontos ismerete. Javasolt már üzemelő tartályokkal kapcsolatos szakirodalom áttanulmányozása, a gyártói tapasztalatok kikérése, ajánlások figyelembevétele. A tárolandó folyadék tulajdonságai meghatározzák többek között a felhasznált szerkezeti anyag kiválasztását, valamint az alkalmazandó védelmi infrastruktúrát (például úszótető, nitrogénpárna, automata oltóberendezés stb.).
- Külső környezet. A terület sajátosságainak feltárása – például geotechnikai vizsgálatok, szeizmikus jellemzők, ár- és belvíz veszélyeztetés stb. – alapján kell az alapozást megtervezni, szilárdsági számításokat elvégezni. Ellenőrizendő többek között a figyelembe vett szélterhelés és hóterhelés nagysága, a talajvízszint változása miatti esetleges tartályfelúszás veszélye, valamint a földrengésveszélyre vonatkozó számítások.
- Belső dominóhatás. A tartály elhelyezésére vonatkozóan számos jogszabály – többek között az Országos Tűzvédelmi Szabályzatról szóló 54/2014. (XII. 5.) BM rendelet – tartalmaz általános előírásokat, amelyek a belső dominóhatás bekövetkezésének csökkentése céljából a létesítmények, építmények között védőtávolságokat határoznak meg. A biztonsági jelentésben, biztonsági elemzésben a veszélyes anyagokkal kapcsolatos súlyos baleset által való veszélyeztetés értékelése során belső dominóhatás kialakulásának lehetőségét figyelembe kell venni. Amennyiben a mennyiségi kockázatelemzés eredménye indokolja, a belső dominóhatás bekövetkezési valószínűségének csökkentésére megelőző intézkedést kell hozni. Megelőző intézkedés lehet például a tartályvédőgyűrű-magasság megemelése, külső nyomásra való méretezése, annak érdekében, hogy a belső tartály számára a külső lehetséges hatások – repeszhatás, túlnyomás, hősugárzás – esetén teljes védelmet biztosítson.
- Biztonságos üzemeltetéshez szükséges műszaki és folyamatirányítási feltételek. A tervezés során elkészül a tartálylétesítés engedélyezési dokumentációja, amely egy komplex tervdokumentum. A létesítési engedélyezési terv tartalmazza a tervezett tartály általános ismertetését – a tartály rendeltetése, feladata, telepítés, nyomáshatárolás, anyagminőség, műszaki adatok, tartályfenék-kialakítás, tartályköpeny, merevtető és acélszerkezetek kialakítása, kezelő-, járófelületek, menekülési utak, csonkok, nyílások, műszercsatlakozások, tűzvédelmi felszerelések, hőszigetelés, villámvédelem, földelés stb. részeket –, valamint a tartály gyártására és létesítésére vonatkozó – tartályelemek előgyártása, hegesztés, roncsolásmentes varratvizsgálatok, hegesztés utáni hőkezelés, helyszíni szerelési előírások, szerkezeti vizsgálat, vízpróba, tartály kalibrálása, felületvédelem, szállítás, tárolás – előírásokat. A komplex tervdokumentáció további részei a szilárdsági számítások bemutatása, a különböző rajzok (helyszínrajz,

csőkapcsolási rajz), valamint a szakági, többek között a mélyépítésre, a statikára, az irányítástechnikára, a tűzjelzésre és -oltásra, a villamosenergia-ellátására vonatkozó tervek. A létesítési engedélyezési tervdokumentáció készítése során a katasztrófavédelmi-iparbiztonsági szakértőnek, valamint a tervezőnek javasolt a már korábban említett „What If… (Mi történik, ha…)" vagy a HAZOP módszerrel ellenőrizni, hogy az összes lehetséges meghibásodásra a tervekben megtörtént-e ellenintézkedés megtétele. A vizsgálat során ki kell térni a tartályhoz közvetlenül kapcsolódó technológiákra, a tartály töltésére és a tartályban lévő alapanyag felhasználásának útvonalára. A teljesség igénye nélkül néhány fontosabb szempont a tervezett műszaki megoldások és monitoring ellenőrzéséhez: kapcsolódó csővezetékek, vibráció, rezgés, hőtágulás, tartályfenék-lyukadás jelzése, tartályban lévő belső nyomás, túlnyomás, vákuum, túltöltés, belső hőmérséklet, tartályszivárgás, tűzjelzés. Javasolt ellenőrizni, hogy a tervezett műszaki megoldás, monitoring, védelem meghibásodására vonatkozóan érkezik-e jelzés az üzemelést majd felügyelő operátorhelyiségbe. A tervezés során az esetleges meghibásodások következményei csökkentésének lehetőségeire is műszaki megoldást kell találni, például a belső tartálysérülés esetén a védőgyűrűbe került veszélyes anyag eltávolítására. Műszaki megoldás lehet a védőgyűrűbe beépített lezárt (leblindelt) ürítő vezeték, amely esetén ad hoc jelleggel, akár egy flexibilis vezeték kapcsolódása révén, végrehajtható a védőgyűrűbe került veszélyes anyag kitárolása.

A létesítési tervdokumentációnak nem része a folyamatirányítás pontos szabályozása, ugyanakkor már ajánlást kell megfogalmazni a kiépítendő műszerek, kontrollberendezések körére. A létesítési terv alapján kiviteli terv készül, amely minden munkarészre kiterjedően, az építők, szerelők, gyártók számára kellő részletességgel tartalmazza a szükséges információkat, utasításokat. A kiviteli tervezés, az üzembe helyezés (használatbavétel, veszélyes tevékenység engedélyezése), az üzemeltetés (beleértve a karbantartást), valamint a felszámolás kérdéseivel a következő publikációban foglalkozunk.

7. Összefoglalás

A veszélyesanyag-tárolótartály létesítése szigorú jogszabályi feltételekhez kötött, a létesítését megelőzően létesítési engedélyezési terv készül. A „Budapest Főváros Kormányhivatalának egyes ipari és kereskedelmi ügyekben eljáró hatóságként történő kijelöléséről, valamint a területi mérésügyi és műszaki biztonsági hatóságokról" szóló 365/2016. (XI. 29.) Korm. rendeletben foglaltak alapján a veszélyes folyadékok és olvadékok – nyomástartó berendezésnek nem minősülő – tárolótartályai és tárolólétesítményei létesítésének engedélyezését hatóságként a fővárosi és megyei kormányhivatal végzi.

A katasztrófavédelmi-iparbiztonsági szakértőnek már a létesítési engedélyezési terv készítését megelőzően feladata van, az üzemeltető általi elgondolások megvalósíthatóságának – tartályméret, -elhelyezés, tartálytípus – ellenőrzése, alapadatszolgáltatás

a tartálytervező részére. Az alapadatszolgáltatás egy iterációs folyamat eredménye, számos üzemeltetői elgondolás elemzése. Tapasztalat szerint már ezen eredmények birtokában javasolt a katasztrófavédelmi-iparbiztonsági hatóság – mint önálló hatóság – megkeresése, tájékoztatása.

Az elkészült létesítési engedélyezési tervben foglaltakat a tervezőnek és a katasztrófavédelmi-iparbiztonsági szakértőnek „What If… (Mi történik, ha…)" vagy a HAZOP módszerrel javasolt ellenőrizni, felülvizsgálni, indokolt esetben további szükséges kockázatcsökkentő műszaki megoldásokat alkalmazni.

Bár a tartály létesítése nem minősül hagyományos értelemben vett építési engedélyezési eljárásnak, ugyanakkor a létesítési engedélyezési terv alapján javasolt a katasztrófavédelmi-iparbiztonsági hatóság részére engedélyezési dokumentáció elkészítése és vizsgálat lefolytatása, annak érdekében, hogy a szükséges üzemeltetői döntések, intézkedések még időben meghozhatók legyenek.

Felhasznált irodalom

Committee for the Prevention of Disasters – TNO (Purple Book): Guidelines for Quantitative Risk Assessment. CPR 18E. The Director-General of Labour, The Netherlands, 1999.

Cimer Zsolt – Kátai-Urbán Lajos – Vass Gyula: Katasztrófakockázatok: a településrendezési tervezés szerepe a megelőzésben. In Hábermayer Tamás (szerk.): Katasztrófák, kockázatok, önkéntesek. Szekszárd, Tolna Megyei Katasztrófavédelmi Igazgatóság, 2020. 56–63. Online: https://tolna.katasztrofavedelem.hu/application/uploads/documents/2020-05/71152.pdf

Cimer Zsolt – Szakál Béla – Kátai-Urbán Lajos – Sárosi György – Vass Gyula: Iparbiztonsági szakismeretek. Módszertani kézikönyv a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezéssel foglalkozó gyakorló szakemberek részére. Hungária Veszélyesáru Mérnöki Iroda Kft., 2020.

European Comission: *JRC Science Hub, MINERVA Portal.* Online: https://emars.jrc.ec.europa.eu/en/emars/statistics/statistics

Csorba Gábor: Alkalmazott Betontechnológia – A beton élete a szabványoktól a szerkezetek átadásáig. Budapest, Forum Média Kiadó Kft., 2018.

Kátai-Urbán, Lajos – Zsolt Cimer – Ádám Berger: Remediation board versus protective ring. Fire Engineering & Disaster Management Prerecorded International Scientific Conference, 2021. Online: http://vedelem.hu/hirek/0/3259#K%C3%A1tai-Urb%C3%A1n,%20L-Cimer,%20Zs-Berger,%20%C3%81:%20Remediation%20board%20versus%20protetctive%20ring

MSZ 4798:2016 Beton. Műszaki követelmények, tulajdonságok, készítés és megfelelőség, valamint az EN 206 alkalmazási feltételei Magyarországon. Online: https://tinyurl.hu/i4P2/

Vass Gyula – Kátai-Urbán Lajos: Küszöbérték alatti üzemek felügyeletének műszaki előírásai II. rész. Védelem Tudomány, 1. (2016), 4. 100–117. Online: http://vedelemtudomany.hu/articles/08-vass-katai.pdf

Jogi források

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről
216/2019. (IX. 5.) Korm. rendelet a veszélyes folyadékok vagy olvadékok tárolótartályainak, tároló-létesítményeinek műszaki-biztonsági hatósági felügyeletéről

Internetes források

American Petroleum Institute: API Standard 650. Welded Tanks for Oil Storage. Online: www.api.org/~/media/Files/Publications/Whats%20New/650%20e12%20PA.pdf
Képek © CNES / Airbus, Landsat / Copernicus, Maxar Technologies, 2021: Budapest, XXI. kerület. Online: www.google.hu/maps/place/Budapest,+XXI.+ker%C3%BClet/@47.4327508,19.0627636,2853m/data=!3m1!1e3!4m5!3m4!1s0x4741e7ee650b9249:0x500c4290c1ed680!8m2!3d47.4243579!4d19.066142?hl=hu
Z.E.H. Energetikai és Építőipari Kft.: Eurocode ismertető. Online: www.tartalyhaz.hu/Blog%20Posts/az-eurocode-az-epuletek-tartoszerkezeteinek-meretezesere-vonatkozo-europai-szinten-harmonizalt-szabvanycsomag.html

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
16. évfolyam (2021) 3. szám 97–118.
DOI: 10.32567/hm.2021.3.6

Herczeg Gergely,[1] Bérczi László[2]

Gyermekek és fiatalok szűkítésen keresztüli áramlásának vizsgálata

Examining Children's and Youth's Flow through a Bottleneck

A gyermekek és a fiatalok menekülőképessége különbözhet a felnőttek menekülőképességétől. A menekülőképesség vizsgálatára a leggyakrabban felnőtt résztvevőkkel kerül sor, azonban fontos lenne tudni, hogy mennyiben tér el a gyermekek és fiatalok menekülőképessége attól, amit a felnőtt populáció adatai alapján határoznak meg. A menekülőképesség egyik tényezője a szűkítések átbocsátókapacitása. Kiürítési számítás során az átbocsátóképességet egyetlen fix értékkel veszi figyelembe a hatályos tűzvédelmi műszaki irányelv, nincs külön érték megállapítva gyermekek és felnőttek vonatkozásában. Az épületben tartózkodó személyek biztonsága függ attól, hogy az épület kiürítése meg tud-e történni addig, amíg a menekülő személyek életfeltételei adottak. A szerzők vizsgálat tárgyává tették a gyermekek menekülőképességét, amit ebben a cikkben foglalnak össze. A tanulmány a menekülőképesség egy aspektusát vizsgálja, amely a szűkítések átbocsátóképessége, jóllehet a menekülőképesség nem csupán ettől függ. A menekülőképesség egyéb tényezőinek vizsgálata további kutatás tárgya lehet. A szerzők e cikkben számolnak be a kutatás során végzett megfigyeléseikről, méréseikről. Bemutatják továbbá a szűkítéseken keresztüli gyalogosáramlásra vonatkozó hazai és nemzetközi szakirodalmat. Ez a kutatás megteremti annak lehetőségét, hogy kiderüljön, érdemes-e eltérő értéket megállapítani a kiürítési számítások során alkalmazandó átbocsátóképességre külön gyermekekre és felnőttekre vonatkozóan, továbbá lehetőséget ad további vizsgálatok megalapozására.

Kulcsszavak: **gyermekek menekülőképessége, gyalogosáramlás, kiürítés, kiürítési számítás, átbocsátóképesség**

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktori hallgató, e-mail: herczeggergely@gmail.com
[2] BM Országos Katasztrófavédelmi Főigazgatóság, országos tűzoltósági főfelügyelő, e-mail: berczi.laszlo@katved.gov.hu

Children and adults may have different evacuation capability. Evacuation capability is most often examined with adult participants. However, it would be important to know, how the children's and youth's evacuation capability differs from that determined based on data from adult population. The flow rate is one of the elements of the evacuation capability. During the evacuation calculation, the flow rate is considered with a single fixed value in the current Fire Protection Safety Guideline. There is no different value for children and adults. The safety of people in the building depends on whether the building can be evacuated as long as the living conditions are given inside the building. The author has examined the evacuation capability of children, which is summarised in this article. The author has examined one aspect of evacuation capability, which is the flow rate through a bottleneck. Although evacuation capability does not depend solely on this. Examination of other factors of evacuating capability may be the subject of further research. In this paper the author reports on his observations and measurements during the research and also presents the Hungarian and international literature related with adult's and children's flow rate through a bottleneck. This research provides an opportunity to see if it is worthwhile to establish a separate value for the flow rate through a bottleneck to be used in evacuation calculations for children and adults separately; and it provides an opportunity to substantiate further investigations.

Keywords: **evacuation capability of children, pedestrian flow, evacuation, evacuation calculation, unit width flow rate**

1. Bevezetés

A gyermekek és fiatalok menekülőképességének meghatározása módot ad a felnőttekkel mért adatokkal való összehasonlításra. Ezáltal lehetőség nyílik arra, hogy jobban megismerjük a populáció egyes csoportjainak menekülőképességét és pontosabb adatok álljanak rendelkezésre a kiürítési számításhoz. Ebben a cikkben a menekülőképesség több mérhető tényezője közül a szerzők csak a szűkítések átbocsátóképességét vizsgálták. A menekülőképesség további tényezőinek és a kiürítés komplex rendszere egészének vizsgálata nem volt tárgya e kutatásnak.

Nem tárgya e kutatásnak a kiürítési számításhoz szükséges további adatok (mint például a haladási sebesség) elemzése, az átmeneti védett terek, a kiürítési irányok, a viselkedési és magatartási befolyásoló tényezők vizsgálata. Nem foglalkoznak a szerzők ebben a cikkben az átbocsátóképesség mérési módszereinek fejlesztésével és egységesítésével sem.

Lehetséges, hogy a gyermekekkel és fiatalokkal vizsgálva a szűkítések átbocsátóképessége eltér a felnőttekkel mért értéktől. Cél, hogy meghatározzák a szerzők az épületek kiürítési útvonalán lévő szűkítések (mint például ajtók) átbocsátóképességét önállóan menekülő gyermekek és fiatalok vonatkozásában. A gyermekekkel és fiatalokkal meghatározott átbocsátóképesség alkalmazása kiterjeszthető más olyan gyalogosáramlási helyzetekre, amelyek során nem épületekből menekülnek személyek, hanem például járművekből vagy a szabadból, akkor, ha az ottani viszonyok nem különböznek lényegesen az épületekben tapasztalható jellegzetességektől.

Az szolgálja az épületekben tartózkodók életének védelmét és biztonságát, ha veszély (például tűz) esetén az épületből biztonságosan ki tudnak menekülni. Az Országos Tűzvédelmi Szabályzatról szóló 54/2014. (XII. 5.) BM rendelet állapítja meg a tűzeseti menekülés feltételeinek elvárt biztonsági szintjét, valamint a tűzvédelmi követelmények megvalósításának célját.[3] A tűzvédelmi követelmények egyik célja az életvédelem, amely célhoz hozzátartozik, hogy biztosítva legyen az épületben tartózkodók menekülése, valamint a menekülés során az életfeltételek.[4] Biztosítani kell az épületben tartózkodók részére, hogy menekülés esetén meghatározott időn vagy – geometriai módszer alkalmazása esetén – távolságon belül biztonságba (például a szabadba) jussanak.[5] Az épület kialakítása lehetővé kell tegye, hogy elégséges átbocsátóképességű kijáraton elhagyhassák tartózkodási helyüket a bent tartózkodó személyek a kiürítés első szakaszában.[6] A kiürítési számítás a kiürítés tervezésének egyik megengedett módja.[7] Kiürítési számítással igazolható a kiürítésre előírt normaidők teljesülése.[8] Tűzvédelmi műszaki irányelv tartalmazza a kiürítési számítás leírását és szabályait.[9] Ennek a számításnak része annak meghatározása, hogy a kiürítés során bejárt útvonalon lévő szűkítéseken (például ajtók) hány személy tud a megengedett idő alatt áthaladni. Az irányelvben meghatározott átbocsátóképességet lehet figyelembe venni a számítás során, ennek értéke 41,7 fő/(min·m).[10] Ez az érték az össznépesség átlagos menekülőképességén alapul, figyelembe véve a csökkent mozgásképességű, de önállóan menekülni képes személyek lassító hatását is.[11] Figyelembe kell venni, hogy az előbbi érték csak önállóan menekülni képes személyek vonatkozásában használható.[12]

Önállóan menekülésre képes személynek tekinti a jogszabály azt, aki önállóan vagy esetleg kiegészítő irányítás mellett képes a menekülésre. Jogszabály szerint menekülésben korlátozott az a személy, aki életkora – 0–10 éves vagy 65 év feletti –, értelmi, vagy fizikai-egészségi állapota alapján nem képes az önálló menekülésre. Az olyan menekülésben korlátozott személy, aki fizikai segítség vagy irányítás mellett képes a menekülésre, segítséggel menekülő személynek tekintendő.[13] A kényszertartózkodás menekülésre gyakorolt hatását jelen kutatás nem vizsgálja.

Tehát a 10 év alatti gyermekek olyan menekülésben korlátozott személyek, akik segítséggel menekülő személynek tekinthetők, ha annak feltételei adottak. A 6–10 év közötti gyermekek segítséggel menekülőnek tekinthetők.[14]

Az átbocsátóképesség definíciója: az egységnyi szabad szélességű szűkítésen egységnyi idő alatt áthaladni képes személyek maximális száma.[15]

A gyalogosáramlást az alábbi alapegyenlettel jellemezhetjük:

[3] 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról.
[4] 54/2014. (XII. 5.) BM rendelet 5. §.
[5] 54/2014. (XII. 5.) BM rendelet 6. §.
[6] 54/2014. (XII. 5.) BM rendelet 51. §.
[7] 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról 52. §
[8] 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról 63. §
[9] TvMI 2.3:2020.01.22. Tűzvédelmi Műszaki Irányelv – Kiürítés.
[10] TvMI 2.3:2020.01.22. 6.3.8.2.
[11] TvMI 2.3:2020.01.22. 6.1.5.
[12] TvMI 2.3:2020.01.22. 6.1.6.
[13] 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról 4. §.
[14] TvMI 14.1:2020.01.22 3.4.2. c) Tűzvédelmi Műszaki Irányelv – Kockázati osztályba sorolás.
[15] TvMI 2.3:2020.01.22. 2.2.1.

$q = v \cdot d$, ahol
q az átbocsátóképesség [fő/(s·m)];
v az áramlás sebessége [m/s];
d a létszámsűrűség [fő/m²].[16]

A kiürítési útvonalon elhelyezett szűkítések egyik oldalán nagyobb létszámsűrűség adódik, míg a másik oldalán kisebb a létszámsűrűség, mivel a továbbhaladás nagyobb keresztmetszeten lehetséges; ez a szűkítések torlasztó hatása.

A szűkítések átbocsátóképességével, gyalogosáramlást befolyásoló hatásával több kutatás is foglalkozott. Beljajev vezette az Orosz Művészeti Akadémia Építészeti Kutatóintézete kutatását, amelyben több mint 200 mérés alapján határozták meg a kiürítési számításhoz használt szabványosított adatokat és a számítás rendszerét.[17] Az adatokat 1938-ban publikálták, ezáltal ez az egyik legrégebbi forrás, ami a szűkítések átbocsátóképességével foglalkozik. Az előbbi kutatásban 25–50 fő haladt át egy 0,6 m szélességű kijáraton percenként. A legkedvezőtlenebb 25 fő/min érték alkalmazását javasolták, mivel az értékek jelentős szórást mutattak.[18] Ezen érték alkalmazását Magyarországon 30 évvel az adat publikálását követően, 1968-ban vezették be, amely kerekítve 41,7 fő/(min·m), és mind a mai napig ez az irányelvben rögzített érték a kiürítési számításhoz.[19]

Korábbi kutatásaikban a szerzők megállapították, hogy a kiürítési számításhoz alkalmazott átbocsátóképesség által meghatározottnál nagyobb átbocsátás is lehetséges kijáratokon.[20]

Elég sok kutatásban foglalkoztak már az átbocsátóképesség meghatározásával, de ezek közül kevés az, amely gyermekek bevonásával vagy kizárólag gyermekekkel történt vizsgálatokon alapul.

A jellemzően kisebb testméretekkel rendelkező 3–5 éves gyermekekkel végzett kísérletek során lineáris összefüggést találtak az áramlás erőssége és a szűkítés szélessége között:

$J = 5{,}11x - 0{,}95$, ahol
J az áramlás erőssége [fő/s];
x az ajtó szabad szélessége [m].[21]

2018-ban publikált chilei kísérletek során 1,45–3,24 fő/(s·m) (87–194,4 fő/[min·m]) átbocsátóképességet mértek kijárati ajtókon, 3–18 éves tanulók vegyes csoportján.[22]

[16] Peter Thompson et al.: Evacuation Models are Running Out of Time. *Fire Safety Journal,* 78. (2015), 252.
[17] Sz. V. Beljajev: *Evakuacija zdanyij masszovovo naznacsenyija.* Moszkva, Izdatyelsztvo Vszeszojuznoj Akagyemii Arhityekturi, 1938. 3.
[18] Sz. V. Beljajev: *Evakuacija zdanyij masszovovo naznacsenyija.* Moszkva, Izdatyelsztvo Vszeszojuznoj Akagyemii Arhityekturi, 1938. 38.
[19] TvMI 2.3:2020.01.22.
[20] Herczeg Gergely – Bérczi László: Közösségi rendeltetésű épületek kiürítési gyakorlatainak tapasztalatai. *Védelem Tudomány,* 4. (2019), 2. 84–103.
[21] Hongliu Li et al.: A Comparative Study on the Bottleneck Flow between Preschool Children and Adults under Different Movement Motivations. *Safety Science,* 121. (2020), 30–41.
[22] Alan Poulos et al.: Validation of an Agent-based Building Evacuation Model with a School Drill. *Transportation Research Part C: Emerging Technologies,* 97. (2018), 82–95.

Óvodás korú gyermekeken megfigyelték, hogy akár 4,615 fő/(s·m) átocsátást is el tudnak érni szűkítéseken való áthaladáskor. Ezt azzal magyarázták, hogy a gyermekek – kisebb testméreteikből adódóan – kisebb helyet foglalnak el.[23]

A szűkítések átbocsátóképessége, 4–12 éves gyermekekkel végzett kísérletek alapján, egy kutatás szerint átlagosan 1,6 fő/(s·m).[24]

Holland kutatók által végzett kísérletek alapján az átbocsátóképességet 3,31 fő/(s·m) értékben állapították meg. A vizsgálatban részt vevő személyek életkori megoszlása: 90%-uk 11 éves, míg 10%-uk 18–65 év közötti volt. Ez a minta volt hivatott az általános iskolában tartózkodó személyeket reprezentálni.[25]

A kifejezetten gyermekekkel végzett kutatások kis száma mellett igen sok forrás tartalmaz felnőttekkel végzett kísérletekre és megfigyelésekre alapozott adatokat a szűkítések átbocsátóképességére vonatkozóan.

Predtechenskii és Milinskii 1978-ban publikált kísérletei szerint a szűkítések átbocsátóképessége a 1,6 fő/(s·m) (azaz 96 fő/[min·m]).[26]

A szűkítés átbocsátóképessége 1,74 fő/(s·m) (azaz 104,4 fő/[min·m]) értékre adódott Kretz és munkatársai kísérleteiben, amelyet 0,7 m széles és 0,4 m hosszú szűkítésen mértek.[27]

Egy kutatás szerint az ajtók átbocsátóképessége sportcsarnok kiürítésénél végzett megfigyelések alapján 0,92 fő/(s·m).[28]

Seyfried és munkatársai a szűkítések átbocsátóképességét 1,61 fő/(s·m) (azaz 96,6 fő/[min·m]) értékben állapították meg egy 80 cm széles, 2,8 m hosszú szűkítésen áthaladó személyekkel végzett kísérlet alapján.[29]

DiNenno 2012-ben publikált adatai szerint a szűkítések átbocsátóképessége 1,3 fő/(s·m) (azaz 78 fő/[min·m]).[30]

Egy 2014-ben publikált kutatásban megállapították: ha a kijáratok összesített szélessége állandó, a kijáratok számának növelésével a kijáratok átbocsátóképessége csökken. Az áramlás erőssége és a kijárat szélessége között nemlineáris összefüggést találtak:

$$J = 1{,}287x^2 + 0{,}267\ x + 0{,}5538, \text{ ahol}$$
J az áramlás erőssége [fő/s];
x az ajtó szabad szélessége [m].[31]

[23] Yishu Yao – Wei Lu: Children's Evacuation Behavioural Data of Drills and Simulation of the Horizontal Plane in Kindergarten. *Safety Science,* (2021), 133. 105037.

[24] Glenn N. Hamilton – Patrick F. Lennon – John O'Raw: Toward Fire Safe Schools: Analysis of Modelling Speed and Specific Flow of Children During Evacuation Drills. *Fire Technology,* 56. (2020), 605–638.

[25] W. Daamen – S. P. Hoogendorn: Emergency Door Capacity: Influence of Door Width, Population Composition and Stress Level. *Fire Technology,* 48. (2012), 1. 55–71.

[26] V. Predtechenskii – A. I. Milinskii: *Planning for Foot Traffic Flow in Buildings.* Washington D.C., National Bureau of Standards, US Department of Commerce, and the National Science Foundation, 1978.

[27] Tobias Kretz – Anna Grünebohm – Michael Schreckenberg: Experimental Study of Pedestrian Flow through a Bottleneck. *Journal of Statistical Mechanics: Theory and Experiment,* (2006), 10. P10014.

[28] S. M. V. Gwynne et alii: Questioning the Linear Relationship between Doorway Width and Achievable Flow Rate. *Fire Safety Journal,* 44. (2009), 1. 80–87.

[29] Armin Seyfried et al.: Empirical Data for Pedestrian Flow through Bottlenecks. *Traffic and Granular Flow'07*. Berlin, Springer, 2009. 189–199.

[30] Philip J. DiNenno et alii: *SFPE Handbook of Fire Protection Engineering*. Quincy, National Fire Protection Association, 2012. 3-371 (905).

[31] Shuai Wang et al.: Setting the Width of Emergency Exit in Pedestrian Walking Facilities. *Procedia – Social and Behavioral Sciences,* 138. (2014), 233–240.

Lineáris kapcsolatot állapított azonban meg egy másik kutatás 1100–2200 mm szélességű gyalogosáramlásoknál az áramlás szabad szélessége és az áramlás erőssége között:

$J = 1{,}55x + 0{,}257$, ahol
J az áramlás erőssége [fő/s];
x az áramlási keresztmetszet szabad szélessége [m].[32]

86 fiatal hallgatóval végeztek kísérletet, ahol a résztvevők átlagéletkora 21,7 év, átlagos testmagasságuk 1,69 m volt. A kísérleteket elvégezték úgy, hogy a résztvevők futva haladtak át a szűkítésen, és úgy is, hogy csak sétáltak. Futva haladó résztvevőkkel az alábbi lineáris összefüggést állapították meg a szűkítés szélessége és az áramlás erőssége között:

$J_r = 2{,}55x + 0{,}27$, míg sétáló résztvevőkkel
$J_w = 2{,}08x + 0{,}17$ összefüggés adódott, ahol
J az áramlás erőssége [fő/s];
x az ajtó szabad szélessége [m].[33]

Egy 2018-as kísérlet szerint, a kijárat szélessége és átbocsátóképessége nem egyenesen arányos. Ezt pánikhelyzetben lévő egereken figyelték meg. Mivel az egerek stresszre adott válaszreakciói hasonlítanak az emberi viselkedésre, így az egerek alkalmas helyettesítői az embereknek a pánikhelyzeti menekülés vizsgálatánál.[34]

Az átbocsátóképességet mérték kísérletek során tömegközlekedési járművek ajtóin, és megállapították, hogy 600–2000 mm közötti szélességű ajtókon az átbocsátóképesség 1,822–2,061 fő/(s·m).[35]

Az NFPA 130 (2017) tűzvédelmi irányelv *(National Fire Protection Association, USA)* szerint vasútállomások kiürítésének tervezésekor, kétszárnyú kijárati ajtóknál, 81,9 fő/(min·m) átbocsátóképesség vehető figyelembe.[36]

20–55 év közötti életkorú felnőttek 80 fős mintáján végzett kísérlet eredményei szerint egy 0,72 m széles ajtó átbocsátóképessége 1,01–2,41 fő/s. Az átbocsátóképesség egységnyi szélességre átszámított értéke az előbbi adatok alapján 84,17–200,83 fő/(min·m). Az értékek nagyobb szórását magyarázhatja, hogy a kísérleteket eltérő magatartású csoportokkal végezték. Volt, hogy a résztvevőket előzékeny magatartásra kérték fel a kísérlet előtt, míg máskor az volt az előírt magatartás, hogy ne fordítsanak figyelmet az előzékenységre.[37]

[32] Kosuke Fujii – Tomonori Sano: Experimental Study on Crowd Flow Passing Through Ticket Gates in Railway Stations. *Transportation Research Procedia,* 2. (2014), 630–635.
[33] Xiangxia Ren – Jun Zhang – Weiguo Song: Flows of Walking and Running Pedestrians in a Corridor through Exits of Different Widths. *Safety Science,* 133. (2021), 105040.
[34] Teng Zhang et al.: Collective Behavior of Mice Passing Through an Exit under Panic. *Physica A: Statistical Mechanics and its Applications,* 496. (2018), 233–242.
[35] Rodrigo Fernández – Alejandra Valencia – Sebastian Seriani: On Passenger Saturation Flow in Public Transport Doors. *Transportation Research Part A,* 78. (2015), 102–112.
[36] NFPA 130: Standard for Fixed Guideway Transit and Passenger Rail Systems. 5.3.7.1. 2020.
[37] Alexandre Nicolas – Sebastián Bouzat – Marcelo N. Kuperman: Pedestrian Flows through a Narrow Doorway: Effect of Individual Behaviours on the Global Flow and Microscopic Dynamics. *Transportation Research Part B: Methodological,* 99. (2017), 30–43.

Pastor és munkatársai szerint a szűkítések átbocsátóképessége 2,43–2,63 fő/(s·m) (azaz 145,8–157,8 fő/[min·m]), amit egy 69 cm-es szűkítésen végzett megfigyelés alapján írtak le.[38]

Huang és munkatársai a színházakban, mozikban, lelátókon jellemző, széksorok közötti 0,4–0,6 m széles közlekedőn történő haladást vizsgálták. Megállapították, hogy a szűk közlekedő átbocsátóképessége 2,5–4,29 fő/(s·m) (azaz 150–257,4 fő/[min·m]).[39]

A kiürítés számítógépes modellezése során – külföldi adatok alapján – egységes értéket alkalmaznak a szűkítések átbocsátóképességére, amely érték jellemzően 80 fő/[min·m].[40]

A szűkítések átbocsátóképességére Magyarországon is egyetlen, egységes érték van használatban.

Egy 2015-ben publikált kutatás szerint a nemzetközileg általános 1,33 fő/(s·m) átbocsátóképesség-érték csökkentése javasolt 36%-kal 0,85 fő/(s·m) értékre. Ennek okaként a kutatásban a túlsúlyos személyek és a mozgássérültek arányának növekedését jelölték meg az eredetileg alkalmazott értéket megalapozó kutatások óta eltelt időre vonatkoztatva.[41]

A szűkítések előtt elhelyezett akadály – bizonyos esetekben – növelheti is az átbocsátóképességet. Egy kutatásban vizsgálták, hogy a helyiségen belül, a kijárati ajtó előtt elhelyezett megfelelő méretű és helyzetű oszloppal a kijárat átbocsátóképessége növelhető, különösen akkor, ha a helyiség egyik sarkában helyezték el a kijáratot. Ha az ajtó nem a helyiség sarkán volt elhelyezve – oszlop nélkül – az ajtó átbocsátóképessége 2,67 fő/(s·m) értékre adódott átlagosan 1,31 m/s sebességgel haladó személyekkel, 1,2 m széles ajtón mérve. Az átbocsátóképesség 3,18 fő/(s·m) értékre növekedett a helyiség sarkában elhelyezett kijárattal és megfelelő méretű és helyzetű oszlop alkalmazásával.[42]

A University of Melbourne helyszínén, 60–120 cm-es szűkítéseken áthaladó személyekkel, 114 fő részvételével végeztek kísérletet. E kísérlet alapján a szűkítések átbocsátóképessége: 1,67–3,93 fő/(s·m) (azaz 100,2–235,8 fő/[min·m]).[43]

A szakirodalomban fellelhető egyik legnagyobb – kísérletekkel alátámasztott – átbocsátóképesség 3,7 fő/(s·m) (azaz 222 fő/[min·m]).[44]

Az 1. ábra mutatja be a különböző források szerinti fajlagos átbocsátóképesség értékeit. Ahol rendelkezésre álltak a kísérletek körülményeinek részletei, ott azokat az előbbiekben ismertettük.

[38] José M. Pastor et al.: Experimental Proof of Faster-is-slower in Systems of Frictional Particles Flowing through Constrictions. *Physics Rev. E,* 92. (2015), 6. 062817.

[39] Shenshi Huang et al.: Experimental Study on Occupant Evacuation in Narrow Seat Aisle. *Physica A: Statistical Mechanics and its Applications,* 502. (2018), 506–517.

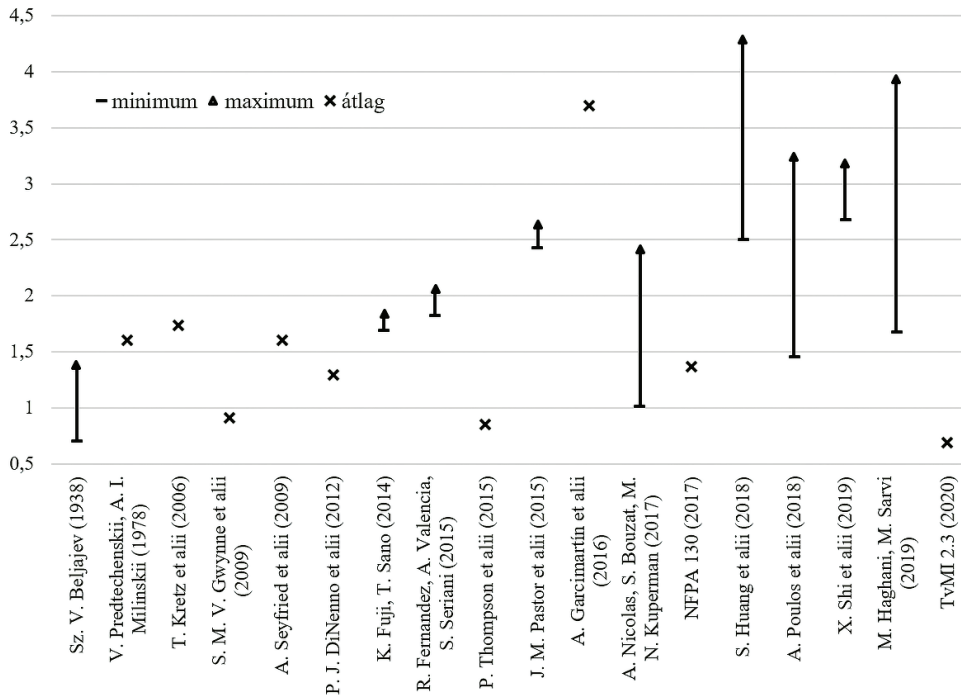
[40] Thompson et al. (2015): i. m. 252.

[41] Thompson et al. (2015): i. m.

[42] Xiaomeng Shi et al.: Examining Effect of Architectural Adjustment on Pedestrian Crowd Flow at Bottleneck. *Physica A: Statistical Mechanics and its Applications,* 522. (2019), 350–364.

[43] Milad Haghani – Majid Sarvi: Simulating Pedestrian Flow through Narrow Exits. *Physics Letters A,* 383. (2019), 2–3. 110–120.

[44] Angel Garcimartín et al.: Flow of Pedestrians through Narrow Doors with Different Competitiveness. *Journal of Statistical Mechanics: Theory and Experiment,* (2016), 4. 043402.



1. ábra

Az átbocsátóképesség fajlagos értékei különböző források szerint [fő/(s·m)]

Forrás: a szerzők szerkesztése

A hazai és nemzetközi szakirodalomban fellelhető vonatkozó adatokat eltérő körülmények és kísérleti feltételek alapján határozták meg, ezt az összehasonlításukkor figyelembe kell venni. Mivel nincs egységesített mérési módszer, így kényszerűségből a következtetéseket a rendelkezésre álló adatokból lehet és kell levonni. Több esetben nem tartalmazta a forrás a kísérlet egyes körülményeit, ahol igen, azok alapján megállapíthatjuk, hogy eltérő volt a személyek életkora, ruházata, viselkedése. Figyelemmel kell lenni az emberi viselkedésformákra, amikor személyek vészeseti menekülésére kívánunk kísérletekből következtetéseket levonni. Rendkívüli esemény során az emberi viselkedésformák eltérnek a szokványostól.[45] Megjelenthet gyermeteg viselkedés, kezdeti ijedtségi reakció és testi-szellemi bénultság.[46]

Ritkán adódik lehetőség tervszerű megfigyeléseket és kísérleteket végezni, úgy, hogy a személyek viselkedésmintázata a valós veszélyben tapasztalhatóval azonos vagy ahhoz igen közeli legyen. Így az átbocsátóképesség vizsgálatára olyan helyszínt és módszert kell választani, amiben a személyek viselkedése a leginkább hasonlít

[45] Restás Ágoston: Tűzoltók szemtől szemben az érintettekkel: Viselkedésformák tűz- és káreseteknél. *Bolyai Szemle,* 13. (2014), 3. 25–35.

[46] Restás Ágoston: Pszichológia a tűz frontvonalában. *Védelem Tudomány,* 1. (2016), 3. 46–56.

a veszélyhelyzeti menekülésre, azonban várhatóan így is el fog térni attól kisebb vagy nagyobb mértékben.

2. Módszer

Mivel e kutatás célja a szűkítések átbocsátóképességének kifejezetten gyermekek részvételével történő vizsgálata, így a szerzők a megfigyelés helyszíneként gyermekintézményeket választottak. A megfigyeléseket a szerzők kiürítési gyakorlatok alkalmával végezték, amikor az épületben tartózkodók egyszerre hagyták el az épületet. Ez a megfigyelési módszer alkalmas arra, hogy közelítse a személyek viselkedésmintázatát a valós veszélyben történő épületkiürítésnél tapasztalhatóhoz. Gyermekintézményekben relatív nagy számú gyermek relatív kis számú felnőttel tartózkodik, így a kijáratokon áthaladó személyek döntő része gyermekek közül kerül ki.

A megfigyeléshez kiürítési gyakorlatok azért megfelelőek, mert a gyermekek viszonylag nagy számban haladnak át a kijáraton mint szűkítésen, azaz a szűkítés gyalogosáramlást korlátozó hatása érvényesül: a szűkítés előtt feltorlódnak a gyermekek, a szűkítés után szabad terület van, ahol akadály nélkül tovább haladhatnak. A szűkítésen keresztül zajló egyirányú áramlás a kiürítési gyakorlatok alkalmával jól érvényesül. A kísérlet során a gyalogosáramlás egyirányúsága jelentős, egyrészt azért, mert a menekülés során is az egyirányú áramlás jellemző a szűkítéseken, másrészt azért, mert a kétirányú áramlás során a főárammal szemben haladók szükségszerűen csökkentik a főáramlás keresztmetszetét.

A szerzők választása a megfigyeléshez egy nyolc évfolyamos középiskolára és két általános iskolára esett. A kutatásba bevont középiskola tanulói jellemzően 10–18 évesek, míg az általános iskolákban a 6–14 éves korosztályú tanulók a jellemzők. A kiürítési gyakorlatok minden esetben egy tanóra vége előtt 5 perccel kezdődtek, így minden tanuló a tantermekben tartózkodott pedagógusi felügyelettel. A kiürítési gyakorlat a tűzjelzés helyben szokásos módon történő megszólaltatásával kezdődött. Az épületben tartózkodók a tűzjelzésre elindultak tartózkodási helyükről, és az épületet a legközelebbi szabad kijáraton át elhagyták. A kijárati ajtók a mérés során kinyitott és teljesen kitárt állapotban rögzítve voltak. Mivel a kutatás célja a szűkítések átbocsátóképességének gyermekekkel és fiatalokkal történő vizsgálata volt, és nem volt tárgya a kutatásnak egyéb tényezők – kijáratot követő további szűkítés visszatorlasztó hatása, időjárási körülményekre adott személyes reakciók hatása stb. – közrehatásának vizsgálata, így a résztvevők figyelme fel lett hívva arra, hogy az épületből való kilépést követően távolodjanak el az épülettől, ezáltal ne akadályozzák az épületből még ki nem jutott személyek haladását. Ezenkívül figyelmet fordítottak a szerzők a kiürítési gyakorlatok szervezése során arra, hogy azokra kedvező időjárási körülmények között kerüljön sor. Így elkerülhető az eső, a hideg és egyéb időjárási körülmények a személyek magatartására gyakorolt kedvezőtlen hatása.

A méréshez épületenként ki kellett jelölni egy kijáratot, ahol a megfigyelés és mérés megtörténhet. Az első szerző 16 gyermekintézményben több mint 100 kiürítési gyakorlatot bonyolított le és elemzett az elmúlt nyolc évben, így tapasztalatai alapján azt a kijáratot választotta ki, amelyiken a várhatóan a legtöbb személy fog áthaladni.

Az épületek kiválasztott kijáratának szabad szélességét a szerzők lemérték, a méréshez fém mérőszalagot használtak. Az épületek kiválasztott kijáratainak szabad szélességi értékeit az 1. táblázat tartalmazza.

1. táblázat

Az épületek kiválasztott kijáratainak szabad szélességi értékei

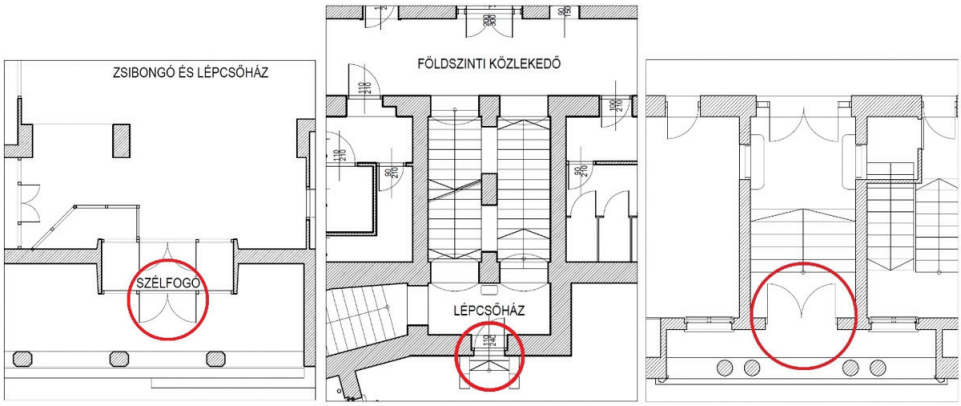
Épület jele	**Kiürítési gyakorlat száma**	**Az épületben tartózkodó tanulók életkora**	**A kijárat szabad szélessége**	**A vizsgált kijáraton áthaladó résztvevők létszáma**
A	1	6–14 év	1,92 m	197 fő
A	2	6–14 év	1,92 m	238 fő
B	3	6–14 év	0,86 m	115 fő
B	4	6–14 év	0,86 m	108 fő
C	5	10–18 év	1,47 m	400 fő
C	6	10–18 év	1,47 m	235 fő

A kijáratok mellé kamerát szereltek fel, amely a kijáraton áthaladó személyeket felülnézetből rögzítette. A felvételeket később értékelték ki a szerzők. Ez a módszer lehetővé tette, hogy meghatározzák minden kiürítési gyakorlatnál azokat az időintervallumokat, amelyeken kialakul a szűkítés előtti torlódás. Ezen időintervallumokban határozták meg a kijárat átbocsátását. Ez ahhoz szükséges, hogy a szűkítésen valóban a lehetséges legnagyobb átbocsátóképességet lehessen megállapítani.

A felvételek elemzésekor csak az előzőekben leírt feltételek teljesülésekor lett mérve az áthaladó személyek száma és az eltelt idő. Amennyiben a szűkítés előtt a torlódás kialakult és 50 áthaladó személy után sem szűnt meg, akkor a szerzők minden 50 fő után rögzítették az eltelt időt és számították az átbocsátást. Az időmérés az ajtónyílás síkját először érintő személy áthaladásakor indult. A mérés indításának pillanata a jármű külső síkjának a személy általi érintése volt. Az időmérés addig tartott, amíg az épületen belül, az ajtó előtt a torlódás megszűnt. Ezen időpontot követően csak egy-két személy haladt át a kijáraton. Mivel ekkor az áramlás már nem volt folyamatos, így nem lett volna mérvadó ennek figyelembevétele a szűkítés átbocsátóképességének meghatározásához. Az időmérés közben az áthaladó személyek számát rögzítették.

Mindegyik megfigyelés során az volt tapasztalható, hogy a résztvevők nem használtak segédeszközt (például mankót, kerekesszéket, járókeretet stb.) a közlekedéshez. Ez azért jelentős, mert a segédeszközzel közlekedők esetében csökkenhet az átbocsátóképesség.

A 2. ábra mutatja be a kutatásban érintett épületek alaprajzainak részletein a vizsgált kijáratokat, amelyeket piros kör jelez.



2. ábra

A kutatásban érintett épületek alaprajzainak részlete, a vizsgált kijáratokat piros kör jelzi (jobbról balra az A, B és C jelű épület)

Forrás: a szerzők szerkesztése

A mérés során gyűjtött adatok statisztikai feldolgozása is megtörtént. Ez magában foglalta az átlag, a medián, a korrigált empirikus szórás, a középérték közepes hibája, valamint Student-féle t-eloszlással a hibahatár és a konfidenciaintervallum meghatározását is.

Azért alkalmaztuk a Student-féle t-eloszlást, mert ezzel a statisztikai módszerrel megállapítható, hogy a minta elemszáma figyelembevételével a teljes vizsgált populációra vonatkozó értékek egy meghatározott valószínűséggel (95% vagy 99%) milyen intervallumon belül lesznek. Ilyen módon a minta elemszáma nem torzítja az eredményt, az a figyelembe vett valószínűséggel a meghatározott intervallumon belül marad. A szerzők a biztonság javára térnek el azáltal, hogy a konfidenciaintervallum alsó határértékét javasolták a kiürítési számítás során figyelembe venni. Így kijelenthető, hogy vizsgált populáció átlagos menekülőképessége által meghatározott átbocsátóképesség 95%, illetve 99% valószínűséggel a meghatározottnál nem kisebb.

3. Az átbocsátóképesség meghatározása

3.1. Általános iskolákban végzett megfigyelés és mérés

Az általános iskolák (A és B jelű épület) kiürítési gyakorlatainál végzett mérés adatait a 2. táblázat tartalmazza. Az átbocsátóképesség normális eloszlását feltételezzük.

2. táblázat

Az általános iskolák kiürítési gyakorlatainál végzett mérés adatai

Forrás: a szerzők szerkesztése

Épület jele	Kiürítési gyakorlat száma	Idő	Áthaladó személyek száma	Kijárat szélessége	Átbocsátás	
		(s)	(fő)	(m)	(fő/[m·s])	(fő/[m·min])
A	1	10	50	1,92	2,604	156,25
A	1	17	50	1,92	1,532	91,91
A	1	20	50	1,92	1,302	78,13
A	1	12	24	1,92	1,042	62,50
A	1	8	23	1,92	1,497	89,84
A	2	14	38	1,92	1,414	84,82
A	2	18	50	1,92	1,447	86,81
A	2	20	50	1,92	1,302	78,13
A	2	18	50	1,92	1,447	86,81
A	2	20	50	1,92	1,302	78,13
B	3	13	24	0,86	2,147	128,80
B	3	29	51	0,86	2,045	122,69
B	3	32	40	0,86	1,453	87,21
B	4	30	49	0,86	1,899	113,95
B	4	21	35	0,86	1,938	116,28

A részt vevő gyermekek életkora az általános iskolák esetében 6–14 év között volt. A szerzők a mérés során megfigyelték, hogy az átbocsátás legnagyobb értéke 6–10 év közötti gyermekek áthaladása során volt kimutatható. Ennek magyarázata lehet, hogy a fiatalabb gyermekek jellemzően kisebb testméretekkel rendelkeznek, mint idősebb társaik.

Az A és B épületeknél mért átbocsátás mediánja 1,453 fő/(m·s), a további számított értékeket az alábbiakban részletezzük.

Az átlag számítása:[47]

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n} = 1{,}625 \ \frac{\text{fő}}{\text{s·m}}$$

[47] Nagy Péter: Leíró statisztika: a populáció és a minta jellemzése. In Fidy Judit – Makara Gábor (szerk.): *Biostatisztika.* Budapest, Informed 2002 Kft., 2005. 22.

A korrigált empirikus szórás az alábbi összefüggés alapján számítható:[48]

$$SD = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1}} = 0{,}4137 \ \frac{\text{fő}}{\text{s·m}}$$

A középérték közepes hibája:[49]

$$SEM = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n(n-1)}} = \frac{SD}{\sqrt{n}} = 0{,}1068 \ \frac{\text{fő}}{\text{s·m}}$$

Student-féle t-eloszlással vizsgálva a hibahatár 95%-os valószínűséggel:[50]

$$\Delta_{95} = t_{1-\frac{\alpha}{2}}^{(n-1)} \cdot SEM = t_{0{,}975}^{(14)} \cdot 0{,}1068 = 2{,}14 \cdot 0{,}1068 = 0{,}2286 \ \frac{\text{fő}}{\text{s·m}}$$

Az átbocsátóképesség várható értékének p = 95%-os megbízhatóságú konfidencia-intervalluma:

$$\mu(95) \in [\bar{x} - \Delta_{95}; \bar{x} + \Delta_{95}] = [1{,}625 - 0{,}2286; 1{,}625 + 0{,}2286] = [1{,}3964; 1{,}8536]$$

A hibahatár, valamint a várható érték konfidenciaintervallumának meghatározása p = 99%-os megbízhatósággal:

$$\Delta_{99} = t_{1-\frac{\alpha}{2}}^{(n-1)} \cdot SEM = t_{0{,}995}^{(14)} \cdot 0{,}1068 = 2{,}98 \cdot 0{,}1068 = 0{,}3183 \ \frac{\text{fő}}{\text{s·m}}$$

A fentiekből látszik, hogy a mérés szerint a jelen kutatásban vizsgált általános iskolai populáció átlagos menekülőképessége alapján az ajtók átbocsátóképessége 95%-os, illetve 99%-os megbízhatósággal az alábbi konfidenciaintervallum szerint alakul:

$$\mu(95) = \bar{x} \pm \Delta_{95} = 1{,}625 \pm 0{,}2286 \frac{\text{fő}}{\text{s·m}} = \ 97{,}5 \pm 13{,}72 \frac{\text{fő}}{\text{min·m}}$$

$$\mu(99) = \bar{x} \pm \Delta_{99} = 1{,}625 \pm 0{,}3183 \frac{\text{fő}}{\text{s·m}} = \ 97{,}5 \pm 19{,}1 \frac{\text{fő}}{\text{min·m}}$$

[48] Nagy (2005): i. m. 22.
[49] Nagy (2005): i. m. 22.
[50] Kenyeres Erika: Statisztikai becslések. In Korpás Attiláné (szerk.): *Általános statisztika II.* Budapest, Nemzeti Tankönyvkiadó, 1997. 36.

3.2. Nyolc évfolyamos gimnáziumban végzett megfigyelés és mérés

A kutatás során vizsgált nyolc évfolyamos gimnázium (C jelű épület) kiürítési gyakorlatánál végzett mérés adatait a 3. táblázat tartalmazza. Az átbocsátóképesség normális eloszlását itt is feltételezzük.

3. táblázat

A nyolc évfolyamos gimnázium kiürítési gyakorlatainál végzett mérés adatai

Forrás: a szerzők saját szerkesztése

Épület jele	**Kiürítési gyakorlat száma**	**Idő**	**Áthaladó személyek száma**	**Kijárat szélessége**	**Átbocsátás**	
		(s)	**(fő)**	**(m)**	**(fő/[m·s])**	**(fő/[m·min])**
C	5	25	50	1,47	1,361	81,63
C	5	28	50	1,47	1,215	72,89
C	5	23	50	1,47	1,479	88,73
C	5	24	50	1,47	1,417	85,03
C	5	22	50	1,47	1,546	92,76
C	5	24	50	1,47	1,417	85,03
C	5	26	50	1,47	1,308	78,49
C	5	26	50	1,47	1,308	78,49
C	6	20	50	1,47	1,701	102,04
C	6	23	50	1,47	1,479	88,73
C	6	24	50	1,47	1,417	85,03
C	6	22	50	1,47	1,546	92,76
C	6	15	35	1,47	1,587	95,24

A részt vevő gyermekek, és fiatalok életkora a nyolc évfolyamos gimnázium esetében 10–18 év között volt. A C épületnél mért átbocsátás mediánja 1,417 fő/(m·s), a további számított értékeket az alábbiakban részletezzük.

Az átlag számítása:[51]

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n} = 1{,}445 \ \frac{\text{fő}}{\text{s·m}}$$

[51] Nagy (2005): i. m. 22.

A korrigált empirikus szórás az alábbi összefüggés alapján számítható:[52]

$$SD = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1}} = 0{,}1317 \ \frac{\text{fő}}{\text{s·m}}$$

A középérték közepes hibája:[53]

$$SEM = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n(n-1)}} = \frac{SD}{\sqrt{n}} = 0{,}03653 \ \frac{\text{fő}}{\text{s·m}}$$

Student-féle t-eloszlással vizsgálva a hibahatár 95%-os valószínűséggel:[54]

$$\Delta_{95} = t_{1-\frac{\alpha}{2}}^{(n-1)} \cdot SEM = t_{0{,}975}^{(12)} \cdot 0{,}03653 = 2{,}18 \cdot 0{,}03653 = 0{,}07964 \ \frac{\text{fő}}{\text{s·m}}$$

Az átbocsátóképesség várható értékének p = 95%-os megbízhatóságú konfidencia-intervalluma:

$$\mu(95) \in [\bar{x} - \Delta_{95}; \bar{x} + \Delta_{95}] = [1{,}445 - 0{,}07964; 1{,}445 + 0{,}07964] = [1{,}3654; 1{,}5246]$$

A hibahatár, valamint a várható érték konfidenciaintervallumának meghatározása p = 99%-os megbízhatósággal:

$$\Delta_{99} = t_{1-\frac{\alpha}{2}}^{(n-1)} \cdot SEM = t_{0{,}995}^{(12)} \cdot 0{,}03653 = 3{,}05 \cdot 0{,}03653 = 0{,}1114 \ \frac{\text{fő}}{\text{s·m}}$$

$$\mu(99) \in [\bar{x} - \Delta_{99}; \bar{x} + \Delta_{99}] = [1{,}445 - 0{,}1114; 1{,}445 + 0{,}1114] = [1{,}3336; 1{,}5564]$$

A fentiekből látszik, hogy a mérés szerint a jelen kutatásban vizsgált 10–18 éves populáció átlagos menekülőképessége alapján az ajtók átbocsátóképessége 95%-os, illetve 99%-os megbízhatósággal az alábbi konfidenciaintervallum szerint alakul:

$$\mu(95) = \bar{x} \pm \Delta_{95} = 1{,}445 \pm 0{,}07964 \frac{\text{fő}}{\text{s·m}} = \ 86{,}7 \pm 4{,}778 \frac{\text{fő}}{\text{min·m}}$$

$$\mu(99) = \bar{x} \pm \Delta_{99} = 1{,}445 \pm 0{,}1114 \frac{\text{fő}}{\text{s·m}} = \ 86{,}7 \pm 6{,}684 \frac{\text{fő}}{\text{min·m}}$$

[52] Nagy (2005): i. m. 22.
[53] Nagy (2005): i. m. 22.
[54] Kenyeres (1997): i. m. 36.

3.3. Az értékek összevetése

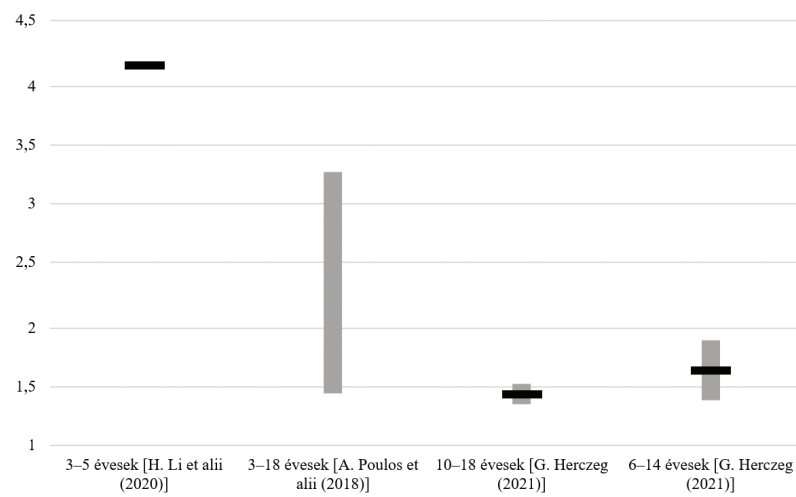
A mérések alapján 95%-os valószínűséggel megállapítható, hogy kisebb testméretekkel rendelkező fiatalabb gyermekek esetében nagyobb a szűkítések átlagos átbocsátóképessége, mint a nagyobb testméretekkel rendelkező idősebb gyermekek, illetve fiatalok esetén.

A nyolc évfolyamos gimnáziumban végzett mérés értékeiből azt a következtetést vonhatjuk le, hogy az $n = 13$ elemszám mellett kellően pontos adatokat kaphatunk a jelen kutatásban vizsgált 10–18 éves populáció átlagos menekülőképességére vonatkozóan. Jelen kutatás a gyermekekre és fiatalokra fókuszál, így a felnőttek aránya a megfigyelés során alacsony, 5–10% közötti maradt.

Az $n = 15$ elemszámmal vizsgált általános iskolai populáció mérési adataiból számított szórás csökkenthető további kutatások során, amennyiben nagyobb elemszám vizsgálatára nyílik lehetőség. Ez igaz a nyolc évfolyamos gimnáziumi populáción mért adatokra is. A jelen kutatásban meghatározott értékekből mégis arra lehet következtetni, hogy a fiatalabb gyermekek nagyobb átbocsátást tudnak elérni szűkítésen való áthaladáskor, idősebb társaikhoz képest.

Az értékeket a gyakorlatban elegendő optimálisan 95%-os megbízhatósággal megállapítani Student-féle t-eloszlással, így 86,7 ± 5,5% fő/(min·m) érték adódik a szűkítések átbocsátóképességére a 10–18 éves korosztálynál, és 97,5 ± 14% fő/(min·m) érték a 6–14 éves korosztálynál, amelyek közül az alacsonyabb érték is több mint kétszerese a jelenleg alkalmazott 41,7 fő/(min·m) értéknek.

A megállapított átbocsátóképesség-értékek akként lettek differenciálva életkor szerint, hogy külön értéket határoztunk meg a 10–18 éves korosztályra és szintén külön értéket a 6–14 éves korosztályra.



3. ábra

A kifejezetten gyermekekkel, illetve fiatalokkal mért átbocsátóképesség különböző források szerinti értékeinek összehasonlítása a jelen kutatásban meghatározott intervallumokkal [fő/(s·m)]

Forrás: a szerzők szerkesztése

Az átlagos értékeken felül az is látszik a mérési eredményekből, hogy a gyakorlati átbocsátóképesség maximuma a 6–14 éves korosztály esetében legalább 156,25 fő/(min·m), illetve a 10–18 éves korosztály esetében legalább 102,04 fő/(min·m).

A szerzők által meghatározott érték beleillik a szakirodalomban fellelhető értékek sorába, amit a 4. táblázat mutat be.

4. táblázat

Az átbocsátóképesség átlagainak összehasonlítása jelen mérés eredményével

Forrás: a szerzők szerkesztése

Adat forrása	Az átbocsátóképesség átlaga (fő/[m·s])
P. Thompson et al. (2015)	0,850
S. M. V. Gwynne et al. (2009)	0,920
P. J. DiNenno et al. (2012)	1,300
G. Herczeg – L. Bérczi (2021): 10–18 éves gyermekek és fiatalok	*1,445*
A. Seyfried et al. (2009)	1,610
G. Herczeg – L. Bérczi (2021): 6–14 éves gyermekek	*1,625*
A. Nicolas – S. Bouzat – M. N. Kuperman (2017)	1,710
T. Kretz et al. (2006)	1,740
K. Fuji –T. Sano (2014)	1,760
R. Fernandez – A. Valencia – S. Seriani (2015)	1,942
A. Poulos et al. (2018)	2,345
J. M. Pastor et al. (2015)	2,530
M. Haghani – M. Sarvi (2019)	2,800
X. Shi et al. (2019)	2,925
S. Huang et al. (2018)	3,395
A. Garcimartín et al. (2016)	3,700

A szerzők által meghatározott értékek az értékek növekvő sorában az alsó és középső harmad határán helyezkednek el, ami a szerzők által meghatározott értékeknek az elmúlt 15 évben publikált mérési adatokkal történő összevetésével megállapítható.

A legtöbb fellelhető átbocsátóképességi értéket kísérletek során állapították meg. A kísérletek összehasonlíthatóságának feltétele az azonos kísérleti körülmények megléte. A fellelt források több esetben tartalmazzák ugyan a kísérlet körülményeinek részletes leírását (például személyek életkori megoszlása, ruházat, minta nagysága stb.), azonban vannak olyan publikációk, ahol a szerzők az előbb felsorolt tényezőkről nem tesznek említést annak ellenére, hogy azok befolyásolhatták a kísérletek eredményeit.

A szakirodalomban fellelt átbocsátóképességi értékeket a szerzők ennek ellenére azért szerepeltetik, mivel az előzőekben felsorolt fenntartásokkal ugyan, de alkalmasak az összevetésre a szerzők által végrehajtott mérések eredményével és az átbocsátóképesség Magyarországon alkalmazott értékével. Az összevetés során, a korábbi kísérletek körülményeire vonatkozó adatok ismeretének hiányában is megállapítható, hogy az átbocsátóképesség kiürítési számítás során Magyarországon alkalmazott értéke minden más kutató által eredményül kapott értéknél alacsonyabb, akár gyermekekkel, akár felnőttekkel végezték a méréseket.

4. Összefoglalás

Jelenleg nincs Magyarországon olyan előírás vagy iránymutatás, amely a felnőttektől eltérően a gyermekek és fiatalok vonatkozásában külön átbocsátóképesség-értéket adna meg. Ilyen érték csak önállóan menekülni képes, 10 évesnél idősebb személyekre létezik. Az épületek kiürítése során a szűkítések átbocsátóképességének gyermekekre és fiatalokra vonatkozó adatainak meghatározása lehetőséget ad arra, hogy a kiürítési számítás során külön érték lehessen alkalmazható akkor, ha ez indokolt. Lehetőséget ad továbbá arra is, hogy a populáció egyes csoportjai menekülőképességének ezen aspektusát jobban megismerjük.

E cikkben a szerzők a menekülőképesség több tényezője közül csak az átbocsátóképességet vizsgálták.

Az épületek kiürítésének ellenőrzésére szolgál a kiürítési számítás, amelynek része a szűkítések átbocsátóképességének figyelembevételével annak megállapítása, hogy a szűkítések lehetővé teszik-e a biztonságos menekülést. A kiürítési számítás során a szűkítések átbocsátóképességére Magyarországon alkalmazott érték 41,7 fő/(min·m), amely önállóan menekülni képes, 10 évesnél idősebb személyekre alkalmazható.

Elemezték a szerzők e cikkben a nemzetközi szakirodalomban található – szűkítésen keresztüli gyalogosáramlásra vonatkozó – adatokat, amelyek a szűkítések átbocsátóképességére vonatkoztak. A fellelt értékeket a szerzők grafikonon ábrázolták. Az egyes források eltérően határozták meg az összefüggést a gyalogosáram erőssége és a szűkítés szélessége között: konstans, lineáris és négyzetes összefüggés is előfordult. Nem volt a szerzők célja a gyalogosáramlás erőssége és a szűkítés szélessége közötti összefüggés megállapítása. A cél az volt, hogy gyermekekre és fiatalokra vonatkozó átlagos átbocsátóképesség-értéket határozzanak meg, amely könnyen beilleszthető a jelenlegi kiürítési számítási módszerbe és az önállóan menekülni képes gyermekek és fiatalok átlagos menekülőképességét jól reprezentálja.

A jelenleg alkalmazott átbocsátóképesség-érték fogalmának, arányának publikálásakor, 1938-ban nem ismertették, hogy az értéket milyen életkori eloszlású személyeken mérték, ezen személyek közül használtak-e a gyalogos közlekedéshez segédeszközöket, és azt sem, hogy milyen ruházatot viseltek.

A szerzők által megállapított átbocsátóképesség értéke a 6–18 éves magyar populáció átlagos tulajdonságain alapul. Számos tényező, mint a ruházat, az életkor, a segédeszközzel közlekedők aránya befolyásolhatja a menekülőképességet,

és ezáltal a szűkítések átbocsátóképességét. A szerzők által megállapított érték a jelenleg alkalmazotthoz hasonlóan egységesítésre alkalmas átlagérték, amely a vizsgált korcsoport átlagos menekülőképességén alapul. Az átbocsátóképességen kívül a bejárt útvonal hossza, a haladási sebesség, az épület tűzvédelmi jellemzői (például tűzszakasz mérete, tűzjelző berendezés stb.) szintén befolyásolják az épületben tartózkodók biztonságát.

Ebben a cikkben megállapították a szerzők az épületekből való menekülés során bejárt útvonalon elhelyezkedő szűkítések átbocsátóképességét 6–18 éves gyermekek és fiatalok vonatkozásában. Ezen értéket általános iskolák és egy nyolc évfolyamos gimnázium kiürítési gyakorlatainak megfigyelésével és áramlásra jellemző mennyiségek mérésével állapították meg egy $n = 15$ és egy $n = 13$ elemszámú mintán. A vizsgálatban részt vevő személyek összlétszáma 1269 fő volt.

A szerzők a megfigyelést azért kiürítési gyakorlatok alkalmával végezték, mivel az egyirányú gyalogosáramlást megnyugtató pontossággal csak ilyenkor lehet könnyen vizsgálni. A megfigyelt kijárat meghatározásához a szerzők figyelembe vették az elmúlt nyolc évben általuk lebonyolított több mint 100 kiürítési gyakorlat tapasztalatait. A szerzők kidolgozták a mérés módszertanát, valamint meghatározták a mérés gyakorlati végrehajtásához szükséges feltételeket. A mérést a szerzők végezték, a mérés helyszíneiről rajzot mutattak be, amelyen jelölték a méréshez figyelembe vett kijáratokat.

A mérés eredményét a szerzők statisztikai módszerekkel elemezték, megállapították 95%-os és 99%-os megbízhatósággal a szűkítések gyermekekre vonatkozó átbocsátóképességének mértékét, valamint az átlagértéket összehasonlították a más szerzők által meghatározottakkal.

A szerzők javasolják a szűkítések 6–18 éves korosztályra vonatkozó átbocsátóképességének kiürítési számítása során figyelembe vehető értékét 10–18 éves populáció alacsonyabb mért értéke 95%-os megbízhatóságú konfidenciaintervalluma alsó határa szerint (kerekítve) 80 fő/(min·m) értékben megállapítani. Ehhez a kiürítésről szóló tűzvédelmi műszaki irányelv módosítása szükséges. A kiürítés meglévő komplex rendszerébe az új érték akként is adaptálható, ha eltérő értékben határozzák meg a 10–18 éves és a felnőtt populáció vonatkozásában a szűkítések átbocsátóképességét.

A 6–18 éves intervallum nehezen hasonlítható össze az életkori sajátosságok eltérése miatt, ezért az egységes érték megállapításakor – a biztonság javára – az átbocsátóképesség értékét a 10–18 éves populáció alacsonyabb mért értéke alapján határoztuk meg.

Az ebben a cikkben közölt érték konfidenciaintervalluma tovább pontosítható a minta elemszámának növelésével.

Jelentős szórás figyelhető meg a különböző források szerinti átbocsátóképességi értékekben. Ennek különféle okai lehetnek, ami egyben rávilágít arra, hogy nincs jelenleg egységesen elfogadott módszer az átbocsátóképesség meghatározására. További kutatások során lehetőség nyílik a szűkítésen keresztül történő gyalogosáramlás jobb megismerésére és a kiürítési számítás további fejlesztésére.

Felhasznált irodalom

Beljajev, Sz. V.: *Evakuacija zdanyij masszovovo naznacsenyija.* Moszkva, Izdatyelsztvo Vszeszojuznoj Akagyemii Arhityekturi, 1938.

Daamen, W. – S. P. Hoogendorn: Emergency Door Capacity: Influence of Door Width, Population Composition and Stress Level. *Fire Technology,* 48. (2012), 1. 55–71. Online: https://doi.org/10.1007/s10694-010-0202-9

DiNenno, Philip J. – Dougal Drysdale – Craig L. Beyler – Douglas W. Walton – Richard L. P. Custer: *The SFPE Handbook of Fire Protection Engineering.* Quincy, National Fire Protection Association, 2002.

Fernández, Rodrigo – Alejandra Valencia – Sebastian Seriani: On Passenger Saturation Flow in Public Transport Doors. *Transportation Research Part A,* 78. (2015), 102–112. Online: https://doi.org/10.1016/j.tra.2015.05.001

Fujii, Kosuke – Tomonori Sano: Experimental Study on Crowd Flow Passing Through Ticket Gates in Railway Stations. *Transportation Research Procedia,* 2. (2014), 630–635. Online: https://doi.org/10.1016/j.trpro.2014.09.105

Garcimartín, Angel – D. R. Parisi – J. M. Pastor – C. Martín-Gómez – I. Zuriguel: Flow of Pedestrians through Narrow Doors with Different Competitiveness. *Journal of Statistical Mechanics: Theory and Experiment,* (2016), 4. 043402. Online: https://doi.org/10.1088/1742-5468/2016/04/043402

Gwynne, S. M. V. – E. D. Kuligowski – J. Kratchman – J. A. Milke: Questioning the Linear Relationship between Doorway Width and Achievable Flow Rate. *Fire Safety Journal,* 44. (2009), 1. 80–87. Online: https://doi.org/10.1016/j.firesaf.2008.03.010

Haghani, Milad – Majid Sarvi: Simulating Pedestrian Flow through Narrow Exits. *Physics Letters A,* 383. (2019), 2–3. 110–120. Online: https://doi.org/10.1016/j.physleta.2018.10.029

Hamilton, Glenn N. – Patrick F. Lennon – John O'Raw: Toward Fire Safe Schools: Analysis of Modelling Speed and Specific Flow of Children During Evacuation Drills. *Fire Technology,* 56. (2020), 605–638. Online: https://doi.org/10.1007/s10694-019-00893-x

Herczeg Gergely – Bérczi László: Közösségi rendeltetésű épületek kiürítési gyakorlatainak tapasztalatai. *Védelem Tudomány,* 4. (2019), 2. 84–103. Online: http://vedelemtudomany.hu/articles/04-herczeg-berczi.pdf

http://vigimodell.hu/kep/jelleg/wgc_media/photos/Alstom.jpg

Huang, Shenshi – Shouxiang Lu –Siuming Lo – Changhai Li – Yafei Guo: Experimental Study on Occupant Evacuation in Narrow Seat Aisle. In *Physica A: Statistical Mechanics and its Applications,* 502. (2018), 506–517. Online: https://doi.org/10.1016/j.physa.2018.02.032

Kenyeres Erika: Statisztikai becslések. In Korpás Attiláné (szerk.): *Általános statisztika II.* Budapest, Nemzeti Tankönyvkiadó, 1997. 30–69.

Kretz, Tobias – Anna Grünebohm – Michael Schreckenberg: Experimental Study of Pedestrian Flow through a Bottleneck. *Journal of Statistical Mechanics: Theory and Experiment,* (2006), 10. P10014. Online: https://doi.org/10.1088/1742-5468/2006/10/P10014

Li, Hongliu Jun Zhang – Libing Yang – Weiguo Song – Kwok Kit Richard Yuen: A Comparative Study on the Bottleneck Flow between Preschool children and Adults under Different Movement Motivations. *Safety Science,* 121. (2020), 30–41. Online: https://doi.org/10.1016/j.ssci.2019.09.002

Nagy Péter: Leíró statisztika: a populáció és a minta jellemzése. In Fidy Judit – Makara Gábor (szerk.): *Biostatisztika.* Budapest, Informed 2002 Kft., 2005. 20–41.

NFPA 130: Standard for Fixed Guideway Transit and Passenger Rail Systems. 5.3.7.1. Online: www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=130

Nicolas, Alexandre – Sebastián Bouzat – Marcelo N. Kuperman: Pedestrian Flows through a Narrow Doorway. Effect of Individual Behaviours on the Global Flow and Microscopic Dynamics. *Transportation Research Part B: Methodological,* 99. (2017), 30–43. Online: https://doi.org/10.1016/j.trb.2017.01.008

Pastor, José M. – Angel Garcimartín – Paula A. Gago – Juan P. Peralta – César Martín-Gómez – Luis M. Ferrer – Diego Maza – Daniel R. Parisi – Luis A. Pugnaloni – Iker Zuriguel: Experimental Proof of Faster-is-slower in Systems of Frictional Particles Flowing through Constrictions. *Physics Rev. E,* 92. (2015), 6. 062817. Online: https://doi.org/10.1103/PhysRevE.92.062817

Poulos, Alan – Felipe Tocornal – Juan Carlos de la Llera – Judith Mitrani-Reiser: Validation of an agent-based building evacuation model with a school drill. *Transportation Research Part C: Emerging Technologies,* 97. (2018), 82–95. Online: https://doi.org/10.1016/j.trc.2018.10.010

Predtechenskii V. – A. I. Milinskii: *Planning for Foot Traffic Flow in Buildings.* Washington D.C., National Bureau of Standards, US Department of Commerce, and the National Science Foundation, 1978.

Ren, Xiangxia – Jun Zhang – Weiguo Song: Flows of Walking and Running Pedestrians in a Corridor through Exits of Different Widths. *Safety Science,* 133. (2021), 105040. Online: https://doi.org/10.1016/j.ssci.2020.105040

Restás Ágoston: Pszichológia a tűz frontvonalában. *Védelem Tudomány,* 1. (2016), 3. 46–56. Online: www.vedelemtudomany.hu/articles/04-restas.pdf

Restás Ágoston: Tűzoltók szemtől szemben az érintettekkel. Viselkedésformák tűz- és káreseteknél. *Bolyai Szemle,* 13. (2014), 3. 25–35. Online: https://tinyurl.hu/5LGK/

Seyfried, Armin – Bernhard Steffen – Andreas Winkens – Tobias Rupprecht – Maik Boltes – Wolfram Klingsch: Empirical Data for Pedestrian Flow through Bottlenecks. *Traffic and Granular Flow'07.* Berlin, Springer, 2009. 189–199. Online: https://doi.org/10.1007/978-3-540-77074-9_17

Shi, Xiaomeng – ZhiruiYe – Nirajan Shiwakoti – Dounan Tang – Junkai Lin: Examining Effect of Architectural Adjustment on Pedestrian Crowd Flow at Bottleneck. *Physica A: Statistical Mechanics and its Applications,* 522. (2019), 350–364. Online: https://doi.org/10.1016/j.physa.2019.01.086

Thompson, Peter – Daniel Nilsson – Karen Boyce – Denise McGrath: Evacuation Models are Running Out of Time. *Fire Safety Journal,* 78. (2015), 251–261. Online: https://doi.org/10.1016/j.firesaf.2015.09.004

TvMI 2.3:2020.01.22. *Tűzvédelmi Műszaki Irányelv – Kiürítés*

Wang, Shuai – Hao Yue – Binya Zhang – Juan Li: Setting the Width of Emergency Exit in Pedestrian Walking Facilities. *Procedia – Social and Behavioral Sciences,* 138. (2014), 233–240. Online: https://doi.org/10.1016/j.sbspro.2014.07.200

Yao, Yishu – Wei Lu: Children's Evacuation. Behavioural Data of Drills and Simulation of the Horizontal Plane in Kindergarten. *Safety Science,* 133. (2021), 105037. Online: https://doi.org/10.1016/j.ssci.2020.105037

Zhang, Teng – Xuelin Zhang – Shenshi Huang – Changhai Li – Shouxiang Lu: Collective Behavior of Mice Passing Through an exit under Panic. *Physica A. Statistical Mechanics and its Applications,* 496. (2018), 233–242. Online: https://doi.org/10.1016/j.physa.2017.12.055

Jogi forrás

54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról

HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 3. szám 119–137.
DOI: 10.32567/hm.2021.3.7

Kovács László[1]

Offenzív kiberműveletek II.: Kibererők és képességeik

Offensive Cyber Operations Part Two: Cyber Units and Their Capabilities

A kibertér biztonságának megteremtése számos tevékenység összehangolt megvalósítását igényli. A kiberbiztonság komplex rendszerében a szabályozási és eljárási kérdések mellett aktív kibervédelmi műveleteket is találunk. Ugyanakkor a védelmi célú kibertérműveletek önmagukban nem mindig elégségesek a teljes és átfogó kiberbiztonság megteremtéséhez. Így a védelmi kibertérműveletek mellett offenzív kiberműveletek végrehajtására is szükség lehet. Emellett az offenzív kibertérműveletek, és az abban foglalt eszközök és eljárások természetszerűleg nemcsak a saját oldali rendszereink védelméhez járulnak hozzá, hanem az ellenérdekelt fél infokommunikációs rendszereinek lefogásával, azok működésének akadályozásával, vagy azokból információk kinyerésével más műveleti terekben végrehajtott tevékenységek támogatásához járulnak hozzá hatékony módon. Jelen tanulmány első része az offenzív kiberműveletek általános jellemzőit mutatta be, a második rész, azaz jelen írás az offenzív kiberműveleti képességek gyakorlati megvalósítását és alkalmazhatóságát elemzi, valamint kitér a kiberműveleti erőkre, az általuk alkalmazható eszközökre és eljárásokra.

Kulcsszavak: **kiber, offenzív kiberképesség, támadás, hadviselés, kiberstratégia**

Creating cybersecurity requires coordinated implementation of many activities. In the complex system of cybersecurity, in addition to regulatory and procedural issues, we also find active cyber defence operations. However, cyberspace operations for defence purposes alone are not always sufficient to provide full and comprehensive cybersecurity. Thus, in addition to defence cyberspace operations, it may be necessary to perform offensive cyber operations. The offensive cyberspace operations, together with tools and procedures, naturally not only contribute to

[1] Magyar Honvédség Parancsnoksága, kibervédelmi haderőnemi szemlélő, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Elektronikai Hadviselés Tanszék, egyetemi tanár, e-mail: kovacs.laszlo@uni-nke.hu

the protection of our own systems, but also effectively support activities in other dimensions by intercepting, disrupting, or extracting information from counterparty infocommunication systems. The first part of the present study presents the general characteristics of offensive cyber operations, the second part analyses the practical implementation and applicability of offensive cyber operations capabilities and covers the forces of cyber operations and the tools and procedures they can apply.

Keywords: **cyber, offensive cyber capability, attack, warfare, cyber strategy**

1. Bevezetés

A kiberbiztonság és annak megteremtése jelen korunk egyik nagy kihívása. A 21. században általunk használt és alkalmazott ezernyi infokommunikációs eszköz, rendszer, megoldás és szolgáltatás olyannyira a mindennapjaink részévé vált, hogy azok valódi létfontosságú elemekké váltak életünkben.

Így a biztonság megteremtése létkérdés ezen rendszerek esetében. A fentiekben megfogalmazottak azonban magukkal hozták a hadviselés változását is, hiszen egy ország elleni támadás ma már nem igényli fizikai határainak átlépését, a globális hálózatoknak köszönhetően a rosszindulatú beavatkozás egy-egy jól kiválasztott információs rendszerbe – jellemzően számítógép-hálózatba, vagy annak egyes elemeibe – gyakorlatilag a világon bárhonnan kivitelezhető, és abban komoly – akár a teljes működésképtelenséget is előidéző – kár okozható. A hadviselés tehát változik, mint az emberi történelem során eddig mindig.

Ahogy a korábbi nagy technikai felfedezések, úgy a kibertérben használt infokommunikációs eszközök és rendszerek is változást eredményeznek a hadviselés eljárásaiban és a harcok megvívásának elveiben is. A kibertér jellemzői nagyban segítik azokat az eljárásokat, amelyekkel a hadviselést egyébként jellemezni szoktuk. A különböző támadásokhoz, az azok előkészületeihez szükséges információszerzéstől kezdve a rejtőzködésen át a nagy távolságból végrehajtott csapásokig a kibertér ideális terep a hadviselés számára.

Természetszerűleg jelent meg tehát a hadviselés eddig is színes palettáján a kibertéri műveletek egész sora, amelyekkel a fenti támadások megvalósíthatók. A kérdés csak az, hogy szükséges-e egy adott ország számára kibertámadó, illetve a tágabb értelemben vett offenzív kiberképességeket kiépíteni, azokat fenntartani. A válasz már jelen tanulmány első részéből is körvonalazható volt. Ez a válasz pedig egyértelműen igen, szükséges ilyen képességekkel rendelkeznie egy országnak.

Jelen tanulmány első része az offenzív képességek általános hátterét vizsgálta. Ennek során az olyan kérdések elemzését végeztük el, mint az offenzív kiberképességek összetevői és az offenzív kiberképességek stratégiai megfontolásai. Az írás első részében megvizsgált kérdések egy végső következtetés levonását indukálták, amely nem más, mint annak megállapítása, hogy a jövőben a kibertéri dominancia és a kibertér uralása elengedhetetlen lesz a győzelem kivívásához. Ezért a kibertéri fölény, illetve a kibertérben történő sikeres tevékenység offenzív a kibertéri képességeket is magában foglaló kibererők felállítását igényli. Ma már ezek a képességek elengedhetetlen részét képezik az adott ország biztonsági összetevőinek.

Amennyiben a fentieket elfogadjuk, úgy egy másik, nem sokkal egyszerűbb kérdést, illetve kérdések egész sorát kell megválaszolnunk. Ez pedig nem más, mint az, hogy hogyan is nézzen ki az a szervezet, amely mindezeket a képességeket fel tudja mutatni. Egyáltalán milyen elvek mentén szükséges ezeket a képességeket kialakítani? Ki legyen a felelőse a képességek kialakításának? Milyen módszerek és eljárások járulhatnak hozzá a kiberbiztonsági stratégiákban meghatározott kiberképességek kialakításához? Milyen szerepe van az egyes tagországoknak a NATO offenzív kiberképességének kialakításában?

Ezernyi kérdés, amelyekre jelenleg nem, vagy csak nagyon nagy vonalakban tudunk válaszolni. Jelen írás ezekre a kérdésekre igyekszik – tudományos munka esetében eléggé el nem ítélhető módon a teljesség igénye nélkül – választ adni.

A tanulmányban összegzett vizsgálatok irodalomkutatásra építenek, esetenként az összehasonlító elemzés, majd szintézis módszerének alkalmazásával kiegészítve.

Az elvégzett vizsgálatokból levont következtetések a szerző sajátjai, azok nem feltétlenül esnek egybe sem a Nemzeti Közszolgálati Egyetem, sem a Magyar Honvédség hivatalos véleményével vagy álláspontjával.

2. Az offenzív kiberképességek szükségessége

Az offenzív kiberképességek kialakításának egyik legfőbb indoka az, hogy a lehető legtávolabb tartsuk a potenciális támadó (szemben álló fél, ellenség) rosszindulatú kibertevékenységét a saját rendszereinktől. Ez akkor a leghatékonyabb, amennyiben még a rendszereink megtámadása előtt a potenciális támadót elrettentjük a támadás kivitelezésétől – például olyan védelmi rendszer kiépítésével, amely csak aránytalanul nagy energiabefektetéssel törhető át –, vagy olyan mértékben csökkentjük képességeit, amelyekkel már nem tud hatékony támadást indítani rendszereink ellen. Ez utóbbi esetben van szükség az offenzív kiberképességek meglétére.

Az offenzív, és benne a kibertámadó képességek kialakítása előtt azonban szükséges feltárni azokat a kihívásokat és veszélyeket, amelyek a kibertérben jelentkeznek. Ezek alapján lehet meghatározni az offenzív kiberképességek kialakításához szükséges feltételeket, eszközöket és módszereket. A kihívások és veszélyek feltárása mellett azonban szükség van a köztük lévő összefüggések, illetve azok hatásainak vizsgálatára is.

Az okok között természetesen ott vannak azok a leggyakoribb kibertéri veszélyek, amelyek a technológia sérülékenységeit kihasználva jelentkeznek. Ezek vagy rosszindulatú programokban, vagy az azokra épülő olyan eljárásokban vannak jelen, amelyeket a támadók különböző célokkal alkalmaznak.

Számos olyan infokommunikációs eszközt és rendszert használunk, amelyek vagy vegyes használatúak, azaz polgári és katonai célra egyaránt alkalmazzák őket vagy olyan rendszerek és eszközök, amelyek bár polgári rendszerek (például Commercial off the Shelves, COTS, azaz kereskedelmi forgalomban kaphatók), de mégis katonai célra is használjuk. Ebből következően az ezeket a rendszereket és eszközöket fenyegető veszélyeket is fel kell mérni. A csak katonai célú eszközök és rendszerek esetében a helyzet sok esetben furcsa mód sokkal nehezebb, mint a polgári célú eszközök esetében. Ennek oka elsősorban abban keresendő, hogy a csak katonai

célra alkalmazott eszközök és rendszerek életciklusa – többek között azok bekerülési költsége miatt – sokkal hosszabb, mint ami a polgári rendszerek esetében megszokott. Ennek megfelelően azokat sokkal hosszabb ideig tartjuk rendszerben, így azok időközben napvilágra kerülő sérülékenységei is sokkal hosszabb ideig fennállhatnak. Ráadásul ez a hosszabb időtartam azt is jelenti, hogy a korszerűbb, a kibervédelmet szolgáló megoldások beépítése és alkalmazása egy-egy működő katonai rendszerbe csak lényegesen később és nagyobb energiabefektetéssel valósítható meg.

Egy másik probléma az olyan, a polgári életben már nagy népszerűségnek örvendő és igen elterjedt szolgáltatásoknak a hadseregek életében történő megjelenése, mint amilyenek például a közösségimédia-platformok. Ezek nem önmagukban jelentenek kockázatot vagy veszélyt, hanem a nem tudatos használat révén. A katonák vagy a hadseregben dolgozó civil alkalmazottak meggondolatlan és sok esetben felelőtlen közösségimédia-jelenléte nagyon sokszor komoly információforrást jelent a szemben álló fél vagy a potenciális támadó számára.

A kibertámadó képességek, illetve azok alkalmazásának okait vizsgálva számos közvetett okot is fel tudunk tárni. Ezek közül az első ok azonban rögtön egy komplex problémát takar. Egyrészt ma már számos olyan összetett infokommunikációs rendszert és -eszközt használunk, amelyek mind a civil, mind a katonai (védelmi) szféra működésében megtalálhatók. Sok esetben még ezek felhasználásának primer céljai is azonosak, hiszen alapvetően kommunikációra, adatfeldolgozásra és adattovábbításra használjuk ezeket az eszközöket és rendszereket. A legtöbb esetben még funkcionális értelemben is azonosak a célok, hiszen alapvetően a vezetés támogatása, illetve maga a vezetés megvalósítása az egyik legfontosabb célja ezeknek a rendszereknek. Ennek a problémának a komplexitását azonban az adja, hogy jelen korunk társadalma – és ez alól nem képez kivételt a kor modern hadserege sem – komoly függőséggel rendelkezik ezekkel az eszközökkel és rendszerekkel szemben. A függőség egyben sérülékenységet is jelent. Ráadásul az említett rendszerek komplexitása, a részrendszerek és elemek összekapcsoltsága és egymásra gyakorolt, a működést alapvetően befolyásoló hatása még inkább növeli ezt a sérülékenységet. Ez nyilvánvalóan azt a veszélyt is magában hordozza, hogy egy-egy részelem vagy részrendszer kiesése alapjaiban lehet negatív befolyással az egész rendszerre. Ez adott esetben a társadalom egy-egy funkciójának a teljes leállásához, vagy ezzel analóg módon egy-egy hadsereg valamely fontosabb funkciójának a leállásához vezethet.

Mindezen okok miatt szükséges a lehető legtávolabb tartani a támadó felet a saját rendszereinktől, illetve a védelmi célú kiberműveletek alkalmazása mellett offenzív műveletekkel megfosztani a támadás lehetőségétől.

3. Katonai offenzív kiberműveleti képességek

A 21. századi korszerű hadseregek egyik jellemzője, hogy a katonai céllal készült infokommunikációs eszközök és rendszerek mellett számos civil megoldást is használnak. Ilyen megoldás például a kommunikáció és adatátviteli célokra használt civil mobil kommunikáció, a 4G vagy az 5G mobil technológia. Ennek több oka van, amelyek között az egyik legfontosabb az, hogy a civil eszközök és rendszerek a hadsereg részéről

jelentkező bekerülési és fenntartási költségei jóval kisebbek vagy elenyészők a kimondottan saját katonai célú technológia-fejlesztés költségeihez viszonyítva. Ugyanakkor ezek a technológiák egyfajta limitációt is jelentenek, hiszen értelemszerűen ezeket az eszközöket és rendszereket háborús körülmények között nem, vagy csak időszakosan tudja használni a hadsereg, mert ezek lesznek az ellenérdekelt fél részéről az elsődlegesen pusztítandó olyan célok, amelyek működésének gátlása a hadsereg vezetésének rombolását és így annak részleges működésképtelenségét is jelenti.

Természetesen ez a polgári technológia esetén önmagában is igaz, hiszen minél több fejlett technológiát használ a civil társadalom, annál inkább nő annak a lehetősége, hogy ezeket támadva lehet – akár katonai – eredményeket is elérni. Itt vonatkoztassunk el attól, hogy ez a nemzetközi jogi szabályozásba ütközik-e vagy sem. Jelen tanulmány első része igyekezett a jogi, illetve nemzetközi jogi kérdéseket nagyon röviden felvillantani és részben megvizsgálni.[2]

Ugyanakkor a hivatkozott első részben azt kellett megállapítani, hogy ez ma a gyakorlatban még egyáltalán nem, vagy csak részben szabályozott terület. Ennek ellenére, vagy éppen emiatt jelenthetjük azt ki, hogy a civil infokommunikációs eszközök és rendszerek, ezeken keresztül pedig az adott ország fontos, ráadásul nagyértékű célpontok lesznek egy esetleges fegyveres konfliktusban, illetve az azzal párhuzamosan megjelenő kiberműveletekben. Természetesen az a tény, hogy a hadsereg civil infokommunikációs eszközöket és rendszereket alkalmaz, magával hozza azt is, hogy az ezekben meglévő vagy az ezekben a későbbiekben felfedezett sérülékenységekkel a hadseregnek is számolnia kell.

A katonai kiberképességek egyik legfontosabb célja természetszerűleg a saját infokommunikációs rendszerek kibervédelmének a biztosítása. Emellett értelemszerűen azonban a hadsereg tevékenysége nem korlátozódik csak a saját rendszereinek védelmére. Ezeknek a képességeknek hozzá kell járulniuk az ország szuverenitásának védelme érdekében tett katonai tevékenységek komplexitásához. A magyar honvédelmi törvény által megfogalmazottak szerint műveleti területnek minősül „a műveleti tervben meghatározott és kijelölt földrajzi terület és a felette levő légtér, továbbá a kibertér".[3] A hazai Nemzeti Biztonsági Stratégia (NBS) szintén rögzíti ezt a célt: „[H]aderőt úgy kell fejleszteni, hogy képes legyen hatásokat kiváltani a hazánk szempontjából releváns összes műveleti térben: a szárazföldön, a levegőben és a kibertérben egyaránt."[4]

Mindezekből azt a következtetést kell levonnunk, hogy a katonai kibertérműveleti képességek, köztük az offenzív kiberképességekkel az ország kibervédelmi képességeinek szerves részét képezik. Ezek a képességek – az ország más kibervédelmi és kiberműveleti képességeivel együtt – hozzájárulnak az ország adaptív ellenállóképességéhez.

Ugyanakkor számos egyéb kiberképesség szükséges egy adott ország kiberbiztonságának megteremtéséhez, fenntartásához, illetve a kibertéri szuverenitás biztosításához. Ezek a sok esetben civil képességösszetevők mintegy komplementer-, azaz kiegészítő

[2] Kovács László: Offenzív kiberműveletek I.: Az offenzív kiberműveletek természete. *Hadmérnök,* 16. (2021), 2. 187–204.

[3] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről 80. §. 22.

[4] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 135. pont.

képességként teremtik meg a katonai kiberképességekkel együtt az ország megfelelő kibervédelmi képességét. Az ország megbízhatóan működni képes kibervédelmi rendszere a kibertéri tevékenységekért felelős szervezetek számára világos feladatrendszert, egyértelműen megfogalmazott hatás- és jogköröket kell, hogy jelentsen. Ugyanakkor ennek megteremtése során azt is figyelembe kell venni, hogy ez nem egy állandó, több évre vagy évtizedre meghatározott szisztéma, hanem a társadalmi, valamint a technikai és technológiai változásokat követni, azokhoz megfelelő módon alkalmazkodni képes rendszert szükséges kialakítani és fenntartani. Ennek egyik alapfeltétele az, hogy a kibervédelmi szereplők közel azonos módon lássák és értékeljék a kibertéri helyzetet. Ez már a nemzeti kiberbiztonsági stratégiában rögzített módon meg kell (vagy kellene), hogy jelenjen, hiszen annak felépítésével, azaz a változó kihívásokhoz alkalmazkodni képes stratégiai céloktól kezdődően a stratégia által meghatározott tevékenységeken át, a szintén a stratégia által meghatározott szervezeti struktúráig számos elemnek kell mindezt, vagyis az alkalmazkodásra és szükség esetén változásra való képesség elvét tükröznie.

A katonai offenzív kiberműveletek szükségessége stratégiai szinten abból indul ki, hogy az országnak joga van megvédenie a szuverenitását a kibertérben is, és joga van rosszindulatú kibertevékenységekkel szemben fellépni. A kibertéri védelem pedig sok esetben nem, vagy csak részlegesen működik kizárólag védelmi kiberműveletek alkalmazásával.

Természetszerűleg az offenzív kiberműveletek alkalmazása során nagy jelentősége van a kiberműveletek életciklusának. Ebben – a már korábban bemutatott életcikluselemek mellett – az egyik legfontosabb tényező az, hogy minél kisebb teret engedjünk az ellenérdekelt fél tevékenységének, ugyanakkor a saját tevékenységeink mozgás- és cselekvési szabadságát biztosítsuk a kiber-, fizikai és információs térben egyaránt.

A katonai offenzív kiberműveletek alkalmazása során számolni és tervezni kell a műveletek közvetlen és közvetett következményeivel is. Az offenzív kiberműveletek végrehajtásához számos feltételnek kell teljesülnie. Sok olyan előfeltétel megléte szükséges, amelyek mind jogilag, mind technikailag megalapozzák és lehetővé teszik e műveletek végrehajtását. Ugyanakkor az offenzív kiberképességek alkalmazása során számolni kell azok hatásaival. A hatások előrejelzése, különösen a járulékos, azaz a közvetett hatások felmérése sok esetben nem, vagy nem megfelelő mértékben lehetséges. Ennek oka a korábban már vizsgált infokommunikációs rendszerek intra- és interdependenciája, valamint azok egyéb – például kiberfizikai – rendszerekhez való összetett kapcsolódása.

Ugyanakkor a katonai offenzív kiberműveleti képességek nem nélkülözhetik az ipari, a kis- és a közepes vállalatokkal, valamint az akadémiai szférával és a kutatóintézetekkel történő együttműködést, csakúgy, mint a nemzetközi kooperációt és kapcsolatokat sem.

4. Kibererők: példák és az azokból levonható következtetések

A katonai kibertéri feladatokat ellátó erők országonként eltérő módon épülnek fel. Ezt a felépítést az adott ország kibervédelméért, valamint a kiberműveletekért felelős

szervezetek időbeni kialakítása, a civil és a katonai feladatok felosztása, valamint az adott ország politikai, kiberszakmai döntései és a kialakított jogszabályi háttér határozza meg. Nagyon röviden, nem tudományos alapossággal és csak a legfontosabb tényezőket felvillantva négy ország – az Amerikai Egyesült Államok, Németország, Lengyelország és Magyarország – kiberműveleti erőit tekintjük át, a katonai kibererőkre fókuszálva. A cél az azokban esetlegesen fellelhető azonos pontok feltárása, ezek mentén igyekszünk olyan általános érvényű következtetéseket levonni, amelyekből jól kivehetők a kiberműveleti erők legfontosabb jellemzői.

4.1. Amerikai Egyesült Államok

Az Egyesült Államokban a katonai kibererőket integráló szervezet az Egyesült Államok Kiberparancsnoksága, azaz a US Cyber Command. A szervezet 2009-ben jött létre az Egyesült Államok Stratégiai Parancsnokságának *(US Strategic Command)* alárendeltségében. Mint alárendelt parancsnokság a US Cyber Command 2010-ben érte el a műveleti készenlétet, és 2018-ban vált önálló komponensparancsnoksággá.

Ugyanakkor a szervezet életében az egyik meghatározó mérföldkő ezt megelőzően az úgynevezett Cyber Mission Force, magyarul a Kiberműveleti Erő létrehozása volt 2013-ban, hiszen gyakorlatilag ez a US Cyber Command végrehajtó ereje. A US Cyber Command – jelen tanulmány írásakor – parancsnoka, Paul Nakasone tábornok, aki 2018 óta látja el ezt a tisztséget, és aki nem mellesleg egyben az Egyesült Államok Nemzeti Hírszerző Ügynökségének (*National Security Agency,* NSA) a vezetője is, a szervezet stratégiai jövőképét felvázoló kiadványában így foglalja össze a szervezet legfontosabb feladatát: „A USCYBERCOM hozzájárul a nemzeti stratégiai elrettentésünkhöz. Felkészítjük, működtetjük és együttműködünk a harcoló parancsnokságokkal, fegyvernemekkel, szövetségesekkel és az iparral annak érdekében, hogy folyamatosan akadályozzuk és megmérettessük az ellenséges kibertér szereplőit, bárhol is találjuk őket."[5]

Meg kell jegyezni, hogy az említett kiadványnak már a címe is rendkívül beszédes: „A kibertéri fölény elérése és fenntartása. Parancsnoki jövőkép az Egyesült Államok Kiberparancsnoksága számára" (angolul: *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command*).[6]

A US Cyber Command 133 Cyber Mission Force (CMF), azaz 133 önálló kiberműveleti csoport kiképzését felügyeli. Ezek az egységek a különböző haderőnemek kiberparancsnokságai alárendeltségében működnek, ugyanakkor maguk a haderőnemi kiberparancsnokságok is a US Cyber Command szakmai felügyelete alá tartoznak. A CMF-ek egységes felkészítése és kiképzése óriási előnnyel jár abból a szempontból, amely az egységes terminológiai értelmezéstől kezdődően a kihívásokra adott egységes és koherens technikai válaszokig bezárólag jelentkezik.[7]

[5] US Cyber Command: Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command. (2018. április).
[6] US Cyber Command (2018): i. m.
[7] US Cyber Command: *Cyber Mission Force achieves Full Operational Capability.* (2018. május)

Meg kell jegyezni azonban, hogy a CMF-ek felkészítése és azok képességeinek magasabb szintre emelése nem megy mindig zökkenőmentesen. Ennek adott hangot az Egyesült Államok Számvevőszéke (*Government Accountability Office,* GAO), amikor kritikát fogalmazott meg ezzel kapcsolatban: „A Védelmi Minisztérium a CMF építéséről annak fejlesztésére helyezte át a hangsúlyt. A minisztérium kidolgozta a CMF transzformációs tervét, amely az alapozó (második fázis[8]) képzési szakasz felelősségét átruházza a haderőnemekre. A szárazföldi haderőnek és a légierőnek azonban nincs elég időkerete az alapozó tanfolyamok CYBERCOM szabványoknak megfelelő érvényesítéséhez. Továbbá a haderőnemek tervei nem tartalmazzák a CMF összes képzési követelményét, például a kiképzésre szoruló létszámot. A CYBERCOM nem tervezi a szükséges független értékelők felállítását a kollektív (harmadik fázis) CMF-képzés következetességének biztosítása érdekében."[9]

A US Cyber Command részt vett az amerikai elnökválasztásba beavatkozni kívánó külföldi kibererők elleni tevékenységben, valamint egy 2018-ban, a Belbiztonsági Minisztérium (*Department of Homeland Security,* DHS) és a Védelmi Minisztérium (*Department of Defense,* DoD) között született megállapodás alapján a kritikusinfrastruktúra-védelemben is komoly szerepet kap. Azonban a US Cyber Command talán egyik leghíresebb művelete az úgynevezett Glowing Symphony művelet volt, amely során a Joint Task Force-Ares – a US Cyber Command által offenzív kiberműveletek végrehajtására dedikált egyik – csapat az ISIS nemzetközi terrorszervezet ellen mért célzott kibercsapásokkal az „ISIS média és online műveleteit célozta meg, megfosztva infrastruktúrájától, és megakadályozva az ISIS tagjait a propaganda kommunikációjában és közzétételében".[10]

A fenti, 2016-ban végrehajtott offenzív kiberművelet, illetve műveletek együttese nagy vonalakban ma már tanulmányozható, hiszen számos olyan dokumentum titkosítását feloldotta az NSA, amilyenek például a támadásokról szóló jelentések voltak. Ugyanakkor ezek a ma már nem titkos minősítésű jelentések legtöbb részletükben kitakartak, így csak a legfontosabb történésekbe kapunk betekintést.[11]

4.2. Németország

Németország meglehetősen egyedi utat választott a kibertérműveleti erők kialakítása során. 2016 áprilisában Ursula von der Leyen, az akkori német szövetségi védelmi miniszter bejelentette, hogy Németország egy Kiber- és Információs Domain Parancsnokságot állít fel, amely közel 13 500 fő katona és civil szakembert foglal majd magában.[12]

[8] A CMF kiképzési modell négy fázisból áll, alap egyéni kiképzés, egyéni alapozó kiképzés, kollektív kiképzés, szinten tartó kiképzés.

[9] United States Government Accountability Office: DOD TRAINING. U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force. (2019. március).

[10] Mark Pomerleau: What Cyber Command's ISIS operations means for the future of information warfare. *C4ISRNet,* 2020. június 18.

[11] National Security Archive: USCYBERCOM 30-Day Assessment of Operation Glowing Symphony. (2016. december 13.).

[12] Zeit Online: Bundeswehr rüstet gegen Attacken aus dem Internet. (2016. április 26.).

A szervezet a Bundeswehr alakulataként 2017 áprilisában létre is jött. Az új Kiber- és Információs Domain Parancsnokság számos korábbi alakulatot integrált, így kiterjedt feladatrendszerrel alakult meg. Ezek közül a feladatok közül – természetszerűleg a Bundeswehr saját információs rendszereinek a védelme és azok üzemeltetése mellett – a legfontosabbak a felderítés (hírszerzés, megfigyelés) a kibertérben és az elektromágneses spektrumban végzett aktív műveletek, valamint a geoinformációs szolgáltatások ellátása.[13]

Ezek a feladatok magukban foglalják tehát a hadsereg infokommunikációs rendszereinek üzemeltetését, azok 24 órás felügyeletét, a szoftverfejlesztést, a szimulációs rendszerek IT- és geoinformációs támogatását.[14] Az offenzív kiberműveleti feladatok mellett megjelenő elektronikai hadviselési tevékenységek jól jellemzik azt a tényt, hogy a német kibertér-értelmezés eltér a hagyományos kibertér-értelmezéstől, például attól, amit a NATO hivatalosan is követ, hiszen a NATO Kibertér Műveleti Doktrínája a kiberteret a következőképpen határozza meg: [Kibertér] „Globális tartomány, amely magába foglalja mindazon infokommunikációs és egyéb elektronikai rendszereket, hálózatokat és azok adatait, beleértve az elkülönült vagy független rendszereket, hálózatokat, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak."[15]

Ezzel szemben, vagy talán ezt megerősítve a német kibertér-értelmezés szerint a kibertér tartalmazza az elektromágneses spektrumot és a kognitív dimenziót is. Ez magyarázhatja az elektronikai hadviselés és a kognitív dimenzióra ható információs domain integrálását is.

A szervezet számos nemzeti és nemzetközi kapcsolatot tart fenn különböző kiberbiztonsági és kiberműveleti szervezetekkel, aminek során az egyik legfontosabb feladat az információcsere megvalósítása.[16]

Az alakulat felállítása és annak széles körű feladatai nagyon jól beleillenek abba a feladatrendszerbe, amelyet a német nemzetbiztonsági stratégia 2016-ban meghatározott.[17] (Németország fehér könyvként adja ki a nemzetbiztonsági stratégiáját, amely nemcsak a biztonságpolitikai célokat, hanem a hadsereg, azaz a Bundeswehr szerepét és stratégiai feladatait is meghatározza.)

4.3. Lengyelország

Lengyelországban a Védelmi Minisztérium égisze alatt alakították meg a Nemzeti Kiberbiztonsági Központot 2019-ben. A központ feladata a védelmi minisztérium és a lengyel hadsereg IT-üzemeltetési és -fejlesztési feladatain túl a nemzeti szintű kiberbiztonság koordinálása, valamint számos kriptográfiai tevékenység ellátása, továbbá a szervezet alárendeltségébe tartozik a katonai eseménykezelő központ

[13] Bundeswehr: Kommando Cyber- und Informationsraum. (é. n.).
[14] Ludwig Leinhos: The German Cyber and Information Domain Service as a Key Part of National Security Policy. *Ethics and Armed Forces,* (2019), 1.
[15] AJP-3.20 Allied Joint Doctrine for Cyber Space Operations Edition A Version 1, 2020. 4.
[16] Bundeswehr: The Cyber and Information Domain Service. (é. n.).
[17] Ludwig Leinhos: Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr. *Connections: The Quarterly Journal,* 19. (2019), 1. 9–19.

(*Computer Security Incident Response Team – Ministerstwa Obrony Narodowej,* CSIRT-MON) is[18]. A Központ egyik fontos szervezeti eleme a Kiberműveleti Központ, amely a „katonai műveletek teljes spektrumában hajt végre kibertéri műveleteket, olyan körülmények között is, amikor a hagyományos erők alkalmazása nem lehetséges vagy nem célszerű".[19]

A központ felállítása előtt a lengyel kiberbiztonsági rendszer sok elemből állt. Az eltérő közigazgatási szervezethez (például különböző minisztériumokhoz) tartozó kiberbiztonsági csoportok és feladataik megosztott helyzetet teremtettek, az abban megvalósuló koordináció, illetve annak nem kielégítő volta azonban sok kritikát kapott. Természetesen volt jól működő eleme is a rendszernek, például az eseménykezelés, amely folyamatosan jól teljesített.[20]

2019-ben a védelmi minisztérium életre hívta az úgynevezett Cyber.Mil.Pl programot, amelynek két legfontosabb eleme a kibertérvédelmi erők létrehozásának támogatása, valamint a védelmi minisztérium kiberbiztonsági feladatainak az integrálása.[21]

A program stratégiai célja természetesen az ország kiberbiztonságának növelése. Ennek érdekében a programban olyan szervezetek is részt vesznek, mint a varsói Katonai Műszaki Egyetem, a lengyel Haditengerészeti Akadémia, a Katonai Kommunikációs Intézet, amely az 1950-es évek óta működő kutatóintézet, valamint szerepet kapnak a programban a lengyel területvédelmi erők is.[22]

2020-ban adták át a Nemzeti Kiberbiztonsági Központ szakmai irányítása alá tartozó Kiberbiztonsági Képzési Kiválósági Központot *(Cyber Training Centre of Excellence),* amely újabb lépés lehet a szakmailag felkészült utánpótlás biztosítására a lengyel kibervédelmi és kiberműveleti erők számára.[23]

4.4. Magyarország

Hazánk szintén sajátos utat jár be a kibererők építése során. A hazai kiberbiztonság megteremtése során az egyik legfontosabb állomás a 2013-ban megjelent információbiztonsági törvény, hivatalos megnevezéssel 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.), illetve annak 2015-ös jelentős módosítása. Ez azonban csak a kiberbiztonság civil szervezeti keretét határozta meg, és csak érintőlegesen tárgyalta a honvédelmi ágazatot, illetve a hadsereg szerepét a kiberbiztonság megteremtésében.[24]

Ennek megfelelően, Magyarországon a kiberbiztonság civil szervezetei közül az egyik legfontosabb elem a Belügyminisztérium irányítása alatt működő Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NKI). Az NKI magában foglalja a nemzeti információbiztonsági hatóságot, a kormányzati hálózat- és eseménykezelő központot,

[18] CSIRT-MON: *Ministerstwa Obrony Narodowej*. (2021)
[19] Cyber.Mil.PL: Cyber Operations Center. (2021)
[20] Joanna Świątkowska – Izabela Albrycht – Dominik Skokowski: National Cyber Security Organisation: POLAND. Tallinn, NATO CCDCOE, 2017. 13.
[21] Cyber.Mil.Pl: O Nas. (2021)
[22] Cyber.Mil.Pl: i. m.
[23] Cyber Security Training Centre of Excellence: What we do. (é. n.).
[24] Kovács László: Kiberbiztonság és -stratégia. Budapest, Dialóg Campus, 2018. 242.

illetve a sérülékenységvizsgálatot végző szervezeti elemet. Ebből következően az NKI elsősorban az eseménykezelésre, az elektronikus információbiztonság hatósági feladataira és a sérülékenységvizsgálatra, valamint nem utolsósorban a biztonságtudatosság növelésére fókuszál. Ugyanakkor sem a civil kiberbiztonsági szervezetek, sem az NKI nem rendelkezik a jelen tanulmányban megfogalmazott kritériumoknak megfelelő kiberműveleti erővel és offenzív kiberképességekkel.

A honvédelmi ágazaton belül két kiberműveleti szervezet alakult meg az elmúlt években. A Katonai Nemzetbiztonsági Szolgálatnál (KNBSZ) 2017-ben létrejött a Kibervédelmi Központ, amely 2021-től új néven, mint KNBSZ Kibertér Műveleti Központ látja el az ágazati elektronikus információbiztonsági eseménykezelés feladatait, valamint e szervezet egyik eleme a honvédelmi ágazati elektronikus információbiztonsági hatóság is. A honvédelmi ágazat másik kiberszervezete a Magyar Honvédség (MH) Parancsnoksága (MHP) alárendeltségében 2019-ben megalakult Kibervédelmi Haderőnemi Szemlélőség, illetve annak szakmai vezetésével várhatóan létrejövő Magyar Honvédség Katonai Kibertér Műveleti Központ (MH KKMK). A Szemlélőség fő feladata, hogy stratégiai szinten felügyelje és irányítsa az MH katonai kibertér műveleti erőinek kialakítását, fejlesztését, majd azok működtetését. A Szemlélőség szakirányítási feladatköre kiterjed a kiberszakterületet érintő valamennyi haderőfejlesztési és -fenntartási programra. A kiberszakterületen „szakmai felelős" jog- és hatáskörrel rendelkezik. A Szemlélőség határozza meg az MH kibervédelmi és kiberműveleti szakterülete vezetéséhez szükséges szervezeti kialakítás alappilléreit, valamint a kialakítandó kibervédelmi szervezetek struktúráját. Természetszerűleg a Szemlélőség szorosan együttműködik az MHP Infokommunikációs és Információvédelmi Csoportfőnökséggel, amely szervezet a honvédség IT-rendszereinek üzemeltetéséért és elektronikus információbiztonságáért felelős. A Szemlélőség szakmai irányításával megkezdődött az MH Katonai Kibertér Műveleti Központ kialakítása, amely a következő években várható folyamatos fejlődése során a katonai kibervédelem és a kiberműveletek szervezeti hátterét is nyújtja majd. Ez azt is jelenti, hogy a szervezet a kiberműveletek tervezéséhez és végrehajtásához szükséges adat- és információfeldolgozó képességgel, valamint offenzív kiberműveleti képességekkel és azok hatásait elemezni képes szervezeti elemekkel is fog rendelkezni. Az MH KKMK magában foglalja a már korábban, 2019-ben megalakult kiberképzési központot (Kiberakadémia) is.

A katonai kiberműveleti képességek kialakításáról a már említett új Nemzeti Biztonsági Stratégia rendelkezik. A stratégia az offenzív kiberműveleti képességeket is magába foglaló katonai fejlesztést és képességépítést a következő módon határozza meg: „A katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a haderő kinetikus műveleteinek kibertérbeli támogatására, ki kell alakítani a kiberműveletekben alkalmazható offenzív képességeket. Ennek érdekében fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit."[25] Az NBS által meghatározott katonai kiberműveleti képességek alkalmazására a honvédelmi törvény ad felhatalmazást, illetve szab feladatot a 2020. január 1-jével a törvénybe bekerült katonai kibertérműveleti erőkre vonatkozó szabályokkal. Ezek többek között tartalmazzák, hogy az MH katonai kibertérműveleti erői folyamatosan ellátják „a honvédelmi szervezetek, gyakorlatok,

[25] 1163/2020. (IV. 21.) Korm. határozat 135. pont, 159. pont.

műveletek kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmét, az arra történő felkészülést és a kapcsolódó biztonsági feladatokat",[26] „a folyamatban lévő, kibertérből érkező támadás megszakításához szükséges intézkedések végrehajtását, vagy annak kezdeményezését",[27] valamint „külön döntés szerint a Magyarország biztonságát, honvédelmi érdekeit, vagy szövetségesi kötelezettségeit sértő vagy fenyegető rendszerekkel szembeni katonai kibertérműveleti fellépést".[28]

Mindezek a katonai kibertérműveleti erők alkalmazásához szükséges, de nem elégséges feltételek, ugyanis számos egyéb olyan tényező is szükséges ezen erők alkalmazásához, mint amilyenek például a fenti – honvédelmi törvényből idézett – „külön döntés alapján" kitételek. Ez többek között a Kormány döntését jelenti, amely a törvény meghatározása alapján más elemek fennállása – például különleges jogrendi helyzet – esetén szükséges egy-egy támadó jellegű kibertérművelet végrehajtásához.

4.5. A felvázolt kibererők elemzéséből levonható következtetések

Már a fentiekben bemutatott néhány kiberműveletekért felelős szervezet vizsgálata alapján is azonosítani tudunk olyan általános jellemzőket, amelyek a legtöbb ország kibertérműveleti szervezetei esetében igazak. Ezek a szervezetek – természetszerűleg a fentiekben megfogalmazottaknak megfelelően országonként eltérő módon, de mégis jól azonosíthatóan – három nagy területre koncentrálnak. Ezek a területek, amelyeket jelen tanulmány első részében részletesen is bemutattam, az információszerző, célkiválasztó, célazonosító és célkövetési, valamint szimulációs képesség, a kibertámadás képessége és a hatások értékelésének képessége területek. Bár a fent bemutatott kibervédelmi és kiberműveleti szervezetek országonként eltérő feladatrendszerrel rendelkeznek, de többnyire ezek mégis a kibertérre és esetenként az információs dimenzióra vonatkozó feladatokat is jelentenek.

Az azonban a többé-kevésbé eltérő feladatrendszer ellenére is világosan látszik, hogy minden ország a katonai kibererőitől az adott ország teljes kibervédelmi képességeinek a növelését várja, illetve ezekben az erőkben látja ennek garanciáját. A katonai feladatok mellett esetenként megjelenik az adott ország kritikus infrastruktúrája védelmének feladata is. Természetszerűleg az Egyesült Államok katonai kiberműveleti erői sok esetben olyan feladatokat is ellátnak, amelyek egy-egy európai ország katonai kiberműveleti erői esetében békeidőben nem feladatok (például a politikai választások informatikai rendszereinek a védelme, vagy aktív hírszerző/felderítő tevékenység).

A bemutatott katonai kiberműveleti erők elemzése azt is világossá teszi, hogy ezeknek a szervezeteknek a kialakítása, majd felkészítése és aktív, offenzív műveletek végrehajtására is kész képesség birtokába hozása hosszú időt vesz igénybe, ami 3-4 évet, de a teljes készenlét elérése akár 10 évet is jelenthet. Ugyanakkor fontos hangsúlyozni, hogy egy katonai kibertérműveletek ellátására alkalmas szervezetről sosem jelenthető ki, hogy az kész van, hiszen időről-időre újabb és újabb kibertéri

[26] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről, 62/A. §. (1) a) pont.
[27] 2011. évi CXIII. törvény 62/A. §. (1) b) pont.
[28] 2011. évi CXIII. törvény 62/A. §. (1) c) pont.

kihívásokkal kell szembenézni, ami megköveteli a szervezet és/vagy annak képességbeli változását. Ugyanez igaz a személyi állományára is, hiszen az ő felkészítésük nem ér véget egy-egy tanfolyam vagy képzés elvégzésével. A különböző műveletek végrehajtása során felhalmozott tapasztalat és annak átadása szintén hozzájárul az állomány folyamatos fejlesztéséhez. Itt azonban egy problémát szükséges jelezni. Ez pedig a szakértő kiberműveleti állomány megtartása. Megfelelő bérezés, megfelelő munkakörülmények és nem utolsósorban megfelelő és inspiráló szakmai kihívások azok a tényezők, amelyek megtartó erőként szolgálhatnak. Egy ideig. Ugyanis a jól képzett, gyakorlott, megfelelő szakmai és nem utolsósorban műveleti tapasztalattal rendelkező kiberműveleti szakember értéke a munkaerőpiacon évről évre exponenciálisan nő. A civil – főleg a multinacionális – cégek által nyújtott fizetési és egyéb juttatásokkal a közszféra, így a katonai terület sem tud versenyezni. Ez még az Egyesült Államokra is igaz.

Egy másik, bár meglehetősen triviális megállapítás a fentiek alapján, hogy minden ország rendkívül fontosnak tartja a szakemberek utánpótlásának folyamatos biztosítását. Ez már a középiskolák és az ott tanuló diákok képzésében és toborzásában is megjelenik. Ezt teszi a US Cyber Command. A parancsnokság létrehozta a Cyber Patriot STEM (*Science, Technology, Engineering, and Mathematics,* STEM, magyarul mérnöki és matematikatudományi) programot, amely keretében helyi középiskolákkal folytat együttműködést, illetve több mint 50 egyetemmel végez közös munkát, amely egyrészt közös kutatás-fejlesztést, másrészt tehetséges jövőbeni munkavállalók felkutatását és kiválasztását is jelenti.[29]

Hasonló programot indított a lengyel Nemzeti Kibervédelmi Központ is, amely az úgynevezett Cyber.Mil.Pl program keretében a varsói Katonai Műszaki Egyetem támogatásával kiberbiztonsági tematikájú középiskolai osztályt, illetve e mellett kiberbiztonsági egyetemi mesterképzést is indított 2019 őszén.[30]

Németország is hasonló lépéseket tett, hiszen a müncheni Bundeswehr Egyetemen kiberbiztonsági mesterképzést indított.[31]

Hazánk is komoly lépéseket tett az oktatás és az utánpótlás területén. Számos egyetemen indult el az informatikai szakokon kiberbiztonsági témájú tárgy oktatása, illetve a Nemzeti Közszolgálati Egyetem elindította a Kiberbiztonság nevű kétéves mesterképzési szakját is.[32]

A vizsgált országok mindegyikében kiemelt szerepet kap a kutatás-fejlesztés a kiberbiztonság és a kiberműveletek területén. A kibertéri erők ehhez sok esetben igénytámasztóként jelennek meg, de természetszerűleg maguk is kell, hogy rendelkezzenek K + F képességekkel, amelyek a kevésbé energia- és időigényes fejlesztési feladatokat látják el. Ugyanakkor az akadémiai szférával – például egyetemekkel, kutatóintézetekkel –, valamint a civil IT-szektorban és/vagy a kiberbiztonsági iparban dolgozó és kutató vállalatokkal történő kapcsolattartás és szoros együttműködés szintén elengedhetetlen. A jól működő K + F hosszú távú folyamat, amely azokra az igényekre ad gyakorlatban is használható választ (eredményt), amelyek a potenciális

[29] US Cyber Command: Cybercom Media Roundtable. (2019. május 7.)
[30] Cyber.Mil.Pl program i. m.
[31] Universität der Bundeswehr München: Studiengang Master Cyber-Sicherheit. (é. n.).
[32] Nemzeti Közszolgálati Egyetem: Kiberbiztonsági mesterképzési szak. (é. n.).

szemben álló fél polgári és/vagy katonai rendszereinek védelméhez, illetve támadásához szükségesek.

A kutatás-fejlesztés egyik nagyon jó példája, és ha tetszik, reklámja is az amerikai Dreamport kezdeményezés, amelyben azok a legújabb kutatás-fejlesztési és innovációs projektek és azok eredményei kapnak helyet, amelyeket a kormányzati szervezetek – mint például a US Cyber Command –, az akadémiai szféra és az ipari szereplők közösen végeznek és érnek el.[33]

Németország a haderő támogatásával egy kiberbiztonsági kutatóintézetet alapított Berlinben, amely szintén ellát K + F feladatokat.[34] Hazánkban a Nemzeti Közszolgálati Egyetemen alakítottak meg egy Kiberbiztonsági Kutatóintézetet, amely alkalmas lehet a jövőben a kiberterület tudományos alapjainak megteremtése és kutatása mellett K + F feladatok elvégzésére, illetve azok akadémiai szférán belüli koordinálására.

5. Az offenzív kiberképességek és a NATO

A NATO nagy utat tett meg azóta, hogy 2016-ban a Varsói Csúcsértekezleten a negyedik műveleti térré minősítette a kiberteret.

A kibertér műveleti térré nyilvánításával egy időben a tagországok egyöntetűen állást foglaltak abban, hogy kibervédelmi képességeiket fejlesztik. Ez az úgynevezett Cyber Pledge, azaz Kibervállalás, amelyet azóta is évente nagyon következetes módon a NATO ellenőriz. Ennek során nemcsak az ellenőrzésen van a hangsúly, hanem a szervezet tanácsokat és segítséget is nyújt a kibertéri képességek kialakításában, illetve fejlesztésében.

A Cyber Pledge esetében is igaz az a tény, amelyet a nemzeti kibervédelmi képességek során már megállapítottunk. Nevezetesen, hogy ez nem csak katonai, hanem össztársadalmi feladat. Ezt támasztja alá a NATO hivatalos közleménye is, amely a Cyber Pledge-dzsel kapcsolatosan a következőket jelenti ki: „A Pledge-et a washingtoni szerződés 3. cikkével összefüggésben fogadták el, amely kimondja, hogy »a szövetségesek fenntartják és fejlesztik egyéni és kollektív képességüket a fegyveres támadások ellen.« Mivel ebben a térben lehetetlen teljesen szétválasztani a katonai, polgári és ipari kérdéseket, a NATO-nak komoly érdeke fűződik a Szövetségen kívüli szervezetek kibervédelmi képességeinek javításához."[35]

A NATO-nak önmagának nincsenek offenzív kiberképességei. Ilyen képességekkel a tagországok rendelkeznek, de mivel nem minden tagország mutatja be vagy vállalja fel nyilvánosan e képességeit, ezért pontos számot vagy képességet csak becsülni lehet. Néhány ország ezeket a képességeit felajánlotta a NATO számára, így róluk biztosan tudhatjuk, hogy rendelkeznek offenzív kiberképességekkel. A tagállamok által önkéntesen felajánlott offenzív kiberképességekre a NATO egy sajátos terminológiát is alkotott, amelyet az angol kifejezésből származtatott mozaikszóval SCEPVA-nak (*Sovereign Cyber Effects Provided Voluntarily by Allies,* azaz a Szövetségesek Önkéntes

[33] Maryland Innovation & Security Institute: https://dreamport.tech/
[34] Bundeswehr: Zentrum für Cyber-Sicherheit der Bundeswehr. (é. n.).
[35] Laura Brent: NATO's role in cyberspace. NATO, 2019. február 12.

Hozzájárulásán Alapuló Kiberhatások) neveznek.[36] Ennek fontosságát hangsúlyozza Libicki egy tanulmányában: „Bár a NATO-nak nincs saját támadó kiberképessége, de a kiberműveletek növekvő jelentősége a NATO hatékony kollektív védelme és elrettentése szempontjából megköveteli annak alapos megértését, hogy a kiberképességek kihasználása hogyan befolyásolhatja a konfliktusok dinamikáját."[37]

Németország az egyik olyan ország, amely felajánlotta kiberképességeit a Szövetségnek. Az akkori német védelmi miniszter, a már említett Ursula von der Leyen nem részletezte a felajánlott kiberképességek mibenlétét, de úgy fogalmazott: „Ahogy a szárazföldi haderőkkel, a légierővel és a haditengerészeti erőkkel támogatjuk a NATO-t, most abban a helyzetben vagyunk, hogy a rendelkezésünkre álló nemzeti és jogi keretek között biztosítsuk a NATO képességeit kiberügyekben."[38]

Mindezeket a tagországi felajánlásokat is koordinálja a NATO Kibertér Műveleti Központja (*Cyberspace Operation Center,* CyOc), amit a NATO parancsnoki struktúrájának részeként állítottak fel. A CyOc a SHAPE, a NATO Európai Erők Főparancsnokságán (*Supreme Headquarters Allied Powers Europe,* SHAPE) J6 besorolású, azaz az infokommunikációs főnökség része. Dedikáltan ez a – 2017-es felállítását követő három évben magyar tábornok, Vass Sándor által vezetett – szervezet lehet az egyik legfontosabb szereplője a kibertámadások összehangolásának a Szövetségen belül.

Ugyanakkor a kiberműveletek területén a NATO egyik legnagyobb kérdése, ha tetszik legfontosabb problémája a tagországok eltérő kibervédelmi fejlettsége. Ez részben igaz az offenzív kiberképességek területére is. Azért csak részben, mert ezen a területen egyéb kérdések is felmerülnek. Az első ilyen kérdés az, hogy abban az esetben, ha egy tagország felajánlja kibertámadó képességeit a NATO-nak, és azt alkalmazzák, akkor a nemzet vagy a Szövetség lesz-e a felelős a művelet végrehajtásáért, illetve azok esetleges következményeiért?

A fentiek mellett a NATO még egy hatalmas problémával küzd, amely nem más, mint a háborús küszöbszint alatt tartott kiberkonfliktusok problémája. Korábban már említettük, hogy ez a helyzet talán a „még nincs háború, de már nem beszélhetünk békéről" kifejezéssel jellemezhető. Ez az időszak óriási kihívás elé állítja a kiberbiztonság területén dolgozó szakembereket. Az ilyen módon alkalmazott offenzív kiberműveletek nem elsősorban technikai értelemben vett kihívást, sokkal inkább politikai, jogi és diplomáciai problémát jelentenek.

Ezeknek a kérdéseknek a kutatása kiemelten fontos. Itt ki kell emelni a NATO Kibervédelmi Kiválósági Központjának (*Cooperative Cyber Defence Centre of Excellence,* CCDCOE) munkáját. A 2008-ban alakult kutatóközpont a NATO-hoz hasonlóan önmaga is hatalmas utat járt be a kiberbiztonság kutatásának területén, és mára az egyik meghatározó szereplőjévé vált a témának. A stratégiai kérdésektől és az azokban a tagországoknak nyújtott segítségtől kezdődően, a kiberbiztonság területén végzett különböző kutatásokig elmenően hatalmas oktatási, képzési munkát is végez a központ. A szervezet által készített és rendszeresen publikált tanulmányokban nem csak a NATO-tagországokból származó kutatók a fenti kérdésekre keresik a választ.

[36] AJP 3.20 (2020): i. m. 1.16. pont.
[37] Martin C. Libicki – Olesya Tkacheva: Cyberspace Escalation: Ladders or Lattices? In A. Ertan et al. (szerk..): Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCDOE, 2020. 61.
[38] AFP: Germany to Let NATO Use its Cyber Skills. *Security Week,* 2019. február 14.

Ezeknek a kérdéseknek a korántsem egyértelmű megítéléséről így ír Libicki és társa a CCDCOE-nek, a NATO-val szembeni kiberfenyegetéseket 2030-as idősíkon elemző kötetében:[39] „A kibertérben véget nem érő konfrontációk ellenére a stratégiai kiberháború azon lehetősége, hogy komoly károkat okozzon a modern gazdaságban, továbbra is vita tárgya […] Minél nehezebb előre kitalálni a [kiberháború] hatását, annál nagyobb a nézeteltérés annak megítélésében, hogy az ilyen műveletek elkezdődnek-e."[40]

6. Összefoglalás, következtetések

Az ma már nem kérdés, hogy a kibertér és annak biztonsága az egyik legfontosabb biztonság- és védelempolitikai és ezzel együtt katonai kérdés is egyben. Az új műveleti tér a hadviselés változásával, és nem utolsósorban az ehhez a térhez (is) történő adaptációjával új típusú katonai szervezetek létrehozását is indukálta világszerte.

A jelen írásban bemutatott néhány ország, köztük hazánk kiberműveleti képességeiből számos következtetés vonható le, amelyek közül az egyik az, hogy e képességek egyre növekvő mértékben tartalmazzák az offenzív kiberműveleti képességeket.

Az offenzív kiberképességek megjelenését leginkább az indokolja, hogy ezzel a képességgel, annak akár aktív alkalmazásával, akár csak egyszerű deklarálásával (amely mögött azonban a korábban említett valódi képességeknek meg kell lenniük) a saját rendszereinktől, legyenek azok katonai vagy civil rendszerek, a lehető legtávolabb tartsuk a potenciális rosszindulatú kibertevékenységeket. Ez jelenthet egyfajta elrettentést is, de jelentheti azt is, hogy olyan mértékben csökkentjük az ellenérdekelt fél (kiber)képességeit, amelyekkel már nem tud hatékony támadást indítani az információs rendszereink ellen.

A katonai kibertérműveleti képességek azonban nem csak, és nem elsősorban katonai célokat szolgálnak. Ezek a képességek az ország kibervédelmi képességeihez alapvető módon járulnak hozzá, annak szerves részét képezik. A katonai kiberképességek, az ország civil kibervédelmi és kiberműveleti képességeivel együtt jelentik az ország adaptív ellenállóképességének egyik igen fontos elemét.

A tanulmányban bemutatott négy ország kiberműveleti erőinek elemzéséből levonható következtetések is mutatják, hogy a katonai kibertéri feladatokat ellátó erőket országonként eltérő módon alakították ki és részben eltérő feladatokat is látnak el. Ugyanakkor – szervezeti kialakítástól függetlenül – megállapíthatók az azonos feladatok és felelősségi területek. Az információszerző, célkiválasztó, célazonosító és célkövetési, valamint szimulációs képesség, a kibertámadás képessége és a hatások értékelésének képessége területek a bemutatott országok katonai kiberműveleti erői esetében is fellelhetők.

A helyenként eltérő feladatrendszer ellenére is világosan látszik, hogy minden országban a katonai kiberműveleti erők az adott ország teljes kibervédelmi képességeinek a növeléséhez szignifikáns módon járulnak hozzá.

[39] A. Ertan et al. (szerk.): Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCDOE, 2020.
[40] Libicki–Tkacheva (2020): i. m. 67.

A bemutatott katonai kiberműveleti erők elemzése során látható, hogy ezeknek a szervezeteknek a kialakítása, felkészítése és aktív, offenzív műveletek végrehajtására is kész, egységes szemlélettel rendelkező, ütőképes erővé való fejlesztése minimum 3-4 évet, de azok teljes műveleti készenlétének elérése akár 10 évet is igénybe vehet.

Az elemzésekből levonható további markáns következtetés, hogy a technikai fejlesztéseken kívül a szakemberek utánpótlásának biztosítása, illetve a szakemberek megtartása kiemelten fontos kérdés. Az ezeket a kérdéseket kezelni képes oktatási és továbbképzési rendszer, a szakembereknek a szintén elengedhetetlen kutatás-fejlesztés feladataiba való – minél korábban történő – bevonására is komplex módon ki kell terjedjen.

A NATO-t kiberműveleti szempontból röviden megvizsgálva kijelenthető, hogy a Szövetségnek önmagának nincsenek offenzív kiberképességei. Ilyen képességekkel csak a tagországok rendelkeznek, amelyeket önkéntes alapon ajánlanak fel a szervezetnek. Ezek a felajánlott képességek, illetve azok alkalmazásai, bár hozzájárulnak a NATO elrettentési politikájához, mégis számos – elsősorban jogi és felelősségi – kérdést vetnek fel, amelyekre jelenleg számos tudományos kutatás keresi a választ.

A fentiekben idézett Libicki-gondolat is rávilágít arra, hogy sem a NATO, sem a nagyhatalmak, sem a kisebb országok nem lehetnek teljesen biztosak a kibertér, illetve az abban folytatott műveletek jövőbeni szerepében. Ennek megfelelően szükséges akár a Szövetség, akár az egyes országok kiberképességeit a védelmi képességek mellett az offenzív képességeket is magában foglaló módon építeni.

Felhasznált irodalom

AFP: Germany to Let NATO Use its Cyber Skills. *Security Week,* 2019. február 14. Online: www.securityweek.com/germany-let-nato-use-its-cyber-skills

AJP-3.20 Allied Joint Doctrine for Cyber Space Operations Edition A Version 1, 2020.

Brent, Laura: *NATO's role in cyberspace.* NATO, 2019. február 12. Online: www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Bundeswehr: *Kommando Cyber- und Informationsraum.* (é. n.). Online: www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum

Bundeswehr: *The Cyber and Information Domain Service.* (é. n.). Online: www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service

Bundeswehr: *Zentrum für Cyber-Sicherheit der Bundeswehr.* (é. n.). Online: www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-informationstechnik-der-bundeswehr/zentrum-fuer-cyber-sicherheit-der-bundeswehr

CSIRT-MON: *Ministerstwa Obrony Narodowej*. (2021). Online: https://csirt-mon.wp.mil.pl/pl/

Cyber.Mil.PL: *Cyber Operations Center.* (2021). Online: www.cyber.mil.pl/articles/o-nas-f/2018-10-23c-centrum-operacji-cybernetycznych/

Cyber.Mil.Pl: *O Nas.* (2021). Online: www.cyber.mil.pl/o-nas/

Cyber Security Training Centre of Excellence: What we do. (é. n.). Online: https://cstcoe.mil.pl/en/pages/what-we-do/

Ertan, A. – K. Floyd – P. Pernik – T. Stevens (szerk.): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* NATO CCDOE, 2020. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

Kovács László: Offenzív kiberműveletek I.: Az offenzív kiberműveletek természete. *Hadmérnök,* 16. (2021), 2. 187–204. Online: https://doi.org/10.32567/hm.2021.2.13

Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018. Online: http://kovacsx.hu/download/books/KovacsLaszlo_A_kiberbiztonsag_es_strategia.pdf

Leinhos, Ludwig: Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr. *Connections: The Quarterly Journal,* 19. (2019), 1. 9–19. Online: https://doi.org/10.11610/Connections.19.1.02

Leinhos, Ludwig: The German Cyber and Information Domain Service as a Key Part of National Security Policy. *Ethics and Armed Forces,* (2019), 1. Online: www.ethikundmilitaer.de/en/full-issues/20191-conflict-zone-cyberspace/leinhos-the-german-cyber-and-information-domain-service-as-a-key-part-of-national-security-policy/

Libicki, Martin C. – Olesya Tkacheva: Cyberspace Escalation: Ladders or Lattices? In A. Ertan – K. Floyd – P. Pernik – T. Stevens (szerk..): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* NATO CCDOE, 2020. 60–73. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

National Security Archive: *USCYBERCOM 30-Day Assessment of Operation Glowing Symphony.* (2016. december 13.). Online: https://nsarchive.gwu.edu/dc.html?doc=6655596-National-Security-Archive-5-USCYBERCOM

Nemzeti Közszolgálati Egyetem: *Kiberbiztonsági mesterképzési szak.* (é. n.). Online: https://antk.uni-nke.hu/oktatas/mesterkepzes/kiberbiztonsagi-mesterkepzesi-szak

Pomerleau, Mark: What Cyber Command's ISIS operations means for the future of information warfare. *C4ISRNet,* 2020. június 18. Online: www.c4isrnet.com/information-warfare/2020/06/18/what-cyber-commands-isis-operations-means-for-the-future-of-information-warfare/

Świątkowska, Joanna – Izabela Albrycht – Dominik Skokowski: National Cyber Security Organisation: POLAND. Tallinn, NATO CCDCOE, 2017. Online: https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017.pdf

United States Government Accountability Office: *DOD TRAINING. U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force.* (2019. március). Online: www.gao.gov/assets/gao-19-362.pdf

Universität der Bundeswehr München: *Studiengang Master Cyber-Sicherheit.* (é. n.). Online: www.unibw.de/inf/studium/studiengang-cyber-sicherheit

US Cyber Command: *Achieve and Maintain Cyberspace Superiority, Command Vision for US Cyber Command.* (2018. április). Online: www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

US Cyber Command: *Cyber Mission Force achieves Full Operational Capability*. (2018. május). Online: www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/
US Cyber Command: *Cybercom Media Roundtable*. (2019. május 7.). Online: www.cybercom.mil/Portals/56/Documents/FOIA%20Reading%20Room%20Docs/2019-05-07_CYBERCOM_Media_Roundtable_Transcript.pdf?ver=2020-01-24-095943-620
Zeit Online: *Bundeswehr rüstet gegen Attacken aus dem Internet*. (2016. április 26.). Online: www.zeit.de/politik/deutschland/2016-04/ursula-von-der-leyen-bundeswehr-aufruestung-cyberkrieg-angriffe-internet

Jogi források

2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 3. szám 139–156.
DOI: 10.32567/hm.2021.3.8

Magas Bianka[1]

A megfigyelés és a kínai típusú szociális kreditrendszer társadalmi megítélése

The Social Judgment of Surveillance and the Chinese-type Social Credit System

A mesterséges intelligencia egyre nagyobb teret nyer magának mindennapjainkban, az általunk használt eszközök, szolgáltatások révén megkerülhetetlen részét képezi életünknek. Számtalan felhasználási területe közül a lakosság állami, vállalati megfigyelését egyre nagyobb érdeklődés övezi. Az állampolgárokról hatalmas mennyiségben gyűjtött adatok mesterséges intelligenciával való feldolgozása, kiértékelése számos ajtót megnyit az azokat birtokló vállalatoknak, államoknak. Kérdés azonban az, hogy vajon a társadalom is akar a megfigyelés társadalmává válni? Kínában már kiépülőben van egy, a lakosokat 24 órás megfigyelés alatt tartó rendszer, amely pontozza, pontjaik szerint pedig jutalmazza vagy bünteti az állampolgárokat. Vajon lehetséges egy szociális kreditrendszer Nyugaton is? Támogatnák-e az emberek a privát szférájuk szűkülését a szolgáltatásukért és biztonságukért cserébe? Írásunk egy kérdőíves felmérés segítségével meghatározza, a technológiaelfogadás-modellt alapul véve, hogy mekkora támogatottságot élvezne a széles körű digitális állami megfigyelés, milyen tényezők befolyásolhatják ennek a megítélését. A kérdőíves felmérés részét képezi a vállalati megfigyeléshez való lakossági viszonyulás is, ahol a dolog támogatottságát, a támogatottságot befolyásolható tényezőket vizsgálja.

Kulcsszavak: mesterséges intelligencia, megfigyelés, big data, kínai szocális kreditrendszer

The role of artificial intelligence in our everyday life has been growing since its presence in our gadgets and the services that we use. The plenty of areas in which AI has used the interest in applying it for the surveillance of the people has been intensifying. The huge amount of data collected from the citizens and processed by artificial

[1] Nemzeti Közszolgálati Egyetem, Államtudományi és Nemzetközi Tanulmányok Kar, hallgató, e-mail: mbius98@gmail.com

intelligence opens numerous doors for companies and states. The question arises whether society really wants to become a surveillance society. In China, a system will be introduced nationwide which is based on the constant surveillance of the citizens. According to their behaviour, they receive credits, based on their credit they get reward or punishment. Would it be possible to introduce a system like this in western society? Would the people support it for the benefits and their security even if they must give up their private sphere? With an online survey, the author defines the support of people for an extensive digital state surveillance system and what factors influence opinions. The survey also includes the opinion of the people about the surveillance done by tech companies and the factors that affect them. With this research, we get an inside view of the people's acceptance of surveillance.

Keywords: **artificial intelligence, surveillance, big data, Chinese social credit system**

1. Bevezetés

A mesterséges intelligencia[2] egyre nagyobb teret nyer magának mindennapjainkban, az általunk használt eszközök, szolgáltatások révén megkerülhetetlen részét képezi életünknek. Számtalan felhasználási területe közül a lakosság állami, vállalati megfigyelését egyre nagyobb érdeklődés övezi. Az állampolgárokról hatalmas mennyiségben gyűjtött adatok mesterséges intelligenciával való feldolgozása, kiértékelése számos ajtót megnyit az azokat birtokló vállalatoknak, államoknak. Felhasználási módját tekintve pedig nagyon fontos, hogy a témát minél szélesebb körben feszegessük, mert egyre közelebb kerül a mindennapjainkhoz.

Arra, hogy egy szuperhatalom hogyan használja tömeges magatartásbefolyásolásra, már napjainkban is látunk példát. Kínában egy, az állampolgárokat 24 órás megfigyelés alatt tartó, szociális kreditrendszer kiépítését szorgalmazta a párt az elmúlt években, országos szintű kiterjesztéséről 2014-ben döntöttek. Alapját a mesterséges intelligencia és a *big data*[3] szolgáltatja. Lényege a lakosság folyamatos megfigyelése és értékelése, majd az értékelésen alapuló jutalmazás vagy büntetés. A lehető legkülönbözőbb forrásokból gyűjtenek hatalmas mennyiségű adatot az állampolgárokról, úgymint a tevékenységükből a közösségi médián, böngészési előzményekből, pénzügyi előzményekből, vásárlási szokásokból. A nagy mennyiségű adat feldolgozását és kiértékelését pedig mesterséges intelligencia végzi.[4]

[2] Peter Jackson megfogalmazása szerint „A mesterséges intelligencia a számítógéptudomány azon részterülete, amely az ember olyan kognitív (megismerő) képességeit emuláló számítógépi programok tervezésével és alkalmazásával foglalkozik, mint a problémamegoldás, vizuális érzékelés és a természetes nyelvek megértése." A mesterséges intelligenciát értelmezhetjük emberi módon gondolkodó rendszereknek, emberi módon cselekvő rendszereknek, racionálisan gondolkodó rendszereknek és racionálisan cselekvő rendszereknek. Forrás: Mihály-Deák Tamás: A mesterséges intelligencia alapjai. Előadás. 2018. február 3.

[3] A Big data „olyan adatbázist ír le, amelyet gyakran frissített adatok (sebesség) hatalmas mennyisége (terjedelem) jellemez, s ezen adatok különféle formátumban lelhetők fel, úgymint numerikusan, szövegesen, kép/videó formában (változatosság)." Andreas Kaplan – Michael Haenlein: Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence. *Business Horizons,* 62. (2019), 1. 15–25.

[4] Genia Kostka – Lukas Antonie: China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval. *Policy Studies Organization,* 21. (2019), 7. 1565–1593.

Az állampolgárok folyamatos felügyeletét lehetővé teszik az utcákon, üzletekben kihelyezett okos CCTV-kamerák. 2018-ban 394 millió térfigyelő kamera volt kihelyezve, azonban ezek száma folyamatosan növekszik, különösen a koronavírus-járvány következtében. 2021-re Kínában összesen akár 567 millió térfigyelő kamera is lehet egyes becslések szerint.[5] Célja, hogy megbízhatóságra és törvénytiszteletre ösztönözze az állampolgárokat, vállalatokat, szervezeteket és állami szerveket. A népi kormányok feketelistát tesznek közzé, amelyen a megbízhatatlannak bélyegzett vagy illegális magatartást tanúsító személyek szerepelnek, akik további szankciókat is kapnak viselkedésükért (például nagysebességű vonatjegy-vásárlás ellehetetlenítése). Ugyanakkor a megbízhatónak minősített személyek és szervezetek számára új listát tesznek közzé, illetve azok jutalomban részesülnek (például adócsökkentés, könnyebb hozzáférés állami szolgáltatásokhoz).

Az állampolgárok mesterséges intelligenciával történő megfigyelésének és akár pontozásának gondolata pedig nem korlátozódik csupán az említett országra, a nyugati világban is szárnyukat bontogatják az államok, óriásvállalatok (például a Google, Facebook) által.[6] A felhasználók folyamatos megfigyelésének egyik célja a vállalatok részéről főként a profitszerzés. Olyan algoritmus kialakítására törekszenek például a közösségi oldalak, amelyek szokásainkat elemezve próbálják kitalálni, mi az a tartalom, ami érdekelhet minket. Figyelik, hogy milyen témákban olvasunk, milyen oldalakat látogatunk, eszerint szelektálva jutunk hírekhez, hirdetésekhez. Így, ha a felhasználó például elkötelezett egy párt vagy ideológia iránt, jó eséllyel egy idő után csak ilyen tartalmakkal találkozik, az ellenvéleménnyel aligha. Ezzel lehetőség nyílik a felhasználók befolyásolására.[7] A mesterséges intelligencia által támogatott megfigyelésen túl találkozhatunk a kreditrendszer bizonyos formáival is. Az Airbnb algoritmusa pedig a „gyanús" profilokat képes kiszűrni. Ugyanúgy az Instagramnak is van ilyen szűrője, amely Kaylen Ward kapcsán vált híressé, aki az ausztráliai bozóttűz áldozatainak szervezett gyűjtést Twitter-fiókján keresztül úgy, hogy meztelen képeket ajánlott fel azoknak, akik bizonyítottan adakoztak az ausztrál vöröskeresztnek vagy a koalakórházaknak. S bár az Instagramját nem használta gyűjtésre, mégis le lett tiltva a profilja, mert viselkedésével megsértette az Instagram szexuálisan szuggesztív tartalomra vonatkozó irányelveit.[8] Van egy terület az Egyesült Államokban, ahol a vállalati megfigyelés és a kreditrendszer találkozik: a bankszektor. Hitelfelvételnél működik egy kreditrendszer, amely az állampolgárt egy 300-tól 850-ig terjedő skálán pontozza, meghatározva ezzel milyen valószínűséggel tudja visszafizetni a hitelét.[9] Ezt a kreditpontot pedig a közösségi médián posztoltak is befolyásolhatják.[10]

[5] Nectar Gan: China is Installing Surveillance Cameras Outside People's Front Doors ... And Sometimes Inside Their Homes. *CNN Business,* 2020. április 28.
[6] Shoshana Zuboff: *The Age of Surveillance Capitalism*. London, Profile Books Ltd., 2019.
[7] Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. (2016), 1. 61–81.
[8] Herczeg Márk: Eljött az idő, amikor az online tevékenységed alapján pontozzák, mennyire vagy megbízható állampolgár. *444,* 2020. január 27.
[9] Joe Resendiz: Average Credit Score in America: 2021 Report. *Valuepengiun,* 2019. július 9.
[10] Craig Johnson: The truth about how Facebook can affect your credit score. *Clark,* 2017. december 17.

Az Amerikai Egyesült Államokat tekintve a nagy techóriások, közösségimédia-felületek által végzett megfigyelése pedig összeér az állami megfigyeléssel valahol a nemzetbiztonság területén. Erre szolgált például az Edward Snowden által megszellőztetett precedens is, ahol a National Security Agency[11] 3 milliárd telefonhívást hallgatott le, illetve fért hozzá a Google, Facebook, Apple és más techcégek által szolgáltatott rögzített adatokhoz.[12] Nem elképzelhetetlen annak a gondolata, hogy a megfelelő technológiával rendelkező államok is használatba veszik a nagy techóriások által kínált technológiát, ahogy erre egyre több példát látunk.[13] Továbbá egyre több vállalkozás, kormány használja a felhasználók online tevékenységét annak eldöntésére, hogy a lakosok, illetve ügyfelek megbízhatóak-e.

Különösen aktuálisnak érzem a témát, hisz rengeteg jogi, társadalmi, gazdasági, filozófiai kérdést felvet, kezdve az emberi jogi kérdésektől, a túlzott állami hatalom kiépítésén át a tömeges magatartásbefolyásolás etikai oldaláig. Azért is érdemes ezzel többet foglalkozni, mert a terület robbanásszerű fejlődését nem követik megfelelő mértékű emberi jogi intézkedések. A felhasználók, állampolgárok zöme nincs tudatában a vállalatok általi megfigyelésnek, a már működő rendszereknek, nem érti, milyen veszélyeket rejthet. Azonban már megoszló nézeteket vallanának, ha tudnák, hogy az állam vagy magáncégek mekkora befolyást és hatalmat szereznek az önként átadott személyes adataik révén az életük felett.

2. Módszertan

Vajon a társadalom is akar a megfigyelés társadalmává[14] válni? Kutatásom célja, hogy felmérjem az állami, vállalati megfigyelés lakossági támogatottságát és az ezt befolyásoló tényezőket egy kérdőív segítségével.

A kérdőív összeállításához áttanulmányoztam a vállalati, állami digitális megfigyelésre vonatkozó szakirodalmat, és kiválasztottam azokat, amelyek alapjául szolgálnak a kérdéssorom összeállításának.[15] Az összeállítás során felhasználtam 4, az Egyesült Államokban a Pew Research által 2014 és 2015 között lefolytatott online felmérés (Privacy Panels 1–4) kérdéseit is.[16] A saját kérdések összeállításánál a technológiaelfogadás-modell továbbfejlesztett változata (TAM 2) alapján fogalmaztam

[11] Magyarul Nemzetbiztonsági Ügynökség, az Amerikai Egyesült Államok hírszerzéssel foglalkozó egyik szervezete.

[12] Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36.

[13] Nem kell messze menni, ha a techcégek és a kormányzatok együttműködésére szeretnénk példát találni. A Sandy-hurrikán (2012) miatt New York város Polgármesteri Hivatala együttműködött a különböző web 2.0-s oldalakkal. A Google-lel együttműködve például interaktív krízistérképet készítettek, amelyen valós időben lehetett követni a hurrikán helyzetét, így tájékoztatva a lakosságot és segítve a katasztrófaelhárítást. Bányász Péter: A közösségi média szerepe a katasztrófaelhárításban a Sandy-hurrikán példáján keresztül. In Horváth Attila (szerk.): *Fejezetek a kritikus infrastruktúra védelemből.* Budapest, Magyar Hadtudományi Társaság, 2013. 281–292.

[14] A megfigyelés társadalma egy olyan társadalmat jelöl, ahol a megfigyelésre használt technológiával az emberek mindennapi tevékenységét nyomon követik. Forrás: Collins English Dictionary*:* Surveillance Society Definition and Meaning. (é. n.).

[15] Taewoo Nam: What Determines the Acceptance of Government Surveillance? Examining the Influence of Information Privacy Correlates. *The Social Science Journal,* 56. (2019), 4. 535.

[16] Elérhetők: www.pewresearch.org/internet/datasets/.

kérdéseket. A TAM modell lehetővé teszi, hogy megvizsgáljam egy technológiai innováció felhasználói fogadtatását, bemutatva ezzel hibáit, hiányosságait. A TAM 2 már bevonja például a szubjektív normákat is (többek között, hogy az egyén közvetlen környezete mit gondol az adott technológiáról). [17] Ennél kíváncsi voltam, milyen esetekben támogatnának a kitöltők egy kínai típusú kreditrendszert.

A kérdőívben több területet is vizsgáltam. Kérdéseim kiterjedtek arra, hogy mennyire érdekli őket, vannak tudatában a felhasználók a vállalati megfigyelésnek, hogyan értékelik ezt az életükre nézve. Kíváncsi voltam, mekkora kontrollt éreznek az adataik felett egy napjuk során, hisz a kontroll érzete befolyásolja az adatvédelemmel kapcsolatos aggodalmaikat.[18] Ugyanakkor nem elhanyagolható szempont, hogy mennyire találják egyszerűnek a kontroll visszaszerzését, a privát böngészést. Technológiaelfogadás-modellt alkalmaztam az állami megfigyelésre koncentráló kérdéseknél, külön kitérve egy kreditrendszer elfogadhatóságára. Az összeállításnál a következő faktorokat vettem figyelembe:

- használat észlelt egyszerűsége;
- észlelt hasznosság;
- szándék;
- bizalom;
- referenciacsoport;
- ár.

A kormányzati megfigyelés elfogadhatóságánál azt is megvizsgáltam, hogy elfogadhatósága hogyan változik, ha csak különböző társadalmi csoportokra irányul. A kérdőív kitöltése online, önkéntes alapon zajlott, igyekeztem a lehető legtöbb társadalmi csoportot (különböző nemű, korcsoportú, végzettségű, politikai irányultságú stb.) megszólítani.

Az adatok kiértékelését az IBM SPSS Statistics 26 programcsomaggal, kereszttábla-elemzéssel végeztem. Segítségül használtam Sajtos László és Mitev Ariel SPSS kutatási és adatelemzési kézikönyvét is.[19] A kereszttábla segítségével meg lehet állapítani, hogy két nominális vagy ordinális változó között van-e összefüggés. A Khi-négyzet (X^2) próbával kimutatható, hogy van-e a két minőségi változó között szignifikáns kapcsolat. Az SPSS program cellák megfigyelt esetszámait hasonlítja össze azzal az elvárt esetszámmal, amelyet akkor kapnánk, ha nem lenne kapcsolat a két változó között. A Khi-négyzet próba egyik alapfeltétele, hogy az elvárt gyakoriság minden cellában legalább 5 legyen, kevesebb az összes cella 20%-ában lehet csupán. Amennyiben ez nem teljesül, eredményünket statisztikai szempontból nem lehet figyelembe venni. Ezért több esetben szükséges volt adattisztítást végeznem, hogy figyelembe vehessem a kapott értékeket. A Phi és Cramer's V asszociációs együtthatóval pedig a két nominális változó közötti kapcsolat szorosságát állapítottam meg.

[17] Keszey Tamara – Zsukk János: Az új technológiák fogyasztói elfogadása. *Vezetéstudomány,* 48. (2017), 10. 38–39.

[18] Tao Zhou: Understanding Location-based Services Users' Privacy Concern: An Elaboration Likelihood Model Perspective. *Internet Research,* 27. (2017), 3. 506–519.

[19] Sajtos László – Mitev Ariel: *SPSS kutatási és adatelemzési kézikönyv.* Budapest, Alinea, 2007.

Az érték szorosságát 0 és 1 között határozza meg a program, ahol az 1 jelöli a szoros összefüggést, a 0 pedig a függetlenséget.[20]

A kutatási téma feldolgozása során a következő hipotéziseket állítottam fel:

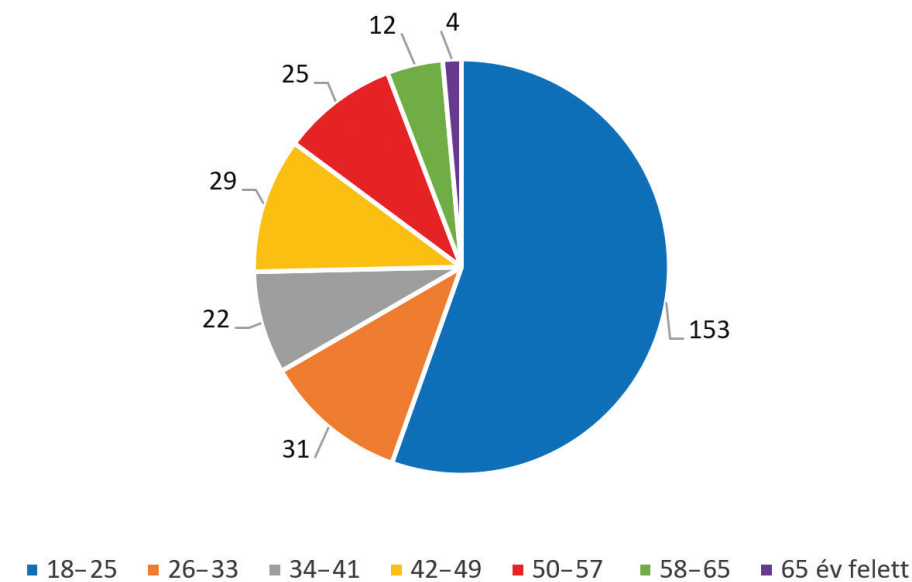
H1: A magukat nyitott embernek tekintők jobban egyetértenek az online szolgáltatások hatékonyabbá válásával azáltal, hogy adatokat gyűjtenek róluk.

H2: Azon emberek szerint, akik úgy érzik, hogy digitális eszközeik a nap 24 órájában megfigyelik őket, a kormányzatnak jobban kellene szabályoznia azt, hogy a hirdetők hogyan használják fel a felhasználók adatait.

H3: Az érzékelt adatvédelmi tudatosság befolyásolja a kínai szociális pontrendszer és a különböző csoportokra irányuló, erőteljesebb állami megfigyelés megítélését.

3. A kérdőíves felmérés eredményei

Kérdőívemet 276-an töltötték ki (n = 276), amelyből 68,8% nő volt. A legtöbb kitöltés a 18–25 évig terjedő korcsoportból volt (55,4%), a legkevesebb a 65 év felettiekéből (n = 4).



1. ábra

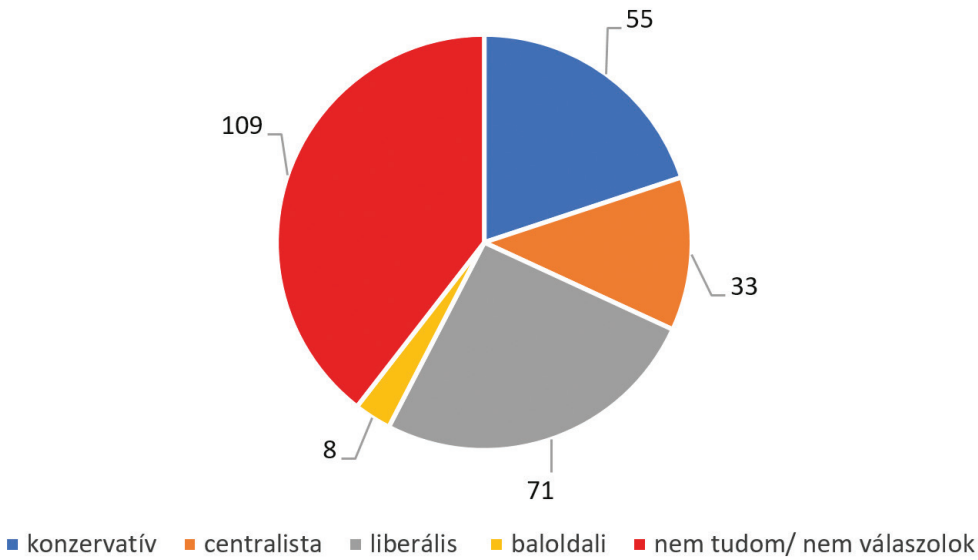
A kérdőívet kitöltők megoszlása korcsoport szerint

Forrás: a szerző szerkesztése

A politikai világnézetre vonatkozó kérdésnél megoszlottak a válaszok, 39,5%-uk nem tudta/nem kívánta megválaszolni a kérdést. Ugyanakkor 25,7%-uk liberálisnak,

[20] SPSS ABC: Khi négyzet próba jelentése és alkalmazása az SPSS-ben. (é. n.).

19,9%-uk konzervatívnak, 12% pedig centralistának vallotta magát. A magukat baloldalinak vallók száma csupán 8 (n = 8). Fontos kiemelni, hogy a politikai világnézetre irányuló kérdés önbevalláson alapszik, tehát előfordulhat, hogy az egyén magáénak tartott irányultsága nem egyezik a szakirodalmakban tárgyaltakkal.



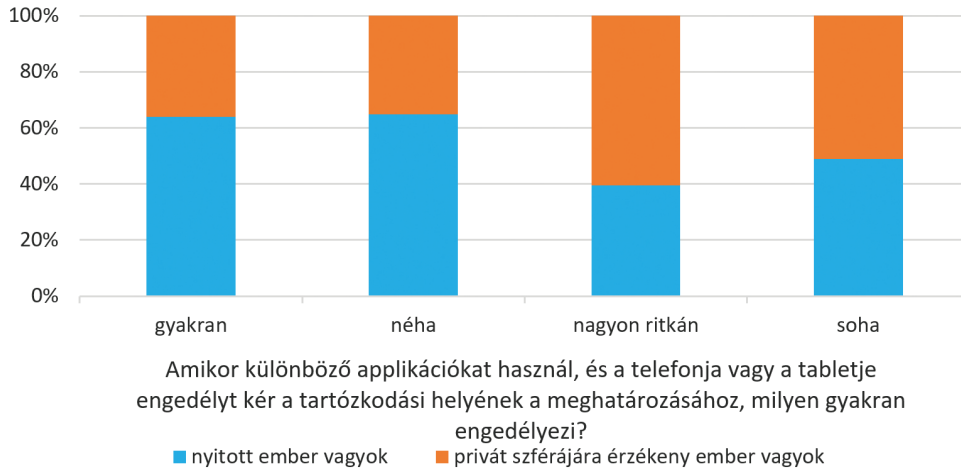
2. ábra

A kérdőívet kitöltők megoszlása politikai világnézet szerint

Forrás: a szerző szerkesztése

A válaszadók 55,8%-a (n = 154) magát nyitott embernek gondolja, a többiek inkább privát szférájukra érzékenyként definiálták önmagukat. A közösségimédia- és internethasználat felmérésénél (adattisztítást követően) világossá vált, hogy a kitöltők többsége napjában többször: 1. használja okostelefonját (n = 266); 2. használ valamilyen keresőmotort, például Google-t vagy Binget (n = 257); 3. látogat közösségi oldalakat, például Facebookot, Instagramot (n = 245).

A válaszadók önértékelését, tehát, hogy nyitottnak vagy privát szférájukra érzékeny embernek tartják-e magukat, összevetettem a tartózkodási helymeghatározás engedélyezésének gyakoriságával (lásd 3. ábra). A válaszadók 44,9%-a úgy nyilatkozott, hogy nagyon ritkán, 26,4%-uk néha, 19,2%-uk soha, 9,4%-uk pedig gyakran osztja meg tartózkodását. A Khi-négyzet teszt ($X^2 = 13{,}471$; df = 3) kétoldali szignifikanciaszintje 0,004, tehát kapcsolat állapítható meg a két változó között. A Cramer's V mutató megfigyelt értéke 0,221, tehát nem túl erős, moderált kapcsolatot állapíthatunk meg a között, hogy valaki mennyire vallja nyitottnak magát és milyen gyakran engedélyezi a tartózkodási helyének megosztását.

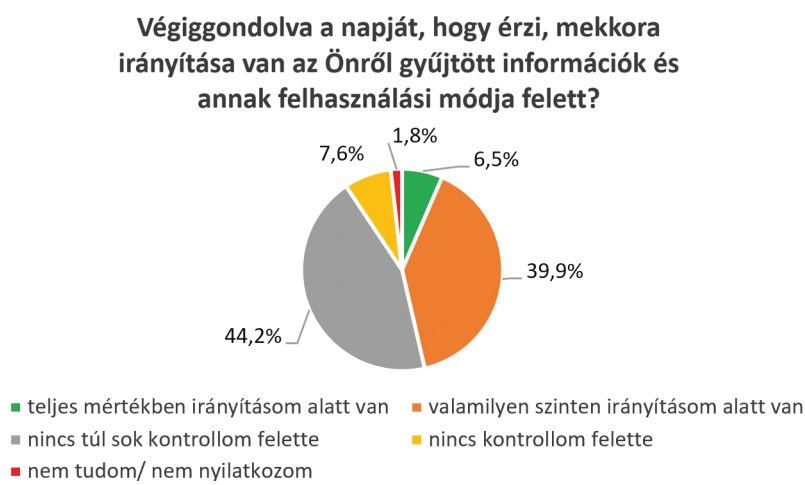


3. ábra

A privát szférára való érzékenység és a tartózkodási hely megosztására való hajlandóság közti összefüggés

Forrás: a szerző szerkesztése

Kíváncsi voltam arra, hogy a kitöltők mekkora kontrollt érzékelnek a róluk gyűjtött adatok felett, amikor interneten böngésznek, okostelefont használnak. A 4. ábrán látható, hogy a válaszadók 44,2%-a (n = 122) szerint nincs túl sok kontrollja a róla gyűjtött adatok és azok felhasználása felett. Azonban 39,9%-uk (n = 110) úgy véli, valamilyen szinten az irányítása alatt vannak a róla gyűjtött információk.

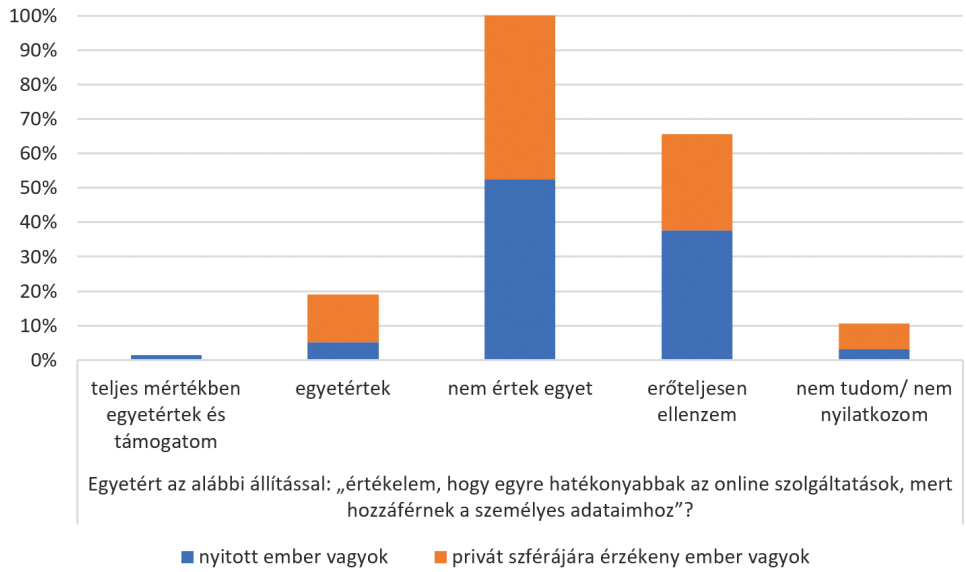


4. ábra

Az adatok feletti kontroll érzékelése

Forrás: a szerző szerkesztése

Így megállapítható, hogy nincs túl nagy eltérés a nem sok kontrollt és a valamilyen szintű irányítást érzékelők mennyisége között. Csupán 6,5% gondolta úgy, hogy teljes mértékben az irányítása alatt állnak az információk. További Khi-négyzet próbának vetettem alá, hogy vajon a privát szférára való érzékenység és annak a megítélése, hogy az online szolgáltatások a felhasználókról gyűjtött adatok miatt egyre hatékonyabbak között van-e kapcsolat.



5. ábra

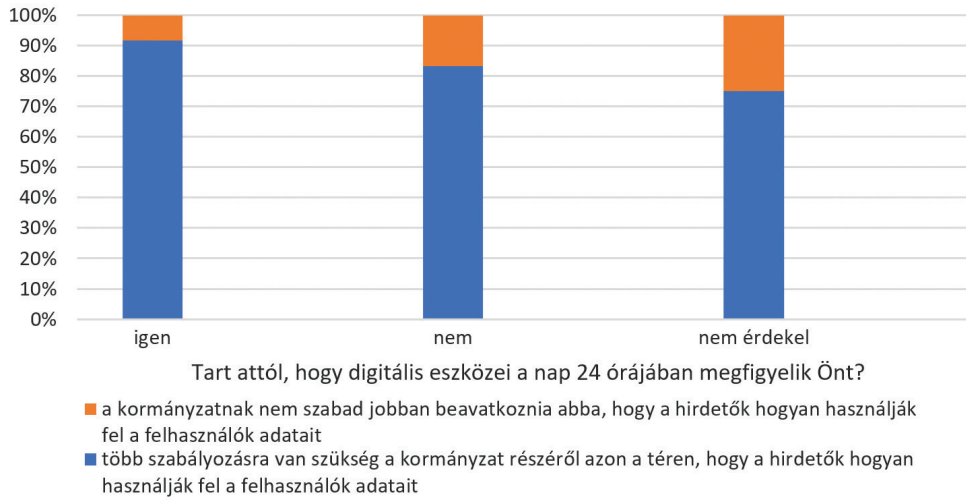
A privát szférára való érzékenység és az online szolgáltatások felhasználói adatgyűjtéssel való hatékonyabbá válásának kapcsolata

Forrás: a szerző szerkesztése

A Khi-négyzet megfigyelt értéke 11,624 (df = 4), a kétoldali szignifikanciaszint pedig 0,02, vagyis jelentős kapcsolat áll fenn. A Cramer's V mutató értéke 0,205, tehát egy nem túl erős kapcsolatról beszélhetünk. Tehát az, hogy valaki érzékeny-e a privát szférájára, befolyásolja az online szolgáltatások adataink általi hatékonyabbá válásának megítélését.

Megvizsgáltam, hogy az emberek tartanak-e attól, hogy digitális eszközeik a nap 24 órájában megfigyelik őket. 52,2% igennel, 26,1% pedig nemmel válaszolt, 21,7%-ukat nem érdekelte. Az ezekkel kapcsolatos érzéseket összevetettem azzal, hogy szerintük jobban kellene-e a kormányzatnak szabályozni azt, hogy a felhasználókról gyűjtött adatokat hogyan használják fel a hirdetők. Itt a válaszadók jelentős többsége, 85,9%-a gondolta úgy, hogy nagyobb szabályozásra szorul e terület. A vizsgálat Khi-négyzet megfigyelt értéke 10,212 (df = 2), kétoldali szignifikanciaszintjének értéke p = 0,006, tehát megállapítható, hogy a két változó közötti kapcsolat szignifikáns. A Cramer's

V mutató értéke 0,192, tehát egy laza, gyenge kapcsolatról beszélünk. Az eredményt a 6. ábrán ábrázoltam.



6. ábra

A digitális megfigyeléstől való félelem és a kormánytól elvárt magatartás a hirdetők adatfelhasználásával kapcsolatos összefüggése

Forrás: a szerző szerkesztése

A kérdőív harmadik részében a digitális állami megfigyelés több aspektusáról is megkérdeztem a válaszadókat. A 7. ábrán látható, mennyire érdekelné a digitális állami megfigyelés a kitöltőket.

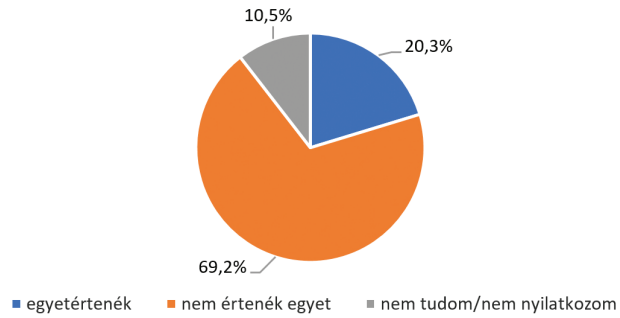
7. ábra

Az esetleges digitális állami megfigyeléssel szemben tanúsított érdeklődés a kitöltők szerint

Forrás: a szerző szerkesztése

Látható, hogy 68,8%-ot nagyon is érdekelné, ha felügyelnék őt az állami szervek, amit a valamennyire érdeklődők követnek. Csupán 4,3%-uk vélekedett úgy, hogy egyáltalán nem foglalkozna ezzel. A következő ábrán a bűnmegelőzés, bűnüldözés elősegítése érdekében történő megfigyelés támogatottsága látható.

Egyetért azzal, hogy a kormányzat adatokat gyűjtsön Önről (pl. közösségi oldalak használati szokásai, telefonhívásai, térfigyelő kamerák) a hatékony bűnmegelőzés és bűnüldözés elősegítése érdekében?



8. ábra

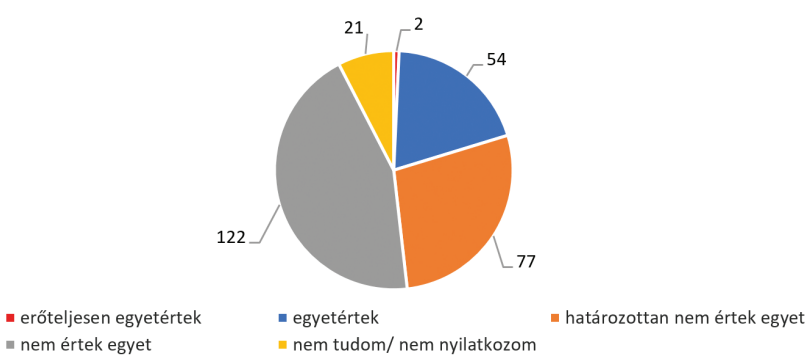
A digitális állami megfigyelés elfogadhatósága a bűnüldözés, bűnmegelőzés elősegítése esetén

Forrás: a szerző szerkesztése

A kitöltők többsége, 69,2% nem értene egyet akkor sem a digitális állami megfigyeléssel, ha az a bűncselekmények elleni védekezést, megelőzést segítené elő. 20,3%-uk pedig egyetértene vele.

Megvizsgáltam, hogy a kitöltők mennyire éreznék hasznosnak, ha az emberek azt hinnék, valaki folyamatosan figyeli az online tevékenységüket.

Hasznos lenne a társadalomnak, ha az emberek azt hinnék, valaki folyamatosan felügyeli az online tevékenységüket?



9. ábra

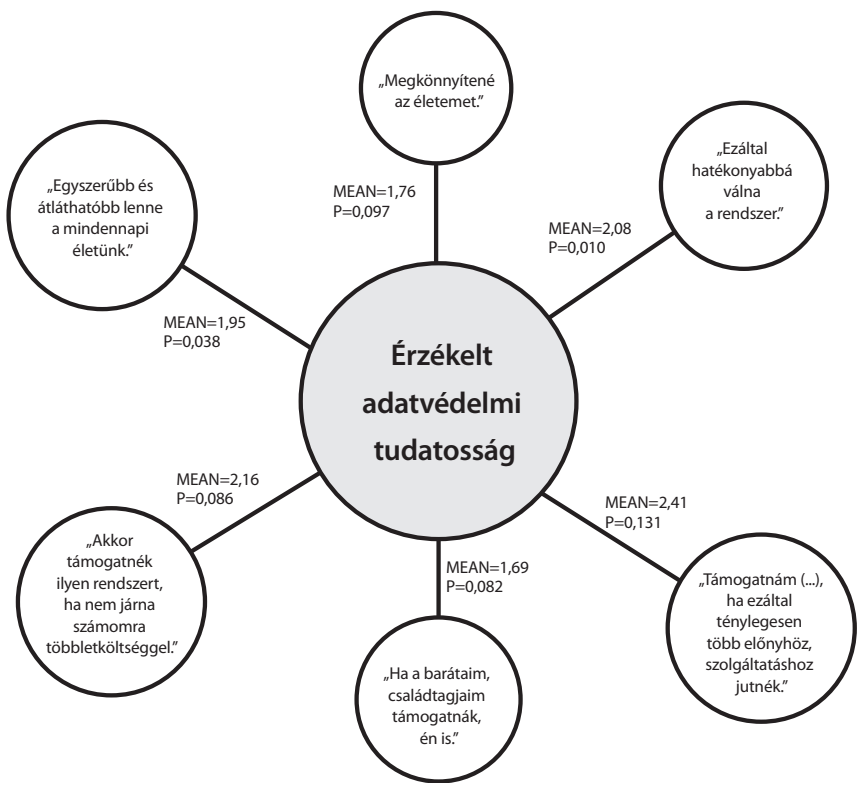
Az online tevékenység folyamatos figyelésébe vetett hit vélt társadalmi hasznossága

Forrás: a szerző szerkesztése

A kitöltők 44,2%-a nem értett egyet, 77-en pedig határozottan nem értettek egyet. 19,6% viszont egyetértett, csupán 2 személy támogatta erőteljesen.

A 26. kérdésben röviden felvázoltam a kínai szociális kreditrendszer jellemzőit, és kértem a kitöltőket, hogy egy 1-től 5-ig terjedő Likert-skálán fejezzék ki véleményüket (az 1 a határozottan nem értek egyet, az 5 pedig a határozottan egyetértek) bizonyos szempontok alapján. A válaszok nagy része ellenezte az ilyen típusú rendszer bevezetését, azonban kíváncsi voltam, a vélt adatvédelmi tudatosság mennyire befolyásolja az egyes kérdésekre adott választ. Megnéztem továbbá, hogy aszerint, hogy a feltételezett online tevékenység megfigyelésének társadalmi hasznosságát hogyan ítélték meg, van-e különbség a csoportok között, ha a digitális állami megfigyelésről beszélünk.

Ennek érdekében lefuttattam a Kruskal–Wallis-tesztet. A K–W-teszt egy nonparaméteres megfelelője az egyszempontos varianciaanalízisnek (ANOVA), amely megmutatja, hogy van-e vagy nincs statisztikailag szignifikáns különbség három vagy több különböző, független csoport középértéke között.[21]



10. ábra

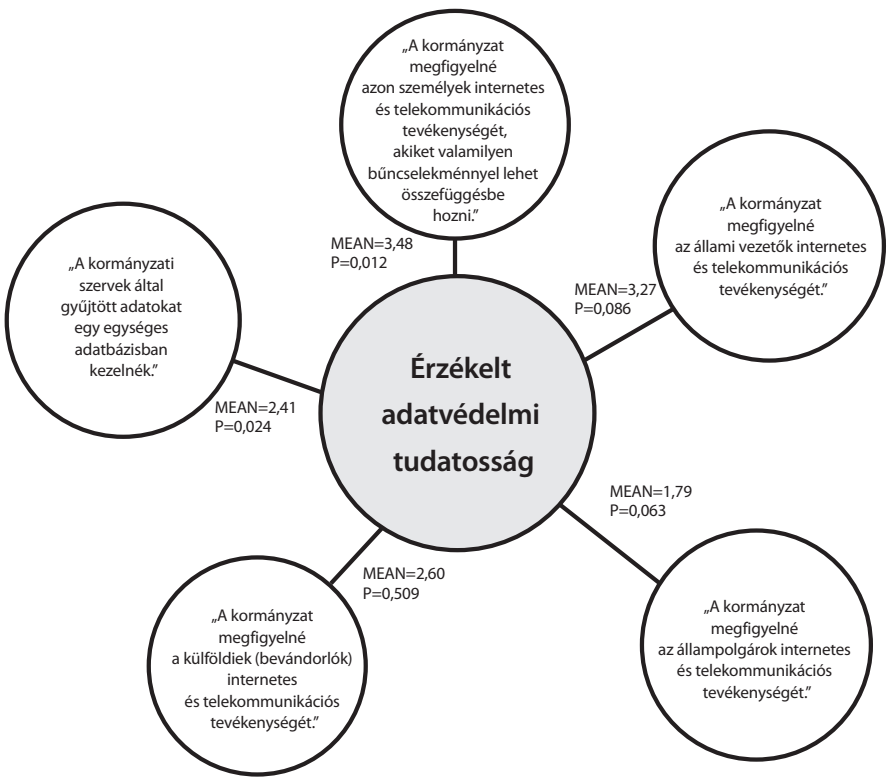
Az érzékelt adatvédelmi tudatosság hatása a kínai szociális rendszer megítélésére

Forrás: a szerző szerkesztése

[21] Kruskal–Wallis Test: Definition, Formula, and Example. *Statology* (blog), 2019. január 18.

A középértékek 1,69 és 2,41 között változtak, tehát a „határozottan nem értek egyet" és a „nem értek egyet" között. Szignifikáns különbség mutatkozik meg a vélt adatvédelmi tudatosság alapján besorolt csoportok között két esetben. Az egyszerűbb, átláthatóbb életre vonatkozó állításnál és a hatékonyságra vonatkozó kérdésnél a szignifikanciaszint 0,05 alatt van, tehát a nullhipotézist elvethetjük. Ezekben az esetekben a legmagasabb rangátlaga a magukat nem adatvédelmileg tudatosnak vallóknak van, tehát sorban náluk a legmagasabb az egyetértésre való hajlam. A legalacsonyabb rangátlaga pedig a magukat tudatosnak vallóknak van. Nem tapasztalható azonban különbség a csoportok között a többi állításra vonatkozó kérdés esetén.

A 27. kérdésben arra voltam kíváncsi, hogy az állami megfigyelést mennyire tartják a kitöltők elfogadhatónak, ha különböző csoportokra irányulna, úgymint állampolgárok, bűncselekménnyel összefüggésbe hozható személyek, állami vezetők, külföldiek (bevándorlók). Ennél a kérdésnél rákérdeztem egy egységes állami, személyhez köthető adatbázis támogatottságára is. Ezt összevetettem a vélt adatvédelmi tudatossággal.



11. ábra

Az érzékelt adatvédelmi tudatosság hatása a digitális állami megfigyelésre, bizonyos csoportokra való irányulás esetén

Forrás: a szerző szerkesztése

Itt már a középértékek többnek bizonyultak bizonyos esetekben az előző kérdéshez képest. Viszonylag magas a középérték a bűncselekménnyel összefüggésbe hozható személyek digitális állami megfigyelésére adott válaszok esetén. Ugyanígy az állami vezetőkre és bevándorlókra irányuló megfigyelés esetén. Szignifikáns különbség tapasztalható a csoportok között abban az esetben, ha a bűncselekménnyel összefüggésbe hozható személyek megfigyeléséről van szó, illetve a kormányzati szervek által létrehozott egységes adatbázis esetén. A legmagasabb rangátlaga szintén a magukat nem tudatosnak vallóknak van, a legalacsonyabb pedig a magukat tudatosnak vallóknak.

Megvizsgáltam, hogy a „Hasznos lenne a társadalomnak, ha az emberek azt hinnék, valaki folyamatosan felügyeli az online tevékenységüket?" kérdésre adott válaszok csoportjai között van-e szignifikáns különbség, ha a kínai típusú szociális kreditrendszer megítéléséről van szó. Adattisztítást végeztem annak érdekében, hogy megfelelően tudjam vizsgálni az adott csoportokat. Így az „erőteljesen egyetértek" és „egyetértek" választ adók csoportját összevontam.

12. ábra

A online tevékenység megfigyelésének társadalmi hasznosságával való egyetértés hatása a kínai szociális rendszer megítélésére

Forrás: a szerző szerkesztése

Különbség tapasztalható a csoportok között három esetben is. Amennyiben a kreditrendszer nem járna többletköltséggel, több előnnyel és szolgáltatással járna és a barátok,

családtagok is támogatnák a kiépülését, szignifikáns az eltérés a válaszadók között. A legalacsonyabb rangátlaga a „határozottan nem értek egyet" választ adók csoportjának van, tehát sorban náluk a legnagyobb az elutasításra való hajlam. A legmagasabb rangátlaga pedig az „erőteljesen egyetértek/egyetértek" csoportnak van.

Megvizsgáltam a csoportokat a 27. kérdésre adott válaszok esetén is. Eredményemet a következő ábrán szemléltettem.

13. ábra

A online tevékenység megfigyelésének társadalmi hasznosságával való egyetértés hatása a digitális állami megfigyelésre, bizonyos csoportokra való irányulás esetén

Forrás: a szerző szerkesztése

Majdnem minden válasz esetén tapasztalható a különbség a csoportok között, csak a bűncselekménnyel összefüggésbe hozható személyek esetén áll fenn a nullhipotézis esete. Sorban azoknak a legmagasabb a rangátlaga, akik szerint hasznos lenne a társadalomnak, ha az emberek azt hinnék, valaki megfigyeli őket, legalacsonyabb pedig azoknak, akik ezt ellenzik.

4. Következtetések

A kutatási téma feldolgozása során a következő eredményeket kaptam:

T1: A privát szférára való érzékenység befolyásolja az online szolgáltatások adatgyűjtésük általi hatékonyabbá válásának megítélését, a magukat nyitottabbnak vallók egyetértőbbnek bizonyultak.

T2: Azon emberek szerint, akik úgy érzik, hogy digitális eszközeik a nap 24 órájában megfigyelik őket, a kormányzatnak jobban kellene szabályozni azt, hogy a hirdetők hogyan használják fel a felhasználók adatait.

T3: Az érzékelt adatvédelmi tudatosság befolyásolja a kínai szociális pontrendszer egyes aspektusainak és az egyes csoportokra irányuló, erőteljesebb állami megfigyelés megítélését.

A kérdőíves felmérésből megállapíthatom, hogy a válaszadók kicsivel több mint fele magát nyitott emberként definiálja. Nagy részük, 59,4%-uk pedig többé-kevésbé adatvédelmileg tudatosnak gondolja önmagát. Azonban a Facebook alkalmazáshoz szükséges engedélyek számának eltévesztése kimagasló volt az adatvédelmileg tudatos, nem tudatos és többé-kevésbé tudatosok körében is, nincs összefüggés az érzékelt tudatosság és a tudás között e tekintetben. Megállapíthatom továbbá, hogy a privát szférára való érzékenység befolyásolja a tartózkodási hely megosztására való hajlandóságot. Minél nyitottabb valaki, annál valószínűbb, hogy megosztja ezen adatait. A mesterséges intelligencia prognosztikus képességét igaznak vagy többé-kevésbé igaznak ítélték meg az emberek, megítélésük és privát szférára való hajlandóságuk között nincs szignifikáns kapcsolat.

Az emberek többsége úgy érzi, hogy nincs túl sok kontrollja a róla gyűjtött adatokról, és tart attól, hogy digitális eszközei a nap 24 órájában megfigyelik őt. Ez a félelem összefüggésben áll azzal, hogy szerintük a kormánynak több intézkedést kell tenni azon a téren, hogy a hirdetők hogyan használják fel a felhasználók adatait. Érdekes, hogy míg a nagy techcégek a megfigyelés pozitívumaként hozzák fel a személyre szabottabb tartalmat, a kérdőívből inkább az látszik, hogy az emberek nem értékelik annak, főleg, ha az adataik átadása a magánszféra szűkülésével jár. A kreditrendszerre és állami megfigyelésre vonatkozó kérdésnél láthattuk, hogy az emberek többségében nem támogatják, azonban vannak olyan szempontok (nem jár többletköltséggel, több szolgáltatáshoz való hozzáférés), amelyek vonzóbbá tehetik. A kínai szociális kreditrendszer gyakorlatában a bűncselekménnyel összefüggésbe hozható személyek internetes és telekommunikációját tartják a leginkább elfogadhatónak. Szignifikáns különbség tapasztalható a csoportok között abban az esetben, ha a bűncselekménnyel összefüggésbe hozható személyek megfigyelését feltételezem, illetve, ha a kormányzati szervek által gyűjtött adatok egységes adatbázisban történő kezeléséről van szó.

Felhasznált irodalom

Bányász Péter: A közösségi média szerepe a katasztrófaelhárításban a Sandy-hurrikán példáján keresztül. In Horváth Attila (szerk.): *Fejezetek a kritikus infrastruktúra védelemből.* Budapest, Magyar Hadtudományi Társaság, 2013. 281–292. Online: http://real.mtak.hu/94342/1/A_kozossegi_media_szerepe_a_katasztrofae.pdf

Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. (2016), 1. 61–81. Online: http://real.mtak.hu/47801/1/A_kozossegi_media_szerepe_a_lelektani_mu.pdf

Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36. Online: http://real.mtak.hu/72506/1/nbszemle_20152_banyasz.original_u.pdf

Collins English Dictionary: *Surveillance Society Definition and Meaning.* (é. n.). Online: www.collinsdictionary.com/dictionary/english/surveillance-society

Gan, Nectar: China is Installing Surveillance Cameras Outside People's Front Doors … And Sometimes Inside Their Homes. *CNN Business,* 2020. április 28. Online: https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html

Genia Kostka – Lukas Antonie: China's social credit systems and public opinion: Explaining high levels of approval. *New Media&Society,* 21. (2019), 7. 1565–1593. Online: https://doi.org/10.1177/1461444819826402

Herczeg Márk: Eljött az idő, amikor az online tevékenységed alapján pontozzák, menynyire vagy megbízható állampolgár. *444,* 2020. január 27. Online: https://444.hu/2020/01/27/eljott-az-ido-amikor-az-online-tevekenyseged-alapjan-pontozzak-mennyire-vagy-megbizhato-allampolgar

Joe Resendiz: Average Credit Score in America: 2021 Report. Valuepenguin, 2021. július 9. Online: www.valuepenguin.com/average-credit-score

Johnson, Craig: The truth about how Facebook can affect your credit score. *Clark,* 2017. december 11. Online: https://clark.com/personal-finance-credit/social-media-facebook-credit-scores/

Kaplan, Andreas – Michael Haenlein: Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence. *Business Horizons,* 62. (2019), 1. 15–25. Online: https://doi.org/10.1016/j.bushor.2018.08.004

Keszey Tamara – Zsukk János: Az új technológiák fogyasztói elfogadása. *Vezetéstudomány,* 48. (2017), 10. 38–47. Online: https://doi.org/10.14267/VEZTUD.2017.10.05

Kruskal–Wallis Test: Definition, Formula, and Example. *Statology* (blog), 2019. január 18. Online: www.statology.org/kruskal-wallis-test/

Mihálydeák Tamás: *A mesterséges intelligencia alapjai.* Előadás. 2018. február 3. Online: https://arato.inf.unideb.hu/mihalydeak.tamas/Mest_int_2017_18_2_print.pdf

Pew Research: Privacy Panels 1-4. Elérhetőek: www.pewresearch.org/internet/datasets/ Letöltés dátuma: 2020. szeptember 10.

Sajtos László – Mitev Ariel: *SPSS kutatási és adatelemzési kézikönyv.* Budapest, Alinea, 2007.

Shoshana Zuboff: *The Age of Surveillance Capitalism*. London, Profile Books Ltd, 2019.

SPSS ABC: Khi négyzet próba jelentése és alkalmazása az SPSS-ben. (é. n.). Online: https://spssabc.hu/ketvaltozos-elemzes/khi-negyzet-proba/

Taewoo Nam: What Determines the Acceptance of Government Surveillance? Examining the Influence of Information Privacy Correlates. *The Social Science Journal,* 56. (2019), 4. 530–544. Online: https://doi.org/10.1016/j.soscij.2018.10.001

Zhou, Tao: Understanding Location-based Services Users' Privacy Concern: An Elaboration Likelihood Model Perspective. *Internet Research,* 27. (2017), 3. 506–519. Online: https://doi.org/10.1108/IntR-04-2016-0088

Zuboff, Shoshana: *The Age of Surveillance Capitalism*. London, Profile Books Ltd., 2019.

HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 3. szám 157–172.
DOI: 10.32567/hm.2021.3.9

Marlok Tamás[1]

Virtuális valóság alapú taktikai szimulációs kiképző eszközök hazai fejlesztési lehetőségei

3. rész: A technológia korlátai a kiképzés szemszögéből

Domestic Development Opportunities of Virtual Reality-based Tactical Simulation Training Tools.

Part 3: Limitations of Technology from a Training Perspective

Az informatika és mikroelektronika technológiai fejlődésével a virtuálisvalóság-eszközök egyre hatékonyabbá válnak, egyre nagyobb beleélést, a valóság egyre pontosabb szimulációját teszik lehetővé. Ezt a technológiát a gazdaságilag fejlettebb államok katonai és rendvédelmi szervezetei már több mint egy évtizede kezdték el alkalmazni különböző területeken. Jelen tanulmányban azt kívánom igazolni, hogy ez a technológia mára elérte azt a fejlettségi szintet és modularitást, amikor alkalmazott kutatások eredményeként olyan saját eszközöket tudunk fejleszteni, amelyek akár nemzetközi szinten is piacképes alternatívát jelenthetnek a magas költségű rendszerekkel szemben, és amelyekkel a kiképzés bizonyos területei forradalmasíthatók. A cikksorozat harmadik részében a technológia korlátait vizsgálom a kiképzési terület szemszögéből. Azaz a virtuálisvalóság- (VR-) eszközöket kiképzési célokra használva milyen tényezőkre, paraméterekre kell különösen figyelnünk, hol vannak még gyenge pontok?

Kulcsszavak: **virtuális valóság, harcászati szimuláció, szimuláció, gyakoroltató eszköz, kiképzés**

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

Through the recent immense developments in information technology and microelectronics, virtual reality (VR) devices have become increasingly sophisticated, providing close-to-real life experiences. VR technology has proved to be an essential training tool in various military and law enforcement applications for over a decade. My article series is aimed at uncovering the remarkable in-house development possibilities based on the modular nature of this technology. Through applied research, these state-of-the-art VR platforms may deserve recognition and have the potential to revolutionise certain components of training methods. In the third part of my series, my objective is to investigate the limitations and drawbacks of VR technology from the aspects of military and law enforcement training. My goal is to examine the parameters and specifications to explore the deficiencies of these equipment, which require attention in an in-house development.

Keywords: **virtual reality (VR), tactical simulation, military training, law enforcement training**

1. Bevezetés

A cikksorozat előző részeiben a virtuálisvalóság- (VR-)[2] eszközök technikai adottságait, majd kiképzésben való felhasználhatóságukat elemeztem, elsősorban a taktikai jellegű kiképzési területek (lőkiképzés, harcászat és intézkedéstaktika) igényeinek szempontjából. A lehetőségeket és előnyöket már ismerjük, de fontos a hátrányokat, korlátokat is górcső alá venni. Az előző cikkben azt elemeztem, hogy a virtuálisvalóság-technológia hogyan teremtheti meg bizonyos taktikai készségek kialakításának lehetőségét. Ezen a kiképzési területen fontos a helyváltoztatási formák, testhelyzetek gyakorlása (például fedezékek közötti mozgás), finommotoros mozgások pontos kivitelezése (fegyverek, eszközök kezelése), a térbeli helyzetfelismerés és az izommemória kialakítása, ezért a hagyományos számítógépes szimulációk itt nem túl hasznosak. A VR-technológia viszont le tudja cserélni az ember-gép közötti interfészekben található indirekción keresztüli beviteleket (egér, billentyűzet) természetes beviteli formákra, szenzorokat és szenzorfúziót alkalmazva, amivel máris közelebb kerülünk a taktikai kiképzésben történő alkalmazhatóság egy magasabb szintjéhez. Láthattuk, hogy a vizuális megjelenítés minősége és a sztereoszkópikus érzékelés lehetővé teszi a felhasználó virtuális térbe történő beemelését, az abban történő pontos navigációját, a HMD-k[3] segítségével. A fizikai fáradozás szimulálására a helyváltoztatás digitalizálása által, virtuális taposómalmokkal (ODT[4]) vagy más testhelyzet-érzékelő megoldásokkal – mint például szenzorok ruhán történő elhelyezése – van lehetőség. A megfelelő készségek kialakításához a felszerelés virtualizációja is meg kell hogy történjen. Szoftveres modellezéssel ki kell alakítani a valós eszközök, fegyverek, tárak

[2] VR: Virtual Reality: virtuális valóság.
[3] HMD: *Head Mounted Display,* fejre rögzített kijelző, virtuálisvalóság-szemüveg, vagy virtuálisvalóság-„sisak".
[4] ODT: *Omni-directional Treadmill.*

digitális „ikerpárjait",[5] illetve azok virtuális környezetben történő alkalmazhatóságát. Ha e lehetőségek mellé a fejlesztéshez szükséges hardver- és szoftveradottságokat, környezetet is felmérjük, látszik, hogy a megfelelő szakmai kompetenciák megléte esetén viszonylag kockázatmentesen lehet belekezdeni egy ilyen eszköz fejlesztésébe. A VR-rendszerek természetesen nem használhatók minden kiképzési feladat kiváltására, főleg, ha adottnak tekintjük a beszerezhető termékek körét, vagy ha a fejlesztésre fordítható erőforrások korlátozottak. A költségvetés és a fejlesztési idő növelésével viszont olyan magas fejlettségi szintű berendezések építhetők, amelyekkel olyan készségeket is ki lehet alakítani, amelyek költséges és hosszú gyakorlás során sajátíthatók csak el. Hatalmas előny, hogy a kiképzési feladatok komplexitása a kiképzés alanyának képességeihez és gyakorlati felkészültségéhez igazítható, többletköltség nélkül. Ezekkel az előnyökkel szemben mindenképpen meg kell vizsgálnom azokat a tényezőket is, amelyek negatívan befolyásolják a VR-technológia taktikai kiképzésben történő alkalmazását. Olyan tényezőket, műszaki paramétereket fogok vizsgálni, amelyek nemcsak az ezen, hanem a más területen történő alkalmazást is megnehezíthetik. Mint látni fogjuk, ezek a hiányosságok már most is áthidalhatók, nem akadályozzák érdemben a kiképzésben történő felhasználhatóságot, de a technológia fejlődése eredményeként várhatóan teljesen el fognak majd tűnni. Azok a korlátok, hiányosságok ugyanakkor, amelyeket a gyártók még nem tudtak megszüntetni, megkerülhetők a virtuális kiképzési, felkészítési feladatok előrelátó tervezésével. Alapvetően a széles körben elterjedt és könnyen hozzáférhető első és „másfeledik" generációs eszközök technikai adottságaiból indulok ki, mint például az Oculus Rift S és a Magyar Honvédségben is alkalmazott[6] HTC Vive Pro virtuálisvalóság-készletek, de már említésre kerülnek újabb generációs eszközök is az összehasonlítások során.

2. A VR-rendszerek vizualizációs korlátai

Az előnyöknél megfogalmazódott, hogy az egyik legfontosabb tényező a szimuláció grafikai megjelenítésének minősége. Mint a későbbiekben láthatjuk, a megfelelő hardver rendelkezésre állása esetén a virtuális tér részletgazdag megjelenítése a számítási kapacitás szemszögéből nem okoz gondot, de a VR HMD-kben alkalmazott kijelzők paraméterei korlátokat jelenthetnek.

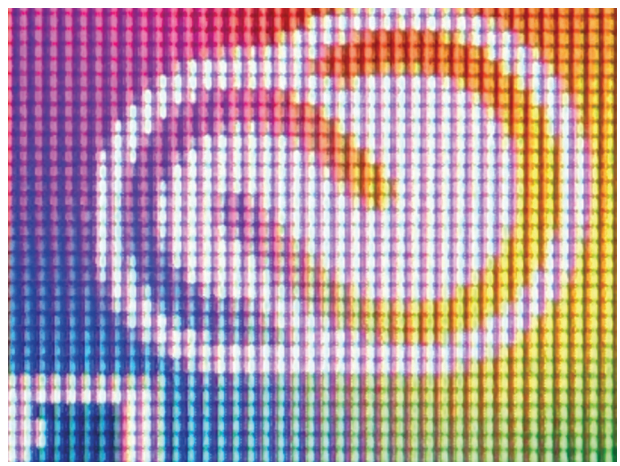
2.1. A kijelzők felbontása és a kis felbontás hatásai

Az egyik legfontosabb paraméter az a sík kijelzők (televíziókészülékek, monitorok) esetén is jól ismert jellemző, amely a vizuális élményt (információt) nagyban befolyásolja, a kijelző felbontása. A tanulmány előző részeiből kiderült, hogy a VR HMD-k esetén alkalmazott megjelenítő panelek viszonylag kis méretűek, képátlójuk 5,5 col

[5] Digitális ikerpár, az angol *Digital Twin* kifejezésből tükörfordítással nyert kifejezés, amelynek jelentése, hogy a valós eszközöket, tárgyakat, környezetet nagy pontossággal, mélységében, digitálisan modellezve valós működést szimulálhatunk, méréseket végezhetünk, tesztelhetünk, elméleteket igazolhatunk.

[6] Trautmann Balázs: Képzelt repülés. *Honvédelem.hu,* 2019. április 16.

(12-13 cm) körül mozog. Ezek a kijelzők pixelrácsokból[7] állnak, a kijelző felbontása pedig annál nagyobb, minél több a pixelrácsban található sorok és oszlopok száma. A pixelrács a gyakorlatban a pixelekből és az azok közötti üres részekből áll. A pixeleket alpixelek *(sub-pixel)* alkotják, amelyek a jelenlegi technológiák esetén RGB- (piros, zöld, kék) fényforrásokat jelentenek. E három (vagy több) miniatűr forrás fényerejének egyenkénti szabályozásával keverhető ki a pixel színe (1. ábra).



1. ábra

A korszerű monitor kinagyított pixelrácsa, amelyen jól látható az egyes színes pixelek (képpontok) közötti üres (fekete) rész is

Forrás: a szerző saját felvétele, Adobe Cloud alkalmazás ikonja, Dell P2414H típusú monitoron, közelről fényképezve

A pixelek színeit és fényességét így egyenként lehet vezérelni, ebből áll össze a teljes látható kép. A legtöbb, jelenleg is széles körben elterjedt VR-rendszer esetén is nagyon különböző paraméterekkel találkozhatunk. Az egy szemre jutó felbontás esetén a kijelzők felbontása vízszintesen 2160 és 3840 képpont; függőlegesen pedig 1200 és 2160 képpont közé esik. Saját tapasztalat és korábbi kiképzési célra fejlesztett rendszerek alapján az immerzivitás, azaz a „beleélhetőség", avagy a saját jelenlét élménye szempontjából már a kisebb felbontás is bőven elegendő, mégis meg kell említeni a korlátokat.

Ha az Oculus Rift S rendszert vesszük példaként, annak egy szemre jutó felbontása 1280 × 1440 pixel. Az eszköz által biztosított, teljes (műszaki leírásban megadott) látómező 110 fok vízszintesen, tehát a két szem összesen ekkora látószöget láthat a két képből összeállítva. Az emberi sztereó vízszintes látómező (amelyet mindkét szem egyszerre lát) 90–100 fok közé esik, ami alapján látható, hogy a sztereó, térérzetet keltő kép körülbelül 1280 pixel oszlopból áll vízszintesen. Összehasonlítva ezt egy (már elavultnak számító) „*Full HD*" (1920 × 1080) felbontású sík képernyővel, amely 1920 képpont oszlopot biztosít, máris látszik, hogy a VR-eszközök vízszintes

[7] Pixel: képpont.

felbontása már ebben is valamivel alulmarad. Hozzá kell vennünk azt is, hogy a sík képernyő nem a teljes látóterünket tölti ki, hanem egy lényegesen kisebb szögtartományra fókuszálunk, ezért például egy 25 colos (körülbelül 63 cm) képátlójú, 16 : 10-es képarányú monitor vízszintes szélessége mindössze 21,5 colt (körülbelül 55cm-t) tesz ki a látómezőnkből. Ezt a monitort 90 cm-ről nézve, a teljes kép a sztereoszkópikus fókuszált látómezőnkből csupán körülbelül 32 fokot ad ki, azaz ezen a területen láthatjuk besűrítve a teljes felbontást, ami a VR-eszköz esetén körülbelül 100 fokra oszlik el, azaz annak jóval kisebb a hasznos érzékelt szögfelbontása. A fentiek alapján mélyebb technikai elemzés nélkül is belátható, hogy a hasonló képminőség elérése érdekében a virtuálisvalóság-kijelzőknél lényegesen nagyobb felbontásra lenne szükség, mint sík képernyők esetén. A kisebb szögfelbontás hatására a távolban lévő részleteket már pár méterről is pixelesen látjuk, a nagy távolságban lévő tárgyak pedig már nagyon pontatlanul látszanak, 100 méterről egy emberalak, illetve ruházatának színe felismerhető, de felszerelése már nem.

2. ábra

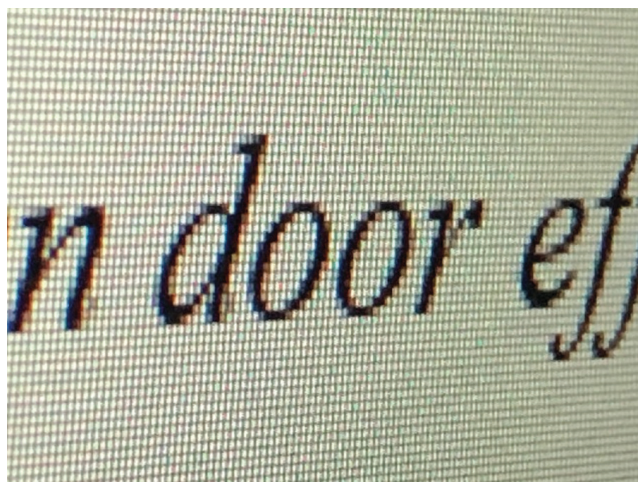
A Varjo VR-2 Pro felbontásának szemléltetése az első generációs VR HMD-k kijelzőihez viszonyítva

Forrás: a Varjo VR-2 Pro gyártói oldala: https://varjo.com/products/vr-2-pro/

A kijelzők felbontásának növelésével az új eszközök látványosan tudják csökkenteni ezt a hiányosságot, mint az a Varjo VR-2 Pro professzionális, űrhajósok felkészítésében is használt VR-eszköz esetén is látható a 2. ábrán.[8] Ez, illetve utódja, a VR-3 azért is érdekesek, mert a technológiai korlátok miatt nem egyszerűen csak a kijelző felbontását növelték meg, hanem két különböző felbontású kijelzőt kombináltak össze az élesebb kép elérése érdekében. Szemenként a 27 × 27 fokosra állított fókuszterületet egy 1920 × 1920 pixel felbontású, a perifériás területet pedig egy 2880 × 2720 pixel felbontású kijelző fedi le.[9]

[8] Varjo: Varjo & Boeing: A New Era in Astronaut Training using Virtual Reality. (é. n.).
[9] Varjo: Varjo VR-3 specifikációja (é. n.).

Az alacsony pixelszámból eredő gyenge szögfelbontás a távolban lévő tárgyak grafikai elnagyoltságán kívül más negatív hatást is eredményez, amelynek fényforrások közötti üres helyek az okozói. Az emberi szem átlagosan 1 szögperces felbontású, ami azt jelenti, hogy 1 méter távolságból 0,3 milliméteres méretű (nagy kontrasztú, fókuszban lévő) pontokat tud megkülönböztetni.[10] Mivel a VR-eszközök kijelzőit, típustól és beállítástól függően 3–7 cm távolságból, fókuszáltan nézzük, a mikrométeres méretű pixelrács már a látható felbontás tartományába esik és a 3. ábrán látható képet eredményezi, amit *screen door effect*-nek *(SDE),* azaz a „szúnyoghálós ajtó" hatásnak nevezünk.



3. ábra

A „screen door effect" (SDE) monitort közelről fényképezve. A látvány olyan, mintha szúnyoghálón keresztül néznénk a képet

Forrás: a szerző saját felvétele, Microsoft Word dokumentumról, Dell P2414H típusú monitoron közelről fényképezve

A jelenség – tapasztalataim szerint – nem túlzottan zavaró, és a felbontás növelésével kiküszöbölhető, de ennek ellenére több módszert alkalmaznak teljes eltüntetésére. Az egyik, már elterjed megoldás a hatás csökkentése érdekében, hogy a pixeleket alkotó elemi RGB alpixeleket nem egymás után szervezik, hanem különböző mintákat és kiegészítő alpixeleket alkalmaznak.[11] Az ilyen megoldások alkalmazásával, mint például a *Samsung PenTile Matrix* esetén, nem szabályos sorba esnek a pixelek, így kevésbé markánsan láthatók egyenes vonalakból álló rácsok. A *screen door effect* csökkentésének további technikai lehetősége, hogy a pixeleket optikailag vagy mechanikailag elmossák, ezáltal megpróbálva a pixelrácsra való fókuszálást megakadályozni. Az optikai megoldások közé tartozik a Valve cég (a Valve Index VR-eszköz gyártójának)

[10] Rafael Navarro: The Optical Design of the Human Eye: a Critical Review. *Journal of Optometry,* 2. (2009), 1. 3–18.
[11] Michael E. Miller et al.: P-34: Image Quality Impact of Pixel Patterns and Image Processing Algorithms for RGBW OLED Displays. *SID Symposium Digest of Technical Papers,* 36. (2005), 1. 398–401.

szabadalma, amely egy mikrolencsékből álló optikát helyez a lencse és a felhasználó szeme közé azzal a céllal, hogy elmossa a pixelrács kontúrjait.[12] Az optikai megoldások közé tartoznak még a különböző flexibilis átlátszó filmrétegek, mint például poli-etilén-tereptalát alapú oxigénplazmába ágyazott átlátszó anyagok, amelyek a fény hullámhosszához közeli felbontású mikromintázatokat tartalmaznak. Ez a megoldás sajnos rontja, ködösíti a látott képet, amely hatást poli-dimetilsziloxán (PDMS-) bevonat alkalmazásával próbálják csökkenteni.[13] Hasonló elven alapuló megoldás difraktív flexibilis műanyag filmrétegek alkalmazása, ahol a cél szintén véletlenszerű fénytörés kialakítása.[14] A fókuszálást megakadályozó, azaz a pixelek összeolvasztását célzó megoldás lehet még a kijelző mechanikai manipulálása, amely során a piezo-elektromos aktuátorokkal a pixeleket fizikailag is mozgatják.[15]

A jövőbeni kijelzők a fenti problémákat a felbontás növelésével fokozatosan ki fogják küszöbölni, de addig is a kiképzési feladatok tervezésénél ezt a tényezőt figyelembe lehet és kell is venni. Tapasztalati szabályként kezelhető, hogy a jelenlegi technológiai színvonalon a felhasználó a feladatait a virtuális térben lehetőleg 50 méteren belül oldja meg.[16] Már ma is lehet elvétve kapni nagyobb felbontású 2 × 4K (2 × 3840 × 2160) kijelzővel szerelt eszközöket, de a saját fejlesztés szempontjából vizsgálva tudni kell, hogy ezek a termékek még nem annyira közismertek, ezért kompatibilitásuk, szoftveres támogatásuk jóval kisebb, a meghajtóhardver-igényük sokkal nagyobb, mint a korábban említett, elterjedt típusoké. A nagy felbontású kijelzők alkalmazását nemcsak az első cikkben említett Pimax Vision 8K sorozata vagy a Varjo VR termékei célozzák meg, hanem az összes piaci szereplő a felbontás növelésének irányába halad.

2.2. Optikai hiányosságok

Az HMD-k által szolgáltatott vizuális információ nemcsak az előzőekben tárgyalt felbontástól, hanem a kijelzők egyéb paramétereitől (fényerő, kontraszt, képfrissítési frekvencia), valamint a szem és a kijelző közötti lencse (vagy lencsék) minőségétől is nagyban függ. Ugyan nem validált mérésről van szó, de a lencsén keresztül fotózott képeken (4. ábra) is jól látható, hogy a virtuális műszerek olvashatósága nem mindig a legnagyobb felbontású kijelzőn a legjobb. A gyártók ezért törekszenek arra, hogy a cikksorozat korábbi részében említett, a VR-eszközökben használt Fresnel-lencsék optikai hiányosságait kiküszöböljék. Az ilyen lencsék főleg a széleken torzítanak, illetve optikai torzítás lép fel, ha nem merőleges szögben nézünk bele. A HMD-t emiatt pontosan kell elhelyezni a fejen, azaz a lencse közepénél kell a szemnek elhelyezkednie, illetve a lencsének pont merőlegesnek

[12] Szabadalmi bejegyzés: Valve Corporation, Bellevue WA (US): Mitigation of Screen Door Effect in Head Mounted Displays. Pub. No.: US 2018/0038996 A1, 2018. 02. 08. United Stated Patent Application Publication Hudman.

[13] Won Seok Cho et al.: Air-gap-embedded robust hazy films to reduce the screen-door effect in virtual reality displays. *Nanoscale,* 12. (2020), 16. 8750–8757.

[14] Brett Sitter et al.: 78-3: Screen Door Effect Reduction with Diffractive Film for Virtual Reality and Augmented Reality Displays. *SID Symposium Digest of Technical Papers,* 48. (2017), 1. 1150–1153.

[15] Jilian Nguyen et al.: Screen door effect reduction using mechanical shifting for virtual reality displays. In *Optical Architectures for Displays and Sensing in Augmented, Virtual, and Mixed Reality (AR, VR, MR).* 2020. 11310.

[16] Stew Magnuson: Navy Cautious About Use of Virtual Reality Goggles in Training, Simulation. *National Defense,* 2017. 11. 29.

kell lennie a szem tengelyére, különben az érzékelt kép homályos lehet, torzíthat, vagy a Fresnel-lencsére jellemző koncentrikus körvonalak láthatóvá válhatnak. Ha a kijelző a megfelelő pozícióban van, arra is figyelni kell, hogy az stabilan legyen rögzítve, mivel dinamikusabb mozgás hatására elmozdulhat. A gyártók a rögzítő mechanizmusokat nagy gondossággal fejlesztik azért, hogy a lencse mindig optimális helyzetben legyen a szemhez képest, de a felhasználót minden esetben tájékoztatni kell a helyes viselésről. A Fresnel-lencsék kialakítása is változott a fejlesztések során, hogy jobban megfeleljenek a virtuálisvalóság-eszközök igényeinek, kevésbé legyenek érzékenyek az elmozdulásra. Az Oculus Rift S gyártója, a *Facebook Technologies,* szabadalmat is benyújtott, amiben a Fresnel-lencse közepén található normál lencse méretét növelte, ezzel egy hibrid lencsét létrehozva, és így biztosítva a jobb képminőséget.[17]

4. ábra

Ugyanazon képrészlet kinagyítva, különböző felbontású eszközök esetén, lencsén keresztül fényképezve (Oculus Quest 2: 1832 × 1920, VRgineers XTAL 8K: 3840 × 2160, HP Reverb G2: 2160 × 2160)

Forrás: Tyriel Wood – VR Tech: TTL the Most Expensive VR – XTAL 8k vs Reverb G2 vs Quest 2! Youtube, 2021. február 11.

A nagy görbületű lencsék széleken tapasztalható erős geometriai torzítása okozhatna még problémát, de a megjelenített képen szoftveres megoldással inverz torzítást végeznek, így a látott kép pont megfelelő lesz (5. ábra). Ezt a javítást minden rendszerben az optikához igazodva végzik, külső szoftveres alkalmazást nem igényel és a geometriai torzítás teljes mértékben kiküszöbölhetővé válik, így a kiképzés szempontjából nem okoz gondot.

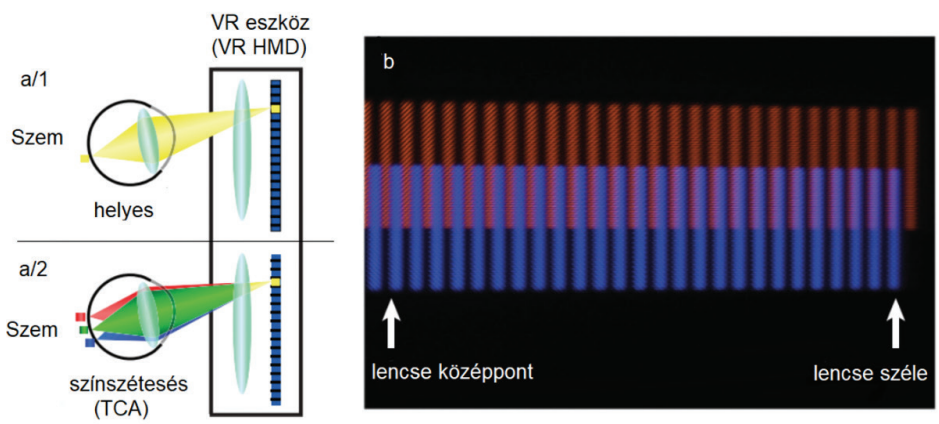
[17] United States Patent and Trademark Office: Facebook Technologies LLC, Menlo Park, CA (US): Hybrid Fresnel Lens with Reduced Artifacts. United States Patent, Wheelwright et al. Patent No.: US 10,133,076 B2, 2018. 11. 20.

5. ábra

Lencse torzításának szoftveres javítása; középső kép: a lencse torzítása; bal oldali kép: alkalmazott szoftveres inverz torzítás; jobb oldali kép: a lencsén keresztül látott kép

Forrás: Sora Thompson: VR Lens Basics: Present And Future. Tom's Hardware, 2018. január 1.

A lencsék esetén a szélek felé, azaz a látómező középpontjától kifelé haladva nemcsak a geometriai torzítás okoz gondot, hanem az úgynevezett „színek szétesése" (*transverse chromatic aberration,* TCA) effektus is. Ez a hatás más optikai rendszerben is előfordul, több formája is létezik, de lényege, hogy a lencse szélei felé haladva az a fehér fényt egyre nagyobb törésű prizmaként alkotóelemeire bontja, ami miatt színszétesés figyelhető meg (6. ábra). A 6. ábra *a/1, a/2* részábráin a VR-eszköz sematikus felépítését (kijelző + lencse) láthatjuk. Az *a/1* esetben nincs színszétesés; míg az a/2 esetben látszik, hogy a fehér fény alkotórészei különböző helyekre fókuszálódnak a retinán, azaz szétesik. A *b* ábrán látható, hogy a látómező (lencse) széle felé a piros és kék vonalak szétesnek a TCA miatt, míg a látómező közepén egybeesnek. A mérés Oculus Rift eszközzel történt, ahol a *lencse széle* jelzés a 15 fokos eltérést jelenti a középvonaltól.



6. ábra

A színszétesés jelenségének magyarázata

Forrás: a szerző szerkesztése Ryan Beams – Andrea S. Kim – Aldo Badano: Transverse chromatic aberration in virtual reality head-mounted displays. Optics Express, 27. (2019), 18. 877–884. ábra alapján

Tapasztalatom szerint a színszétesés hatása szintén nem zavaró, a fókuszált látómezőben minimálisan érzékelhető.

A nagy kontrasztú, nagy fényerejű képek esetén érzékelhetők az úgynevezett „szellem-" vagy „isten-" sugarak *(ghost-rays, god's rays).* Ez hasonló a felhőkön, kis területeken átszűrődő erős fény esetén látható fénysugarak látványához, de a jelenség a kiképzési célú igénybevétel szempontjából szintén nem befolyásolja érdemben az immerzivitás élményét. A kiképzési környezet tervezése, fejlesztése esetén, empirikus úton megközelítve, főleg a fényviszonyokra, kontrasztokra nagyobb figyelmet fordítva teljesen kiküszöbölhető.

Mint korábban említettem, a VR-eszközökben szemenként külön kijelzőt és külön lencsét találhatunk. A lencsék egymástól való távolsága fontos tényező, mivel a két lencsének külön-külön is középen és merőlegesen kell elhelyezkednie a szem tengelyéhez viszonyítva. Fontos tehát, hogy a felhasználók pupillái közötti távolság (interpupillary distance, IPD) és a lencsék középpontjának távolsága lehetőleg azonos legyen. A lencsék pozicionálása bizonyos HMD-k esetében fix, Oculus Rift S esetében például 63,5 mm. A gyártó szerint 61,5 mm és 65,5 mm közötti pupillatávolsággal jól használhatók az eszközök, viszont azoknál a felhasználóknál, akik pupillatávolsága nem ebbe a sávba esik, kellemetlen lehet a használata, a kép is torzulhat. További szoftveres korrekció bizonyos értékeken belül még lehetséges szoftveres átkonfigurálás segítségével. Más eszközök, mint például a HTC Vive Pro esetén az IPD mechanikusan is állítható, ezzel kiküszöbölve ezt a problémát.

3. A virtuális helyváltoztatás problémái

A VR-eszközök lényege, hogy a teljes látómezőnket lefedve, a külvilágot kiiktatva, a virtuális térben szabadon helyet változtathatunk. A mozgás a taktikai kiképzésben kulcsfontosságú elem, annak igazodnia kell a feladat végrehajtásához, a felhasználó végezhet normál járást, futást, felvehet különböző testhelyzeteket például fedezékhasználathoz, esetleg járműben utazhat.

3.1. A szimulátorbetegség

Az alap VR-készletek esetén (HMD + kézi kontrollerek) az ilyen mozgásokból a helyváltoztatás, azaz a futás, járás okozhat problémát, mivel a kontrolleren működtetett gomb vagy thumbstick *(joystick)* segítségével lehet haladni a virtuális térben. Ilyenkor jelentkezik a szimulátorbetegség *(simulator sickness),* ami olyan tünetegyüttest produkál, mint amilyet különböző mozgásbetegségek *(motion sickness),* például a tengeribetegség is okoz. A jelenség gyökere, a korábban már többször említett beviteli indirekció, azaz a természetes mozgás felváltása valamilyen ember–gép interfész működtetésével. A jelenség kellemetlen velejárója lehet a VR-rendszerek használatának, ami alapvetően abból adódik, hogy a vizuálisan (HMD képe), illetve a test többi része által érzékelt ingerek (gyorsulások) nincsenek szinkronban. Az elfogadott elméletek szerint a mozgásbetegségek valamilyen érzékelési konfliktus vagy érzékelési eltérés eredményei,

amikor is az egyensúlyi érzékszervek, a látás és a kinesztetikus (mozgási) rendszer bejövő ingereinek mintázata nem egyezik az elvárttal.[18] Az elvárt mintázat azt jelenti, hogy a teljes érzetet a mozgásnál a különböző érzékszervek és mozgási rendszer együttes ingerei adják, és adott mozgásra egy már megszokott ingeregyüttest vár a szervezet. Nagyon hasonló eset, amikor autóban ülve fékezünk, a testünket önkéntelenül is megfeszítjük, hogy megtartsa magát az eredeti helyzetében, a lassulást kompenzálva. Ha ez a lassulás valamiért elmarad, akkor is megfeszítjük, előrefeszítjük a testünket a fékpedál megnyomásakor, a lassulás hiánya így egy furcsa, kellemetlen érzést kelt. J. R. R. Stott által 1986-ban publikált 3 pontos „ökölszabály" modell még mindig elég praktikus, és a VR-ra vetítve láthatjuk, hogy az első pontja a vizuális-vesztibuláris (képi-egyensúlyrendszeri) pont nem teljesül, amely szerint a fej mozgása esetén a külső, látott képnek ellenkező irányba kell mozognia.[19] A fent említett egyszerű VR-eszközökkel való mozgásnál a fej nem mozog előre, de a külső látott kép ellenkező irányba mozog, mintha haladnánk előre, tehát a konfliktus fennáll. Az érzékelések közötti folyamatos konfliktus eleinte szédülést, a gyomorban diszkomfortérzést okozhat még a kevésbé érzékenyeknél is. Tapasztalatom viszont az, hogy mivel ez a fajta önkéntelen reakció is tanult (beidegződött), fokozatos gyakorlással a szimulátorbetegség hatása csökkenthető. Első alkalommal, hirtelen mozgások esetén pár perc után is kellemetlen lehet a VR használata, de pár nap után (napi gyakorlással) kitolható órákra is a tünetmentes használat.[20] Nem reprezentatív, 8 fős végzett saját teszteken láthattam, hogy az állva történő folyamatos haladásból *(locomotion)*[21] történő megállás esetén még fél óra tapasztalat után is 6 felhasználó automatikusan előredől, majd meginog, mivel a megállás okozta erőket kompenzálni próbálja. A tudományos irodalomban eltérő vélemények olvashatók a szimulátorbetegség tüneteinek csökkentési lehetőségeiről, de a kiképzésben használható megoldások, amelyeket a fejlett, kiképzésre használt VR-rendszerek is alkalmaznak, ezt már teljesen kiküszöbölik.[22]

3.2. A helyhez kötöttség problémája

A technológia felmérésénél már említettem a VR-rendszerek helyhez kötöttségét, aminek fő oka a nagy sávszélességigény miatt alkalmazott kábeles megoldások használata. A fejen lévő HMD és a központi egység (számítógép) között kábeles összeköttetés szükséges, ezért a kábelek nemcsak a bejárható teret határozzák meg, de a mozgásban is gátolhatják, zavarhatják a felhasználót. Bizonyos drágább

[18] J. F. Golding: Chapter 27 – Motion sickness. *Handbook of Clinical Neurology,* 137. (2016), 371–390.

[19] J. R. R. Stott. Mechanisms and Treatment of Motion Illness. In Christopher J. Davis – Gerry V. Lake-Bakaar – David G. Grahame-Smith (szerk.): *Nausea and Vomiting: Mechanisms and Treatment.* Berlin, Springer-Verlag, 1986. 110–129.

[20] A szerző saját megfigyelése 3 fős végzett, nem reprezentatív, nem formális mérés.

[21] A virtuális valóság szakirodalmában, gyakorlatában a virtuális térben, a helyváltoztatás indirekt, nem természetes beviteli módszerek esetén (joystick, billentyűzet) kétféle gyakorlat az elfogadott. A folyamatos mozgatása a virtuális látótérnek (felhasználónak) az úgynevezett *locomotion,* az ugrásszerű mozgatás pedig az úgynevezett *teleport*.

[22] Natalia M. Dużmańska-Misiarczyk – Paweł M. Strojny – Agnieszka Strojny: Can Simulator Sickness Be Avoided? A Review on Temporal Aspects of Simulator Sickness. *Frontiers in Psychology,* 9. (2018), november 6.

eszközökhöz létezik vezeték nélküli átvitel, illetve vannak már önálló, azaz olyan virtuálisvalóság-sisakok (HMD-k), amelyek tartalmazzák a számítógépet is, de ezek a hardver korlátozott kapacitása miatt jelentősen csökkentik a szimuláció lehetséges részletgazdagságát.[23] A helyhez kötöttség problémájának egy köztes megoldási lehetősége – amit más katonai szimulációs rendszerekben is használnak[24] –, hogy a mennyezeten lévő, mozgatható, a felhasználót követő rugós mechanikán, csigákon keresztül, a fej fölül lógatják be a kábelt, így az nem csavarodik, nem botlik el benne a felhasználó. Szerencsére a kiképzés szempontjából a fenti problémák megoldhatók, mind a szimulátorbetegség, mind a helyhez kötöttség problémája kiküszöbölhető további felszerelések alkalmazásával.

3.3. A helyváltoztatás problémájának megoldásai

Ha adottnak vesszük a rendelkezésre álló eszközöket, és nem természetes bevitellel hozzuk létre a mozgást, akkor is van szoftveres megoldásra lehetőség. Mint az előzőekben szó volt róla, ezek még így sem alkalmasak a kiképzési célok elérésére, de ha csak alapkészlettel rendelkezünk, a szimulátorbetegség kialakulását megelőzhetik. A videójáték-ipar egyik ilyen megoldása a „teleportálás", amely során a virtuális térben egy „lézer" mutatóval kijelöljük, hogy hova szeretnénk ugrani, és a helyváltoztatás ugrásszerűen történik, az nincs rossz hatással a felhasználó érzékszerveire. A másik megoldás, hogy a perifériális látómezőt kitakarják a folyamatos mozgás *(locomotion)* során, így egy filmvetítés érzését kelti, nem pedig azt, mintha a felhasználó teljes testtel mozogna. Mint említettem, egyik megoldás sem felel meg a taktikai kiképzés kívánalmainak, viszont demonstrációs célokra ezek a megoldások már komfortosan használhatók.

Egy komplexebb és akár taktikai kiképzésben is használható megoldás a virtuális taposómalom (*Omni-directional treadmill,* ODT) alkalmazása, ez esetben a járás, futás beviteléhez egy speciális eszközt lehet alkalmazni, ami a láb mozgását alakítja át a virtuális térben történő mozgásra (7. ábra) úgy, hogy a derék rögzítve van. Ez a megoldás már taktikai kiképzőeszközökben is megjelent, és csökkenti ugyan a szimulátorbetegség kialakulását, de dinamikus irányváltoztatásra, futásból megállásra, hirtelen elindulás szimulálására nem alkalmas, a felhasználónak nagyon oda kell figyelnie arra, hogy az eszközből ne csússzon ki a lába. A fekvő testhelyzet felvétele sem megoldott, ugyanakkor az ODT-k alkalmazásával a számítógépet és a HMD-t összekötő kábelek zavaró hatását is ki lehet küszöbölni, mivel azt a fej mögötti csatornában lehet elvezetni. A virtuális taposómalmok még egy nagy előnye, hogy a virtuális tér teljesen korlátlan minden irányban, illetve a futás miatti fáradtságérzetet is képes előidézni. A nagy területek bejárhatóvá tétele nem alapvető tényező taktikai kiképzések esetén, de egy kiterjedt hadgyakorlat szimulálásakor előnyös lehet.

[23] Oculus Quest gyártói oldala: www.oculus.com/quest.
[24] Arirang News: Korean startup releases VR simulators for military training. *Youtube,* 2016. július 19.

7. ábra

A KAT VR virtuális taposómalmokat gyártó cég KAT VR Premium terméke

Forrás: KAT VR gyártói honlapja: www.kat-vr.com/products/kat-walk-premium-vr-treadmill

A legjobb megoldás a helyhez kötöttség problémáira a háton viselt számítógép alkalmazása (8. ábra), amelynek segítségével a teljes szimuláció a felhasználó hátára rögzített számítógépen futtatható, a felhasználók tevékenységének szinkronizálásához szükséges adatforgalom pedig már vezeték nélküli kapcsolaton keresztül megoldható.

8. ábra

A MotionReality cég Dauntless termékénél alkalmazott viselhető számítógép

Forrás: Motion Reality Inc. Twitter oldala: https://twitter.com/motionreality/status/1224377479550447622/photo/1

Itt egy kis technikai kitérőt érdemes tenni, mert a háton viselt számítógép paraméterei, számítási lehetőségei is igen fontosak. A virtuálisvalóság-szimuláció alkalmazása a szórakoztatóiparban fejlődött ki, ezen belül is a számítógépes játékok területén vált a vonzó és elterjedt megoldássá. A háromdimenziós játékok készítéséhez eddig is modellezni kellett a virtuális teret, a szereplőket, illetve a modelleket megfelelő atmoszférában, megfelelő textúrákkal ellátva, fényekkel megvilágítva, a játékos szemszögéből nézve kellett megjeleníteni. Ehhez kétdimenziós képet kell generálni háromdimenziós modellek, fények, egyéb tényezők adataiból, másodpercenként minimum 20-szor, de szimulátorok esetén, a minél kisebb reakcióidő miatt inkább a másodperceként 60–90 képkocka az elvárt. A modellek, textúrák, fényhatások, egyéb vizuális effektusok egyre részletesebbek lettek az idő folyamán, így a létrehozott 2D képek felbontása is nőtt, azaz egyre nagyobb lett a számítási kapacitási igény. A VR-eszközök két külön képből álló sztereó képet renderelnek, ezért a számításikapacitás-szükséglet, ha nem is kétszeres, de jóval nagyobb egy monitoron megjelenített szimulációhoz képest. A 2021-es évben forgalomban lévő, háromdimenziós virtuális szimulációt futtató eszközben csak a grafikus processzor (GPU) akár 28,3 milliárd tranzisztort is tartalmazhat, 628,4 mm^2-es lapkán, 8 nm-es gyártástechnológia mellett.[25] Az alkalmazott GPU-hoz dedikált memória pedig általában 8–11 Gigabyte méretű és GDDR5[26] vagy GDDR6 típusú. A kiképzéshez használható katonai, nagy felbontású komplex 3D modelleket tartalmazó, esetleg mesterséges intelligenciát is futtató szimulációkat kiszolgáló rendszerek konfigurációjára is ez lehet a minimumkövetelmény. Szerencsére a már többször említett, hátra szerelhető, VR-használatra optimalizált hardverek pont ilyen igényekhez lettek kifejlesztve, figyelembe veszik a katonai szabványokat és kereskedelmi forgalomban is beszerezhetők.[27]

4. Összegzés

Annak ellenére, hogy elemzésem szerint a technikai háttér jelenlegi fejlettségi szintje alapján a lehető legjobb időben vagyunk egy professzionális rendszer fejlesztéséhez, fontos tudni, hogy milyen korlátokkal kell szembenéznünk. A VR-rendszerek problémái főleg a vizuális megjelenítés és a mozgások szimulálásának kérdéseire korlátozódnak. A vizuális problémák már a mostani eszközök esetén is elhanyagolhatók, a hardvereszközök folyamatosan fejlődnek, paramétereik javulnak, valamint a szoftverfejlesztési keretrendszerek szabványosodásával, folyamatos bővülésükkel az eszközök közötti váltás, az újabb hardvertermékekre való átállás egyre kevesebb többletfejlesztési munkát indukál.[28] A fejlesztett kiképzőeszközök esetén a hardver adottságait a szakmai tervezésnél viszont figyelembe kell venni, empirikus úton tesztelni

[25] nVIDIA: nVIDIA Ampere GA102 GPU Architecture. Whitepaper. 2021.

[26] Graphics Double Data Rate 5 Synchronous Dynamic Random-Access Memory: a legelterjedtebb memóriatípus a korszerű grafikus kártyákban.

[27] A HP Mil-Std-810G teljesítésére tervezett viselhető számítógépe a HP VR Backpack G2: www8.hp.com/h20195/v2/GetDocument.aspx?docname=c06274598.

[28] Steam VR és Open VR platformok egységes interfészt adnak több VR-hardvereszköznek is. A programok fejlesztése nem igényel hardverközeli programozást.

szükséges a kialakított rendszer virtuálisan megépített modelljeit és használhatóságát vizuális szempontból. Ha saját fejlesztésben gondolkodunk, akkor a mozgással kapcsolatos problémák is áthidalhatók, viszont többletfigyelmet és előzetes tervezési döntéseket igényel a terület. A jelen cikkben ugyan nem említettem, de fontos sarokköve a saját fejlesztésű VR-kiképzőrendszereknek a valós eszközök virtuális térbe történő beemelése és tökéletesen egyező működése, de mivel számos ilyen megoldást láthattunk a cikksorozat előző részeiben, a hardverfejlesztési kompetencia megléte esetén ez nem jelent akadályt. Eddigi elemzéseimből kiderülhetett, hogy egy hazai fejlesztés elindításának nincs akadálya a technológia oldaláról nézve. A következő cikkben, egyet hátra lépve, a sikeres fejlesztéshez szükséges kompetenciákat és a fejlesztési környezetet fogom áttekinteni és elemezni, szintén a saját fejlesztés megindításának lehetőségeire fókuszálva.

Felhasznált irodalom

Beams, Ryan – Andrea S. Kim – Aldo Badano: Transverse chromatic aberration in virtual reality head-mounted displays. *Optics Express,* 27. (2019), 18. 877–884. Online: https://doi.org/10.1364/OE.27.024877

Cho, Won Seok – Park – Choi J. Y. – Cho C. S. – Baek S.-H. S. – J.-L. Lee: Air-gap-embedded robust hazy films to reduce the screen-door effect in virtual reality displays. *Nanoscale,* 12. (2020), 16. 8750–8757. Online: https://doi.org/10.1039/C9NR10615D

Golding, J. F.: Chapter 27 – Motion sickness. *Handbook of Clinical Neurology,* 137. (2016), 371–390. Online: https://doi.org/10.1016/B978-0-444-63437-5.00027-3

Magnuson, Stew: Navy Cautious About Use of Virtual Reality Goggles in Training, Simulation. *National Defense,* 2017. 11. 29. Online: www.nationaldefensemagazine.org/Articles/2017/11/29/Navy%20Cautious%20About%20Use%20of%20Virtual%20Reality%20Goggles%20in%20Training%20Simulation

Miller, Michael E., Michael J. Murdoch – Paul J. Kane – Andrew D. Arnold: P-34: Image Quality Impact of Pixel Patterns and Image Processing Algorithms for RGBW OLED Displays. *SID Symposium Digest of Technical Papers,* 36. (2005), 1. 398–401. Online: https://doi.org/10.1889/1.2036456

Natalia M. Dużmańska-Misiarczyk – Paweł M. Strojny – Agnieszka Strojny: Can Simulator Sickness Be Avoided? A Review on Temporal Aspects of Simulator Sickness. *Frontiers in Psychology,* 9. (2018), november 6. Online: https://doi.org/10.3389/fpsyg.2018.02132

Navarro, Rafael: The Optical Design of the Human Eye: a Critical Review. *Journal of Optometry,* 2. (2009), 1. 3–18. Online: https://doi.org/10.3921/joptom.2009.3

Nguyen, Jilian – Clinton Smith – Ziv Magoz – Jasmine Sears: Screen door effect reduction using mechanical shifting for virtual reality displays. In *Optical Architectures for Displays and Sensing in Augmented, Virtual, and Mixed Reality (AR, VR, MR).* 2020. 11310. Online: https://doi.org/10.1117/12.2544479

nVIDIA: *nVIDIA Ampere GA102 GPU Architecture.* Whitepaper. 2021. Online: www.nvidia.com/content/PDF/nvidia-ampere-ga-102-gpu-architecture-whitepaper-v2.pdf

Sitter, Brett – Joseph Yang – Jimmy Thielen – Nathan Naismith – Jeffrey Lonergan 78-3: Screen Door Effect Reduction with Diffractive Film for Virtual Reality and Augmented Reality Displays. *SID Symposium Digest of Technical Papers,* 48. (2017), 1. 1150–1153. Online: https://doi.org/10.1002/sdtp.11846

Stott, J. R. R.: Mechanisms and Treatment of Motion Illness. In Christopher J. Davis – Gerry V. Lake-Bakaar – David G. Grahame-Smith (szerk.): *Nausea and Vomiting: Mechanisms and Treatment.* Springer-Verlag, Berlin, 1986. 110–129.

Thompson, Sora: VR Lens Basics: Present And Future. *Tom's Hardware,* 2018. január 1. Online: www.tomshardware.com/news/virtual-reality-lens-basics-vr,36182.html

Trautmann Balázs: Képzelt repülés. *Honvédelem.hu,* 2019. április 16. Online: https://honvedelem.hu/hirek/hazai-hirek/kepzelt-repules.html

Jogi források

United States Patent and Trademark Office: Facebook Technologies LLC, Menlo Park, CA (US): Hybrid Fresnel Lens with Reduced Artifacts. United States Patent, Wheelwright et al. Patent No.: US 10,133,076 B2, 2018. 11. 20. Online: https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=10133076&IDKey=D43B19EFAF55%0D%0A

Valve Corporation, Bellevue WA (US): Mitigation of Screen Door Effect in Head Mounted Displays, Pub. No.: US 2018/0038996 A1, 2018. 02. 08. United Stated Patent Application Publication Hudman. Online: www.freepatentsonline.com/20180038996.pdf

Internetes források

Arirang News: Korean startup releases VR simulators for military training. *Youtube,* 2016. július 19. Online: www.youtube.com/watch?v=Et5BsV0U1Lw

Varjo: *Varjo & Boeing: A New Era in Astronaut Training using Virtual Reality* (é. n.) Online: https://varjo.com/boeing-starliner/

Varjo: *Varjo VR-3 specifikációja* (é. n.). Online: https://varjo.com/products/vr-3/#-fulltechspecs

Wood, Tyriel – VR Tech: TTL the Most Expensive VR – XTAL 8k vs Reverb G2 vs Quest 2! *Youtube,* 2021. február 11. Online: www.youtube.com/watch?v=S7nhlQciLlM

HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 3. szám 173–187.
DOI: 10.32567/hm.2021.3.10

Dub Máté[1]

A social engineering támadások megelőzésének lehetőségei[2]

The Opportunities for Social Engineering Attacks Prevention

Társadalmunk rohamos technológiai fejlődésével párhuzamosan új típusú kihívások és fenyegetések jelentek meg, és nem pusztán a kibertérben, hanem mindennapi életünk folyamán, az offline térben is fenyegetettségként jelentkeznek. A támadások számában szignifikáns növekedést, a támadási technikák szempontjából pedig egyre nagyobb szofisztikáltságot tapasztalhatunk. Gyakran elhangzik, már-már közhelyként, hogy a kiberbiztonság leggyengébb láncszeme a humán tényező. Ez a gondolat akármennyire is régóta előfordul a kiberbiztonsággal kapcsolatos publikációkban, annak érvényessége a mai napig fennáll, ugyanis a támadók leggyakrabban a nem kellően biztonságtudatos felhasználókat veszik célba, és e személyek tevékenysége miatt a legkiválóbb szoftverek sem nyújthatnak megfelelő biztonságot abban az esetben, ha a kezelő nem rendelkezik a megfelelő kompetenciákkal.

A nem kellően biztonságtudatos emberek számára kifejezetten nagy veszélyt jelentenek az egyre kifinomultabb social engineering szintjén zajló támadások, így e technika támadási keretrendszereinek és támadási modelljeinek vizsgálatával a megelőzés és az elkerülés minél hatékonyabb működését érhetjük el. Természetesen e tekintetben a tudatosítás és az oktatásba történő bevezetés fontosságát sem szabad elhanyagolnunk.

Kutatásomban a cél a védettség prosperálási lehetőségeinek vizsgálata volt a fentebb részletezett kiberfenyegetettségekkel szemben. Empirikus kísérletek elemzésével, a social engineering szintjén zajló támadások megelőzésével kapcsolatban a fő kérdést úgy fogalmazhatjuk meg, hogy vajon az adat- és információbiztonság,

[1] Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar, hallgató, e-mail: mate.dub@protonmail.ch

[2] A kutatás és a publikáció az Innovációs és Technológiai Minisztérium ÚNKP-20-1-I-NKE-71 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.

a biztonságtudatosság potenciálisan növelhető-e az érdeklődés felkeltése, a személyes, problémaorientált példák és az oktatásba való implementálás mentén?

Kulcsszavak: **social engineering, adat- és információbiztonság, biztonságtudatosság, adatvédelem, kiberbiztonság, közszolgálat**

In parallel with the rapid technological development of our society, new types of challenges and threats have emerged, and they are emerging as threats not only in the cyberspace, but also in our daily lives, in the offline space. There is a significant increase in the number of cyberattacks, while in terms of attack techniques we can see an increasing sophistication. It is often said, almost as a commonplace, that the weakest link in cybersecurity is the human factor. As often as this idea occurs in cybersecurity publications, it is still valid today, as attackers are most often targeted at users who are not sufficiently security-conscious, and even the best software cannot provide adequate security through the actions of these individuals if the user does not have the appropriate competencies.

People, who are not sufficiently security-conscious are especially at risk from increasingly sophisticated social engineering attacks, so by examining the attack frameworks and attack models of this technique, we can achieve the most effective prevention and avoidance. Of course, the importance of awareness raising and introduction into education should not be underestimated in this regard either.

The aim of my research was to investigate the possibilities of prosperity of protection against cyber threats, which have been detailed above. Regarding the analysis of empirical experiments and the prevention of social engineering attacks, the main question can be formulated as to whether data and information security, security awareness can potentially be increased along the lines of interest, personal, problem-oriented examples and implementation in education.

Keywords: **social engineering, data and information security, security awareness, data protection, cybersecurity, public service**

1. Bevezető

Az infokommunikációs technológiák rohamos terjedésével napjaink egyik legjelentősebb biztonsági kockázataként a kiberteret azonosíthatjuk. A nyilvánosságra kerülő, bejelentett kibertámadások száma drasztikusan növekszik, amely a trendek alapján várhatóan a privát, a vállalati és az állami szférában egyaránt jelentősen emelkedni fog. A támadók motivációi között szerepelhet többek között anyagi haszonszerzés, államok belpolitikai döntéshozatalának befolyásolása, kritikus infrastruktúrák elleni támadás, illetve a legkülönbözőbb bűncselekmények elkövetése.

A kibertámadásokkal szemben rendkívül nehéz védekezni, mivel annak költségei jelentősen magasabbak, mint a támadásoké. Az egyik legfontosabb és egyben legköltséghatékonyabb módja a védekezésnek a felhasználók kiberbiztonsági tudatosságának erősítése. Az internetezők adat- és információbiztonsági tudatosságának

szintje – függetlenül korosztálytól, nemtől, iskolai végzettségtől, beosztástól – nem nevezhető magasnak.

Ahogy a védelmi megoldások, úgy a támadások is egyre szofisztikáltabbak, komplexebbek, ezért a támadók elsősorban a rendszerek leggyengébb láncszemén, a nem kellően biztonságtudatos felhasználón keresztül igyekeznek hozzáférni a védett rendszerekhez. A szakirodalom az ilyen jellegű támadásokat social engineering támadásként definiálja. E támadási technikát egyaránt alkalmazzák a bűnözők, a terroristák és a hírszerzők céljaik elérése érdekében, ami rendkívül eltérő lehet, irányulhat információszerzésre, informatikai rendszer befolyásolására, dezinformálásra és számos egyéb tevékenységre.[3]

1.1. Social engineering

A social engineering fogalmának legjobb meghatározása Kevin Mitnick nevéhez köthető, amely szerint: „A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."[4]

Egy social engineering támadás négy fázisból épül fel: információgyűjtés; kapcsolat kiépítése; kapcsolat kihasználása; támadás végrehajtása.[5]

A social engineering támadások alkalmával a támadó egy személy vagy szervezet azon információihoz akar hozzájutni, amelyek a számára nem elérhetők, és ezen információkhoz az út magán a személyen vagy a szervezet munkatársain át vezet. A támadó a támadás végrehajtása során a célpontról személyes információkat gyűjt, személyes kontaktusba elegyedik, beszélget, és bizalmat, neki kedvező hangulatot teremt. A támadó a célpont emberi magatartására támaszkodva (empátia, segítségnyújtás) kezd el tevékenykedni.[6]

A befolyásolás művészeteként is definiált social engineeringnek számos támadási modellt és módszertant tulajdoníthatunk.[7] A social engineering támadások keretrendszerének alapját a négyfázisú körciklus adja, míg a támadási keretrendszerek összehasonlításának az alapját a különböző támadási szcenáriók adják.[8]

A támadási modell tekintetében a támadók a kommunikációjuk jellegeként használhatnak direkt és indirekt modellt. A támadáshoz a social engineernek meg

[3] Bányász Péter – Bóta Bettina – Csaba Zágon: A Social Engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37.

[4] Kevin Mitnick – William L. Simon: *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker, Illustrated edition.* New York, Back Bay Books, 2012.

[5] Francois Mouton – Louise Leenen – H.S. Venter: Social Engineering Attack Examples, Templates and Scenarios. *Computers and Security,* 59. (2016), 186–209.

[6] Kevin D. Mitnick – William L. Simon: *The Art of Deception: Controlling the Human Element of Security.* John Wiley & Sons, 2003.

[7] Christopher Hadnagy: *Social Engineering: The Art of Human Hacking.* John Wiley & Sons, 2010.

[8] Katharina Krombholz et al.: Advanced Social Engineering Attacks. *Journal of Information Security and Applications,* 22. (2015), 113–122.

kell határoznia emellett a célpontot, a közeget, a célt, valamint a manipuláció alapját és technikáit, emellett el kell döntenie, hogy a támadás több lépcsőfokon keresztül valósuljon-e meg. Mindezek az alkalmazott modelltől függenek.[9]

1.2. Információbiztonság-tudatosság

Az információbiztonság és a social engineering kapcsolatáról elmondható, hogy a social engineer a célponttal – ideértendő a személy mint individuum, mint egy szervezet képviselője vagy mint egy csoport tagja – folytatott szociális interakciói során próbálja meg rábeszélni vagy megtéveszteni és végül meggyőzni az illetékes személyt, hogy egy konkrét kérést teljesítsen.

A kibertér mára információs társadalmunk integráns részét képezi.[10] Személyes és szakmai összefüggésben egyaránt a kibertér rendkívül hatékony eszközzé vált, és lehetővé teszi, hogy a legtöbb ember mindennapjait digitális tevékenységbe ültesse át. Elmondható azonban, hogy ez az életünkbe történő új behatás magával hozza az információbiztonság fontosságát is.[11]

A korszerű technológiákhoz való hozzáférés és használatuk széles körben elérhető bárkinek, ezért a kibertérben a tömegek megjelenésével együtt tapasztalhatjuk a humánalapú támadások szignifikáns növekedését is, azonban a kiberfenyegetések elleni védelemhez szükséges és már meglévő eszközök ismerete ennek ellenére hiányos.[12]

A kibertérben jelentkező veszélyek és kockázatok csökkentése szempontjából a legjelentősebb előrelépést akkor érhetnénk el, ha képzések, tanfolyamok, programok, szimulációk terén kezdenénk el felkészíteni az egyéneket. A megszerzett tudást a felhasználók hasznosíthatnák a mindennapi tevékenységük során és természetesen munkahelyi környezetükben.[13]

1.3. A potenciális veszélyekkel kapcsolatos tudatosság

Korunk új „olaja" az adat. Az adatokra napjainkra új iparágak épültek, amelyek azokat felhasználva teremtenek értékeket vagy profitot. Ugyan a cégek, vállalkozások a lehető legtöbb adatot próbálják begyűjteni a felhasználókról, hogy abból profilokat építsenek, azokat tovább értékesítsék, de Európában ez – a felhasználók javára – nem

[9] Bányász Péter: Social engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77.

[10] Tibor Farkas: Communication and Information Services – NATO Requirements, Part I. *Land Forces Academy Review,* 25. (2020), 4. 281–289; Tibor Farkas: Communication and Information Services – NATO Requirements, Part II. *Land Forces Academy Review,* 26. (2021), 1. 9–15.

[11] Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36.

[12] S. M. Furnell – P. Bryant – A. D. Phippen: Assessing the Security Perceptions of Personal Internet Users. *Computers & Security,* 26. (2007), 5. 410–417.

[13] Jemal Abawajy: User Preference of Cyber Security Awareness Delivery Methods. *Behaviour and Information Technology,* 33. (2014), 3. 237–248; Jemal Abawajy – Tai-hoon Kim: Performance Analysis of Cyber Security Awareness Delivery Methods. In Tai-hoon Kim et al. (szerk.): *Security Technology, Disaster Recovery and Business Continuity.* Berlin, Heidelberg, Springer, 2010. 142–148.

teljes mértékben triviális kérdés az évek óta hatályban lévő általános adatvédelmi rendeletnek (GDPR) köszönhetően.

Ahogy az infokommunikációs társadalmunkat egyre inkább behálózzák a különböző eszközök és technológiai vívmányok, úgy ezek teljesen új perspektívákat nyitnak a világ felé. Eszközeink segítségével szervezhetjük napjainkat, kapcsolatba léphetünk új vagy rég nem látott ismerőseinkkel, valamint teljesen új iparágak épülhetnek ki. Mindezek magukkal hozzák a magasabb szintű technológiához értő szakemberek képzésének szükségességét. Naivan úgy gondolhatjuk, hogy azáltal, hogy egyre többet használjuk ezeket a technológiákat és megfelelő szakembereket képzünk, alkalmazunk a cégeknél, az állami szektorban, legrosszabb esetben is autodidakta módon felismerjük – akár társadalmi szinten – a biztonságtudatosság hiányából fakadó kockázatokat és fenyegetettségeket. Ennek ellenére az emberek többsége továbbra is elszenvedője az imént felsorolt hiányosságoknak. E ránk leselkedő fenyegetések mértékének skálája a kis hatású adatvesztéstől egészen a katasztrofális gazdasági következményekig terjedhet. A kiindulópontot jelentheti például egy spam e-mail, amely egy kiberbűnözői csoporttól érkezett, és különböző kártékony kódokat alkalmazva lop el, korrumpál, vagy semmisít meg adatokat, akár jelentős mértékben.[14]

Az információbiztonság tekintetében a legjelentősebb tényező az emberek információbiztonság-tudatossága. E skálát meghatározhatjuk az alábbi szinteken:

- Alacsony szintű biztonságtudatosságú személyek: nem veszik figyelembe vagy közömbösen tekintenek a különböző biztonsági értesítésekre, valamint automatikusan elfogadnak minden feltételt az alkalmazások kezelésekor, weboldalak látogatásakor, illetve felcsatlakoznak az eszközeikről bármilyen nyílt hálózathoz titkosítás vagy anonimizálás nélkül (például WiFi-hez).
- Közepes szintű biztonságtudatosságú személyek: gondatlanságuk a technológia nem szakszerű alkalmazása mentén fejezhető ki.
- Magas szintű biztonságtudatosságú személyek: hasznosítják tudásukat a mindennapokban a kiberfenyegetettségek elkerülése érdekében, és képesek megelőző intézkedésekre az incidensek megelőzése céljából.

Az egyik legjelentősebb sérülékenységnek a különböző alkalmazások telepítésekor történő engedélymegadást, a webhelyeken történő információhozzáférés engedélyezését és a közösségimédia-oldalakon történő információmegosztást tekinthetjük.[15] A helyzetet az alacsony biztonságtudatossággal rendelkező személyek tekintetében tovább rontja, hogy a támadók leginkább ezt a csoportot veszik célba mint potenciális áldozatot, ugyanis ezek a hackerek ki tudják használni a különböző sérülékenységeket,

[14] Martti Lehto: Cyber Security Competencies – Cyber Security Education and Research in Finnish Universities. In Nasser Abouzakhar (szerk.): *14th European Conference on Information Warfare and Security, 2015.* Hatfield, The University of Hertfordshire, 2015. 179–188; Tóth András: Information-Sharing Challenges and Issues in Multinational Operations. *Land Forces Academy Review*, 25. (2020), 4. 307–316.

[15] R. S. Shaw et al.: The Impact of Information Richness on Information Security Awareness Training Effectiveness. *Computers & Education,* 52. (2009), 1. 92–100; Tóth András: International information security in hungary. In Ivan Majchút et al. (szerk.): *8. medzinárodná vedecká konferencia: National and International Security 2017.* Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2017. 548–557.

szoftveres hibákat és biztonsági hiányosságokat, amelyekről az ezen a szinten lévő felhasználók tudomást sem vesznek.[16]

A kibertérben történő jogsértések elszenvedői jelentős mértékben a biztonságtudatosság hiányából eredő személyekhez köthetők. Mára már elmondható, hogy a különböző vállalatok és az állami szektor széles körben folytat képzéseket és tudatosítási programokat, ám ezek közel sem nehezítik meg eléggé a kiberbűnözők tevékenységét, mindazonáltal a folyamatos tudatosítási kampányokkal az egyéni és szervezeti védettséget is növelhetjük. Az államigazgatás, a vállalati szereplők és a kibertérben tevékenykedő egyének tudatosításának legjobb módszere az, ha megmutatjuk, milyen módszerek alkalmazásával dolgoznak a támadók, és azoknak milyen következményei lehetnek, ezáltal fejlesztve a képességeket. A legfontosabb szempont e tekintetben az, hogy érthető legyen az átadni kívánt kompetencia a kiberbiztonság területén kevésbé jártas egyéneknek is.

2. A vizsgálat tárgya és a célkitűzések

A kutatás tudományos problémája a fentebb megfogalmazottakból ered, és alapjául két empirikus social engineering támadási kísérlet összevetése szolgál.

A kutatás célcsoportjának tagjai a magyar közszolgálat (a széles értelemben vett államigazgatás, Magyar Honvédség, Rendőrség, Katasztrófavédelem) iránt érdeklődő, vagy jelenleg e területeken a felsőoktatási képzésben részt vevők vagy jelenleg is ott dolgozók csoportja adta. Esetükben különösen fontos a megfelelő szintű biztonságtudatosság, hiszen a mindennapos munkavégzés során hozzáférnek – hozzáférhetnek majd – azokhoz a védett rendszerekhez, amelyekben a támadók számára értékes információk találhatók, vagy a döntéshozatalban való szerepük okán a befolyásolásuk értékes lehet. Ezek védelme és a munkatársak felkészítése az ország biztonságának érdekében is kiemelt fontosságú.[17]

Az empirikus kutatás kontrollcsoportjában az IT-biztonság, valamint az adat- és információbiztonság és social engineering iránt érdeklődő személyek szerepelnek.

A vizsgálat tárgyát a két csoport egy social engineering támadás esetén nyújtott viselkedésének elemzése adja.

A kutatás célkitűzése az volt, hogy tudományos vizsgálat során kimutatható-e összefüggés az adat- és információbiztonság, biztonságtudatosság és a social engineering támadások felismerése kapcsán a célcsoport és a kontrollcsoport teljesítménye között. Az érdeklődés felkeltése, a személyes, problémaorientált példák és az oktatásba történő bevezetés kapcsán vajon növelhető-e a személyek biztonságtudatossága?

[16] Tibor Farkas – András Tóth: Electronic warfare in full spectrum operation. In Milos Sotak – Mikulas Sostronek – Roman Beresik (szerk.): *Proceedings of the International Scientific Conference: New Trends in Signal Processing.* 2012. 181–188.

[17] Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. (2016), 1. 61–81; Tamás Szádeczky: Governmental Regulation of Cybersecurity in the EU and Hungary after 2000. *AARMS,* 19. (2020), 1. 83–93.

2.1. Kutatási hipotézisek

A kutatási téma feldolgozása során az alábbi hipotéziseket fogalmaztam meg:

H1. Az információbiztonsági tudatosságról alkotott önpercepció nem párosul valós biztonságtudatossággal kapcsolatos viselkedéssel.

H2. A célcsoportba tartozó személyek nagyobb valószínűséggel adják meg személyes adataikat, mint az adat- és információbiztonság iránt érdeklődő társaik.

H3. A kontrollcsoport tagjai kisebb eséllyel adják hozzájárulásukat olyan adatkezelési nyilatkozathoz, amelynek tartalma nem felel meg a törvényi előírásoknak.

2.2. Kutatási módszertan

A módszertan alapját a Tudás–Képesség–Viselkedés-modell és az információbiztonság humán aspektusa jelentette, emellett az elkészített kérdőíves felmérést tudományos statisztikai módszertannal (kereszttábla-elemzéssel) értékeltem ki, az SPSS Statistics szoftver segítségével. A kutatás során a felmérésekkor kitértem többek között az éberségen alapuló kísérletek elemzésére, valamint a social engineering támadási technika közvetlen, kétirányú kommunikációs modelljére

Fontos megjegyezni, hogy az itt felsorolt kutatási módszertanok mindegyike megfelel a hatályos jogszabályoknak. Vizsgálataim szigorúan az adatvédelmi elveknek megfelelő kutatásra korlátozódnak, amelynek célja az egyének és szervezetek védelmi képességeinek növelése.

A kutatási módszertan leírása egyaránt vonatkozik a célcsoportra, valamint a kontrollcsoportra.

3. Empirikus kutatások bemutatása

A célcsoport és a kontrollcsoport tekintetében is elmondható, hogy a social engineering támadási kísérletet azonos technikával, ám különböző eseményeken végeztem el. A rendezvények jellegéből adódóan különíthetjük el a két csoportot az adat- és információbiztonság, biztonságtudatosság kapcsán laikusokra (célcsoport) és érdeklődőkre (kontrollcsoport). Az alábbiakban részletezett felmérések összevetése által így megállapítható, hogy azonos körülmények között a csoportok tagjai milyen eredményeket mutattak fel.

3.1. Az empirikus kísérlet összeállítása

Mind a két esetben a social engineering támadási kísérlet hátterében egy ingyenes, ám feltételekhez kötött, kisebb-nagyobb értékű tárgyi nyereményeket kínáló sorsolás állt. A két empirikus kísérlet között a különbséget az jelentette, hogy a célcsoportnak több, a támadásra és a nyereményjáték valószerűtlenségére utaló jel állt rendelkezésére. Elmondható, hogy míg a kontrollcsoport az adatvédelmi nyilatkozatból tudta

kézzelfogható módon a támadást felismerni a támadó személyének – vagyis a kutatást végzőnek – attitűdjén, vagy az adatminimalizációs elvek figyelembevételének hiányán kívül, addig a célcsoportnak több lehetősége is volt felismerni a támadást, ezzel kompenzálva az esetleges szakmai hiányosságokat (ezek közé tartozott például az adatkezelési nyilatkozat szabadabb megfogalmazása).

Az alapvetően kérdőíven és kisebb, ezt követő interjúkon alapuló kísérlet magját egy négy részre osztható ív adta. Első oldalának felső részén a különböző rendezvényekkel kapcsolatos statisztikai jellegű kérdések, illetve egy, a kitöltő biztonságtudatossági önpercepciójára, valamint a jelszókezelésére vonatkozó kérdések szerepeltek. Az alsó felén volt található egy táblázat, amelybe a kitöltőnek különböző személyes adatait kellett/lehetett megadnia, egyéb kérdésekre kellett/lehetett válaszolnia, valamint itt szerepelt az adatvédelmi és hozzájáruló nyilatkozat is. A nyilatkozat a legkisebb mértékben sem volt a törvényi előírásokkal és az általános adatvédelmi rendelettel összhangban. Az aláírás alatt szereplő apróbetűs szöveg egyaránt vonatkozott a hozzájáruló személy nevében történő pénzfelvételre, csomagrendelésre és nyíltan tartalmazta a nyereményjáték valótlanságát is. Itt kell szót ejtenem arról, hogy személyes adatok valódi gyűjtésére nem került sor. A felső és az alsó részt egy preparált vonal választotta el, a támadási kísérlet befejezését követően pedig a hozzájáruló nyilatkozatot, valamint a személyes adatokat tartalmazó alsó részt a kitöltők minden esetben megkapták, míg a felső részen, ahol a statisztikai jellegű, jelszavakkal és biztonságtudatossági önpercepcióval kapcsolatos kérdések voltak, megtartottuk. Ezen felső laprész hátsó oldalán X-szel és pipával jelöltük azt, hogy az adott kitöltő mely kérdésekre válaszolt, mely személyes adatait adta meg, és hozzájárult-e a nyilatkozathoz aláírásával. A személyes adatok a két esetben vonatkoztak többek között a névre, életkorra, kapcsolati státuszra, e-mail-címre, telefonszámra, lakcímre és személyigazolvány-számra. A szenzitív jellegéből adódóan az elemzés tárgyát mindezek kapcsán utóbbi két személyes adat megadása, a biztonságtudatossági önpercepció, a jelszókezelési készségek és a nyilatkozat aláírása jelenti.

3.2. Módszertan szerinti elemzés

Ezen alfejezetekben részletezem a különböző módszertanok és modellek leírását, amelyek alapján a csoportokat vizsgáltam, és ismertetem azok eredményét. A leíró statisztika és a különböző kutatásmódszertani elemek mellett bemutatom az empirikus kutatások kereszttábla általi elemzését, amelyet SPSS Statistics szoftverrel készítettem. Meghatározom emellett a hipotézisek alátámasztására vagy megdöntésére vonatkozó eredményeket.

3.2.1. Éberségen alapuló kísérletek

A kísérlet elemzésének tekintetében beszélhetünk az úgynevezett éberségen alapuló kísérletről. Ennek lényege, hogy a kísérlet során arra vagyunk kíváncsiak, hogy a személyek mennyire képesek dinamikusan eloszlatni figyelmüket, a körülöttük zajló

dolgokat milyen valószínűséggel veszik észre, figyelnek-e a kontextusra, gyanakvásra okot adó dolgokra.[18]

Jelszavak és e-mailek

A célcsoport és a kontrollcsoport tagjainak is fel lett téve két különböző kérdés: mi az e-mail-címük és a számukra ideális jelszó.

Megvizsgáltam, hogy a különböző csoportokban a „Milyen az Ön számára a legideálisabb jelszó? Kérjük, mondjon rá példát!" kérdésre valóban adtak-e konkrét jelszópéldát.

Elmondható, hogy a kontrollcsoport tagjai közül 0%, azaz senki nem mondott konkrét jelszóra példát.

A célcsoportról elmondható, hogy a kitöltők közül több konkrét jelszóra érkező példa érkezett, vagyis a kitöltők több mint 33%-a megválaszolta azt. E kitöltők mindegyike megadta az e-mail-címét is, amely további biztonságtudatossági kérdéseket vethet fel a megadott ideális jelszópéldával együttesen.

Jelszóemlékeztető és e-mailek

A célcsoport körében szerepelt egy kérdés, amely arra vonatkozott, hogy rendelkeznek-e a kitöltők jogosítvánnyal, autóval, illetve ehhez kapcsolódóan arra, hogy milyen autón tanultak vezetni – mint egy tetszőlegesen választott tipikus jelszóemlékeztető kérdés.

Elmondható, hogy az összes kitöltő közül, aki rendelkezett jogosítvánnyal, mindenki válaszolt erre a kérdésre, és közülük mindenki megadta az e-mail-címét is kivétel nélkül, mikor pedig fel lett téve a kérdés, hogy asszociáltak-e a jelszóemlékeztetőre, arra senki nem válaszolt igennel. A kérdés feltevését követően viszont többen megerősítették, hogy találkoztak már ezzel a jelszóemlékeztető kérdéssel, és volt, hogy alkalmazták.

Hozzájárulás az adatvédelmi nyilatkozathoz

Ahogy korábban részleteztem, az adatvédelmi nyilatkozat nem a jogszabályi előírásoknak megfelelően volt megfogalmazva, és a két csoport között a nyilatkozat kapcsán alapvető különbség volt, hogy a célcsoportnak jóval szabadabban volt megfogalmazva az, több utaló jelet tartalmazva.

A célcsoportról ennek ellenére elmondható, hogy azok aránya, akik észrevették a hamis nyilatkozatot, mindössze a kitöltők 12%-át tette ki, két kitöltő viszont ennek ellenére is hozzájárult az adatai kezeléséhez, hogy a nyereményjátékon részt vehessen. Mivel mások nem olvasták el az adatvédelmi nyilatkozatot, így nincsenek arra vonatkozó információim, hogy elolvasás után is aláírták volna-e azt.

A kontrollcsoportról a hozzájárulás kapcsán elmondható, hogy a kitöltők mindössze 9%-a tagadta meg az adatvédelmi nyilatkozat aláírását, amely kevesebb a célcsoport eredményénél, viszont közülük három személy olvasta el az adatvédelmi nyilatkozatot, ami arányaiban nagyobb a célcsoport teljesítményénél. Elolvasás melletti aláírásra itt nem került sor.

[18] Matthew L. Jensen et al.: Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems,* 34. (2017), 2. 597–626.

3.2.2. Leíró statisztikák és attitűd

A leíró statisztikák által megállapíthatjuk, hogy a szenzitív adatok megadásának megtagadásában a kontrollcsoport jobban szerepelt. Személyigazolvány-számuk és lakcímük megadását 20%-kal nagyobb valószínűséggel tagadták meg, mint a célcsoport tagjai.

Ahogy az előző alfejezetben leírtam, a hozzájáruló nyilatkozatot arányaiban többen tagadták meg a célcsoport tagjai közül, viszont számukra több utaló jel állt rendelkezésre, valamint a mérleg nyelvét kiegyenlíti továbbá, hogy a kontrollcsoport tagjai közül arányaiban többen olvasták el a nyilatkozatot, illetve nem került sor a nyilatkozat elolvasását követő aláírásra, amely két esetben a célcsoportra jellemző volt.

Összességében tehát elmondható, hogy sem a célcsoport, sem a kontrollcsoport nem nyújtott kiemelkedő teljesítményt az információbiztonság terén, viszont levonhatjuk azt a konzekvenciát, hogy a kontrollcsoport attitűdjét vizsgálva jóval nehezebb a social engineer tevékenysége. Emellett fontos kiemelnünk, hogy nem adnak olyan nagymértékben visszaélési lehetőséget vagy kihasználható humánalapú sérülékenységet a támadóknak az elvégzett értékelések alapján, mint laikus társaik, ami a személyes kommunikáció során volt tapasztalható.

Ezen a ponton a H2. hipotézisemet alátámasztottam. Igazoltam, hogy az információbiztonsági szempontból laikus emberek legalább kétszer nagyobb valószínűséggel adják meg személyes adataikat, mint az információbiztonság iránt érdeklődő személyek.

A H3. hipotézisem az éberségen alapuló teszt elemzése során megdőlt, ugyanis az információbiztonság iránt érdeklődő személyek nagyobb valószínűséggel írják alá az adatvédelmi nyilatkozatot, mint az információbiztonság tekintetében laikus emberek, noha az utóbbi csoportba tartozók kisebb valószínűséggel is olvassák el annak tartalmát. (A hipotézisek értékelésekor természetesen nem hivatkozhatok a kommunikációra és az adatok kinyerésének nehézségére, amely a mérleget az érdeklődők felé döntené.)

3.2.3. A támadási kísérlet modellje

A korábban elméleti jelleggel bemutatott social engineering támadási modell gyakorlati megvalósítása az alábbiak szerint történt:

A célcsoporton, illetve a kontrollcsoporton is egyaránt direkt, kétirányú kommunikációs modellt alkalmaztunk.

A támadáshoz a social engineernek meg kell határoznia mindezek mellett a célpontot, a közeget, az elérendő célt, valamint a manipuláció alapját és a technikákat, emellett el kell döntenie, hogy a támadás több lépcsőfokon keresztül valósuljon-e meg.

Mind a két empirikus kutatásról elmondható, hogy:

- a social engineer személy;
- a célpont személy;
- a manipuláció alapját adja:
  - szimpátia: a rendezvények hangulata, a nyereményjáték és a személyes attitűd által;

  - elkötelezettség vagy következetesség: a nyereményjátékon való részvétel feltételeként volt szükséges megadni a kért adatokat, amelyek kompenzációja a nyeremény;
  - viszonosság/kölcsönösség: mind a két esetben átadtak kis értékű ajándékokat a rendezvényről, illetve a statisztikai felmérés eredménye lehetett a sorsoláson való részvétel;
- hatóság: részben beszélhetünk erről az empirikus kutatással kapcsolatban. Elmondható, hogy a kitöltők minden esetben azt hihették, hogy a szervezők által finanszírozott alkalmazottak vagy önkéntesek vagyunk az esemény javítását szolgáló feladatlapok kitöltésének tekintetében;
- technika szempontjából adathalászatról beszélhetünk. Megvalósult egyrészt az úgynevezett pretexting (ürügy, amely alapul szolgál a támadó számára értékes információk kiadásának igénylésére, ezúttal a személyes adatok elkérésére az áldozattól annak érdekében, hogy a sorsoláson be lehessen azonosítani). Másrészt beszélhetünk baitingről („beetetésről", vagyis hamis ígéretekkel lettek az emberek becsapva, az áldozatok mohóságát vagy kíváncsiságát kihasználva);
- cél a személyes adatok megszerzése és a hozzájáruló nyilatkozatnak az áldozat által történő aláírása volt;
- a közeg a személyes kapcsolatfelvétel volt;
- a támadás egy lépcsőfokban valósult meg.

3.3. Az empirikus kutatások elemzése

A kutatás elemzésének gerincét a két rendezvényen azonos módon felvett adatok összehasonlítása adja. Idetartozik a biztonságtudatossággal kapcsolatos önpercepció, az adatvédelmi nyilatkozathoz való hozzájárulás, illetve a személyes adatok megadása (személyigazolvány-szám, lakcím).

A leíró statisztikák alapján elmondható, hogy a célcsoport tagjai rosszabb eredményeket értek el a kontrollcsoportban szereplő társaikhoz képest. Amennyiben a szenzitív adatnak számító lakhelyet vagy személyigazolvány-számot tekintjük, úgy deklarálhatjuk a tényt, hogy a téma iránt érdeklődők jobban teljesítettek laikus társaiknál.

A kereszttábla-elemzés eredményeképpen a Khí-négyzet próba elemzésével szignifikáns összefüggéseket kutattam, majd amennyiben találtam összefüggést, a Cramer's V együttható vizsgálatának tekintetében, az asszociációs mérőszám által meghatároztam az összefüggés mértékét. Ezek gyakorlati magyarázatát és jelentőségét az első eredmény elemzésénél adom meg.

Kutatási célkitűzéseim tekintetében vizsgáltam azt, hogy az adott rendezvényen való részvétel összefüggésben van-e azzal, hogy az egyének milyen gyakorisággal adnak meg magukról információt.

Eredményként a rendezvényen történő megjelenés és a személyazonosító igazolvány megadására való hajlandóság között szignifikáns összefüggést véltem felfedezni. Khí-négyzetének (X^2) megfigyelt értéke 5,921, ahol a kétoldali szignifikanciaszintjének értéke 0,015, tehát megállapítom, hogy a két változó között az összefüggés

szignifikáns. A kapcsolat erősségét Cramer's V (C V) segítségével vizsgáltam, ugyanis ez tekinthető az egyik legmegbízhatóbb mutatónak. A C V egy asszociációs együttható, amely a két nominális változó közötti szorosságot mutatja meg. A C V értéke 0 és 1 közötti intervallumú, a 0-hoz való közelség függetlenséget, az 1-hez való közelség erős kapcsolatot jelent. Vizsgálatomban a Cramer's V mutató megfigyelt értke 0,214, kétoldali szignifikanciaszintjének értéke szintén 0,015. A 0,214-es érték azonban alacsony korrelációra utal a két változó esetében.

A rendezvényen történt megjelenés és a hozzájáruló nyilatkozat összefüggésében elmondhatom, hogy X^2 megfigyelt értéke 0,308, amelynek kétoldali szignifikanciaszintjének értéke 0,579, tehát megállapíthatom, hogy a két változó között nincs szignifikáns összefüggés.

A rendezvényen történt megjelenés és a lakhely megadása összefüggésében elmondhatom, hogy X^2 megfigyelt értéke 6,926, ennél a kétoldali szignifikanciaszintjének értéke 0,008, tehát megállapíthatom, hogy a két változó között az összefüggés szignifikáns. Vizsgálatomban a C V mutató megfigyelt értéke 0,236, kétoldali szignifikanciaszintjének értéke szintén 0,008. A 0,236-os érték azonban alacsony korrelációra utal a két változó esetében.

Ezen a ponton eredményeimmel szintén megerősítettem a H2. hipotézisemet, ugyanis elmondhatom, hogy a kontrollcsoport tagjai között jóval nagyobb az információbiztonság szintje, hiszen szenzitív (személyazonosító szám, lakhely) adataik kiadását jóval nagyobb mértékben tagadják meg.

Az információbiztonsági tudatosságról alkotott önpercepció mindkét eseményen történő vizsgálata és az adatvédelmi nyilatkozat aláírásának összefüggésében elmondhatom, hogy a X^2 megfigyelt értéke 2,909, amelynek kétoldali szignifikanciaszintjének értéke 0,088, tehát megállapíthatom, hogy a két változó között nincs szignifikáns összefüggés.

Ezen a ponton bizonyítottam a H1. hipotézisemet, vagyis azt, hogy az információbiztonsági tudatosságról alkotott önpercepció nem párosul valós biztonságtudatossággal kapcsolatos viselkedéssel.

4. A kutatás eredményei

A megfogalmazott hipotéziseimmel kapcsolatban az alábbi téziseket állapítom meg:

T1. Bizonyítottam, hogy a laikusok és az információbiztonság iránt érdeklődő személyek, bár biztonságtudatosnak gondolják magukat, a cselekedeteik alapján ez az önpercepció nem helytálló.

T2. Igazoltam, hogy az információbiztonsági szempontból laikus emberek legalább kétszer nagyobb valószínűséggel adják meg személyes adataikat, mint az információbiztonság iránt érdeklődő személyek.

T3. Bizonyítottam, hogy az információbiztonság tekintetében laikus személyek nagyobb valószínűséggel tagadják meg az adatvédelmi nyilatkozat aláírását, még akkor is, ha kisebb valószínűséggel is olvassák el annak tartalmát, ezzel megdöntve H3. hipotézisemet.

5. Összegzett következtetések

Kutatásom fontosságát az exponenciálisan növekvő, egyre fejlettebb humánalapú támadások adják, amelyek az államigazgatási szektor tisztségviselőire és a hivatásos szervek munkatársaira fokozottan érvényesek. A kutatás célja ezáltal az volt, hogy megállapítsam, a biztonságtudatosság növelhető-e az érdeklődés, a problémacentrikus, személyes érintettségen alapuló példák és kísérletek elvégzése által. Fontosnak találtam továbbá a támadási modellek, stratégiák, keretrendszerek és a felismerési lehetőségek ismertetését a védelmi képességek javítása érdekében.

Összegezve a két empirikus kutatást megállapítom, hogy az adat- és információbiztonság-tudatosság, valamint a kiberbiztonsággal kapcsolatos képességek növelhetők az érdeklődés megteremtését követően, ezzel elősegítve az esetleges sajátos, autodidakta elsajátításra történő buzdítást, vagy még jobb esetben az aktív oktatásban történő önkéntes fejlesztést.

Az empirikus kutatások kapcsán megállapítom, hogy az információbiztonság iránt érdeklődők az adataik védelmében sokkal tudatosabbak voltak. A célcsoportról pedig: a biztonságtudatosság optimumának tekinthető szintet nem érte el. A szubjektív, személyes tapasztalat és a leírt kutatási eredmények, valamint a személyek attitűdjének tekintetében elmondható, hogy a kontrollcsoport nagyságrendekkel biztonságtudatosabb.

Végső következtetésként megállapítom, hogy a biztonságtudatosság iránti érdeklődés megjelenésével párhuzamosan növelhetők az egyének képességei is.

Felhasznált irodalom

Abawajy, Jemal: User Preference of Cyber Security Awareness Delivery Methods. *Behaviour and Information Technology,* 33. (2014), 3. 237–248. Online: https://doi.org/10.1080/0144929X.2012.708787

Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1974/1259

Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. (2016), 1. 61–81. Online: http://real.mtak.hu/47801/1/A_kozossegi_media_szerepe_a_lelektani_mu.pdf

Bányász Péter: Social engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1511/829

Hadnagy, Christopher: *Social Engineering: The Art of Human Hacking.* John Wiley & Sons, 2010.

Bányász Péter – Bóta Bettina – Csaba Zágon: A Social Engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37. Online: https://doi.org/10.37372/mrttvpt.2019.1.1

Farkas, Tibor: Communication and Information Services – NATO Requirements, Part I. *Land Forces Academy Review,* 25. (2020), 4. 281–289. Online: https://doi.org/10.2478/raft-2020-0034

Farkas, Tibor: Communication and Information Services – NATO Requirements, Part II. *Land Forces Academy Review,* 26. (2021), 1. 9–15. Online: https://doi.org/10.2478/raft-2021-0002

Farkas, Tibor – András Tóth: Electronic warfare in full spectrum operation. In Milos Sotak – Mikulas Sostronek – Roman Beresik (szerk.): *Proceedings of the International Scientific Conference: New Trends in Signal Processing.* 2012. 181–188.

Furnell, S. M. – P. Bryant – A. D. Phippen: Assessing the Security Perceptions of Personal Internet Users. *Computers & Security,* 26. (2007), 5. 410–417. Online: https://doi.org/10.1016/j.cose.2007.03.001

Jemal Abawajy – Tai-hoon Kim: Performance Analysis of Cyber Security Awareness Delivery Methods. In Tai-hoon Kim – Wai-chi Fang – Muhammad Khurram Khan – Kirk P. Arnett – Heau-jo Kang – Dominik Ślęzak (szerk.): *Security Technology, Disaster Recovery and Business Continuity.* Berlin, Heidelberg, Springer, 2010. 142–148. Online: https://doi.org/10.1007/978-3-642-17610-4_16

Jensen, Matthew L. – Michael Dinger – Ryan T. Wright – Jason Bennett Thatcher: Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems,* 34. (2017), 2. 597–626. Online: https://doi.org/10.1080/07421222.2017.1334499

Krombholz, Katharina – Heidelinde Hobel – Markus Huber – Edgar Weippl: Advanced Social Engineering Attacks. *Journal of Information Security and Applications,* 22. (2015), 113–122. Online: https://doi.org/10.1016/j.jisa.2014.09.005

Lehto, Martti: Cyber Security Competencies – Cyber Security Education and Research in Finnish Universities. In Nasser Abouzakhar (szerk.): *14th European Conference on Information Warfare and Security, 2015.* Hatfield, The University of Hertfordshire, 2015. 179–188.

Mitnick, Kevin D. – William L. Simon: *The Art of Deception: Controlling the Human Element of Security.* John Wiley & Sons, 2003.

Mitnick, Kevin – William L. Simon: *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker.* Illustrated edition. New York, Back Bay Books, 2012.

Mouton, Francois – Louise Leenen – H.S. Venter: Social Engineering Attack Examples, Templates and Scenarios. *Computers and Security,* 59. (2016), 186–209. Online: https://doi.org/10.1016/j.cose.2016.03.004

Shaw, R. S. – Charlie C. Chen – Albert L. Harris – Hui-Jou Huang: The Impact of Information Richness on Information Security Awareness Training Effectiveness. *Computers & Education,* 52. 1. (2009), 92–100. Online: https://doi.org/10.1016/j.compedu.2008.06.011

Szádeczky, Tamás: Governmental Regulation of Cybersecurity in the EU and Hungary after 2000. *AARMS,* 19. (2020), 1. 83–93. Online: https://doi.org/10.32565/aarms.2020.1.7

Tóth András: *International information security in hungary.* In Ivan Majchút – Vladimír Andrassy – Štefan Ganoczy – Michal Hrnčiar – Ondrej Kredatus – Gabriela Kredatusová – Jakub Sasarák – Juraj Šimko – Jaroslav Varecha – Lubomír Belan – Stanislav

Morong (szerk.): *8. medzinárodná vedecká konferencia: National and International Security 2017.* Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2017. 548–557.

Tóth András: Information-Sharing Challenges and Issues in Multinational Operations. *Land Forces Academy Review,* 25. (2020), 4. 307–316. Online: https://doi.org/10.2478/raft-2020-0037

HADMÉRNÖK
VÉDELEMINFORMATIKA
16. évfolyam (2021) 3. szám 189–202.
DOI: 10.32567/hm.2021.3.11

Hankó Viktória[1]

A drónokkal kapcsolatos kockázatok és kezelési lehetőségeik[2]

Risks and their Treatment Options Associated with Drones

A pilóta nélküli légijárművek, vagy rövidebb néven drónok számának növekedésével a technológiával kapcsolatos kérdések száma is arányosan növekedett az utóbbi időben. A tanulmány a kockázatok kérdéskörét dolgozza fel. Elsősorban szükséges a technológia szempontjából releváns veszélyek definiálása. A felmerülő kockázatok tekintetében a személyiségi jogok megsértése, illetve a birtokháborítás és a károkozás tényállása jelenik meg. Ezt követően megjelenik az alkalmazott módszertan, a Preliminary Hazard Analysis (PHA), vagyis az előzetes veszély- és kockázatelemzés, valamint annak elemeinek bemutatása. Jelen esetben ez egy esettanulmányon keresztül elvégzett kockázatelemzést foglal magába. Kifejezetten hangsúlyos egy esetleges incidensben rejlő baleseti és adatvédelmi faktorok bemutatása. Mindemellett megjelennek a kockázatok kezelésének lehetőségei, kifejezetten a felelősségbiztosítás intézménye – hazai szinten összehasonlítva a különböző ajánlatokat. Kitekintésként a SORA módszer kerül bemutatásra.

Kulcsszavak: drón, kockázatelemzés, kockázatkezelés

By the increasing level in number of unmanned aerial vehicles, or drones for short, the number of technology-related issues has also increased proportionately recently. The study addresses the issue of risks. In particular, it is necessary to define technology-relevant hazards. With regard to the risks that arise, the violation of privacy rights and the facts of trespassing and damaging are revealed. This is followed by the methodology used, the Preliminary Hazard Analysis (PHA), and a presentation of its elements. In the present case, it involves a risk analysis carried out through a case study. The presentation of the accident and data protection factors inherent in a possible incident is particularly emphasized. In addition, the possibilities of risk management appear, specifically the institution of liability insurance – comparing different offers at the domestic level. The SORA method is presented as an overview.

[1] Nemzeti Közszolgálati Egyetem, hallgató, e-mail: hanko.viktoria@hallg.uni-nke.hu
[2] A tanulmány az Innovációs és Technológiai Minisztérium ÚNKP-20-1-I-NKE-75 kódszámú Új Nemzeti Kiválósági Programjának szakmai támogatásával készült.

Keywords: **drone, risk assessment, risk management**

1. Bevezetés

A modern technika világában az okoseszközök mellett a mindennapjaink részei a pilóta nélküli légi járművek, azaz drónok. Ezeknek az eszközöknek számos pozitív hozadéka van, azonban különböző veszélyekkel is találkozhatunk a használatuk közben. A kutatásom célja, hogy rávilágítsak a drónok használata során felmerülő kockázatok azonosítására – különös tekintettel az adatvédelmi kockázatokra –, valamint, hogy feltárjam az ezek csökkentésére irányuló lehetséges megoldásokat. Azonban ezek bemutatásához szükség van bizonyos szintű fogalmi áttekintésre. Mindenekelőtt szükséges a pilóta nélküli légi járművek új, törvényi kategóriáinak ismertetése, mint amelyek a későbbiekben fontos elemként jelennek majd meg. 2020 decemberében a Parlament elfogadta a légiközlekedésről szóló 1995. évi törvény módosítását, amely kiegészült a drónhasználattal kapcsolatos alapfogalmakkal és alapszabályokkal. Kategóriák tekintetében – az EU-s szabályozáshoz hasonlóan – a hazai törvényi keret nyílt, speciális és engedélyköteles megnevezéssel illeti őket. A nyílt kategória várhatóan a hobbi jellegű és ipari felhasználókat fogja felölelni. Különböző alapkövetelmények vonatkoznak a felhasználókra, mint például, hogy a pilóta segédeszköz nélkül is lássa az eszközt, illetve, hogy a légi jármű legfeljebb 120 méterre távolodhat el a föld legközelebbi pontjától. Ezen belül A1, A2, A3 alkategóriák jelennek meg. Speciális kategóriába tartozik az eszköz, ha 25 kg-nál nehezebb, vagy olyan műveletet hajt vele végre a pilóta, amelynek ideje alatt nem látható a drón. Emellett bejelentés vagy engedély beszerzése szükséges attól függően, hogy milyen műveletet hajtanak végre. További feltétel, hogy az üzemben tartó – minden esetben – elvégezzen egy kockázatelemzést, amelyhez egy szakértő bevonása javasolt. Végül pedig az engedélyköteles kategóriába tartozó légi járművel mikor lehetséges embertömeg fölött repülni (például ha áru vagy személyszállítás valósul meg a drón segítségével, vagy egy fesztivál során). Ehhez a tevékenységhez viszont sokkal mélyebb elméleti és gyakorlati ismeretek, valamint a pilóta nélküli légi jármű működtetéséhez egyedi eljárások kidolgozása szükséges.[3] A pandémia idején a pilóta nélküli légi járművek alkalmazása a járvány terjedésének felügyeletére is kiterjedt. Nyilvános videórendszerek (kamerák, drónok, robotok) arcfelismerő rendszerrel kiegészülve, illetve műholdak vagy drónok által végzett globális megfigyelések szolgáltathatnak adatokat az ország vezetői számára az állampolgárok mozgásáról, tartózkodási helyéről és egészségi állapotáról, hogy segítsenek felmérni a vírus terjedésének megfékezésére tett intézkedések hatását, és referenciapontokat nyújtsanak további intézkedésekhez.[4]

[3] Drón törvény 2021 – érthetően szakértőktől. *Légtér.hu,* 2021. február 8.

[4] Attila Németh – Sándor Magyar: An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application. *Szakmai Szemle,* 6. (2020), 2. 52–65.

2. Elméleti összefüggések

Az első gondolat, amely többekben felmerül a drónokkal kapcsolatban, hogy megfigyelésre használják ezeket az eszközöket, amelyek sértik a polgárok magánéletét, privát szféráját. A magánszféra a magánéletet, személyes életet jelenti, azaz a nyilvánosságra, a közösségre vagy bárki másra nem tartozó dolgokat, ilyen például valakinek a családi élete. Gyakran privát szféra néven is szoktak rá hivatkozni. Jogi értelemben a magánszférához való jog részei a következők: a névviseléshez, a személyes adatokhoz, a magántitokhoz és a jó hírnév védelméhez, valamint a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához való jog. Ezáltal az, hogy otthon milyen weboldalakat néz valaki, a magánszférája része.[5] A drónok felhasználásával kapcsolatban három jogsértő magatartás különböztethető meg, amelyek a következők:

Személyiségi jogok megsértése és üzletititok-sértés:
A drónok könnyedén be tudnak hatolni a nyilvánosság elől elzárt területek fölé, ahol felvételeket készíthetnek, illetve továbbíthatnak, ezáltal veszélyeztethetik mások privát szféráját. Egy adott drón használata közben könnyen sérülhet valakinek a képmáshoz való joga, valamint feltárulhatnak egyéb, másokra nem tartozó titkai. Ebben az esetben a jogellenes magatartás eredménye elsődlegesen a személyiségi sérelem, azonban komoly vagyoni kárt jelenthet egy üzleti titok kifigyelése is. Ezen ügyek kapcsán nem közvetlenül a drón jelenti a veszélyt, hanem az, hogy az eszközben rejlő műszaki lehetőségeket oly módon használják ki, hogy az sérti mások személyiségi jogait, vagy üzleti titkait. Mindemellett illegális adatgyűjtésre is használhatók ezek a technikai eszközök. A jogellenes működtetés mögött általánosságban szándékos és célzatos magatartás áll, azonban a káresemény egy jogszerű, ámde gondatlan magatartás következménye is lehet. Ebben az esetben az eszköz működtetője nem akar jogsértést elkövetni, de a nem kellően körültekintő magatartása jogsértéshez vezet, például amikor az eladásra kínált lakásról készített felvétel során az ingatlanközvetítő a szomszédos ingatlanok lakóinak tevékenységét is dokumentálja.

Birtokháborítás:
A birtokháborítás akkor valósul meg, amikor a drón más terület fölé behatol. Ez azonban nem feltétlenül szándékos jogsértés, hiszen nem minden esetben tudhatja az eszközt irányító személy, hogy hol húzódnak az ingatlan határai, amelyek nincsenek kerítéssel jelölve.

Károkozás:
A károkozó magatartásokat tekintve a drón ütközhet más légi járművel, épülettel, tereptárggyal, távvezetékkel, emberrel vagy állattal. Fontos megjegyezni, hogy még a kis méretű drónok ütközése alkalmával is olyan nagy energia szabadulhat fel, amely képes akár emberi élet kioltására is, illetve jelentős vagyoni kár okozására. A drónbalesetek csoportosítása kétféleképpen lehetséges: a baleset bekövetkezésének helyszíne, valamint a balesetet okozó hiba oka szerint. Ezek alapján a baleset

[5] Lexiq: Magánszféra szócikk: https://lexiq.hu/maganszfera

bekövetkezésének helyszíne szerint az első csoport az, amikor a drón más repülő tárggyal ütközik, a második csoport a drón lezuhanása vagy nem az eredetileg tervezett leszállás alkalmával más tárggyal vagy személlyel a földön történő ütközése. A balesetet okozó hibák szerinti besorolás alapján beszélhetünk műszaki hibáról, illetve emberi mulasztásról.[6]

A leírtak alapján láthatóvá vált, hogy milyen hatásai lehetnek a drónoknak a privát szférára, valamint az azt érintő jogokra. Ez az alfejezet a kockázatok, kifejezetten a drónok veszélyeinek és kockázatainak bemutatására szolgál. A kockázat, azon belül is az információbiztonsági kockázat magában foglalja azokat a hatásokat, amelyek előfordulhatnak a sebezhetőségek és fenyegetések miatt. Ezeket a szervezet, valamint az érdekelt felek okozhatják az információs rendszerek működtetésével és használatával, valamint idetartozik még az a környezet is, amelyekben ezek a rendszerek működnek.[7] Az információbiztonsági kockázat az esemény valószínűségének és annak következményeinek kombinációja alapján mérhető.[8]

A drón reptetése során különböző kockázati tényezők merülhetnek fel, mint például a jogi szabályozás, illetőleg annak hiánya, vagy a korábbiakban már említett műszaki hiba, vagy akár az emberi tényező. Emellett fontos még megemlíteni a meteorológiai körülményeket is.

A műszaki problémák terén a navigációs rendszerrel kapcsolatos hibára gondolhatunk elsődlegesen. Fontos tudni, hogy a robotpilóta is része lehet a pilóta nélküli légi járművek rendszerének ugyanúgy, mint az ember által vezetett repülőgépek esetében is. Szükség van rá a pontos útvonal tartásához, azonban hibás adatok vagy a navigációs rendszer vételkiesése esetén hiba lehet a döntési folyamatban. Ennek következtében a drón akár le is zuhanhat, megsemmisülhet, vagy kárt okozhat épületekben, szélsőséges esetben az emberi életet is veszélyeztetheti.[9]

Ennek kapcsán felmerül, nem mindegy, hogy ki, hol és milyen szándékkal vezeti az adott pilóta nélküli légi járművet. Az emberi hibalehetőség számos kockázati tényezőt hordoz magában. Bizonyos információk hiányában – legyen szó például a kamera felbontásának elégtelenségéről, vagy az adatátvitel gyengébb sebességéről – a pilóta rossz döntéseket hozhat, ami további veszélyes helyzeteket hordozhat magában. Emellett megemlítendő a meteorológiai ismeretek fontossága is. A szabadtéren történő használat folyamán különböző meteorológiai helyzetek alakulhatnak ki. Ezek nem ismerete akár az eszközünk megsemmisülését is eredményezheti. Ezeknek a légköri viszonyoknak az előrejelzése, megismerése, a repülési terv átdolgozása felelős tervezést igényel, ami a repülési kockázatokat nagymértékben minimalizálhatja, csökkentheti. A jogi, illetve etikai szabályozások tekintetében kockázatot jelenthet a fedélzeti kamerával rögzített videók, képek nem megfelelő adatkezelése, hiszen ezek hanyag vagy szándékos, illetve nem körültekintő

[6] Miskolczi Bodnár Péter: A drónokhoz kötődő aktuális jogalkotási, jogalkalmazási és etikai teendők. In Homicskó Árpád Olivér (szerk.): Egyes modern technológiák etikai, jogi és szabályozási kihívásai. Patrocinium, 2018. 141–142.

[7] Stephen D. Gantz – Daniel R. Philpott: Chapter 3 – Thinking About Risk. In Stephen D. Gantz – Daniel R. Philpott (szerk.): *FISMA and the Risk Management Framework.* Syngress, 2013. 53–78.

[8] Sokratis K. Katsikas: Chapter 53 – Risk Management. In John R. Vacca (szerk.): *Computer and Information Security Handbook (Second Edition).* Morgan Kaufmann, 2013. 905–927.

[9] Wührl Tibor: GPS navigációs problémák UAV alkalmazásokban. *Hadmérnök,* (2006), különszám. 1–7.

felhasználása adatvédelmi törvényeket, személyiségi jogokat is sérthet. Azonban fontos kiemelni, hogy nem ezeknek az eszközöknek a használata jelenti az adatvédelmi problémát, hanem az ezen eszközökre szerelhető kiegészítők által bekövetkező adatkezelés. Továbbá elmondható, hogy az adatkezelő személy könnyen végezhet rejtett megfigyelést, hiszen a drón mérete egészen kicsi is lehet, ami lehetővé teszi a megfigyelést, emellett nehezen vagy egyáltalán nem észlelhető, továbbá gyors, sok esetben észrevétlen helyváltoztatásra is képes.[10] Ebből következik az adatvédelmi kockázat, amely feltételes forgatókönyvként definiálja, hogy a kockázatok forrásai az általános fenyegetettségeket figyelembe véve hogyan, milyen módon tudják a személyes adatokat kiszolgáló infrastruktúra sebezhetőségeit kihasználni annak érdekében, hogy olyan nem kívánt eseményt váltsanak ki, amely személyes adatok jogellenes kezeléséhez vezet és amely hatással van az adatalanyok magánszférájára. A kockázatot két alapvető szempontból érdemes vizsgálni, annak hatása, illetve valószínűsége alapján.[11] Az egyik ilyen kockázat a nem szándékos adatgyűjtés. Egy adott tárgyról, például házról vagy földrészletről a kamerával rendelkező drón által készített felvétel akaratlanul is tartalmazhat más tárgyakat, elemeket, mint például embereket, épületeket vagy a szomszédos földeket. E nem szándékos adatok lehetnek személyes jellegűek vagy nem személyes jellegűek. Ezáltal további kérdések merülnek fel az adatok feldolgozásának módjáról, valamint a tárolásukra és a törlésükre vonatkozóan. Egy másik, ezzel összefüggő kihívás a drónhasználat célja. Ahol a drón által gyűjtött adatok nem feltétlen személyes jellegűek, ott az adatvédelmi keret nem alkalmazandó. Az azonban, hogy nem gyűjtenek személyes adatokat, még nem jelenti azt, hogy a drónt törvényes célra használják. Lehet, hogy egy vállalat egy drónt irányítva megpróbálja kideríteni, milyen új technológiákat vagy eljárásokat használ egy riválisvállalkozás, vagy esetlegesen üzleti titkokba botlik. Egy magánszemély is használhat dróntechnológiát, például annak érdekében, hogy megtudja, hol helyezkednek el a bűnüldöző szervek tisztviselői.[12]

3. Módszertan

A különböző módszerek közül a Preliminary Hazard Analysis (PHA), vagyis az előzetes veszély- és kockázatelemzés technikáját alkalmaztam a kutatásom során. A PHA-t a rendszerek tervezési szakaszában és/vagy projektek során használják, különösen olyan új technológiák alkalmazása esetén, amelyek további információt igényelnek a kockázataikról. Leggyakoribb esetben a kockázatok elemzése még mindig a folyamat tervezési szakaszában történik, így az azonosított kockázatok miatt szükséges változtatások nem jelentenek jelentős költségeket, amellett, hogy a megvalósítás is

[10] Gajdács László – Major Gábor: Az UAV alkalmazásának kockázatai a biztonságtechnika területén. *Repüléstudományi Közlemények,* 30. (2018), 2. 101–112.

[11] Árvai Viktor György et al.: *Az elszámoltathatóság alapelve és az adatkezelői kötelezettségek.* Budapest, Nemzeti Közszolgálati Egyetem, 2018.

[12] Pam Storr – Christine Storr: The Rise and Regulation of Drones: Are We Embracing Minority Report or WALL-E?. In Marcelo Corrales – Mark Fenwick – Nikolaus Forgó (szerk.): *Robotics, AI and the Future of Law. Perspectives in Law, Business and Innovation*. Springer, 2018. 105–122.

könnyebb. Ez a módszer megvizsgálja a kockázatok és folyamatok eltéréseit, amivel célja az okok és következmények kvalitatív megközelítésben történő meghatározása. Ez a kvalitatív megközelítés (okok és következmények) számszerűsíthető egy kockázati mátrixban, annak gyakorisági és súlyossági paramétereit felhasználva. Abból kifolyólag, hogy az eredmények kvalitatívak, nem adnak számszerű becslést. Azonban ezen információk alapján javasolhatók az azonosított veszélyek megelőzése vagy enyhítése érdekében tett intézkedések, közelebbről a különböző elemzett baleseti forgatókönyvek okozta káros hatások kiküszöbölésére vagy csökkentésére. A PHA hatóköre realizálja azokat a veszélyes eseményeket, amelyek okai az elemzett létesítményből, projektből vagy technológiából származnak, felölelve mind az alkatrészek vagy rendszerek meghibásodásait, mind a karbantartási vagy működési hibákat (emberi hibákat).[13]

A PHA-módszer alkalmazásával a kockázatelemzést egy esettanulmányon keresztül mutatom be, amely a Drone Industry Insights (DOII) biztonsági kockázatértékelése alapján készült.[14] Az elemzéshez a következő szimulációt hoztam létre:

„A FoodByDrone nevű cég környezetkímélő stratégiájának elemeként pilóta nélküli légijárművekkel szállítja ki az étel rendeléseket, mely G7 típusú drónokon keresztül valósul meg, melyek teherbírási határa 6 kg. Ez a típusú kiszállítás a korábbi 50-60 perc helyett 20-30 percen belül megérkezik az adott ház elé, vagy igény szerint az erkélyhez, ablakpárkányhoz. Adott egy személy, aki igénybe vette ezt a szolgáltatást. Az ételrendelés teljesítése alatt a drón navigációs rendszere részlegesen meghibásodott, melynek következtében a rendszer helyreállásáig egy másik ingatlan fölött lebegett a drón, rögzítve az ott zajló hétvégi családi rendezvényt. Az érintett család egyik tagja jelentette ezt a cég felé. Annak érdekében, hogy ilyen, vagy ehhez hasonló eset ne történjen meg a vállalat a következő kockázatelemzést hajtja végre."

3.1. Eredmények

A megismert fogalmak és módszertan tisztázása után az esettanulmányon keresztüli kockázatelemzésre és kockázatkezelési lehetőségekre kerül a hangsúly. A fejezetben lépésről lépésre következnek a különböző elemek. Ezt követően a fókuszpontba a felelősségbiztosítás intézménye kerül.

3.2. Kockázatok feltárása

Az esemény kivizsgálásához először egy valószínűségi tábla kidolgozása szükséges, amely a kockázat valószínűségét vagy annak gyakoriságát definiálja, hogy a mekkora eséllyel következhet be az adott kockázat. Minden forgatókönyvet figyelembe kell

[13] Erick Galante – Daniele Bordalo – Marcele Nobrega: Risk Assessment Methodology: Quantitative HazOp. *Journal of Safety Engineering,* 3. (2014), 2. 31–36.

[14] Kay Wackwitz – Hendrik Boedeker: *Safety Risk Assessment for UAV Operation*. Drone Industry Insights, 2016.

venni. A valószínűséget számokkal kell kifejezni, és ezeket a számokat minden valószínűségi szinthez hozzá kell rendelni. Az alábbiakban látható egy általánosan használt ötszintű valószínűségi táblázat:

1. táblázat

Bekövetkezési valószínűség

Forrás: a szerző szerkesztése Wackwitz–Boedeker (2016): i. m. (DOII) alapján

Valószínűség		**Leírás**
5	Nagyon valószínű	A drón rendszere meghibásodik használat közben, és ezzel mások jogait sérti és anyagi kárt is okoz.
4	Valószínű	A drón rendszere meghibásodik használat közben, és ezzel mások jogait sérti vagy anyagi kárt okoz.
3	Lehetséges	A drón rendszere meghibásodik használat közben vagy mások jogait megsérti, vagy anyagi kárt okoz.
2	Valószínűtlen	A drón rendszere nem hibásodik meg használat közben, nem sérti mások jogait és anyagi kárt sem okoz.
1	Kizárt	A fenyegetés nem értelmezhető, vagy a bekövetkezése nem elképzelhető, kizárt.

Emellett szükség van egy, a kockázat súlyosságát bemutató táblázatra is. A biztonsági kockázat súlyosságát a kár mértéke határozza meg, amely előfordulhat az azonosított biztonsági veszély következményeként. A súlyossági értékelés alapulhat sérüléseken (személyeken) és/vagy károkon (drónok és épületek, elektromos vezetékek vagy a költségdimenzió). Ennek az elkészítéséhez figyelembe kell venni a legrosszabb előre látható helyzetet, a súlyosságot számszerűsíthető kritériumok szerint kell kategorizálni, és ezeket a számokat minden valószínűségi szinthez hozzá kell rendelni.

2. táblázat

Bekövetkezés súlyossága

Forrás: a szerző szerkesztése Wackwitz–Boedeker (2016): i. m. (DOII) alapján

	Súlyosság	**Leírás**
E	Katasztrofális	Emberi élet kioltása. Drón, berendezés vagy épület megsemmisülése.
D	Komoly	Komoly személyi sérülés vagy a magánszféra súlyos megsértése, valamint nagyobb kár a berendezésben, épületben.
C	Közepes	Személyi sérülés vagy a magánszféra enyhe megsértése, vagy a további működtetés nem lehetséges nagyobb módosítások nélkül.
B	Minimális	Kisebb személyi incidens, a rendszer teljesítményére gyakorolt kisebb hatás.
A	Elhanyagolható	Nincs személyi sérülés, kisebb rendszeri következmények.

Ebből jön létre a kockázatértékelési mátrix, amely a következőképpen alakul:

3. táblázat

Az esettanulmány kockázatmátrixa

Forrás: a szerző szerkesztése

Kockázat valószínűsége	5	5A	5B	5C	5D	5E
	4	4A	4B	4C	4D	4E
	3	3A	3B	3C	3D	3E
	2	2A	2B	2C	2D	2E
	1	1A	1B	1C	1D	1E
		A	B	C	D	E
		Kockázat súlyossága				

Ez alapján a kockázatelfogadási szintek színkódok szerinti besorolása a következő:

- A vörös a nem elfogadható szint – a következmény valószínűsége/súlyossága elfogadhatatlan. Jelentős enyhítésre vagy újratervezésre van szükség a kockázat következményének, valószínűségének vagy súlyosságának elfogadható szintre való csökkentéséhez.
- A sárga tolerálható, de kockázatcsökkentést igénylő szint – a következmény és/vagy a valószínűség aggodalomra ad okot, intézkedéseket kell végrehajtani a kockázat észszerűen alacsony szintre csökkentéséhez. Ez a kockázat akkor tolerálható, ha megértik és ha szervezeten belül jóváhagyják.
- A zöld az elfogadható szint – a következmény nagyon valószínűtlen, vagy nem elég súlyos ahhoz, hogy aggodalomra adjon okot. A kockázat tolerálható, a biztonsági célkitűzés teljesült.

Ezek alapján a kockázatok azonosítását és kategorizálását a 4. táblázat tartalmazza:

4. táblázat

Az esettanulmány kockázatértékelése

Forrás: a szerző szerkesztése

			Kockázatértékelés			
Kiváltó ok	**Kiváltó ok kategóriája**	**Lehetséges következmény**	**Valószínűség**	**Súlyosság**	**Mátrix-kód**	**Kockázati szint**
Navigációs rendszer meghibásodása	Műszaki	Drón megsemmisülése, emberi sérülés	Lehetséges	Közepes	3C	Tolerálható
Hozzájárulás nélküli adatrögzítés	Adatvédelmi	Magánszféra megsértése	Valószínű	Komoly	4D	Nem elfogadható

A folyamat zárásaként a kockázatot enyhítő intézkedéseket kell foganatosítani, amelyek két fajtája a korrekciós, illetve a megelőző intézkedések. Mindegyik intézkedésformához hozzá kell rendelni egy felelős személyt a megfelelő végrehajtás érdekében.

5. táblázat
Az esettanulmány kockázatenyhítő intézkedései
Forrás: a szerző szerkesztése

			Kockázatértékelés			
Kiváltó ok	**Kiváltó ok kategóriája**	**Lehetséges következmény**	**Valószínűség**	**Súlyosság**	**Mátrix-kód**	**Kockázati szint**
Navigációs rendszer meghibásodása	3C	Tolerálható	Manuális beavatkozás távolról	Rendelést irányító személy	Eszköz gyakori tesztelése	Minőségügyi mérnök
Hozzájárulás nélküli adatrögzítés	4D	Nem elfogadható	Kamera manuális kikapcsolása a leállás idejére	Rendelést irányító személy	Közterületeket[15] érintő útvonal kialakítása	Informatikai vezető

3.3. Kockázatkezelés lehetőségei

Az előző alfejezetet végén látható kockázatértékelési intézkedések esetében a kockázatértékelő dátumot rendel a korrekciós és megelőző intézkedések megvalósításához, hogy egyfajta minőségi kaput illesszen be a kockázatértékelésbe. Ez az eljárás kockázatkezelés néven ismert. A kockázatkezeléshez dokumentált kockázatértékelésre, a becsült kockázatok rendszeres felülvizsgálatára és az intézkedések hatékonyságának ellenőrzésére van szükség. A kockázatértékelő egy drónbiztonsági kockázati térképet használ, amelyben leírja az összes drón repülési veszélyét, beleértve a vonatkozó kockázatértékelési eredményeket is. Ezt a térképet – beleértve a meghatározott kockázati mutatót is – minden hónapban bemutatja a vezérigazgatónak, akinek szüksége van erre az információra a stratégiai értekezletekhez.[16]

Az esettanulmányt figyelmen kívül hagyva is elmondható, hogy ahogyan nő a pilóta nélküli légi járművek vagy pilóta nélküli légi rendszerek alkalmazása, úgy nőnek a magánélet és a biztonság aggályai is. Ennek eredményeként a kockázatkezelés és a kockázatok elleni biztosítás döntő fontosságú lesz mind a gyártók, mind pedig az üzemeltetők szempontjából. Magyarországon jelenleg is szigorú szabályozások vonatkoznak a drónok reptetésére, legyen szó akár az üzleti, akár a hobbi szintű felhasználókról. Mindkét esetben feltétel az eszköz regisztrálása, a légtérhasználati engedély, valamint a drónra kötött felelősségbiztosítás megléte, amennyiben a légi jármű súlya meghaladja a 0,25 kg-ot. Emellett abban az esetben is szükséges, ha nem minősül játéknak és/vagy adatrögzítővel rendelkezik. A pilóta nélküli légi járművek felelősségbiztosítását úgy kell elképzelni, mint a kötelező járműbiztosítást – ebben az esetben is az üzemben tartó felelős az eszközhöz kapcsolódó biztosítás megkötéséért.

[15] Szerzői megjegyzés: ideértendők a közintézmények is, amennyiben azok érintése nem jelent nemzetbiztonsági kockázatot.
[16] Kay Wackwitz – Hendrik Boedeker: *Safety Risk Assessment for UAV Operation*. Drone Industry Insights, 2016.

Az új szabályozás miatt a Groupama Biztosító is újrafogalmazta a felelősségbiztosítás szabályait. A szolgáltatást 30 napra vagy határozatlan időre lehet megkötni. A határozatlan idő egy évet foglal magában, amelyet természetesen fel lehet mondani az évforduló előtt 30 nappal. A havidíjat nem szükséges lemondani, automatikusan megszűnik. Jelenleg azonban cég nevében vagy gazdasági célú reptetés okán nem lehet biztosítást kötni. A biztosítási termékismertetőből értesülhetünk arról, hogy a cég megtéríti a pilóta nélküli légijármű-rendszerrel okozott dologi és személysérüléses károkat, illetve az eseménnyel kapcsolatban az élet, a testi épség, valamint az egészséghez való személyiségi jog megsértése alapján felmerülő sérelemdíjat is. Kiemelendő azonban, hogy a személyiségi jogsértéssel kapcsolatos károk mellett az autonóm üzemmódban okozott károkat sem téríti meg a társaság.[17]

A Groupama mellett az Allianz Hungária Zrt.-nél is van lehetőség felelősségbiztosítást kötni. Biztosítási eseménynek minősül az az esemény, amely a légi jármű jogszerű működtetése során az eszköz, illetve az abból kieső tárgy harmadik fél részére (aki nem vesz részt a repülésben) okozott kár és/vagy személyi sérüléssel összefüggő nem vagyoni sérelem, amelyért a pilóta felelősséggel tartozik abban az esetben, ha az esemény nem kizárt kockázat. Kizárt kárnak minősül például a 16 évesnél fiatalabb pilóta által okozott kár, a formációs repüléssel összefüggésben okozott kár, valamint a napkelte előtti/utáni időpontban történt esemény. A szolgáltatás alanya a regisztrált üzemben tartó, illetve az általa megnevezett távpilóta, azaz a pilóta nélküli légi jármű vezetője. A biztosítás időtartamát tekintve lehetőség van határozatlan időre megkötni, illetve határozott időre is, amely lehet 1 év vagy egy konkrét tevékenység végzésének az ideje (naptári nap szerint meghatározva).[18]

A korábbiakban említett két cégen felül a Generali is rendelkezik a MyDrone elnevezésű felelősségbiztosítással, amely jogvédelmi biztosítást is magában foglal. A biztosítási feltételekben meghatározottak alapján biztosítási eseménynek minősül a szerződő (azaz az üzemben tartó) által működtetett pilóta nélküli légi jármű vagy az abból kieső tárgy okozta személyi sérüléses kár, illetve a szerződésen kívül okozott dologi károk miatti kártérítési kötelezettség, amely a szerződésben megjelölt, jogszabály által előírt nyilvántartásba vett pilóta nélküli légi jármű használata során következett be, s amelyért a biztosított jogszabály szerint helytállni köteles. A felelősségbiztosítás jogvédelmi kiegészítése alapján biztosítási eseménynek minősül továbbá az a magatartás is, amely más személy személyiségi jogát sérti, ezáltal az üzemben tartó sérelemdíj megfizetésére kötelezhető, amennyiben a személyiségi jog megsértése olyan személyi sérüléses vagy szerződésen kívüli dologi kárt okozó magatartással áll közvetlen összefüggésben, amelyért a biztosítottat kártérítési felelősség terheli. A MyDrone biztosítás nem terjed ki a pilóta nélküli állami légi járművekkel végzett UAS-műveletek végzése során, illetve állami szerv feladatának megvalósítása érdekében végrehajtott UAS-műveletek teljesítése során okozott károkra. A társaságnál a szerződés időtartama alapjáraton határozatlan idejű, amennyiben a szerződő felek erről másképp nem rendelkeznek. Határozott idejű szerződés esetén pedig a meghatározott időtartam érvényes.[19]

[17] Groupama felelősségbiztosítás drónokra és repülőmodellekre: www.groupama.hu/hu/Biztositasok/dron-felelossegbiztositas.html

[18] Allianz Hungária Zrt.: Légi- és vízi járművek vagyonbiztosítása, drónok felelősségbiztosítása. (é. n.).

[19] Generali Drónbiztosítás: www.generali.hu/Biztositas/Jarmu/generali-mydrone-biztositas.aspx

A feltételek ismertetése után világossá válik, hogy a műveletek végrehajtásához felelősségbiztosítással kell rendelkeznie a pilótának. Ennek összege azonban nagyban függ az adott biztosítótól, és a drón tömegétől is. 250 g alatti eszköz nem kereskedelmi használatához nem szükséges biztosítást kötni, azonban az ennél nehezebb drónokra mindenképpen – kereskedelmi tevékenység végzése esetén a 785/2004/EK rendeletnek kell megfelelni. Azonban fontos tudni a fedezeti összeghatárokat is, amelyek áttekintését a következő táblázat tartalmazza:[20]

6. táblázat
Kártérítési limitek
Forrás: a szerző szerkesztése

Súly	**Eseményenként**	**Időszakonként**
0,25 kg alatt	nem szükséges	
4 kg alatt	3 000 000 Ft	6 000 000 Ft
4 kg – 20 kg	5 000 000 Ft	10 000 000 Ft
20 kg fölött	egyedi ajánlat	

A hazai felelősségbiztosítás intézménye mellett érdemes lehet nemzetközi szintre kitekinteni. A magyarországi gyakorlattal szemben például az amerikai gyakorlat egy kicsit másképpen alakul a felelősségbiztosítás tekintetében. 2020 februárjában a Szövetségi Légi Irányítás (*Federal Aviation Administration,* FAA) kiadott egy Javasolt Szabályalkotási Értesítést (*Notice of Proposed Rulemaking,* NPRM) a drónokról. Úgy tűnik, hogy ez egy kulcsfontosságú pillanat volt azoknak a vállalatoknak és szervezeteknek, amelyek használják a technológiát, hiszen megfigyelhető, hogy növekszik a kereskedelmi drónműveletek biztosításával kapcsolatos megkeresések száma a Global Aerospace cégnél. Az Amerikai Egyesült Államokban a drónok biztosítók által megvizsgált egyik elsődleges kockázatkezelési eszköze a képzés. A felmerülő veszélyek hatékony feltérképezése nélkül az üzemeltetők nem tudják optimálisan és biztonságosan működtetni az eszközüket. Az NPRM jelezte, hogy az üzemeltetőknek repülésbiztonsági vizsgát kell teljesíteniük. Valószínűsíthetően ez magában foglalja a repülési térképek, a meteorológia, az aerodinamika megértésének bizonyítását. Mint minden repülőgép-üzemeltetésnél, a biztosítás is a kockázatkezelés szerves része. Ez pénzügyi kompenzáció arra az esetre, ha a biztonsági irányítási rendszer nem képes megelőzni a balesetet, vagy ha egy előre nem látható esemény miatt veszteség keletkezett. Míg a szabályozási helyzet folyamatosan változik, a biztosítás tárgya egyre fontosabb a drónt használó közösségen belül. A tulajdonosokat és üzemeltetőket, valamint a gyártókat és más szolgáltatókat egyaránt érdekli a biztosíthatóság és a díjak költségei. A drónbiztosításnak két alapvető kategóriája van:

- a tulajdonos/üzemeltető jogi felelőssége és a fizikai kár;
- a gyártó felelőssége a termékért.

[20] Légtér.hu (2021): i. m.

Az üzemeltetőnek legalább a jogi felelősségbiztosítást figyelembe kell vennie. Ez fedezi az ingatlan javításának vagy a személyi sérüléseknek a költségeit. A további fedezet magában foglalhatja a személyi sérülést (a magánélet megsértését), a nem tulajdonosi kárt (más drónjával való ütközés), az orvosi költségeket, a helyiségek felelősségét és a háborús károkat, például a rosszindulatú cselekményből eredő károkat. Ezenkívül fedezet áll rendelkezésre a drónok fizikai sérülései ellen. Ez fedezi a berendezések javításának költségeit, vagy az emelvény, az egyéb földi berendezések teljes veszteségét. A gyártó vagy a szolgáltató (például tanácsadó, kereskedő) számára elérhető a termékfelelősség. Ez fedezetet nyújtana abban az esetben, ha a biztosított termék veszteséget okozott vagy hozzájárult ahhoz, ez azonban nem terjed ki a jótállás hatálya alá eső igényekre.

Mindezek mellett (kifejezetten) a kereskedelmi felhasználók számára ajánlott egy új módszer elsajátítása, amely a Specific Operations Risk Assessment (SORA), magyarul a Különleges műveleti kockázatértékelés. Ez egy újszerű megközelítése az Unmanned Aircraft Systems (UAS), avagy a pilóta nélküli repülőgép-rendszer működésének biztonságos létrehozására, vezérlésére és értékelésére. A módszer arra összpontosít, hogy egy UAS-művelethez két kockázati osztályt rendeljen, egy Ground Risk Classt, tehát egy földi kockázati osztályt (GRC) és egy Air Risk Classt, vagyis egy légi kockázati osztályt (ARC). A GRC és az ARC alkotják az alapot a Specific Assurance and Integrity Level, az úgynevezett Specifikus Biztonsági és Integritási Szint (SAIL) meghatározására. A SAIL azt a bizalmi szintet képviseli, hogy az UAS-művelet a tervezett művelet határain belül ellenőrzés alatt marad. A SORA lehetővé teszi az üzemeltetők számára – leginkább a kereskedelmi felhasználók részére –, hogy bizonyos fenyegetési korlátokat és/vagy mérséklő intézkedéseket alkalmazzanak mindkét kockázati osztály csökkentésére, és ezáltal a SAIL csökkentésére. A kockázatértékelés utolsó lépése az Operational Safety Objectives, azaz az üzembiztonsági célkitűzések (OSO) ajánlása, amelyet a SAIL szerint teljesíteni kell. A SORA egy módszer az UAS-műveletek integrálására a (kereskedelmi) pilóta nélküli repüléssel, függetlenül az eszköz súlyától és a légtér magasságától, bizonyos szintű biztonsággal. A SORA-folyamat megkönnyítése érdekében emellett Standard Scenario, úgynevezett standard forgatókönyv (STS) kidolgozása lehetséges bizonyos típusú műveletekhez, ismert veszélyekkel és elfogadható kockázatcsökkentésekkel. Az STS-t ezután az üzemeltetők és a szabályozó hatóságok sablonként használhatják az UAS-műveletek jóváhagyásával járó munka mennyiségének csökkentésére.[21]

4. Következtetések

Összegezve a leírtakat elmondható, hogy a drónok alkalmazása rendkívül nagy hatást gyakorolhat a magánszférára, akár a személyiségi jogokat sértve, akár különböző károkat okozva. Ebből következően a pilóta nélküli légi járművekkel kapcsolatos kockázatok igen sokrétűek, gondoljunk akár a műszaki, akár a meteorológiai vagy akár a jogi szabályozásból, netán éppen annak hiányából eredő veszélyekre. Ezeknek az azonosítása,

[21] Eurocockpit: Specific Operations Risk Assessment (SORA). 2019. január 28.

kezelése szükséges mind a magáncélú, mind pedig az üzleti célú felhasználók számára. A bemutatott esettanulmányon keresztül megjelennek a kockázatelemzés egyes mozzanatai. Jelen elemzés kiemeli a műszaki és adatvédelmi kockázatot, amit orvosolni szükséges, valamint a jövőre nézve preventív intézkedések alkalmazása erősen javasolt. Az esettanulmányon keresztül bemutattam, hogy ételkihordásra történő alkalmazásukkor milyen eshetőségekkel találkozhatnak azok a vállalatok, amelyek a jövőben tervezik bevezetni a drónokkal való kiszállítás lehetőségét. Véleményem szerint további fejlődési lehetőséget biztosítanak az eszközök a hagyományos (gépjárművel, robogóval, kerékpárral történő vagy gyalogos) kézbesítés mellett. Akik ezzel a lehetőséggel élni kívánnak, azoknak azonban elsősorban megfelelően tájékozódni szükséges mind az eszközök, mind pedig a szabályozás terén.

Az esettanulmány után pedig kitértem a netán bekövetkező károk enyhítésére, amelyek megtérítésére Magyarországon – a hazai szabályozás egyik irányaként – megjelenik a kötelező felelősségbiztosítás intézménye. Ez valamilyen szinten eltér az amerikai modelltől, ahol például nem három, hanem két kategóriát különböztetnek meg a biztosítást illetően. A hazai pilóták több társaság ajánlatai közül választhatnak – mind a három biztosító cég esetében vannak átfedések, azonban egy-egy eltéréssel is találkozhatunk a kondíciók között. Ez alapján elmondható, hogy minden személy, aki drónnal rendelkezik, legyen szó akár hobbi, akár üzleti felhasználóról, megtalálhatja a számára kedvező ajánlatot.

Mindezek mellett megjelent egy, kifejezetten a pilóta nélküli légijármű-rendszerekre szakosodott módszer is, amely hozzájárulhat az eszközökkel kapcsolatos kockázatok csökkentéséhez, az esetleges incidensek megelőzéséhez. Az új módszer alapján földi és légi kockázati szinteket is szükséges meghatározni, amelyek együttesen az úgynevezett Specifikus Biztonsági és Integritási Szintet alkotják. Meglátásom szerint feltétlenül előnyös a pilóták számára – feltétlenül a kereskedelmi felhasználók tekintetében. Azonban a módszer hatékonyságát egyelőre nem lehet pontosan megállapítani, ez majd az elkövetkezendő években mutatkozik meg.

Felhasznált irodalom

Allianz Hungária Zrt.: *Légi- és vízi járművek vagyonbiztosítása, drónok felelősségbiztosítása.* (é. n.). Online: www.allianz.hu/hu_HU/uzleti/vallalati-biztositasok/legi-vizijarmu-es-dron-biztositasok.html#dronkinek

Árvay Viktor György – Bíró János – Horuczi Szilvia – Majsa Ágnes – Szabó Endre Győző: *Az elszámoltathatóság alapelve és az adatkezelői kötelezettségek*. Budapest, Nemzeti Közszolgálati Egyetem, 2018.

Drón törvény 2021 – érthetően szakértőktől. *Légtér.hu,* 2021. február 8. Online: https://legter.hu/blog/dron-torveny-2021-erthetoen-szakertoktol/

Eurocockpit: *Specific Operations Risk Assessment (SORA).* 2019. január 28. Online: www.eurocockpit.be/positions-publications/specific-operations-risk-assessment-sora

Gajdács László – Major Gábor: Az UAV alkalmazásának kockázatai a biztonságtechnika területén. *Repüléstudományi Közlemények,* 30. (2018), 2. 101–112. Online: https://folyoirat.ludovika.hu/index.php/reptudkoz/article/view/4342/3548

Galante, Erick – Daniele Bordalo – Marcele Nobrega: Risk Assessment Methodology: Quantitative HazOp. *Journal of Safety Engineering,* 3. (2014), 2. 31–36. Online: http://article.sapub.org/10.5923.j.safety.20140302.01.html#Sec1

Gantz, Stephen D. – Daniel R. Philpott: Chapter 3 – Thinking About Risk. In Stephen D. Gantz – Daniel R. Philpott (szerk.): *FISMA and the Risk Management Framework.* Syngress, 2013. 53–78. Online: https://doi.org/10.1016/B978-1-59-749641-4.00003-5

Katsikas, Sokratis K.: Chapter 53 – Risk Management. In John R. Vacca (szerk.): *Computer and Information Security Handbook (Second Edition).* Morgan Kaufmann, 2013. 905–927. Online: https://doi.org/10.1016/B978-0-12-394397-2.00053-2

Lexiq: *Magánszféra.* Szócikk. Online: https://lexiq.hu/maganszfera

Miskolczi Bodnár Péter: A drónokhoz kötődő aktuális jogalkotási, jogalkalmazási és etikai teendők. In Homicskó Árpád Olivér (szerk.): *Egyes modern technológiák etikai, jogi és szabályozási kihívásai.* Patrocinium, 2018. 139–178. Online: www.kre.hu/ajk/images/doc4/Egyes_modern_technologiak_etikai_jogi_es_szabalyozasi_kihivasai.pdf

Németh, Attila – Sándor Magyar: An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application. *Szakmai Szemle,* 6. (2020), 2. 52–64.

Storr, Pam – Christine Storr: The Rise and Regulation of Drones: Are We Embracing Minority Report or WALL-E?. In Marcelo Corrales – Mark Fenwick – Nikolaus Forgó (szerk.): *Robotics, AI and the Future of Law. Perspectives in Law, Business and Innovation.* Springer, 2018. 105–122. Online: https://doi.org/10.1007/978-981-13-2874-9_5

Wackwitz, Kay – Hendrik Boedeker: Safety Risk Assessment for UAV Operation. *Drone Industry Insights*, 2016.

Wührl Tibor: GPS navigációs problémák UAV alkalmazásokban. *Hadmérnök,* (2006), különszám. 1–7. Online: http://hadmernok.hu/kulonszamok/robothadviseles6/wuhrl_rw6.pdf

HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 3. szám 203–218.
DOI: 10.32567/hm.2021.3.12

Katona Gergő[1]

A Covid-19 kiberbiztonsági kihívásai az első hullám idején[2]

The Cybersecurity Challenges of Covid-19 during the First Wave

2019 végén Kínában jelent meg, majd rövid időn belül az egész világon elterjedt egy újfajta vírus, amely az általunk ismert világ berendezkedését átformálta. Világszerte kijárási korlátozásokat vagy éppen tilalmat rendeltek el, amivel a köznyelvben koronavírusként ismert SARS-CoV-2 vírus terjedését próbálták, illetve a mai napig próbálják lassítani. A védelmi intézkedések az élet számos területére nagy hatást gyakoroltak, a gazdasági tevékenységek számos országban szinte teljesen leálltak, emberek milliói veszítették el az állásukat. Egyik napról a másikra egyes közigazgatási szerveknek és a gazdasági vállalatok nagy részének át kellett költözni az online térbe. Ezen átállás számos kiberbiztonsági kihívást rejtett magában. Jelen cikkben megvizsgálom és csoportosítom, hogy milyen támadások voltak jelen a kibertérben az első hullám idején. Illetve megvizsgálom, hogy a hazai kiberbiztonsági szakértők az egyes fenyegetéseket mennyire tartják kockázatosnak szervezetükre nézve.

Kulcsszavak: Covid-19, kiberbiztonság, kiberfenyegetések, világjárvány

At the end of 2019, a new type of virus appeared in China and then spread around the world in a short time, reshaping it to furnish the world we know. There have been worldwide restrictions or bans on trying to slow down the spread of the SARS-CoV-2 virus – commonly known as the coronavirus – to this day. Protection measures are having a major impact on many areas of life, economic activity has come to a complete halt in many countries, and millions of people have lost their jobs. In the fastest way possible, some public administration organisations and most businesses had to switch to teleworking. This switch included a number of cybersecurity challenges. In this article, I examine and group what attacks were present

[1] Puskás Tivadar Műszaki Szakkollégium, e-mail: katonagergo520@gmail.com
[2] A cikk az Innovációs és Technológiai Minisztérium ÚNKP-20-2-II-NKE-84 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.

in cyberspace during the first wave. I also examine the opinions of cybersecurity experts for risks of different threats.

Keywords: **Covid-19, cybersecurity, cyber threats, pandemic**

1. Problémafelvetés

Ahogy a világ átállt az online működésmódra, egyre nagyobb kihívást kezdtek jelenteni azok a fenyegetések, amelyek a kibertérben jelen vannak. Az online vásárlások mértéke világszerte megnőtt, a munkavállalók nagy része, ha munkaköre engedte, otthonról dolgozott, illetve diákok milliói álltak át az online oktatásra általános iskolától kezdve egyetemig bezárólag. Ezen átállás nagy aránya számos kibertérből érkező fenyegetés kockázatának mértékét növelte. Jelen cikkben megnevezem és csoportosítom azokat a támadási típusokat, amelyek gyakoriak voltak a Covid-19 első hullámának idején. Ezt követően kérdőíves kiértékelésemben megnevezem azt, hogy hazai viszonylatban az egyes fenyegetéseket mennyire ítélik meg kockázatosnak a szakértők, és ezen megítélésüket befolyásolják-e egyéb tényezők.[3]

Így a következő hipotéziseket vizsgáltam kutatásom során:

H1: Az első hullám idején újfajta fenyegetések nem jelentek meg, azonban a meglévők számában növekedés mutatható ki, és megjelenésük szofisztikáltabb, mint eddig.

H2: Feltételezem, hogy azon szakértők, akik szerint a szervezetüknél dolgozók sűrűbben szegik meg a szabályokat, kockázatosabbnak tartják a kiberbiztonsági fenyegetéseket.

2. Kutatási módszer

Megvizsgáltam az egyes fenyegetéseket, amelyek jelen voltak az első hullám idején. Ezenfelül kiértékeltem azokat a támadási statisztikákat, amelyek az egyes támadások paramétereit vizsgálták a definiált időszakban.

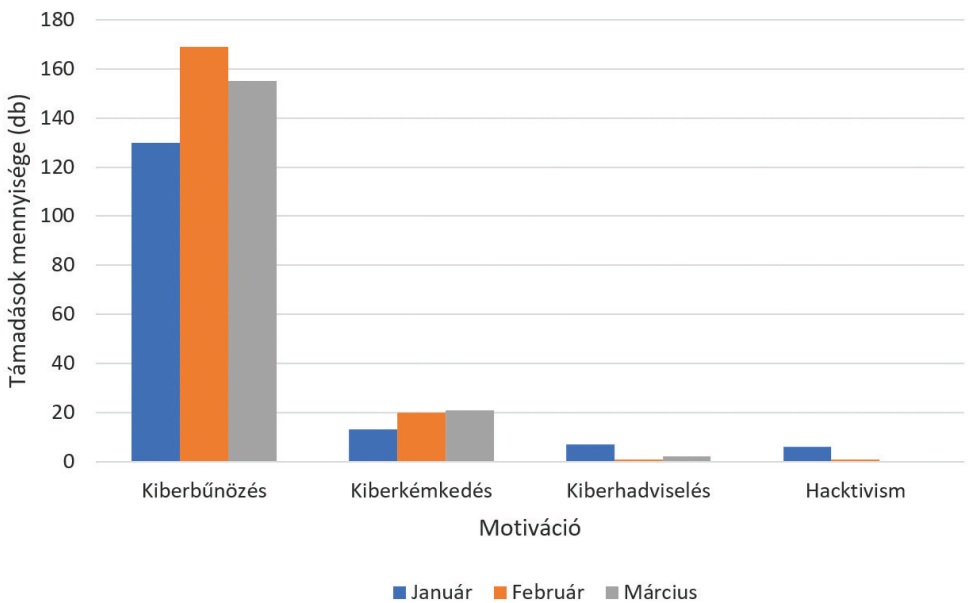
A kérdőívem célcsoportja a hazai kiberbiztonsági szakértők voltak. A kérdőívem kiértékelésére az IBM SPSS Statistics 25 programcsomagot használtam, amiben az eredményeim egy részét Kruskal–Wallis-próba alá vetettem. Ezt követően egyes kérdések kiértékelését osztályozással végeztem el. Kérdéseim egy csoportját kereszttáblás kiértékelés alá akartam vetni, azonban a Khi-négyzet próba azon feltétele nem teljesült, hogy az elvárt gyakoriság minden egyes cellában minimum 5 legyen. Ezért a Kruskal–Wallis-próbát használtam, amely egy típusa az olyan, összetett kontrollcsoportos vizsgálatnak, ahol kettőnél több részminta összehasonlítása történik ugyanazon változó alapján. Ekkor azt szeretnénk megtudni, hogy a részminták között van-e jelentős különbség ugyanazon változó alapján. A Kruskal–Wallis-próba segítségével tesztváltozót vizsgálunk egy csoportosító változóval. A tesztváltozónak és a csoportosító változónak is rangsorolt adatnak kell lennie. Fontosnak tartom kiemelni, hogy kutatásom során azért a Kruskal–Wallis-próbát használtam, nem pedig

[3] Megyeri Lajos – Farkas Tibor: Kockázatelemzés, tudomány vagy kuruzslás?. *Hadmérnök*, 12. (2017), 3. 198–209.

a Mann–Whitney U tesztet, mert a csoportosító változóban a rangsorolt értékek száma kettőnél több volt. A kívánt adatok betöltése és a próba lefuttatása után meg kell vizsgálni az eredményt. Ha az Asymp. Sig. változó, vagyis a szignifikancia nem haladja meg a 0,005-t ($p < 0{,}005$), akkor ki lehet jelenteni, hogy a részminták között jelentős különbség van a csoportosító változó függvényében. Ezután megvizsgáltam a rangátlagot, amely megmutatja a csoportosító változó értékeinek rangsorát a teszt-változó értékeinek függvényében.[4]

3. Eredmények

Ebben a részben bemutatom azokat a támadási formákat, amelyek elterjedtek voltak az agresszorok körében a koronavírus első hullámának idején. Azon adatokat, amelyek alapját adják a vizsgálatomnak, a *Hackmageddon* portál szolgáltatta. E portál adatait egy nemzetközileg elismert kiberbiztonsági szakember, Paolo Passeri gyűjti ki számos olyan forrásból, amelyek kibertámadásokat publikálnak. Látható, hogy motiváció szerint főleg kiberbűnözés volt fellelhető 2020 első negyedévében, továbbá megfigyelhető az is, hogy a támadások főbb célpontjai személyek voltak, de közigazgatás és egészségügy is eléggé nagy arányban állt a támadások középpontjában.

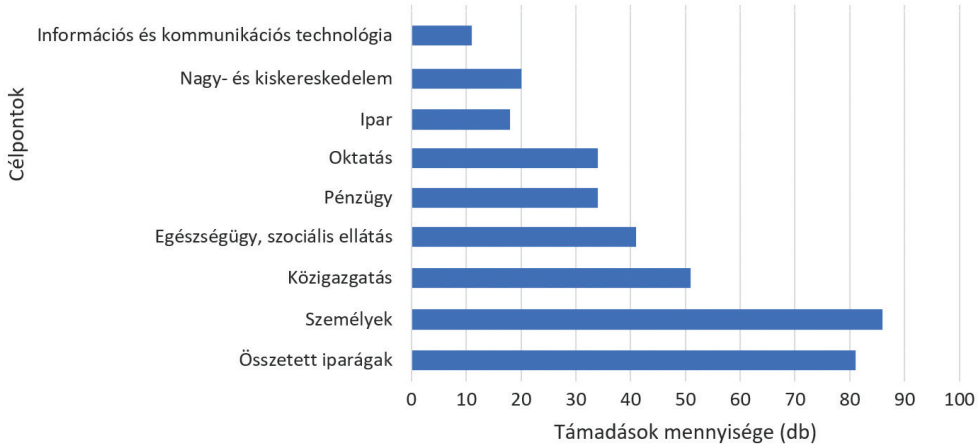


1. ábra

A motivációk havi elosztása 2020 Q1

Forrás: a szerző szerkesztése a *Hackmageddon* adatai alapján

[4] Sajtos László – Mitev Ariel: *SPSS. Kutatási és adatelemzési kézikönyv.* Budapest, Alinea, 2007.

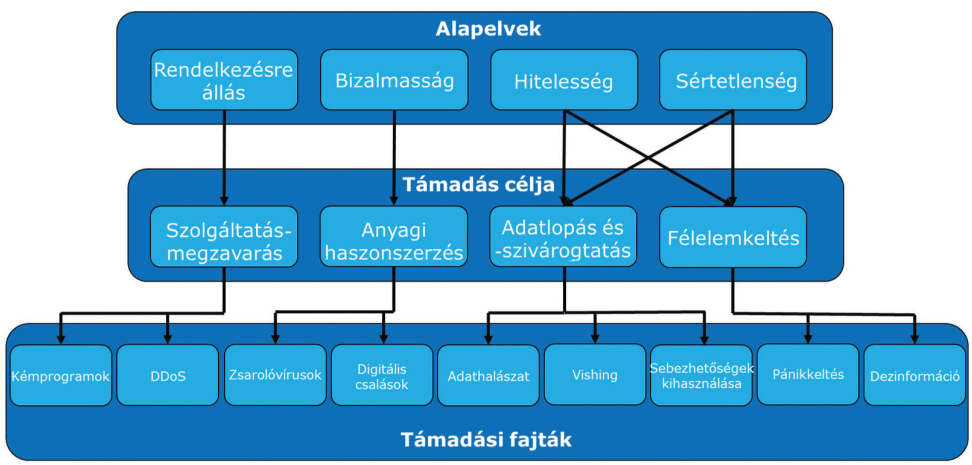


2. ábra

Támadások célpontjai 2020 Q1

Forrás: a szerző szerkesztése a *Hackameddon* adatai alapján

A továbbiakban elemzem, hogy a fenti ábrán látható célpontokat milyen célból, milyen eszközzel támadták az elkövetők, és hogy ezek a támadások mire irányultak. Illetve képet adok arról, hogy a támadók mely kiberbiztonsági fundamentum gyengítésével, megszüntetésével próbálták céljaikat elérni. Látni fogjuk azt, hogy egyes támadások között átfedés van, amely esetünkben azt jelenti, hogy egyes támadások végrehajtásához szükséges egy másik fenyegetés alkalmazása is.



3. ábra

A Covid-19 alatt megjelent támadások csoportosítása

Forrás: a szerző szerkesztése Saqib Hakak et al.: Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. Access IEEE, 8. (2020), 124134–124144. alapján

Bizalmasság: „Az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról."[5]

Zsarolóvírusok: olyan rosszindulatú programok, amelyekkel a támadók a megfertőzött eszközt lezárják, ezzel elérhetetlenné téve az áldozat adatait. Céljuk a haszonszerzés, mivel váltságdíjat követelnek az adatok visszaállításáért, az úgynevezett visszafejtő kulcsért. Az e váltságdíj kifizetésére szabott határidő igen rövid, és legtöbbször a váltságdíjat valamely kriptodevizában kérik, azért, hogy ne lehessen visszakeresni a pénz útját. Ezek a támadók megtalálták a siker vektorát, amely magában foglalja az adatok kritikusságát és az információbiztonsági szegénységi küszöböt. Az információbiztonsági szegénységi küszöb egyensúlyt jelent egy szervezet biztonsági követelményei és a rendelkezésre álló költségvetés között. Egy szervezet a szegénységi küszöb alatt van, ha a biztonsági követelmények meghaladják a rendelkezésre álló költségvetést. A támadók rájöttek, hogy főleg az állami szektor szervezetei gyakran e szegénységi küszöb alá esnek, így ezek a szervezetek is a főbb célpontok között vannak. Bármely olyan szervezet, amely kritikus adatokat kezel elégtelen biztonsági költségvetéssel, tökéletes célpontja ezen anyagilag motivált kibertámadásnak. Az idő múlásával egyértelműen eltolódtak a támadási vektorok, ami bizonyítja a számítógépes bűnözés iparának opportunista tendenciáit. Elsődlegesen háromféle támadóvektor létezik a zsarolóvírus-fertőzés végrehajtására. A *social engineering* igen népszerű, és magában foglalja az adathalász taktikákat is, hogy megtévessze az áldozatot, aki rákattint egy linkre vagy rosszindulatú mellékletre. Más támadási vektorok is egyre népszerűbbek, mint például az ismert sebezhetőségek kihasználása. E vektor szerepe megnőtt a WannaCry segítségével, amely kihasználta a CVE-2017-0144 biztonsági résnek kitett hosztokat. Csak néhány hónappal később a NotPetya kihasználta ugyanezt a biztonsági rést, hangsúlyozva a rutinszerű és hatékony javításkezelés szükségességét. Végül a harmadik vektor a távoli bejelentkezési szolgáltatások kikényszerítése. A gyenge autentikációval rendelkező távoli asztaliprotokoll-szolgáltatásokat a támadók illetéktelen hozzáférésre és ransomware telepítésére kényszerítik.[6]

Online csalások: A tiltott pénzügyi nyereség megkönnyítésére tervezett Covid-19 témájú rosszindulatú programok mellett a koronavírus témájú marketingtevékenységek számának növekedése is megfigyelhető. Ilyenek például a személyes védőeszközök (PPE) vagy más, a Covid-19-hez kapcsolódó termékek csillagászati áron történő eladásának kísérletei. Vagy hamisított és nem jóváhagyott berendezések és termékek értékesítése. Az Interpol-felmérésre válaszoló tagországok körülbelül kétharmada számolt be arról, hogy a járvány kitörése óta a Covid-19-témát jelentős mértékben használják adathalászatra és más online csalásra. 2020 januárja óta az Interpol egyik magánpartnere, a Trend Micro 907 ezer üzenetet észlelt a Covid-19-hez kapcsolódóan, kihasználva a gazdasági visszaesést és az emberek szorongását a világjárvány idején. A kiberbűnözők fokozták social engineering taktikájukat azzal,

[5] Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságáról vezetőknek. Budapest, Nemzeti Közszolgálati Egyetem, 2014. 9.

[6] Pranshu Bajpai – Richard J. Enbody: Attacking Key Management in Ransomware. *IT Professional,* 22. (2020), 2. 21–27.

hogy támadásaik alapjául a Covid-19-et használták.[7] A sértetlenségnél részletesebben kifejtem az adathalászmódszerek működését.[8]

Sértetlenség: „[A]z adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható."[9]

Hitelesség: a CIA-triász legújabb kiegészítése, amelyben a végső cél annak ellenőrzése, hogy a kapott üzenet vagy bármilyen adatcsere csak az eredeti forrásból származik-e. Ezt a célt gyakran statikus és dinamikus hitelesítési módszerekkel történő hitelesítéssel érik el. A járvány során számos rosszindulatú programot hoztak létre, hogy megkönnyítsék a felhasználói adatok és információk eltulajdonítását.[10]

Adathalászat: Fontosnak tartom megjegyezni, hogy a 3. ábrán maga az adathalászat és a Vishing külön szerepel. Ezen felosztás megtalálása azért volt számomra megfelelő, mert attól, hogy a telefonos adathalászat része a phishingnek, mégis olyan, merőben más technikai hátteret és folyamatot igényel, amely megkülönbözteti a többi adathalásztípustól. Az adathalászat szintén gyakori fenyegetés, amelyet a pandémiás helyzetben alkalmaznak a támadók. Az adathalászat alapja, hogy a támadók egy megbízható entitásnak adják ki magukat, mint például pénzintézet, közigazgatási szerv, munkáltató. A támadók meghamisítják az e-mail-címüket, így úgy tűnik, hogy valaki mástól származik. Hamis webhelyeket hoznak létre, és idegen karakterkészleteket használnak az URL-ek leplezéséhez. Különféle technikák léteznek, amelyek az adathalászat égisze alá tartoznak. A támadások kategóriákra bontására többféle módszer létezik. Az adathalász kampány általában két dolog egyikére próbálja rávenni az áldozatot:

- Érzékeny információk megszerzése: Ezeknek az üzeneteknek az a célja, hogy rávegyék a felhasználót a fontos adatok felfedésére, mint például felhasználónév és jelszó, amelyet a támadó felhasználhat a rendszer vagy a fiók megsértésére. A csalás klasszikus változata magában foglalja az e-mailek küldését, amit az emberek millióinak kiküldenek egy ismert bank nevében, így biztosítják, hogy a címzettek legalább egy része ennek a banknak az ügyfele legyen. Az áldozat rákattint az üzenetben található linkre, és egy rosszindulatú webhelyre kerül. Ezen oldalak többségében vagy egy feltört weboldalon helyezkednek el, vagy egy teljesen új domainnel lettek regisztrálva. Az egyik fő árulkodó jel az URL-cím lehet, amely ilyenkor teljesen más, mint az eredeti oldal esetében. Itt az áldozat megadja a belépési azonosítóját, amit már a támadó fel is tud használni.
- Rosszindulatú programok letöltése: A sok spamhez hasonlóan az ilyen típusú adathalász e-mailek célja, hogy az áldozat saját számítógépét megfertőzze rosszindulatú programokkal. Az üzenetek gyakran csalogató információkat ígérnek, mint például küldhető egy HR-munkatársnak olyan melléklet, amely állítólag

[7] Interpol: INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19. (2020. augusztus 4.).
[8] Bányász Péter: Social engineering és közösségi média. *Nemzetbiztonsági Szemle,* 5. (2018), 1. 59–77.
[9] Muha–Krasznay (2014): i. m.
[10] William Stallings – Lawrie Brown: *Computer Security: Principles and Practice.* Boston, Pearson, 2012.

egy álláskereső önéletrajza lehet. Ezek a mellékletek gyakran.zip fájlok vagy rosszindulatú beágyazott kódot tartalmazó Microsoft Office dokumentumok. A rosszindulatú kódok leggyakoribb formája a ransomware – 2017-ben becslések szerint az adathalász e-mailek 93%-a tartalmazott zsarolóvírus-mellékleteket.[11]

Csoportosítani lehet az adathalász-támadásokat az elkövetés módja szerint is:

- Az első, amit meg lehet említeni, az SMS adathalászat, ahol a támadók egy hivatalosnak tűnő SMS-ben kérik az áldozatot, hogy a megadott linkre kattintva adja meg adatait. Számos adathalász-támadás központi eleme egy adathalászoldal, amely egy az egyben másolata azon szervezet oldalának, amelynek nevében az áldozatot felkeresték.
- A következő típus a Spear phishing célzott támadás, ahol a támadók az áldozatokról már tudnak egyes adatokat, mint például beosztás, e-mail-cím, telefonszám. Ezáltal egy személyre szólóbb és célozottabb támadást tudnak végrehajtani.
- A bálna-adathalászat a célzott adathalászat egyik formája, amely a nagyon nagy „halakra" – vezérigazgatókra vagy más fontos célpontokra – irányul. E csalások közül sokan a vállalati igazgatóság tagjait célozzák meg, akiket különösen kiszolgáltatottnak tartanak.

A RiskIQ beszámolt arról, hogy háromnapos időszak alatt (azaz 2020. április 11–13.) több mint 309 000 spam e-mailt fedeztek fel, amelyek vagy „korona", vagy „covid" kifejezést tartalmaztak.[12] Ezekben az e-mailekben a támadók az Egészségügyi Világszervezet tagjának (WHO) vagy egészségügyi szakembernek adták ki magukat, olyan előtagok használatával, mint a „Dr" és a „Professzor". Ezek az e-mailek gyakran tartalmaznak olyan témaköröket, mint a „Covid-19 frissítések", „A városod Covid-19 nyomkövetője", amelyek célja az áldozatok csalogatása a mellékletre való kattintásra, például „.rtf" kiterjesztésű fájlokra.[13]

- Vhishing (Telefonos adathalászat): A távoli ügyintézés (például Távegészségügy) mindennapossá vált a jelenlegi Covid-19-járványban, amelyben a szervezetek rugalmas munkamegállapodásokat kínálnak alkalmazottaiknak. Tekintettel arra, hogy ezek az alkalmazottak üzleti tevékenységük során nagymértékben támaszkodnak a telefonos és az internetes kommunikációra, egy ilyen kommunikációs csatornát a támadók könnyen ki tudnak használni. Például olyan támadásokról számoltak be, hogy az üzleti és személyes kommunikációt eltérítik hangalapú adathalászattal (azaz vishing), robocall-csalások és egyéb technikai támogatású csalások útján. Fény derül arra is, hogy ezek a támadók visszaélnek az IP- (Voice over IP, VoIP) szolgáltatásokkal, hogy becsapják az egyéneket a nem létező szolgáltatások kifizetéséért vagy személyes adataik (például bankszámlaadataik, társadalombiztosítási számaik) megszerzéséért.

[11] Maria Korolov: 93% of phishing emails are now ransomware. *CSO Online,* 2016. június 1.
[12] Hakak (2020): i. m.
[13] CISA. Cybersecurity and Infrastructure Security Agency: COVID-19 Exploited by Malicious Cyber Actors. (2020. április 8.).

- Kiszolgáltatottság kiaknázása: A meglévő társadalmi távolságtartási követelmények eredményeként szüneteltek az olyan szervezetek tevékenységei, mint az egyetemek, a kormányzati szervek ügyfélfogadása és más nem alapvető szolgáltatások. Ez a bezárás az online rendszerek és platformok, például az online tanuláskezelő rendszerek (*Learning Management System,* LMS) és a videokonferencia-alkalmazások és eszközök (például Zoom) jelentős használatát eredményezte. Számos olyan eseményről számoltak be – némelyike nagy nyilvánosságot is kapott –, amelyek során a számítógépes bűnözők azonosítják és kihasználják a fent említett rendszerek és platformok sebezhetőségét.
- Dezinformáció és pánikkeltés: Számos közösségimédia-kampányt figyeltek meg a népszerű közösségimédia-platformokon is, mint például a Facebook, a WhatsApp és a LinkedIn, ahol hamis vagy félrevezető információkat tettek közzé. Ilyen például, hogy egyes gyógyszerek hatékonyak a Covid-19 ellen, vagy a tehén vizeletének fogyasztása megakadályozhatja a vírus átadását. Bár semmilyen tudományos bizonyíték nem igazolja ezeket az állításokat, zavart keltettek a nyilvánosság körében, és egyes esetekben halálesetekhez vagy sérülésekhez vezettek. A közösségi média platformjain keresztül számos cikket és videót osztottak meg, amelyek megtanítják, hogyan hozzanak létre házi készítésű kézfertőtlenítő-szereket és más kapcsolódó termékeket. Természetesen ezeken a felületeken is felmerültek olyan állítások, miszerint a Covid-19 nem valós, és az állampolgároknak figyelmen kívül kell hagyniuk a társadalmi távolságtartás követelményeit és a maszkhasználatot. Az ilyen dezinformálás könnyen vezethet gyorsabban növekedő esetszámokhoz és ezáltal több halálesethez.[14]

Rendelkezésre állás: „annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek."[15]

- DDoS-támadások: A számos létező fenyegetés között az elosztott szolgáltatásmegtagadással járó támadás (*Distributed Denial of Service,* DDoS) viszonylag egyszerű, de nagyon hatásos technika az intranet és az internetes erőforrások megtámadására. Ebben a támadásban a jogosultsággal rendelkező felhasználókat általában nagy mennyiségű gépi erőforrás akadályozza a webalapú szolgáltatások használatában. A DDoS-támadásokat hálózati, szállítási és alkalmazási rétegekben lehet megvalósítani különböző protokollok, például TCP, UDP, ICMP és HTTP használatával. Az Europol a pandémiás helyzetben a DDoS-támadások folyamatos növekedéséről számolt be. Ezeknek a támadásoknak jelentős gyakorlati következményei vannak, mert többek között a társadalmi távolságtartás, az otthoni munkavégzés és az online oktatási tevékenységek miatt is nő az internetezők száma. Ezért alapból az egyes szolgáltatások így nagyobb terhelést kapnak, mint amekkora a vírus előtt megszokott volt.[16]

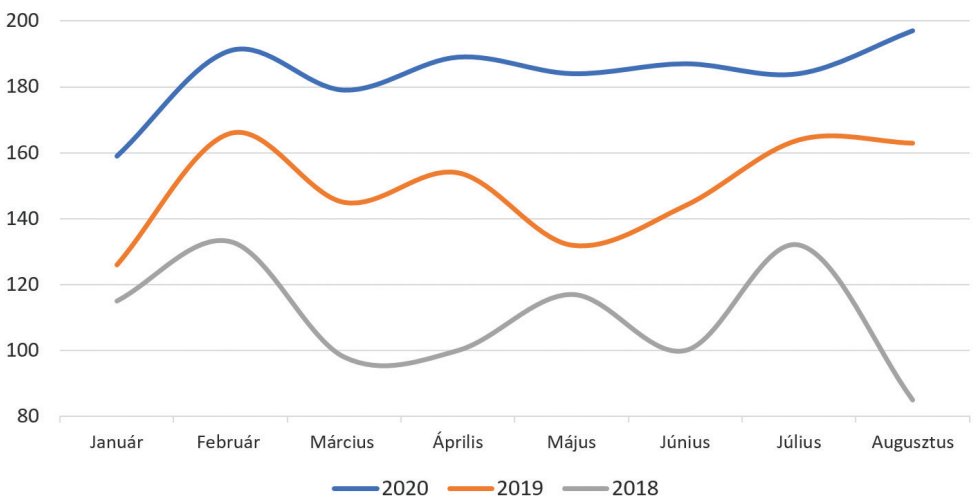
[14] Hakak (2020): i. m.; Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. (2016), 1. 61–81.

[15] Muha–Krasznay (2014): i. m.

[16] Iman Sharafaldin et al.: Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. *International Carnahan Conference on Security Technology.* 2019. 1–8; András Tóth: Information-Sharing Challenges and Issues in Multinational Operations Part 1. *Land Forces Academy Review,* 25. (2020), 4. 307–316.

- Kémprogram-támadások: A kémprogram egy olyan, rosszindulatú szoftver, amelyet rendszerek titkos információinak megszerzésére használnak. Például a COVID-19-hez kapcsolódó nyomkövető-alapú alkalmazásokat állítólag kémprogram-alapú applikációkba ágyazták a felhasználók tevékenységének nyomon követésére. Az ilyen nyomkövető és kontaktkutató alkalmazások különböző kapcsolati típusokat használnak, az adott eszköz és környezete azonosításához, ilyen a GPS, Bluetooth kapcsolat. A GPS alapon működő alkalmazások helymeghatározó adatokat küldenek a központi hatóságoknak időbélyegekkel. Ha kiderült az adott illetőről, hogy fertőzött, ezeket az adatokat össze tudják vetni a más eszközök által küldött adatokkal. Ezáltal értesíteni tudják azon személyeket, akik azonos időben a fertőzött, személy közelében voltak. A Bluetooth technológia képes egyszerre több kapcsolatot létrehozni, és ezeket fenntartani. Ennek a technológiának a megfelelő alkalmazása segítségével szintén beazonosíthatók azon eszközök felhasználói, akik fertőzött személy közelében tartózkodtak és esetleg maguk is megfertőződtek. [17]

A 4. ábrán látható, hogy a kibertámadások számában növekedés mutatható ki az előző évekhez képest, amely növekedésben közrejátszik természetesen a koronavírus megjelenése. Ezen kijelentésemet többek között mind az Interpol-, mind a RiskIQ-források alátámasztják. Azonban azt is ki kell jelenteni, hogy a vírus előtt is folyamatos növekedő tendencia volt jelen e támadások esetében.



4. ábra

A kibertámadások számának alakulása 2018–2020

Forrás: a szerző szerkesztése a *Hackameddon* adatai alapján

[17] Németh Attila – Magyar Sándor: An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application (part 1). *National Security Review,* 6. (2020), 2. 52–64.

A fenti adatok alapján a támadásokat összegezve a T1-es tézisem az lett, hogy az első hullám idején nem jelentek meg új fenyegetések, viszont a már eddig jelen lévők számában növekedés mutatható ki, és e támadások egy részének témája a koronavírus lett. Így a H1 hipotézisem helytállónak bizonyult.

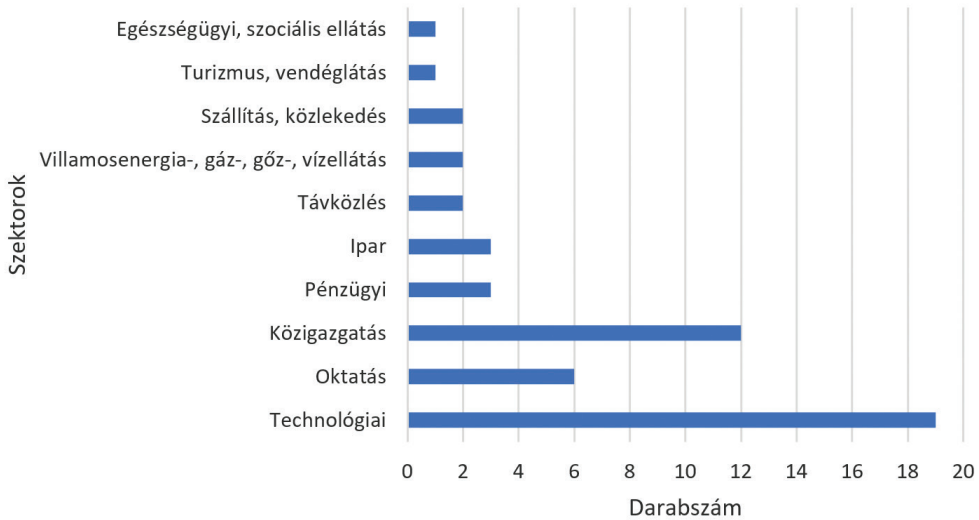
3.1. Kérdőíves felmérés eredménye

Empirikus kutatásom gerincét a kérdőívem jelentette, amelyet hazai információbiztonságban dolgozó személyek körében töltettem ki. A kérdőívem kialakításához több nemzetközi tanulmányt vizsgáltam meg a kérdéskörben.[18] Végül Ulrik Franke és szerzőtársa, Joakim Wernberg által írt *A survey of cyber security in the Swedish manufacturing industry* cikk kérdőívét vettem alapul, és témaspecifikusan reprodukáltam. Kérdőívemben rákérdeztem a távoli munkavégzés megjelenésére, illetve megkérdeztem szakembereket, hogy az egyes fenyegetési típusokat mennyire tartják kockázatosnak saját szervezetükre nézve. A kérdőív két fő részből áll, az első rész általános információkra kérdez rá: itt olyan kérdések találhatók meg, amelyek magára a kitöltő személyre vonatkoznak (például melyik szektorban dolgozik; milyen végezettséggel rendelkezik; milyen beosztásban dolgozik; mióta dolgozik a kiberbiztonságban). A második részben főleg a támadási típusok és a távmunka kérdésköre, illetve a szervezetben dolgozó személyi kör szabályzatkövetési hajlandósága volt a téma (például távmunka volt-e engedélyezve; tettek-e külön intézkedést távmunka kapcsán; milyen típusú fenyegetést mennyire kockázatosnak ítélnek meg a szervezetre nézve; a munkavállalók szabálykövetők-e). A kérdőívem természetesen anonim volt, mivel olyan adatot nem kértem, amivel ki lehet deríteni a kérdőív kitöltőjének személyazonosságát, így megfelel a 2011. évi CXII. törvénynek, és ezáltal az Általános Adatvédelmi Rendeletnek (*General Data Protection Regulation,* GDPR).

Kérdőívemet 51 szakértő töltötte ki, jellegét tekintve nem reprezentatív a felmérés. A legtöbben a technológiai szektorból töltötték ki, szám szerint 19 személy; ezt követte a közigazgatási szektor 12 kitöltővel; majd az oktatás 6; pénzügyi szektor és az ipar 3; és a szállítás, közlekedés; villamosenergia-, gáz-, gőz-, vízellátás; távközlés 2 fő kitöltést kapott. A turizmus, vendéglátást; egészségügyi, szociális ellátást 1-1 ember választotta. A kitöltők 47%-a elektronikus információbiztonsági vezetői képzéssel rendelkezik; 21,6%-nak Certified Information Systems Auditor (CISA-) bizonyítványa van; 17,6%-a rendelkezik Certified Information Security Manager (CISM-) képesítéssel; 5,9% nyilatkozott arról, hogy Certified Information Systems Security Professional (CISSP-) végzetsége van; 11,8% Certified in Risk and Information Systems Control (CRISC-) bizonyítványa van; ISO lead auditor képesítéssel a válaszadók 27,5%-a rendelkezik; ISO internal auditor 11,8%-a megkérdezettek közül; egyéb

[18] Mark Rodbert: Why organisational readiness is vital in the fight against insider threats. *Network Security,* (2020), 8. 7–9; Mohamed Amine Ferrag – Messaoud Babaghayou – Mehmet Akif Yazici: Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *Journal of Information Security and Applications,* 52. (2020), 102500; Ulrik Franke – Joakim Wernberg: A survey of cyber security in the Swedish manufacturing industry. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020.* 1–8; Hakak (2020): i. m.

információbiztonsági képesítéssel a kitöltők 23,5%-a rendelkezik és további 43,1% rendelkezik egyéb nem információbiztonsághoz kötődő végzettséggel. Fontosnak tartom kiemelni, hogy a kitöltők itt több válaszlehetőséget is választhattak, mivel az egyik végzettség nem zár ki más végzettségeket.



5. ábra

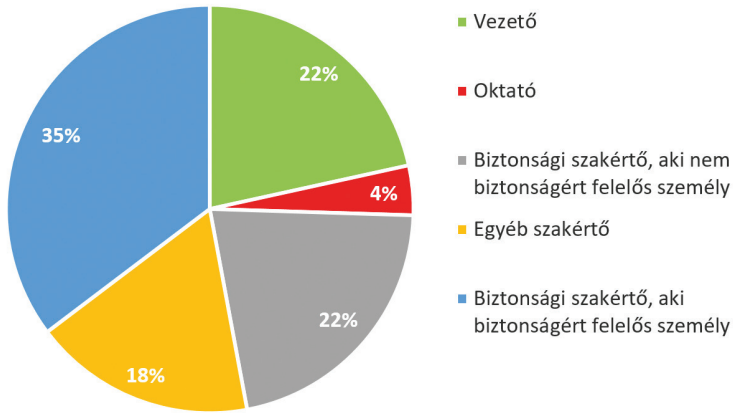
Kitöltők szektorbeli megoszlásai (fő)

Forrás: a szerző szerkesztése

Következő kérdésem arra irányult, hogy milyen beosztásban dolgoznak, ami egy nyitott kérdés volt. Így a kapott válaszokon osztályozó kiértékelést végeztem el. Öt külön osztályt hoztam létre, amelyek a következők voltak:

- vezető (gyakori válaszok: CEO, ügyvezető igazgató, vezető);
- oktató (gyakori válaszok: oktató, oktatás);
- biztonsági szakértő, aki nem biztonságért felelős személy (gyakori válaszok: tanácsadó; IT-biztonsági tanácsadó, IT-biztonsági elemző);
- egyéb szakértő (gyakori válaszok: termékfelelős rendszermérnök, sales, informatikus);
- biztonsági szakértő, aki biztonságért felelős személy (gyakori válaszok: IBF, információbiztonsági felelős, CISO, DPO).

Azt láthatjuk, hogy a kitöltők 22%-a vezető beosztásban dolgozik; 4%-a oktató; 22%-a biztonsági szakértő, aki nem biztonságért felelős személy; 18%-a egyéb szakértő és 35%-a biztonsági szakértő, aki biztonságért felelős személy.



6. ábra

Beosztás szerinti megoszlás (%)

Forrás: a szerző szerkesztése

A kérdőívemben megkérdeztem a szakembereket, hogy mekkora kockázati értéket adnának a következő támadásoknak a következő 1 évre:

- Az üzletmenet-folytonosság megszakításával járó támadás;
- Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok;
- Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például ipari kémkedés);
- Nem szándékos esemény, amely üzletmenet-folytonosság megszakításával jár;
- Távoli munkavégzést kihasználó támadások.

A választási lehetőségek a következők voltak:

- Elhanyagolható kockázat;
- Alacsony kockázat;
- Közepes kockázat;
- Magas kockázat;
- Nagyon magas kockázat;
- Nem tudom.

A szakértők legnagyobb számban közepes kockázati szintet jelöltek meg a támadásoknál (szám szerint 84), ezt követi 69-cel az alacsony kockázati besorolás; majd 54-gyel az elhanyagolható szintű besorolás; az utolsó előtti összmennyiségben a magas kockázat 39-cel; és utolsó 3 db-bal a nagyon magas kockázat. Ebből látható, hogy a szakértők nagy része felkészültnek tartja a szervezeteiket e támadásokra. Ezenfelül az is látható az 1. táblázatból, hogy a magas és a nagyon magas kockázati szint összege a távoli munkavégzést kihasználó támadásoknál a legmagasabb. Ez azt jelenti, hogy a felsorolt támadási típusokból a kitöltők legnagyobb része a távoli munkavégzés kihívásaitól tart legjobban.

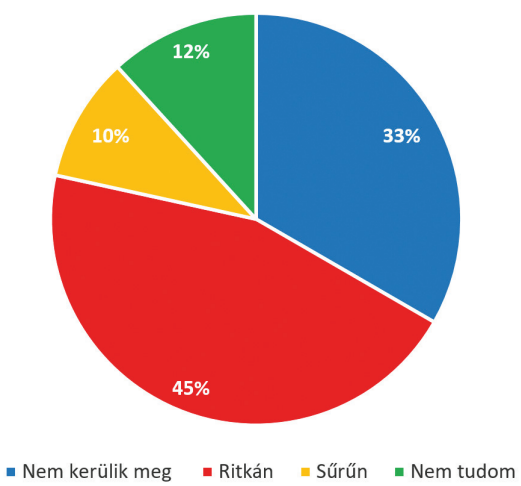
1. táblázat

Egyes fenyegetések bekövetkezési valószínűségének kockázatai a szakértők véleménye szerint (db)

Forrás: a szerző szerkesztése a kérdőív alapján

Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi						
	Az üzletmenet-folytonosság megszakításával járó támadás	**Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok**	**Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például ipari kémkedés)**	**Nem szándékos esemény, amely üzletmenet-folytonosság megszakításával jár**	**Távoli munkavégzést kihasználó támadások**	**Válaszok megoszlása kockázati szintenként**
Elhanyagolható kockázat	13	8	15	9	9	54
Alacsony kockázat	14	18	16	13	8	69
Közepes kockázat	19	18	10	18	19	84
Magas kockázat	3	6	9	8	13	39
Nagyon magas kockázat	0	0	0	2	1	3
Nem tudom	1	0	0	0	0	1

Kérdőívemben kitértem arra is, hogy a szakértők szerint a szervezetükben megszegik-e a szabályokat, és ha igen, akkor ezt milyen sűrűn teszik. A 7. ábrán is látható, hogy a válaszadók 33%-a szerint a szervezetben dolgozó munkavállók nem kerülik meg a szabályokat; 45% gondolja úgy, hogy ritkán, de megkerülik a dolgozók a szabályokat; 10% az az arány a kitöltők esetében, akik azt mondják, hogy a munkavállalók sűrűn megkerülik a szabályokat és 12% nem tudta eldönteni ezt saját szervezetére nézve.



7. ábra

Szabálymegkerülési gyakoriság (%)

Forrás: a szerző szerkesztése

Mind a támadások kockázatára, mind a szabályszegés sűrűségére adott válaszokat megtisztítottam úgy, hogy kikerüljenek azon személyek válaszai, akik valamely kérdésnél a nem tudom opciót választották, így marad 44 válasz, amit külön Kruskal–Wallis-próba alá vetettem. Kíváncsi voltam, hogy van-e összefüggés a megadott fenyegetésekre adott kockázati szint, illetve a szabálykerülés sűrűségének szintje között. A próba lefuttatásában a csoportosító változó a szabálymegkerülési sűrűség és a tesztváltozók az egyes támadások kockázatának mértéke volt. A 2. táblázatból jól lehet látni azt, hogy a szignifikancia értéke egyedül az „Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például ipari kémkedés)" csoportban haladja meg 0,005-t. Ez azt jelenti, hogy a másik 4 csoportban jelentős különbség mutatható ki a kockázati megítélésben a szabálymegkerülés függvényében.

2. táblázat

Kruskal–Wallis-próba szignfikanciaeredménye

Forrás: a szerző szerkesztése az SPSS alapján

	Nem szándékos esemény, amely üzletmenet-folytonosság megszakításával jár	**Távoli munkavégzést kihasználó támadások**	**Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például ipari kémkedés)**	**Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok**	**Az üzletmenet-folytonosság megszakításával járó támadás**
Kruskal–Wallis H	11,566	13,756	4,766	15,140	11,541
df	2	2	2	2	2
Asymp. Sig.	,003	,001	,092	,001	,003

Ezt követően megvizsgáltam azt, hogy a rangátlag ebben a 4 csoportban miként oszlik meg. Ez a rangátlag mutatja meg a csoportosító változó értékeinek rangsorát (milyen sűrűn kerülik meg a szabályokat a szervezetben dolgozók) a tesztváltozó értékeinek (egyes fenyegetésre adott kockázati érték) függvényében. Ennek eredménye a 3. táblázatban látható.

Mind a 4 tesztváltozó esetében azt lehet megfigyelni, hogy a legmagasabb rangátlagot a sűrű szabálymegkerülés kapta, ezt követte a ritka megkerülés, és végül legkisebb rangátlagot a nem kerülik meg csoportosító változó kapta. Ezáltal kijelenthető az, hogy a kitöltésben részt vevő szakértők nagyobb kockázati értéket adtak, ha úgy vélték, hogy a szervezetben dolgozók megszegik a szabályokat. Így azon T2 tézisem született, miszerint azok a szakértők, akik szerint a szervezetüknél a szabálymegkerülés sűrűn fordul elő, nagyobb kockázati értéket adnak az egyes fenyegetéseknek, ezzel alátámasztottam a H2 hipotézisemet.

3. táblázat
A csoportosító értékek rangátlaga a tesztváltozók függvényében
Forrás: a szerző szerkesztése az SPSS alapján

	Nem kerülik meg a szabályokat rangátlaga	Ritkán kerülik meg a szabályokat rangátlaga	Sűrűn kerülik meg a szabályokat rangátlaga
Nem szándékos esemény, amely üzletmenet-folytonosság megszakításával jár	14,53	27,05	29,60
Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok	13,50	27,63	30,50
Az üzletmenet-folytonosság megszakításával járó támadás	14,71	26,77	30,20
Távoli munkavégzést kihasználó támadások	13,85	27,55	29,70

4. Összegzés

Az első hullám idején látható, hogy a legtöbb kibertérből érkező támadás hátterében mint motiváció a kiberbűnözés állt, amely főleg személyeket, közigazgatást és összetett iparágakat célzott meg. Ezen támadások között új nem jelent meg, ami azt jelenti, hogy olyan támadásokat használtak az elkövetők, amelyek 2020 januárja előtt is elérhetők voltak, viszont számukban növekedés mutatható ki, illetve egyes támadások központi témája a koronavírus lett. Hazai viszonylatban az mondható el, hogy a kitöltésben részt vevő szakértők egyes fenyegetéseket illető kockázati besorolására nagy befolyást gyakorol a szervezet szabálykövetése. Ezen eredmény azért lehet figyelemre méltó, mert a kitöltésben részt vevő szakértők végzik nagy eséllyel a szervezetükben a kockázatelemzést, amely alapján priorizálják a kockázatcsökkentő lépéseket. E priorizálás útján tervezik meg a fejlesztéseket és allokálják az egyes erőforrásokat a kockázatcsökkentő lépésekre.

Felhasznált irodalom

Amine Ferrag, Mohamed – Messaoud Babaghayou – Mehmet Akif Yazici: Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *Journal of Information Security and Applications,* 52. (2020), 102500. Online: https://doi.org/10.1016/j.jisa.2020.102500

Bajpai, Pranshu – Richard J. Enbody: Attacking Key Management in Ransomware. *IT Professional,* 22. (2020), 2. 21–27. Online: https://doi.org/10.1109/MITP.2020.2977285

Bányász Péter: Social engineering és közösségi média. *Nemzetbiztonsági Szemle,* 5. (2018), 1. 59–77.
Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. (2016), 1. 61–81.
CISA. Cybersecurity and Infrastructure Security Agency: *COVID-19 Exploited by Malicious Cyber Actors.* (2020. április 8.). Online: https://us-cert.cisa.gov/ncas/alerts/aa20-099a
Franke, Ulrik – Joakim Wernberg: A survey of cyber security in the Swedish manufacturing industry. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. 2020. 1–8. Online: https://doi.org/10.1109/CyberSA49311.2020.9139673
Hakak, Saqib – Wazir Zada Khan – Muhammad Imran – Kim-Kwang Raymond Choo –Muhammad Shoaib: Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. *Access IEEE,* 8. (2020), 124134–124144. Online: https://doi.org/10.1109/ACCESS.2020.3006172
Interpol: INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19. (2020. augusztus 4.). Online: www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
Korolov, Maria: 93% of phishing emails are now ransomware. *CSO Online,* 2016. június 1. Online: www.csoonline.com/article/3077434/93-of-phishing-emails-are-now-ransomware.html
Megyeri Lajos – Farkas Tibor: Kockázatelemzés, tudomány vagy kuruzslás?. *Hadmérnök,* 12. (2017), 3. 198–209. Online: www.hadmernok.hu/173_18_megyeri.pdf
Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságáról vezetőknek.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. Online: https://opac.uni-nke.hu/webview?infile=&sobj=9695&source=webvd&cgimime=application%2Fpdf
Németh Attila – Magyar Sándor: An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application (part 1). *National Security Review,* 6. (2020), 2. 52–64.
Rodbert, Mark: Why organisational readiness is vital in the fight against insider threats. *Network Security,* (2020), 8. 7–9. Online: https://doi.org/10.1016/S1353-4858(20)30092-1
Sajtos László – Mitev Ariel: *SPSS. Kutatási és adatelemzési kézikönyv.* Budapest, Alinea, 2007.
Sharafaldin, Iman – Arash Habibi Lashkari – Saqib Hakak – Ali A. Ghorbani: Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. *2019 International Carnahan Conference on Security Technology,* 2019. 1–8. Online: https://doi.org/10.1109/CCST.2019.8888419
Stallings, William – Lawrie Brown: *Computer Security: Principles and Practice.* Boston, Pearson, 2012.
Tóth András: Information-Sharing Challenges and Issues in Multinational Operations Part 1. *Land Forces Academy Review,* 25. (2020), 4. 307–316. Online: https://doi.org/10.2478/raft-2020-0037

HADMÉRNÖK
FÓRUM
16. évfolyam (2021) 3. szám 219–227.
DOI: 10.32567/hm.2021.3.13

Fejes Zsolt,[1] Matusz Márk Péter[2]

A Covid-19-világjárvány hatása a telemedicina hazai fejlődésére, kapcsolata a haderőfejlesztési programokkal

Impact of the Covid-19 Pandemic on the Development of Telemedicine in Hungary and Its Relationship with Force Development Programs

A világjárvány következtében jelentősen emelkedett a telemedicinális ellátási formákkal kapcsolatos publikációk száma, jól érzékelhetően fokozódtak a kormányzati törekvések a szabályozás minőségi javítására, az egészségügyi szereplők pedig a korábbiakhoz képest nagyobb intenzitással és szélesebb spektrumban kezdték el alkalmazni a rendelkezésre álló technikai lehetőségeket. A bevezetett korlátozások következtében nemcsak az orvosok, hanem a lakosság részéről is megnövekedett igény tapasztalható az online térben zajló konzultációk, tanácsadások és orvosi vizitek lebonyolítására. Cikkünkben azt elemezzük, hogy a jelenleg ismert digitális platformokat és telemedicinális rendszereket mely területen használták fel, mely faktorok indukálták fejlődésüket, illetve hogyan képesek ezek kiszolgálni a katonai betegellátás igényeit a több mint egy éve zajló koronavírus-világjárvány idején. Ugyancsak kísérletet teszünk arra, hogy megtaláljuk a telemedicina, az eHealth és mHealth rendszerek illesztési pontjait a Magyar Honvédség Honvédelmi és Haderőfejlesztési Programjának egyik fő elemét alkotó Digitális Katona Programjával.

Kulcsszavak: **világjárvány–pandémia, egészségügyi vészhelyzet, telemedicina, eHealth, mHealth, digitális platform, digitális katona, stratégiai tervezés, képességfejlesztés**

[1] NATO Összhaderőnemi Parancsnokság, Egészségügyi Szolgálat, Nápoly, Olaszország, orvos ezredes, egészségügyi szolgálat főnökhelyettes; e-mail; fejes.zsolt@hm.gov.hu
[2] MH ARB, Egészségügyi Központ, Budapest, pszichológus százados, egészségügyi központ megbízott parancsnok, e-mail: mark.matusz@gmail.com

The Covid-19 pandemic has significantly increased the number of publications on telemedicine. Government efforts have intensified to improve the quality of regulation, while health care actors have started to use the available technical options with greater intensity and a wider range than before. As a result of the wide scale restrictions, there is an increased demand for online consultations detected from physicians and from the general public side. In our article, we analyse in which areas have the currently known digital platforms and telemedicine systems been used, which factors have triggered development, and how these systems can serve the needs of military health care during the coronavirus pandemic. In the article we are trying to find the interface between telemedicine, eHealth and mHealth systems with the Digital Soldier Program, which is one of the main part of the Defence and Force Development Program of the Hungarian Defence Forces.

Keywords: **pandemic, health emergency, telemedicine, eHealth, mHealth, digital platforms, digital soldier, strategic planning, capability development**

1. Bevezető

A 2019. év végén terjedésnek indult, majd világjárványt okozó SARS-CoV-2 vírus jelentősen megváltoztatta világunk megszokott rendjét, annak korábbi működését és szabályait, társadalmi, köz- és magánéleti berendezkedésünket.[3]

A Covid-19-világjárvány során olyan, korábban nem tapasztalt mértékű, multifaktoriális jelentőségű, egyelőre nem látható következményeket is hordozó kihívások tömegével kell szembesülnünk, ami modern kori történelmünkben ez idáig példa nélküli. Az események komplexitása, a járvány tér- és időbeli kiterjedése minden nap próbára teszi erőforrásainkat, felkészültségünket, alapvetően befolyásolja biztonságérzetünkbe vetett hitünket és folyamatosan naprakész válaszokat igényel. A járvány közvetlen és közvetett következményeit egy éve folyamatosan tapasztaljuk, ugyanakkor jövőbeni alakulásával kapcsolatban mindössze találgatni tudunk, az elszenvedett tényleges károkról pedig csak évek múlva lesznek korrekt elemzéseink. Az elmúlt egy év történései rámutattak arra, hogy hasonló események bekövetkezésével a jövőben is nagy valószínűséggel számolnunk kell. Globális, nemzeti és egyedi szakmai védekezési stratégiák kidolgozására egyaránt szükségünk van annak érdekében, hogy a jelenlegivel azonos vagy ehhez hasonló problémák kezelésére hatékony eszközrendszereket állítsunk hadrendbe.[4] A koronavírus-világjárvány idején ezt az elvárt hatékonyságot képviseli az egészségügy számos területén alkalmazott telemedicina-képesség.

[3] AJMC. The American Journal of Managed Care: A Timeline of COVID-19 Developments in 2020 (2021. január 1.).
[4] WHO: Telemedicine Opportunities and developments in Member States. Global Observatory for eHealth series – Volume 2. (2010.).

2. Globális koronavírus-járványkép

A globális egészségügyi vészhelyzetet 2020. március 11-én hirdette ki az ENSZ Egészségügyi Világszervezete (WHO). Cikkünk elkészülésekor a WHO adatai alapján több, mint 113 315 000 fertőzöttről, és több mint 2 517 000 halottról van tudomásunk.[5]

2.1. Magyarországi koronavírus-járványkép

2020 elején a világjárvány elérte Magyarországot is, aminek következtében kihirdették a vészhelyzetet. Ezt három hónappal később – az első hullám lecsengésével – megszüntették, helyette járványügyi készültség lépett életbe. A koronavírus-járvány második hulláma Európa-szerte 2020 őszén jelentkezett, és az első hullámhoz képest már súlyosabban érintette hazánkat. A kormány ennek hatására novembertől visszaállította a rendkívüli jogrendet és újra kihirdette a veszélyhelyzetet is, amelyet az Országgyűlés később meghosszabbított. Tekintettel a 2021 februárjától újból növekedésnek induló igazolt fertőzések számára, cikkünk írásának időpontjában a kormány ismét életbe léptette a korábbi védelmi intézkedéseket. Ekkor Magyarországon az aktív fertőzöttek száma Budapesten 15 954, vidéken 76 543 fő,[6] míg az összes pozitív eset száma a világjárvány kezdete óta elérte a 428 599-et, a haláleseteké pedig meghaladta a 14 970-et.[7]

3. A Covid-19-pandémia hatása a telemedicinára

A koronavírus-világjárvány kialakulása kezdetétől fokozott terhet ró az egészségügyi ellátórendszerek teljes spektrumára, rendkívüli igénybevételt gyakorolva szinte valamennyi erőforrás-összetevőre (finanszírozás, eszközrendszer, humán erőforrás). Az ellátandó betegek száma többszörösére növekedett az újonnan terjedő vírus okozta fertőzések következtében úgy, hogy közben a lakosság korábbi egészségügyi ellátásra vonatkozó igénye, az ellátásra váró akut és krónikus esetek száma nem csökkent. Ez a trend jellemezte a globális események kezdetét és a kronológiai folyamat felívelő szakaszát egyaránt, az ellátási igény és az ellátóképesség között gyorsan kialakuló diszkrepancia elmélyülését eredményezve világszerte, amely alól a legfejlettebb egészségügyi infrastruktúrával rendelkező országok sem jelentettek kivételt.[8]

Az egészségügyi ellátórendszerek összeomlásának megakadályozása érdekében az európai kormányok nagy része viszonylag hamar vezetett be olyan korlátozó intézkedéseket, amelyek során az elektív ellátásokat bizonytalan ideig halasztották. Tekintettel arra, hogy ezen ellátásokat a fizikai korlátozások ellenére a lakosság

[5] WHO: Coronavirus Disease Dashboard (é. n.).
[6] Tájékoztató oldal a koronavírusról. *Magyarországi koronavírus adatok.*
[7] Hungary: WHO Coronavirus Disease Dashboard. WHO (é. n.): i. m.
[8] Sonu Bhaskar et al.: Telemedicine Across the Globe-Position Paper From the COVID-19 Pandemic Health System Resilience PROGRAM (REPROGRAM) International Consortium (Part 1). *Frontiers in Public Health,* 8. (2020), 1–15.

továbbra is igénybe kívánta venni – az ellátási spektrum egy bizonyos része – amely jogszabályi keretek mellett is végezhető ebben a formában – átköltözött az online térbe. Mindezen tényezők együttesen eredményezték azt a fejlesztési boomot, amely az eHealth (távdiagnosztika és a távmonitorozás mellett az általános egészségügyi felvilágosítást, prevenciót, illetve terápiás foglalkozásokat is magában foglalja), mHealth (fenti szolgáltatások mobileszközön történő biztosítása), illetve a telemedicina-szolgáltatások területén jelenleg is zajlik.[9]

3.1. Magyarországi szabályozás

A koronavírus-világjárvány kezdetén a telemedicinára vonatkozó jogszabályi környezetet a töredezettség és jogszabályi hiányosság jellemezte. 2020 első felében hazai viszonylatban nem volt jelen az egységes törvényi szabályozás, ez sokkal inkább egyfajta szigetszerű, a telemedicinális rendszerek csak bizonyos elemeit szabályozó struktúrában valósult meg, többnyire különálló törvények és rendeletek formájában. Számos kérdés szabályozása továbbra is nyitott, azonban a pandémia következtében kihirdetésre került 157/2020. (IV. 29.) Korm. rendelet a veszélyhelyzet során elrendelt egyes egészségügyi intézkedésekről[10] már megfelelő jogalapot teremt a telemedicinális ellátás teljes spektrumának szabályozására. A rendelet kijelenti, hogy megengedett a telemedicinális szolgáltatások nyújtása, amelyek során nem szükséges feltétlenül az érintett felek személyes jelenléte. A rendelet előírja az egészségügyi szolgáltatók számára az Elektronikus Egészségügyi Szolgáltatási Térben a vizsgálat tényét és szereplőit dokumentáló eseménykatalógus-bejegyzésére, illetve egy, a vizsgálatot szakmai szempontból igazoló elektronikus kórtörténeti dokumentum feltöltésére vonatkozó kötelezettséget. Arról is rendelkezik, hogy amennyiben állapotromlás vagy akár maradandó egészségügyi károsodás veszélye merül fel, úgy a beteg távellátása megszakítandó. E mérföldkő egyértelműsíti, hogy a szakma mellett a jogalkotó is kész a kibertér – mint a betegellátás 21. századi eszköze – felé nyitni, azt törvényhozás útján, kellő jogbiztonságot teremtve támogatni és elősegíteni.[11] Mintegy kilenc hónappal később, 2021. február 10-én életbe lépett az 57/2021. (II. 10.) Korm. rendelet a veszélyhelyzet idején biztosított arcképes azonosítást lehetővé tevő videotechnológián alapuló telemedicináról. Ez a rendelet további előrelépést jelent abban a tekintetben, hogy az egészségügyi szolgáltató a telemedicina útján nyújtott egészségügyi szolgáltatásokat arcképes azonosítást biztosító, videójel és hang továbbítására alkalmas infokommunikációs eszköz útján is biztosíthatja.[12]

[9] WHO: Implementing telemedicine services during COVID-19 (2020. november 13.).
[10] 157/2020. (IV. 29.) Korm. rendelet.
[11] Fejes Zsolt – Helyes Marcell: A COVID-19 világjárvány hatása a telemedicina védelmi besorolására. *Hadmérnök,* 16. (2021), 1. 177–184.
[12] 57/2021. (II. 10.) Korm. rendelet.

3.2. Magyarországi telemedicinális alapok – Elektronikus Egészségügyi Szolgáltatási Tér

Magyarországon 2017. november 1-jén aktiválták az Elektronikus Egészségügyi Szolgáltatási Teret (EESZT), amely minden bizonnyal hosszú távú platformja lesz a telemedicinális adatszolgáltatás és adatkezelés rendszerének. Napjainkra az e-egészségügyi szolgáltató platformhoz a háziorvosi szolgálatok, a járó- és fekvőbeteg-ellátó intézmények, valamint az összes hazai gyógyszertár mellett a magán egészségügyi szolgáltatók nagy része is csatlakozott. A rendszer létrehozásának célja, hogy a lakosság gyors, hatékony és szolgáltatásorientált ellátásban részesüljön. Az egészségügyi szolgáltatást megújító rendszer működésének alapja az ellátó intézmények, a kezelést végző orvosok és gyógyszertárak közötti folyamatos elektronikus kapcsolat biztosítása, amely során az ellátás alatt keletkező írásos és képi információk digitalizált formában, online úton elérhetővé válnak minden jogosult résztvevő számára. A rendszer segítségével nyomon követhetők az ellátási utak, az elvégzett vizsgálatok, a felírt receptek, szakorvosi beutalók, és az úgynevezett eProfil. Ez utóbbi a betegre jellemző, soha, vagy csak nagyon ritkán változó adatokat összesíti annak érdekében, hogy egy esetleges sürgősségi ellátás során ezek minél hamarabb a kezelőorvos rendelkezésére álljanak. Az adatokat egy kiemelt, 5-ös biztonsági szintű rendszerben tárolják, amelyben az érintett nyomon követheti azt is, hogy ki, mikor, mely intézettől és mely adatát kérdezte le. A fejlesztések további lépései során a keletkezett leletek 5 évre visszamenőleg történő elérhetősége is biztosítottá válik.[13]

3.3. Haderőfejlesztés és digitalizáció

A Magyar Honvédség folyamatban lévő Honvédelmi és Haderőfejlesztési Programjának egyik fő eleme a Digitális Katona Program, amelynek fókuszában az ember, a katona áll. A program célja a katonai képességeknek és a katona személyének mint individuumnak a 21. századba történő átvitele, és a kor követelményeinek való megfeleltetése. A fegyverzeti és egyéb haditechnikai eszközök már zajló modernizálása mellett a digitális tartalmú elemek egy rendszerbe történő integrálása elengedhetetlen a program sikere és fenntarthatósága érdekében. A szintézis következtében valósulhat meg a feladatokban részt vevő egységek hatékony működtetése, amelynek alapja valamennyi résztvevő digitális rendszereken keresztüli – a harc megvívásához, vagy a kitűzött feladat ellátásához szükséges – információkkal történő folyamatos ellátása.[14] A teljes digitális rendszer részét képezi majd az egészségügyi modul is, amely rendszer nem más, mint egy telemedicinális platform, amely eHealth és mHealth almodulok igénybevételén keresztül működik. E rendszerek békeidős alkalmazása jelentős segítséget nyújthat a Magyar Honvédség egészségügyi szolgálata számára mindennapi betegellátási feladataiban, illetve az itt megjelenő felhasználási tapasztalatok

[13] Mi az EESZT? *EESZT információs portál.*

[14] „A Digitális Katona Program a Magyar Honvédség teljes gondolkodásmódját meg fogja változtatni" Beszélgetés dr. Böröndi Gábor altábornaggyal, a Magyar Honvédség parancsnokának helyettesével. *Honvédelem.hu,* 2021. február 15.

elősegíthetik a folyamatos fejlesztést igénylő digitális elemek naprakészen tartását, megújítását és hosszú távú, hatékony alkalmazását.

3.4. Katonaegészségügy és digitalizáció

Annak érdekében, hogy a Magyar Honvédség egészségügyi szolgálata a közeljövőben akár a Digitális Katona Program, akár egyéb más fejlesztés keretén belül telemedicinális, eHealth, mHealth rendszerek alkalmazásába kezdjen, és ezeket a hazai vagy műveleti progresszív betegellátási feladatai során hatékonyan, a betegbiztonság érdekében tudja alkalmazni, stratégiai elképzelés kidolgozására van szükség. A stratégiai alapok egyik meghatározó eleme az a gondolat lehet, hogy nem a telemedicinát kell a jelenlegi rendszerbe illeszteni, hanem valamennyi egészségügyi képességfejlesztést már most úgy kell megtervezni, hogy ezek mindegyike digitális platformon fog működni.

3.5. A Magyar Honvédség rendszerében alkalmazható telemedicina-formátumok

A Magyar Honvédség jelenlegi struktúrájába illeszthetően a telemedicinális rendszerelemek több formában is képesek lennének kiszolgálni a katonaegészségügyi képességi követelményeket Role 1 szinttől kezdődően, egészen Role 4 szintig bezárólag, békeidős körülmények között, illetve műveleti területen egyaránt. Ezek a formátumok együttes rendszerben, de akár külön-külön, moduláris jellegben, egymástól függetlenül vagy egymáshoz kapcsolt módon egyaránt alkalmazhatók. Formacsoportjai az alábbi négy kategóriába sorolhatók:

- Valós idejű *(real time)* televizit, amely audio vagy audiovizuális, „élő" kapcsolat formájában valósul meg a beteg és orvosa között.
- Telemonitorozás, amelynek során élettani paramétereket, illetve élettani funkciókkal kapcsolatos adatokat továbbítanak a beteg és orvosa között. Ez megvalósulhat real time vagy non-real time formában egyaránt (vérnyomás, pulzus-, vércukor-, testsúly adatok, aktivitásmérő vagy alváselemző programok adatainak továbbítása).
- Aszinkron *(non-real time)* televizit, amely során adatcsere zajlik orvos és beteg között úgy, hogy ez nem igényli a felek egyidejű jelenlétét az online rendszerben, de az adatcsere tartalma személy- és kórállapot-specifikus (képalkotó és/vagy labordiagnosztikai eredmények továbbítása, E-recept-felírás, beteg-útmanagement).
- Általános tájékoztatás egy-egy betegségre, kórállapotra vonatkozóan, amelynek adattartalom-iránya nem személyspecifikus (tájékoztató anyagok elektronikus továbbítása, podcastok, Gyakran Ismételt Kérdések [GYIK] információk egészségügyi szolgáltatók honlapján).
- Az adat- és információcsere egyik közös platformja a korábban már említett Elektronikus Egészségügyi Szolgáltatási Tér, amely országszerte valamennyi csapategészségügyi rendelőben, illetve az MH Egészségügyi Központ

Honvédkórház Járóbeteg Szakrendelő Intézetében, mind a fekvőbetegellátást biztosító osztályokon elérhető. A valós idejű, illetve a telemonitorozást lehetővé tevő, valamint az általános tájékoztatási formát biztosító platformok köre ugyanakkor meglehetősen tág, a kommunikáció napjainkban ezeken random kiválasztás, sokszor személyes preferencia alapján zajlik (például Skype, MS Teams, Zoom, Face Time, WhatsApp, stb).[15]

4. Javaslatok

Az elmúlt év tapasztalatait összegezve javaslatot teszünk a telemedicinális fejlesztésekhez szükséges stratégiai elképzelések szempontrendszerére vonatkozóan. A fejlesztésekhez szükséges stratégiai elképzelések általunk javasolt szempontrendszere a következő:

- A diagnosztikai és terápiás összetevők digitális platformon fognak működni.
- Az egészségügyi ellátási folyamat progresszív szemlélete változatlan marad.
- A minőségi betegellátás és a betegbiztonság elsődleges tervezési szempont.
- Erőforrás-tervezés hiányában a programok nem valósíthatók meg.
- A hatékony működtetés alapja a progresszív erőforrás-allokáció (finanszírozás, technikai háttér, humán kapacitás, működtetés).
- Külső és belső tényezők miatt erőforrás-optimalizálással folyamatosan tervezni kell.
- A szervezeti és egyéni képzések, felkészítések tervezése és végrehajtása folyamatos igény.
- A sikeres rendszerintegrálás feltétele pilot program végrehajtása.
- A program tervezése és megvalósítása alatt szükséges a programösszetevők folyamatos, egyenkénti elemzése.
- Kiemelten kell kezelni a telemedicinális lehetőségeket igénybe vevő és alkalmazó szervezet, a betegek, valamint az ellátást nyújtó orvosok és egészségügyi szakemberek számára egyaránt értéket teremtő tevékenységeket.
- Cél a standardokon alapuló működtetés, és a protokollon nyugvó egészségügyi szakellátás nyújtása.
- Szükséges a szakmai tapasztalatok rendszeres feldolgozása.

5. Összefoglalás

A több mint egy éve zajló Covid-19-világjárvány következtében – mind kínálati, mind felhasználói oldalon – jelentősen megemelkedett az igény a digitális eszközökkel, online térben végrehajtható egészségügyi szolgáltatásokra. A kormányzati törekvések, a nagy ütemű szolgáltatói fejlesztések és a felhasználói igények együttesen eredményezték

[15] Semmelweis Egyetem, Általános Orvostudományi Kar, Magatartástudományi intézet. Győrffy Zsuzsa et al.: A telemedicina lehetőségei a COVID-19 pandémia kapcsán a nemzetközi és a magyarországi tapasztalatok és ajánlások tükrében. *Orvosi Hetilap,* 161. (2020), 24. 983–992.

azt a folyamatot, amely az eHealth, mHealth és telemedicinális platformok technikai fejlődését generálja, és törekszik ezek biztonságos alkalmazására. Cikkünkben részletesen elemeztük, hogy a jelenleg ismert digitális platformokat és telemedicinális rendszereket a világjárvány idején mely területen használták fel, mely faktorok indukálták ezek fejlődését, illetve hogyan képesek ezek kiszolgálni a civil és a katonai betegellátás során felmerülő igényeket. A Magyar Honvédség Honvédelmi és Haderőfejlesztési Programjának egyik fő elemét alkotó Digitális Katona Program vonatkozásában rámutattunk azokra az illeszkedési pontokra, amelyek a katonai orvosszakmai, illetve a katonai műveleti oldalról támasztott követelmények alapján kapcsolatot jelentenek a haderőfejlesztési program és a már alkalmazásban lévő telemedicina-rendszerek között. Ezen pontok elemzése rámutatott arra, hogy a Magyar Honvédség jelenlegi struktúrájába illeszthetően a telemedicinális rendszerelemek több formában is képesek lennének kiszolgálni a katonaegészségügyi képességi követelményeket Role 1 szinttől Role 4 szintig, mind békeidőben, mind műveleti körülmények között. Az elmúlt év tapasztalatai alapján összegeztük a fejlesztésekhez nélkülözhetetlen stratégiai szempontokat. A stratégiai alapok egyik meghatározó eleme az a felismerés, hogy nem a telemedicinát kell a jelenlegi rendszerbe integrálni, hanem a mutatkozó trendek alapján elfogadni azt a gondolatot, hogy megkezdődött az a folyamat, amelynek eredményeként hamarosan valamennyi egészségügyi képesség digitális platformon vagy annak segítségével fog működni.

Felhasznált irodalom

AJMC The American Journal of Managed Care: *A Timeline of COVID-19 Developments in 2020* (2021. január 1.). Online: www.ajmc.com/view/a-timeline-of-covid19-developments-in-2020

Bhaskar, Sonu – Sian Bradley – Vijay Kumar Chattu – Anil Adisesh – Alma Nurtazina – Saltanat Kyrykbayeva – Sateesh Sakhamuri – Sanni Yaya – Thankam Sunil – Pravin Thomas et al.: Telemedicine Across the Globe-Position Paper From the COVID-19 Pandemic Health System Resilience PROGRAM (REPROGRAM) International Consortium (Part 1). *Frontiers in Public Health,* 8. (2020), 1–15. Online: https://doi.org/10.3389/fpubh.2020.556720

„A Digitális Katona Program a Magyar Honvédség teljes gondolkodásmódját meg fogja változtatni" Beszélgetés dr. Böröndi Gábor altábornaggyal, a Magyar Honvédség parancsnokának helyettesével. *Honvédelem.hu,* 2021. február 15. Online: https://honvedelem.hu/hirek/a-digitalis-katona-program-a-magyar-honvedseg-teljes-gondolkodasmodjat-meg-fogja-valtoztatni.html

Fejes Zsolt – Helyes Marcell: A COVID-19 világjárvány hatása a telemedicina védelmi besorolására. *Hadmérnök,* 16. (2021), 1. 177–184. Online: https://doi.org/10.32567/hm.2021.1.11

Győrffy Zsuzsa – Békási Sándor – Szathmári-Mészáros Noémi – Németh Orsolya: A telemedicina lehetőségei a COVID-19 pandémia kapcsán a nemzetközi és a magyarországi tapasztalatok és ajánlások tükrében. *Orvosi Hetilap,* 161. (2020), 24. 983–992. Online: https://doi.org/10.1556/650.2020.31873

WHO: *Coronavirus Disease Dashboard.* (é. n.). Online: https://covid19.who.int/?gclid=EAIaIQobChMIxof_ndn97gIVAbayCh1XeAlcEAAYASAAEgLsdPD_BwE
WHO: *Implementing telemedicine services during COVID-19* (2020. november 13.). Online: https://iris.wpro.who.int/bitstream/handle/10665.1/14651/WPR-DSE-2020-032-eng.pdf
WHO: *Telemedicine Opportunities and developments in Member States.* Global Observatory for eHealth series – Volume 2 (2010). Online: www.who.int/goe/publications/goe_telemedicine_2010.pdf
Mi az EESZT? *EESZT információs portál.* Elérhető: https://e-egeszsegugy.gov.hu/mi-az-eeszt-

Jogi források

157/2020. (IV. 29.) Korm. rendelet a veszélyhelyzet során elrendelt egyes egészségügyi intézkedésekről. Online: www.kozlonyok.hu/nkonline/index.php?menuindex=200&pageindex=kozltart&ev=2020&szam=91
57/2021. (II. 10.) Korm. rendelet a veszélyhelyzet idején biztosított arcképes azonosítást lehetővé tevő videotechnológián alapuló telemedicináról. Online: https://net.jogtar.hu/jogszabaly?docid=A2100057.KOR&dbnum=1

HADMÉRNÖK
FÓRUM

16. évfolyam (2021) 3. szám 229–243.
DOI: 10.32567/hm.2021.3.14

Zsákai Zsolt[1]

Az emberi csípő, térd és gerinc biomechanikai jellemzői, valamint terhelés hatására létrejött elváltozásainak áttekintő elemzése

1. rész: A csípőízület biomechanikája

An Overview of the Biomechanical Characteristics of the Human Hip, Knee and Spine, as well as the Changes Caused by Exercise

Part 1: Biomechanics of the Hip Joint

Tanulmányomban, amely egy szélesebb kutatás része, a haderő aktív állományának mozgásszervi terhelését és az annak következtében kialakuló panaszokat vizsgálom, a nemzetközi szakirodalomban fellelhető hasonló kutatások áttekintésével. Cikksorozatom első része a csípőízülettel, annak biomechanikai összefüggéseivel, a terhelés következtében fellépő erőhatásokkal és azok következményeivel foglalkozik. A csípőben kialakuló terhelési viszonyok bemutatásával látható, hogy még egészséges, normál anatómiájú csípő esetén is jelentős terhelés esik az ízület porcára. A túlterheléssel, az ízület anatómiai eltéréseinek következtében vagy ezek együttes hatására a panaszok nagyobb valószínűséggel alakulnak ki.

Kulcsszavak: csípőízület, biomechanika, túlterhelés, anatómia, haderő, katonaság

In my study, I examine the musculoskeletal loading and subsequent complaints of the active members of the armed forces by reviewing similar studies in the international literature. The first part of my series of articles describes the hip joint, its

[1] Borsod-Abaúj-Zemplén Megyei Központi Kórház és Egyetemi Oktató Kórház, főorvos, e-mail: zsakaizsolt@zsakaizsolt.com

biomechanical relationships, the forces developing due to loading and their consequences. By presenting the loading conditions in the hip joint, it can be seen that even in the case of a healthy hip joint with normal anatomy, a significant load falls on the cartilage of the joint. In case of overload, due to anatomical abnormalities in the joint or due to their additive effect, complaints are more likely to develop.

Keywords: **hip joint, biomechanics, overload, anatomy, force, military**

1. Bevezetés

Doktori kutatásom az aktív katonai állomány tagjai közt megjelenő mozgásszervi problémákat vizsgálja. E kutatás részeredményeit szeretném megosztani jelen cikkemben, amely a csípőízület túlterhelésével járó következményeket elemzi, egy szélesebb spektrumú irodalmi szemlézés formájában. Írásomban a csípőízületünk anatómiai, biomechanikai jellemzőit is bemutatom, amelyek megértésével nyilvánvalóvá válik az ízület túlterhelésének problémája, azonban hangsúlyozni szeretném, hogy e fejezetekben csak az elengedhetetlenül szükségesnek ítélt anatómiai és biomechanikai információkat taglalom. Jelen írásom nem ezen összefüggések részletes felfedését hivatott elvégezni, azonban a továbbiak megértéséhez, illetve az összefüggések megfelelő módon történő átlátásához, valamint a következtetések elfogadásához elengedhetetlen bizonyos ismeretek megléte. Szintén nem cikkem tárgyköre a csípőízületet érintő betegségek széles körű bemutatása, azonban néhányról említést kívánok tenni, valamint a kutatásom egyik hipotézisét[2] érintő betegségről, a csípőízületi beütődéses kórképről kissé részletesebben is szeretnék információt közölni, irodalmi utalásokkal alátámasztva fontosságát.

2. A csípőízület anatómiája

A csípőízület *(articulatio coxae)* gömb vagy szabad ízületnek nevezett biomechanikai és anatómiai egység. Csontosan az ízvápa *(acetabulum)* és ízfej *(caput femoris)* alkotja. Az ízvápa porca egy C alakú területen helyezkedik el, míg az ízfej nagy része porccal fedett. Az ízvápa szélét egy 5-6 mm vastag, rostos porc gyűrű, a *labrum acetabuli* veszi körül, amelynek a későbbiek taglalásánál látjuk jelentőségét. Az ízület érdekessége, hogy a fej mindennemű szalag és egyéb rögzítés nélkül is bent marad a vápában. Természetesen ízületi tokkal rendelkezik, mint minden ízület, amelyet szalagok borítanak. Ezekből hármat ismerünk: *ligamentum iliofemorale,* amely egyébként a test legerősebb szalagja, *ligamentum pubofemorale* és *ligamentum ischiofemorale.* Érdekességük, hogy mind a három szalag elölről lefelé és hátulról felfelé csavarodik a combcsont nyakára.

[2] Kutatásom egyik hipotézise: „Feltételezem, hogy a csípőízület degeneratív megbetegedése – hasonlóan, a többi degeneratív megbetegedésekhez – nagyobb valószínűséggel jelenik meg az aktív, szolgálatot teljesítő állomány körében."

A negyedik szalag az ízületen belül elhelyezkedő *ligamentum capitis femoris,* amelynek jelentősége – az élet egy szakaszán – a vérellátásban keresendő.[3]

A csípő mozgását az 1. táblázatban feltüntetett izmok végzik.

1. táblázat
A csípő mozgatását végző izmok
Forrás: a szerző szerkesztése

Belső csípőizmok	**Külső csípőizmok**	**A comb közelítő izmai (adductorok)**
musculus iliopsoas	musculus gluteus maximus	musculus pectineus
musculus piriformis	musculus gluteus medius	musculus adductor longus
musculus obturator internus	musculus gluteus minimus	musculus adductor brevis
	musculus tensor fascia latae	musculus gracilis
	musculus quadratus femoris	musculus adductor magnus
	musculus obturator externus	
	musculus gemellus superior	
	musculus gemellus inferior	

A csípő biomechanikai elemzéséhez elsőként érdemes megismerkedni pár fogalommal annak érdekében, hogy értelmezni tudjuk az ízület mozgását és meg tudjuk ítélni, érteni a normálistól eltérő, kóros mozgások jelentőségét, illetve az abból eredő hátrányokat.

Konstrukciós tengely: A combfej középpontja és a felső ugróízület belső egyharmadát jelölő pontot összekötő tengely, amelynek közbeiktatott pontja a térdkalács ín tapadási területe. *(tuberositas tibiae)*

Rotacio: forgómozgás

Abductio: a test középvonalától elfelé tartó mozgás

Adductio: a test középvonala felé tartó mozgás

Flexio: hajlító mozgás

Extensio: feszítő mozgás

Circumductio: a csípőízületben meglévő mozgások, egymással kombinált, kúppalástot leíró mozgásformája

Sagittalis: nyílirányú

Collodiaphysealis szög: a combcsont teste és nyaka közti szög.[4] Az életkor előrehaladtával változik. Felnőtt korban jellemzően 135°, de idős korra 120°-ra lecsökken.[5]

[3] Szentágothai János – Réthelyi Miklós: *Funkcionális anatómia.* 1. kötet. Budapest, Medicina–Semmelweis, 1996. 365–366.

[4] A collodyaphysealis szög (CD szög) az életkor változásával alakul ki. Felnőtt korra jellemző értéke kb. 135–138°. Idős korra 120°-ra csökken. A CD szög normálistól való eltérése, kisebb *(coxa vara)* vagy nagyobb *(coxa valga)* mértékben jelentősen megváltoztatja a csípőízület biomechanikáját, ezáltal a degeneratív betegségek kialakulását fokozza.

[5] Szendrői Miklós (szerk.): *Ortopédia*. Budapest, Semmelweis, 2005. 342.

3. A csípőízület biomechanikája

A combfejek középpontját összekötő haránttengely körül valósulnak meg csípőnk mozgásai: a hajlítás *(flexio)* és nyújtás *(extensio),* a nyílirányú *(sagittalis)* tengely körül a távolítás *(abductio)* és a közelítés *(adductio),* a konstrukciós tengely körül a csavarodó mozgás (*ki-*, és *berotatio*). A normál mozgástartományokat a 2. táblázatban foglaltam össze.

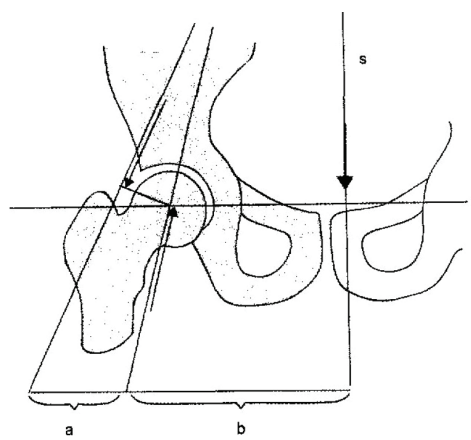
2. táblázat

A csípőízület normál mozgástartományai

Forrás: a szerző szerkesztése Szendrői (szerk.) (2005): i. m. 342. alapján

flexio	0°–130°/140°
extensio	0°–10°
abductio nyújtott csípőnél	0°–30°/45°
abductio 90 fokban hajlított csípőnél	0°–80°
adductio	0°–20°/30°
kifelé rotatio nyújtott csípőnél	0°–30°/40°
kifelé rotatio 90 fokban hajlított csípőnél	0°–40°/50°
befelé rotatio nyújtott csípőnél	0°–40°/50°
befelé rotatio 90 fokban hajlított csípőnél	0°–30°/45°

A csípőízületre ható erőket a pauwelsi[6] biomechanikai rendszer szemlélteti, amit az 1. ábrán mutatok be.



1. ábra

Normális collodiaphysealis szög esetén a teher- és az erőkararány

Forrás: Szendrői (szerk.) (2005): i. m. 343.

a: erőkar; b: teherkar S: súlyvonal. A normál CD szöghöz tartozó teherkar- és erőkararány: 3 : 1 (b: a).

[6] Friedrich Pauwels (1885–1980): a német biomechanika egyik legnagyobb alakja. Munkássága jelentőségét bizonyítja, hogy elnyerte az ortopédia tiszteletbeli professzora címet is. Munkája nagy mértékben hatással volt a modern biomechanikai szemléletek kialakulására.

Tulajdonképpen a fentebb említett mozgásokból adódik össze csípőízületünk helyváltoztató mozgáshoz szükséges komplex működése, amelynek következtében, állás, járás, ugrás és futás tevékenységek váltogatásával érjük el azt, hogy képesek vagyunk eljutni „A" pontból „B" pontba. Az állás és járás az emberi élet minden területén fontos tevékenység, amit koordinált, mozgásszervileg bonyolult izomműködéssel és biomechanikával jellemezhető módon végzünk mindennapjainkban. Bár maga az állás és járás folyamata egyáltalán nem írható le könnyen biomechanikailag, mégis, bizonyos értelemben egyfajta alapfunkcióként tekinthetünk erre a két tevékenységre.

Vizsgáljuk is meg kicsit részletesebben ezeket. A csípőízület mozgása közben, az alsó végtagokat feloszthatjuk egy támaszkodó és egy lengő végtagra, amely végtagok változó szerepben biztosítják haladásunkat. Amíg a lengőoldali végtag ebben a fázisban van, addig a teljes terhelés a támaszkodó végtagra esik, elviselve a gravitációs erő hatását, a törzs súlyát. A lendítő oldali medencefél lebillenését a csípőízület abductor izomzata biztosítja, ez később fontos összefüggéseket tár fel a térdízületünk vonatkozásában is, illetve a gerinc biomechanikájában is változást okoz egy, a csípő abductor izomzatát érintő izomgyengeség. Csípőnk a kétkarú emelő elve alapján működik, ahol az egyensúlyi helyzetben az

$$\text{erő} \times \text{erőkar} = \text{teher} \times \text{teherkar}$$

egyenlet érvényesül. Az erőkar (a) a csípőközpont és az egyensúlyi helyzetet létrehozó abductorok erővektorának vízszintesre vetített távolsága, a teherkar (b) pedig a súlyvonal–csípőközpont távolság vetülete, amely normális anatómiai viszonyok mellett 3 : 1 arányban viszonyul egymáshoz.[7] A kétkarú emelő forgáspontja maga a csípőízület. A számítás alapján egy 70 kg-os ember esetén például a csípőre 280 kg terhelés jut. Könnyű belátni, hogy megváltozott, a normálistól eltérő anatomiájú csípőízület esetén ez a terhelés a sokszorosára is emelkedhet, ami elhasználódásos *(degeneratív)* folyamatok kialakulásához vezet.[8]

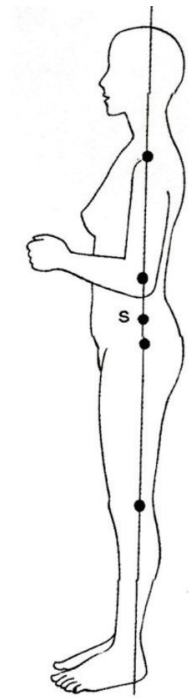
4. Állás és járás

Állás közben a test látszólagos nyugalomban van, a két alsó végtagra támaszkodik, a talpakra helyezve a test súlyát. Nyugodt testtartás mellett a súlyvonal (2. ábra) a külső hallójárat közepétől indul ki, majd a váll-, csípő- és térdízületen keresztül éri el a támaszkodási felszínt. Ennek ismerete azért fontos, mert az ettől eltérő súlyvonal megjelenése a normálishoz képest nagyobb izommunkát igényel. Tulajdonképpen álló testhelyzetben az izomműködés stabilizációja következtében a testünk állandó, kis mértékű mozgást végez izommunka felhasználásával. Az izommunka testtartástól függő tényező. Katonás vigyázzállás esetén mintegy 20%-kal több energia szükséges,

[7] Damien P. Byrne – Kevin J. Mulhall – Joseph F. Baker: Anatomy and Biomechanics of the Hip. *The Open Sports Medicine Journal,* 4. (2010), 1. 51–57.

[8] Szendrői (szerk.) (2005): i. m. 342.

mint könnyed testhelyzet felvétele esetén, sőt ernyedt testhelyzetben is körülbelül 10%-os energiafelhasználás történik az állás biztosítása céljából.[9]



2. ábra
A test normál súlyvonala állás közben
Forrás: Szendrői (szerk.) (2005): i. m. 28.

S: súlypont

Járásunk teszi lehetővé, hogy helyváltoztató életmódunk legyen, amely folyamán az alsó végtagok váltakozó mozgása révén mozdul el a test a kívánt irányba. Alsó végtagjaink mellett a fej, a törzs, a felső végtagok összehangolt mozgása is szerepet játszik a járástípus kialakulásában. Nagy vonalakban elmondható, hogy a járás mindig a stabil és stabilitását vesztett egyensúlyi helyzetek váltakozása révén ölt formát. A járás alapja a lépés, amelyet, ha objektíven szeretnénk leírni, akkor a lépéshosszt és a lépésidőtartamot kell használjuk annak jellemzésére. A lépés két szakaszból áll: támaszkodási és lengési fázis. A ciklusidő hozzávetőleg 60% támaszkodási és 40% lengési időre osztódik fel. A három szakaszra bontható támaszkodási fázis a következő folyamatokból tevődik össze: saroktámasz, gördítés, elrugaszkodás. A lengési fázis végtagrövidülés és végtaghosszabbodás szakaszaiból áll. A járás során egy lépés alatt két kettős támasz és két egyes támasz van, azaz kétszer van olyan periódus,

[9] Szendrői (szerk.) (2005): i. m. 27–29.

amelynél az egyik végtag még, a másik pedig már támaszkodik. A későbbiek megértése szempontjából fontos, hogy gyors járásnál a kettős támasz időtartama jelentősen lecsökken, futásnál pedig megszűnik. Járás során, annak megfelelő kivitelezésénél a medence, a csípőízület, a térdízület és a bokaízület is szerepet játszik. Mindenre kiterjedően ezen ízületek vizsgálata meghaladja a cikk témáját, de a csípőízület vonatkozásában szükséges kitérni e biomechanikai összefüggésekre a könnyebb érthetőség kedvéért.[10]

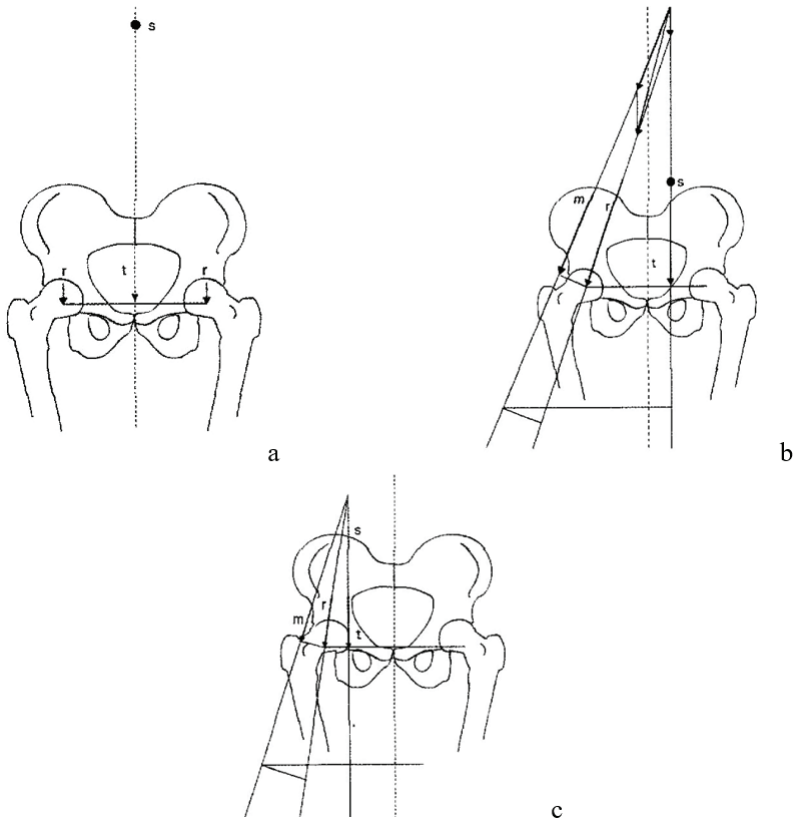
A csípőízületben saroktámasznál 30–40 fokos flexio van jelen, majd fokozatosan extendálódik az ízület, amelynek végén teljes extensio következik be az elrugaszkodási fázis előtt, majd fokozatos flexio kezdődik, a saroktámaszig. A térdízületben a flexio fokozatosan extensióba megy át, majd a végextensiónál, amely a másik oldali láb saroktámaszát jelenti egyben, gyors flexio következik ismét.[11]

Ha megértettük a járást és állást mint alapvető alsó végtagi mozgást, akkor számos további érdekes szempont alapján vizsgálhatjuk, boncolgathatjuk a folyamatot. Születtek tanulmányok, amelyekben a szerzők többek között a nemi különbségekből adódó eltéréseket is vizsgálták. Azt találták, hogy a női láb – általában – kisebb volta miatt a sarok–lábközép–lábujj érintkezése a járás állási fázisában a talaj–láb érintkezési idő összehasonlításában eltérő a férfi lábbal összehasonlítva.[12]

Az ízületek mozgását az azokat mozgató izmok biztosítják, így érdemes kitérni a csípőízület mozgását véghez vivő izmok működésére is. A csípőízületben a *gluteus maximus* (a nagy farizom) a támaszkodási fázis elején működik, az abductorok működése szükséges a medence stabilizálásához. Ha a test súlypontja a lengő oldal felett van, akkor az abductoroknak kifejezetten nagy erőre van szükségük a medence stabilitásának megőrzéséhez, és ellentétesen: ha a támaszkodó oldal felett van a törzs súlypontja, akkor kisebb izomerő is elég a medence stabilizálásához. Kettős támasznál egyenletesen oszlik el a két csípőízület felett a törzs súlya. Az adductorok a sarok támaszkodásánál és az elrugaszkodás után működnek. A flexorok a lengési szakasz kezdetén aktívak. A térdízületben a m. *quadriceps* feladata a sarokra érést követően kezdődik, majd nincs aktivitása, amikor a támaszkodó végtag felett van a testsúly, azonban ismét aktiválódik a támaszkodási fázis végén. A comb flexorok aktivitása a lengőfázis végén és a támaszkodási fázis elején figyelhető meg.[13]

A csípőízületre ható erők a következőképpen alakulnak, ha a támaszkodó és a lengő végtag felett van a test súlypontja. A csípőízületre, annak szövetére, különösképpen a porc és a porc alatti csontszövetre ható mechanikai faktorok mind hatással vannak az ízületre (3. ábra).

[10] Szendrői (szerk.) (2005): i. m. 29–30.
[11] Szendrői (szerk.) (2005): i. m. 30.
[12] Richard C. Nelson – Chaunsey A. Morehouse (szerk.): *Biomechanics IV*. Baltimore, Maryland USA, Macmillan Education, 1974. 85–90.
[13] Nelson–Morehouse (szerk.) (1974): i. m. 30–31.



3. ábra

Súlyeloszlási viszonyok

Forrás: Szendrői M (szerk.) (2005): i. m. 31.

a: a test súlyának eloszlása kettős alátámasztás esetén

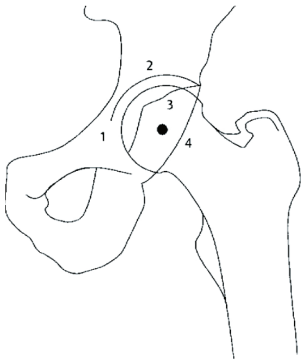
b: a nyomóerő, ha a test súlypontja a lengő végtag felett van

c: a nyomóerő, ha a test súlypontja a támaszkodó végtag felett van

S: a törzs súlypontja; t: testsúly; r: a femur fejre ható nyomás; m: abductor izomerő. b: a lengő oldal felett ható testsúly a hosszú erőkar miatt nagyobb abductor izomerőt kíván a medence lebillenésének megakadályozása érdekében. c: a támaszkodó végtag felett ható testsúly a megrövidült erőkar miatt kisebb abductor izomerőt tesz szükségessé a medence stabilitásához. Járás és egy lábon állás közben hasonlóan alakulnak ezek az erők és erőkarok.

Az ízület alakját legjobban a gömbízületi forma jellemzi, ahol a combcsont feje kongruens az ízületi vápával. Röntgenfilmen könnyű a combcsont fejének kontúrját felismerni, amelynek középpontja egyben az ízület rotációs központja is (4. ábra). A röntgenen látható ízületi vápa és fej kontúrja közti területen található a porcszövet, amely terület felezéspontjában van a tényleges ízületi felszín.[14]

[14] Paul Brinckmann – Wolfgang Frobin – Gunnar Leivseth: *Musculoskeletal Biomechanics*. Stuttgart – New York, Thieme, 2002. 78–79.



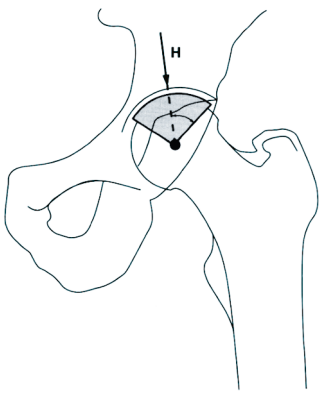
4. ábra

A röntgenfilmen fellelhető csípőízületi kontúrok

Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 79.

1: a csontos femur fej; 2: az acetabulum cranialis conturja; 3: az acetabulum elülső pereme; 4: az acetabulum hátulsó pereme

A terhelő felszín megközelítőleg egy félgömbnek hat a modell alapján, azonban az ízületi vápa peremének alakja miatt igazából kisebb, mint egy félgömb. Kummer, vizsgálata alapján, azt találta, hogy a félhold alakú terhelési felszín szögben kifejezve kétszerese az erővektor és a vápa külső pereme közti szögnek[15] (5. ábra).



5. ábra

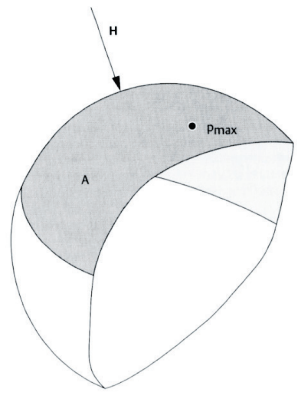
A félhold alakú terhelési felszín kivetülése

Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 80.

H: ez a nyíl mutatja meg a nyomóerő kivetülési pontját. A sötétszürke rész mutatja a teherviselő felszín kivetülését, amely az acetabulum lateralis sarka és a nyomóerő kivetülési pontja közti távolság duplája.

[15] Benno Kummer: Die Beanschpruchung des menschlichen Hüftgelenks. I Allgemeinen Problematik. *Zeitschrift für Anatomie und Entwicklungsgeschichte,* 127. (1968), 4. 277–285.

Brinckmann és munkatársai kimutatták, hogy a csípőízületben fellépő nyomás a 6. ábrán látható helyen terheli az ízületet.[16] A nyomási maximum pedig, a vápa külső peremének elhelyezkedésétől, a terhelési erő nagyságától, a combcsont fejének sugarától, valamint a terhelési erővonal és a perem relatív elhelyezkedésétől függően valahol a perem és a nyomási erő vektorának kivetülési pontja közt helyezkedik el.[17]



6. ábra

A terhelési felszín sematikus ábrája a maximális nyomási pont feltüntetésével

Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 80.

A: terhelési felszín; H: a terhelési vektor; p_{max}: a maximális nyomáspont helye. Látható, hogy a maximális nyomáspont elhelyezkedése a nyomóerő kivetülési pontjától lateralis irányba az acetabulum felső pereme felé tolódik.

Szintén Brinckmann és munkatársai munkájából tudjuk, hogy különböző csípőízületi fedettség esetén máshol és más erőnagysággal van jelen a porcra ható nyomás. Az emberi csípőízületre jellemző helyre eső maximális nyomást mutató pont a 130°-os fedettségnél látható. Természetesen ezt a 180°-os fedettséggel összevetve érdemes vizsgálni, ahol a félgömb centrumában hat a maximális nyomás. További értékeket vizsgálva, a fedettségi szöget csökkentve azt kapták, hogy 110°-nál már konkrétan a vápa peremére helyeződik át ez a nyomásmaximum.[18] Ez pedig nagyon fontos szerepet tölt be a csípőízület terhelése és terhelhetősége szempontjából. Ebből könnyű következtetni arra, hogy nem megfelelő fedettség esetén a csípőízületre jellemző nyomáspont eltérő lehet, ami az ott lévő porc károsodását felgyorsíthatja, ezzel degeneratív betegségek talaját képezheti, panaszok megjelenését indukálhatja.

[16] Paul Brinckmann – Wolfgang Frobin – E. Hierholzer: Stress on the articular surface of the hip joint in healthy adults and persons with idiopathic osteoarthrosis of the hip joint. *Journal of Biomechanics,* 14. (1981), 3. 149–156.

[17] Brinckmann–Frobin–Leivseth (2002): i. m. 81.

[18] Paul Brinckmann – Wolfgang Frobin – E. Hierholzer: Belastete Gelenkflache und Beanschpruchung des Hüftgelenks. *Zeitschrift für Orthopädie und Unfallchirurgie,* 118. (1980), 1. 107–115.

5. A csípőízület túlterhelése a szakirodalomban

A biomechanikai és anatómiai összefüggéseket megismerve és megértve nyilvánvalóbbá válik azon folyamatok fontossága, amelyek a csípőben túlterhelést okozhatnak.

A csípőízületben számos betegséget fel lehet sorolni, amelyek a normál biomechanikai viszonyokat megváltoztatva átalakítják a terhelést, túlterhelve az ízületet. A látványos betegségek közt, mint a balesetek következtében kialakult anatómiai eltérések, gyulladások okozta deformációkon, daganatok csontot és ízületet érintő roncsolásán kívül, vannak kevésbé nyilvánvaló és látványos betegségek is. Ilyenek – a teljesség igénye nélkül – például a gyermekkori combfej-növekedési fuga elcsúszása *(epiphyseolisis capitis femoris)* és a csípőízületi beütődéses kórkép *(impingement coxae),* amely utóbbi tudományos vizsgálatom tárgyát is képezi.

Az *impingement coxae* három formájának – a CAM,[19] a PINZER[20] és a KEVERT[21] típus – jelenléte hagyományos *(anteroposterior)* röntgenfelvétellel is megállapítható, speciális röntgen jelek, mint az ülőtövis *(spina ischiadica)* jel,[22] a hátsó fal jel,[23] a kereszteződési tünet,[24] az ellapult fej és a pisztolymarkolat deformitások[25] alapján. A betegség fontosságát az adja, hogy az átlag populatióban vizsgálva magas arányban találtuk ezen elváltozás valamelyik formáját azoknál, akiknél csípőkopás miatt protézisműtét vált indokolttá. Az esetek 88%-ában jelen voltak a betegségre jellemző röntgentünetek, míg a kontrollcsoportnál ez csupán 8,8%-nak adódott.[26] A már említett kutatásom egyik hipotézise, hogy az aktív szolgálatot teljesítő katonák esetén is magas arányban találunk ilyen elváltozást, amely a megnövekedett terheléssel együtt szerepet játszik a panaszok kialakulásában. A nemzetközi irodalom áttekintése során megerősítést találtam feltevésem igazolhatóságára, kutatásom létjogosultságára.

Harrison és munkatársai írták le először a porc degeneratív elváltozását már kezdődő porckopásban *(arthrosis)* is.[27] Pawels vizsgálatai után megállapította, hogy az ízületi nyomásviszonyok – különösen a vápa peremének környékén – nagy szerepet játszanak az ízület arthrosisának kialakulása szempontjából.[28] Radin és munkatársai kimutatták, hogy az ízületi túlterhelés miatt első lépcsőben a porc alatti trabecularis csont elváltozása következik be, a megjelenő mikrotörések *(microfractura)* miatt, amelynek gyógyulási folyamatai ugyanezt a régiót megerősítik.[29]

[19] A combfej-nyak átmenetben lévő felrakódások következtében kialakult forma.
[20] Az ízületi ajakporc *(labrum)* elmeszesedése, csontosodása, károsodása következtében kialakult forma.
[21] A fenti kettő együttes megjelenését magában hordozó forma.
[22] A *spina ischiadica* (ülőtövis, az ülőcsont egy nyúlványa) háromszög alakban bevetül a medencebemenetbe.
[23] Az ízületi perem hátulsó része, a hátulsó fal vonala, a combfej középpontjához viszonyítva medialisan helyezkedik el.
[24] Az ízületi perem elülső falának vonala fejvégi helyzetben *(cranialisan),* a hátulsó fal vonalához képest kívülre esik, míg a farokvég részen *(caudalisan)* belülre, ezáltal a röntgenen egymást keresztezve vetülnek.
[25] A combcsonti fej–nyak átmenet anatómiai görbülete kiegyenesedik a csontos felrakódások következtében.
[26] Zsákai Zsolt et al.: Primer arthrosisok retrospectív vizsgálata anteroposterior medence felvételek alapján. – A Femoroacetabularis impingement okozta arthrosis. *Magyar Radiológia,* 2015. július 11.
[27] M. H. M. Harrison – F. Schajowicz – J. Trueta: Osteoarthritis of the hip: a study of the nature and evolution of the disease. *The Journal of Bone and Joint Surgery,* 35B. (1953), 4. 598–625.
[28] Friedrich Pauwels: *Biomechanics of the Locomotor Apparatus.* New York, Springer, 1980.
[29] Eric L. Radin – Igor L. Paul – Marc J. Tolkoff: Subchondral bone changes in patients with early degenerative joint disease. *Arthritis & Rheumatology,* 13. (1970), 4. 400–405; Eric L. Radin et al.: Response of joints to impact loading – III: Relationship between trabecular microfractures and cartilage degeneration. *Journal of Biomechanics,* 6. (1973), 1. 51–57.

Látható, hogy az ízületi nyomásviszony és annak változása milyen negatív hatású az ízületekre, köztük a csípőízületre is. Ennek megértése fontos, hiszen megnövekedett terhelés esetén komolyan figyelembe kell vegyük azokat az elváltozásokat, amelyek vagy az anatómiai, vagy a biomechanikai viszonyok miatt jelen vannak az egyénben, és a panaszok kialakulásában is nagy szerepet játszhatnak.

Az aktív katonai szolgálatot teljesítők vonatkozásában a mozgásszervi megbetegedések vizsgálatát elemző hazai szakirodalom nem áll rendelkezésre. Nemzetközi irodalomban természetesen találhatunk ilyen jellegű vizsgálatokat, de még azok közt is nagy számban vannak jelen az olyan tanulmányok, amelyek analógiát vonnak az aktív katonai szolgálat és az egyéb fokozott megterheléssel járó populatiók, mint például a professzionális sportolók megterhelése közt. Kizárólagosan a katonai állományt vizsgáló nemzetközi írás lényegesen kevesebb számban található, és azok hivatkozásaiban is fellelhető a fenti analógia.

Cameron és munkatársai az Amerikai Egyesült Államok Hadseregének aktív állományában előforduló degeneratív ízületi kopás incidenciáját vizsgálták. Azt találták – nagy esetszámot vizsgálva –, hogy a degeneratív ízületi kopások nagyobb százalékban fordultak elő az aktív katonai állományban, mint a vizsgálat során összehasonlított átlag populatióban. Tanulmányuk szerint a megnövekedett kor, az aktív katonai szolgálat, a női nem, az afroamerikai rassz mind összefüggésben van az osteoarthritis megnövekedett incidenciájával.[30] Scher és munkatársai szintén leírták, hogy az aktív szolgálatot teljesítő állományban a női nem, az afroamerikai rassz, a 40 év vagy annál magasabb életkor, a rangidős tiszti rang és a katonai szolgálat, különösen a haditengerészet, tengerészgyalogság állományában, jelent nagyobb rizikótényezőt mozgásszervi betegségek viszonylatában.[31] Jochimsen és munkatársai szerint a veterán katonai populatiónál kialakult arthrosis nagyobb százalékban azonosítható a csípő ütközéses kórképe következményének, mint a civil lakosság körében.[32] Javasolták további vizsgálatok elvégzését, amelyekkel azt vizsgálják, hogy vajon az időben elvégzett arthroscópos beavatkozással megelőzhetővé, vagy késleltethetővé válik-e az aktív populatióban az arthrosis kialakulása, illetve a kórkép kifejlődése.

Az irodalmi utalásokban több helyen feltűnik az arthroscopia (ízületi tükrözés) mint műtéti technika fogalma. Magyarázatként szeretném kifejteni, hogy ezen eljárásnak napjainkban a diagnosztikai értékén kívül jelentős terápiás szerepe is van, mert a technika alkalmazása során számos elváltozást definitíve kezelni tudunk. Néhány ilyen lehetőség: a levált porc eltávolítása, művi microfractura[33] elvégzése, labrum (ajakporc) visszavarrása. Az arthroscópos műtét előnye többek közt a szervezet és a szövetek számára fellépő, jelentősen kisebb megterhelés, a szövődmények kockázatának

[30] Kenneth L. Cameron et al.: Incidence of Physician-Diagnosed Osteoarthritis Among Active Duty United States Military Service Members. *Arthritis & Rheumatology,* 63. (2011), 10. 2974–2982.

[31] Danielle L. Scher et al.: The Incidence of Primary Hip Osteoarthritis in Active Duty US Military Servicemembers. *Arthritis & Rheumatism,* 61. (2009), 4. 468–475.

[32] Kate N. Jochimsen et al.: Femoroacetabular impingement is more common in military veterans with end-stage hip osteoarthritis than civilian patients: A retrospective case control study. *Military Medical Research,* 6. (2019), 1. 27.

[33] Microfractura során a körülhatárolt porcdefektus területén lévő csontkéregállomány átütése történik, amelynek következménye, hogy a kiszivárgó csontvelőben lévő őssejtek képesek lehetnek rostosporc kialakítására.

csökkenése, a rehabilitációs idő lerövidülése, aminek pedig következménye az újbóli hadrendbe állíthatóság várakozási idejének csökkenése.

Blank és munkatársai a csípőtájéki fájdalmakat vizsgálva állapították meg, hogy az aktív katonai szolgálat, a női nemhez való tartozás és a magasabb életkor megnövekedett rizikófaktort jelentenek a degeneratív csípőtájéki fájdalom kialakulásában.[34] Gwatmey és munkatársai a csípő impingement és a túlterheléses csípőbetegségek megnövekedett előfordulását írja le az aktív katonai állományban. Terápiás lehetőségként említi a csípőízület tükrözését mint definitív megoldást ezen esetekben, amely után a csípő terhelhetősége javul és a szolgálat ismét felvehetővé válik.[35] Dutton és szerzőtársai is azt jelentették, hogy a csípő arthroscopia effektív megoldásnak számít az aktív, a csípőízület bizonyos megbetegedéseivel küzdő katonai állomány esetében, valamint a műtét ráadásul lehetővé teszi a szolgálat további folytatását.[36] Yoo és munkatársai egy kisebb esetszámot vizsgáló tanulmányban azt közölték, hogy a csípő arthroscopia eredményessége a katonai populatiót vizsgálva hasonló, mint a civil populatio esetén. A kórházban eltöltött időt többnek találták a civil lakosság kórházban töltött idejéhez képest, azonban az aktivitáshoz való teljes visszatérés hasonlónak mutatkozott.[37] Kuhn és munkatársai azt vizsgálták, hogy a csípőízületi vápa biomechanikai eltérése esetén milyen valószínűséggel alakulnak ki panaszok az érintett csípőben, valamint hogy ez milyen relációban van az ütődéses combnyaktöréssel. Azt közölték, hogy nagyobb százalékban volt jelen az eltérés a stresszes törést elszenvedő katonák esetén.[38] Hasset és szerzőtársai más szempontból is elemezték a bevetések utáni fájdalom mint tünet kialakulását. Úgy találták, hogy alacsony kedélyállapoti szint esetén nagyobb valószínűséggel jelentek meg új panaszként a mozgásszervi fájdalom tünetei.[39] A kiképzések és bevetések közben fellépő biomechanikai hatásokon kívül a speciális eszköz és felszerelés is okozhat mozgásszervi panaszokat, ezért ezek állandó felülvizsgálata és fejlesztése szükséges. A nemzetközi irodalomban megtalálható Lenton és munkatársai közleménye, amelyben a katonai testpáncél viselésével kapcsolatos kutatásaikat összegezték. Azt találták, hogy a testpáncél viselése, használata, nem megfelelő kialakítása növelheti a mozgásszervi sérülések valószínűségét.[40]

Ezen irodalmi példák is jól mutatják, hogy milyen jelentősége van a mozgásszervi irányú szűrésnek és állandó monitorozásnak az aktív állomány esetében. Az irodalmi áttekintésben felhozott közlemények példaként szolgálnak olyan, más szerzőktől

[34] Elizabeth Blank et al.: Incidence of Greater Trochanteric Pain Syndrome in Active Duty US Military Servicemembers. *Orthopedics,* 35. (2012), 7. 1022–1027.

[35] F. Winston Gwathmey Jr. – Warren R. Kadrmas: Intra-articular Hip Disorders in the Military Population: Evaluation and Management. *Clinics in Sports Medicine,* 33. (2014), 4. 655–674.

[36] Jason R. Dutton et al.: The Success of Hip Arthroscopy in an Active Duty Population. *Arthroscopy: The Journal of Arthroscopic and Related Surgery,* 32. (2016), 11. 2251–2258.

[37] Jun-Il Yoo et al.: Outcomes of Hip Arthroscopy in a Military Population Are Similar to Those in the Civilian Population: Matched Paired Analysis at 2 Years. *Arthroscopy: The Journal of Arthroscopic and Related Surgery,* 34. (2018), 7. 2096–2101.

[38] Kevin M. Kuhn et al.: Acetabular Retroversion in Military Recruits with Femoral Neck Stress Fractures. *Clinical Orthopedic Related Research,* 468. (2010), 3. 846–851.

[39] Afton L. Hassett et al.: Association Between Predeployment Optimism and Onset of Postdeployment Pain in US Army Soldiers. *JAMA Network Open,* 2. (2019), 2. e188076.

[40] Gavin Lenton et al.: The Effects of Military Body Armour on Trunk and Hip Kinematics During Performance of Manual Handling Tasks. *Ergonomics,* 59. (2016), 6. 806–812.

eredő közleményekre, amelyek kutatásom szükségességét és gyakorlati alkalmazhatóságát bizonyítják. Tudomásom szerint kutatásom elsőként fogja feltárni, elemezni az aktív, szolgálatot teljesítő állomány hazai viszonylatban előforduló mozgásszervi megbetegedéseit, különös tekintettel a csípő bizonyos rendellenességeire.

Felhasznált irodalom

Blank, Elizabeth – Brett D. Owens – Robert Burks – Philip J. Belmont: Incidence of Greater Trochanteric Pain Syndrome in Active Duty US Military Servicemembers. *Orthopedics,* 35. (2012), 7. 1022–1027. Online: https://doi.org/10.3928/01477447-20120621-14

Brinckmann, Paul – Wolfgang Frobin – E. Hierholzer: Belastete Gelenkflache und Beanschpruchung des Hüftgelenks. *Zeitschrift für Orthop und Unfallchirurgie,* 118. (1980), 1. 107–115. Online: https://doi.org/10.1055/s-2008-1051478

Brinckmann, Paul – Wolfgang Frobin – E. Hierholzer: Stress on the articular surface of the hip joint in healthy adults and persons with idiopathic osteoarthrosis of the hip joint. *Journal of Biomechanics,* 14. (1981), 3. 149–156. Online: https://doi.org/10.1016/0021-9290(81)90021-X

Brinckmann, Paul – Wolfgang Frobin – Gunnar Leivseth: *Musculoskeletal Biomechanics.* Stuttgart – New York, Thieme, 2002.

Byrne, Damien P. – Kevin J. Mulhall – Joseph F. Baker: Anatomy and Biomechanics of the Hip. *The Open Sports Medicine Journal,* 4. (2010), 1. 51–57. Online:: https://doi.org/10.2174/1874387001004010051

Cameron, Kenneth L. – Mark S. Hsiao – Brett D. Owens – Robert Burks – Steven J. Svoboda: Incidence of Physician-Diagnosed Osteoarthritis Among Active Duty United States Military Service Members. *Arthritis & Rheumatology,* 63. (2011), 10. 2974–2982. Online: https://doi.org/10.1002/art.30498

Dutton, Jason R. – Nicholas A. Kusnezov – Joseph T. Lanzi – E'Stephan J. Garcia – Mark P. Pallis: The Success of Hip Arthroscopy in an Active Duty Population. *Arthroscopy: The Journal of Arthroscopic and Related Surgery,* 32. (2016), 11. 2251–2258. Online: https://doi.org/10.1016/j.arthro.2016.05.042

Gwathmey, F. Winston Jr. – Warren R. Kadrmas: Intra-articular Hip Disorders in the Military Population: Evaluation and Management. *Clinics in Sports Medicine,* 33. (2014), 4. 655–674. Online: https://doi.org/10.1016/j.csm.2014.06.013

Harrison, M. H. M. – F. Schajowicz – J. Trueta: Osteoarthritis of the hip: a study of the nature and evolution of the disease. *The Journal of Bone and Joint Surgery,* 35B. (1953), 4. 598–625. Online: https://doi.org/10.1302/0301-620X.35B4.598

Hassett, Afton L. – Joseph A. Fisher – Loryana L. Vie – Whitney L. Kelley – Daniel J. Clauw – Martin E. P. Seligman: Association Between Predeployment Optimism and Onset of Postdeployment Pain in US Army Soldiers. *JAMA Network Open,* 2. (2019), 2. e188076. Online: https://doi.org/10.1001/jamanetworkopen.2018.8076

Jochimsen, Kate N. – Cale A. Jacobs – Stephen T. Duncan: Femoroacetabular impingement is more common in military veterans with end-stage hip osteoarthritis

than civilian patients: a retrospective case control study. *Military Medical Research,* 6. (2019), 1. 27. Online: https://doi.org/10.1186/s40779-019-0218-5

Kuhn, Kevin M. – Anthony I. Riccio – Nelson S. Saldua – Jeffrey Cassidy: Acetabular Retroversion in Military Recruits with Femoral Neck Stress Fractures. *Clinical Orthopedic Related Research,* 468. (2010), 3. 846–851. Online: https://doi.org/10.1007/s11999-009-0969-5

Kummer, Benno: Die Beanschpruchung des menschlichen Hüftgelenks. I Allgemeinen Problematik. *Zeitschrift für Anatomie und Entwicklungsgeschichte,* 127. (1968), 4. 277–285. Online: https://doi.org/10.1007/BF00524417

Lenton, Gavin – Brad Aisbett – Daniel Neesham-Smith – Alvaro Carvajal – Kevin Netto: The Effects of Military Body Armour on Trunk and Hip Kinematics During Performance of Manual Handling Tasks. *Ergonomics,* 59. (2016), 6. 806–812. Online: https://doi.org/10.1080/00140139.2015.1092589

Nelson, Richard C. – Chaunsey A. Morehouse (szerk.): *Biomechanics IV*. Baltimore, Maryland USA, Macmillan Education, 1974.

Pauwels, Friedrich: *Biomechanics of the Locomotor Apparatus.* New York, Springer, 1980. Online: https://doi.org/10.1007/978-3-642-67138-8

Radin, Eric L. – Howard G. Parker – James W. Pugh – Robert S. Steinberg – Igor L. Paul – Robert M. Rose: Response of joints to impact loading – III: Relationship between trabecular microfractures and cartilage degeneration. *Journal of Biomechanics,* 6. (1973), 1. 51–57. Online: https://doi.org/10.1016/0021-9290(73)90037-7

Radin, Eric L. – Igor L. Paul – Marc J. Tolkoff: Subchondral bone changes in patients with early degenerative joint disease. *Arthritis & Rheumatology,* 13. (1970), 4. 400–405. Online: https://doi.org/10.1002/art.1780130406

Scher, Danielle L. – Philip J. Belmont – Sally Mountcastle – Brett D. Owens: The Incidence of Primary Hip Osteoarthritis in Active Duty US Military Servicemembers. *Arthritis & Rheumatism,* 61. (2009), 4. 468–475. Online: https://doi.org/10.1002/art.24429

Szendrői Miklós (szerk.): *Ortopédia.* Budapest, Semmelweis, 2005.

Szentágothai János – Réthelyi Miklós: *Funkcionális anatómia* 1 kötet. Budapest, Medicina–Semmelweis, 1996.

Yoo, Jun-Il – Tae-Ho Lee – Jae-Yoon Kim – Jae-Hyung Kim – Yong-Chan Ha: Outcomes of Hip Arthroscopy in a Military Population Are Similar to Those in the Civilian Population: Matched Paired Analysis at 2 Years. *Arthroscopy: The Journal of Arthroscopic and Related Surgery,* 34. (2018), 7. 2096–2101. Online: https://doi.org/10.1016/j.arthro.2018.02.015

Zsákai Zsolt – Papp Miklós – Huszanyik István – Rácz Olivér – Molnár Péter – Károlyi Zoltán – Róde László: Primer arthrosisok retrospectív vizsgálata anteroposterior medence felvételek alapján. – A Femoroacetabularis impingement okozta arthrosis. *Magyar Radiológia,* 2015. július 11. Online: https://radiologia.hu/kozossegek/kategoria/msk/primer-artrozisok-retrospektiv-vizsgalata-anterioposzterior-_15430362

Tartalom