HADMÉRNÖK

Kiemelt közlemények

19. évf. (2024)
2. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

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

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

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

Tartalom

Fórum

HADMÉRNÖK
BIZTONSÁGTECHNIKA

19. évfolyam (2024) 2. szám 5–15.
DOI: 10.32567/hm.2024.2.1

Gubics Frigyes[1]

SOC kialakítása projektmenedzsment segítségével és az üzemeltetés alapjai

Designing SOC with the Help of Project Management and the Basics of Operation

Absztrakt

A különböző típusú objektumok védelme más-más megközelítést igényel, függően attól, hogy milyen jellegű tevékenység folyik a védendő területen belül, illetve mekkora kockázatokkal dolgozunk, és esetleges bekövetkezés esetén milyen károkat szenvedhetünk el. Azok a szervezetek, amelyeknél van kultúrája az objektumvédelemnek és a biztonsági intézkedéseknek, egymással jól együttműködő, strukturált és egymást kiegészítő biztonsági rendszereket építenek ki, amelyek működését egy központi helyről koordinálják, ez a biztonsági központ. Ennek az objektumrésznek fontos szerepe van a megfelelő biztonsági szint fenntartásában, egyúttal támogatást biztosít a területen dolgozó operatív egységek részére. Prioritást élvez a biztonsági központ védelme, amelynek tervezése során felkészülünk a lehetséges támadásokra, illetve haváriahelyzetekre.

Kulcsszavak: objektumvédelem, biztonsági központ, tervezés, biztonság, fizikai védelem

Abstract

Different facilities require different approach of protection that depends on the profile and risk we need to handle, and also need to recognise what kind of risks we face and what are the possible effects. Organisations that have established a culture of facility protection and security measures, have a well-coordinated, structured and complementary security systems that are coordinated from a central location, which is the security centre (SOC).

[1] Biztonsági igazgató, Lenovo Manufacturing Kft., e-mail: easytwofly@gmail.com

The SOC is part of the facility infrastructure and has the main rule to keep security level high enough and also supports operative activity in the areas. Protecting the SOC effectively is a high priority, and it plays an important role in ensuring an appropriate level of security and provides support to the operational unit in preparing for possible attacks or incidents.

Keywords: facility protection, SOC, planning, security, project management, CCTV

Bevezetés

Az objektumok védelmének célja alapvetően a vagyon elleni cselekmények megelőzése, megakadályozása és az emberi élet védelme. Passzív védelmi eszközök segítségével az objektum területére történő behatolást kívánjuk késleltetni, illetve bizonyos esetekben megakadályozni. Ugyanakkor gondoskodni kell a cselekmény detektálásáról is. Az időben történő észlelés alkalmat ad a késlekedés nélküli válaszreakció megtételére, amelyben jelentős szerep hárul a biztonsági központra.

Az objektumok védelmét több, különféle védelmi eszköz egymástól függetlenül is működő, ugyanakkor egymásra épülő, illetve kiegészítő működtetésével biztosítjuk. Ezeknek az elemeknek a működőképességét, üzembiztosságát biztosítani kell, hiszen a megbízható működés a hatékony védelem alapja.

Az objektumok azok a dolgok, amelyekre az őrzési feladat, védelmi kötelezettség, megbízás kiterjed. Az objektum nem feltétlenül kell hogy fizikailag elhatárolt legyen a környezetétől, habár a hatékony védelemhez kívánatos. Az objektumnak van fizikai kiterjedése, tehát a védelmet is fizikai formában, több lépcsőben építjük fel.

Horváth Tamás szerint[2] nagyvállalatok esetében, ahol a működés holdingszerű, az anyavállalat alkotja meg a biztonsági rendszer kereteit, amelyet az egyes leányvállalatok telephelyein implementál. Ezek a minimumelvárások mintegy belső szabványokként funkcionálnak. Tapasztalatom szerint egy az egyben nem mindig lehetséges ezek használata, szükséges a testreszabásuk a helyi viszonyoknak megfelelően, elsősorban azokban az esetekben, amikor a telephely másik országban van, hiszen ebben a helyi törvényeknek is megfelelően kell eljárnunk és működtetni a rendszereinket. Például a GDPR, mint európai uniós irányelv, a személyes adatok kezelése tekintetében eltérő szabályokat tartalmaz az USA jogszabályi kereteihez képest, így tehát egy amerikai anyavállalat sztenderdjeit módosítani szükséges az európai viszonyokhoz, hogy megfeleljünk a törvényi előírásoknak.

A biztonsági központ

A biztonsági központ sérülékenységét, meghibásodási kockázatait minimálisra kell csökkenteni. Az objektum tervezése során erre fokozott figyelemmel kell lenni. Rendelkezésünkre állnak azon eszközök, amelyeket az egész objektum védelmi rendszerének kiépítése során is alkalmazunk. A védelmi szintet meg kell határozzuk a teljes objektumra és az azon belül elhelyezkedő egyes területekre. Ehhez a kockázatelemzést

[2] Horváth 2018.

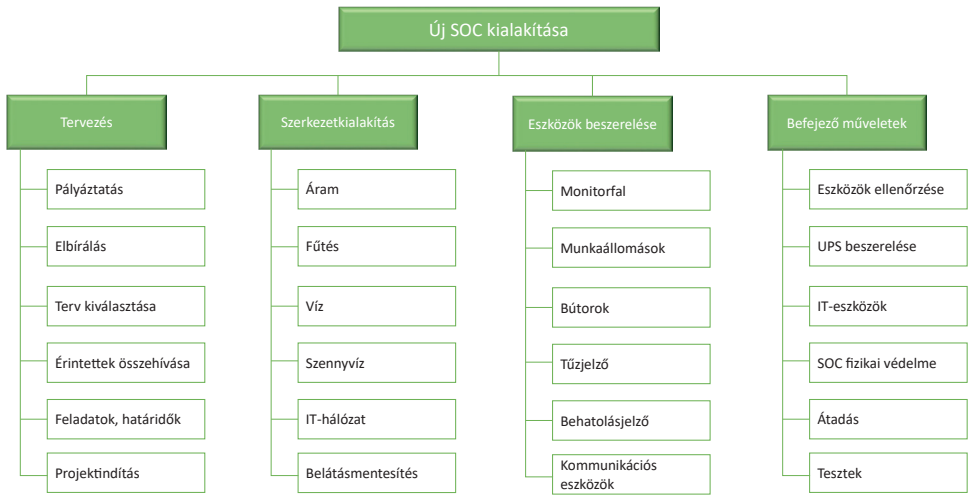
használjuk, amelynek segítségével reális képet kapunk a fennálló kockázatokról és a veszélyeztetettség mértékéről, amelyekhez a védelem szintjét igazítjuk. A biztonsági központ szenzitív, fokozottan védendő területnek számít, mert működésének kiesése esetén a biztonsági szolgálat létfontosságú információktól esik el, hiszen oda futnak be az általa felügyelt objektum őrzésére vonatkozó információk, ezzel együtt kiesése esetén a központ nem képes ellátni vészhelyzeti (például az objektum kiürítésével járó események) irányító funkcióját sem. Ezek részleges vagy teljes kiesése esetén a biztonsági szint csökken, amit azonban egyéb intézkedések bevezetésével bizonyos fokig kompenzálhatunk. Például a behatolásjelző rendszer meghibásodása esetén a vagyonőri létszám növelésével, őrpozíciók megerősítésével vagy újak nyitásával átmenetileg, amíg a hibát kijavítják. A biztonsági központ használhatatlanná válására fel kell készülnünk mint lehetséges kockázatra, amire az ERP[3] külön kitér. Megoldást jelenthet redundáns[4] rendszerek kialakítása: alternatív biztonsági központot hozunk létre egy eltérő helyszínen, lehetőleg nem ugyanazon az objektumon belül, így nem lesz érintve haváriahelyzet[5] esetén mindkét egység. Ez növeli a beruházási költségeket, ebben az esetben is a kockázatok elemzése segít meghozni a döntést, hogy megéri-e egy extra beruházást eszközölni. Piaci gazdasági társaságok esetén a menedzsment szempontjából a fő kérdés, hogy mennyi anyagi ráfordítás kell ahhoz, hogy a szükséges és elégséges védelmi szintet elérjem, és fenn tudjam tartani a kockázatok minimalizálása mellett.

Projektmenedzsment a biztonsági központ kialakítása során

A biztonsági központ kialakítása új épület tervezésekor része a projektnek. Amikor utólagosan, már meglévő, működő objektumba tervezünk SOC[6]-t, akkor a központ kialakítását tekintjük projektnek. Az érdekeltek *(stakeholder)*[7] bevonása fontos, hiszen az SOC létrehozása sok más terület képviselőjének munkáját is befolyásolhatja, segítheti. Például a tűzjelző központ telepítése, amely alapvetően az EHS[8] érdekkörébe tartozik, de észszerű, hogy annak felügyelete és kezelése a biztonsági szolgálat feladata, hiszen a nap 24 órájában, az év minden napján jelen vannak a telephelyen. A munka pályáztatásához meg kell fogalmazni az elvárásokat, amelyeket kiküldünk a pályázó cégek részére. A tender nyertese konzultáció útján pontosítja az igényeket. Ezután történik a költségvetés jóváhagyása. Amikor az anyagi források rendelkezésre állnak, a végleges terveket a pályázatot nyert cég készíti el a biztonsági vezető elvárásai és a szakma követelményei alapján. A tervek jóváhagyása a menedzsment, épületüzemeltetés és EHS osztály vezetőinek bevonásával történik. Az 1. ábra a projektkivitelezés folyamatát mutatja be. Garcia szerint[9] biztonságtechnikai mérnök

[3] ERP: emergency response plan (vészhelyzeti terv).
[4] Redundáns: párhuzamos, egymást helyettesítő rendszerek.
[5] Természeti csapás vagy emberi tevékenység során előállt vészhelyzet.
[6] SOC: surveillance operations center (felügyeleti műveleti központ).
[7] Stakeholder: érdekelt fél.
[8] EHS: environment, health, and safety (környezetvédelem, egészségvédelem, munkabiztonság).
[9] Garcia 2008.

alkalmazása elengedhetetlen, hiszen ő felügyeli a rendszerek integrációját, emellett a projektcsapat vezetőjének tapasztalattal kell rendelkeznie a biztonsági rendszerek kialakítása területén. Ez utóbbi állítást annyiban árnyalnám, hogy amennyiben nem a biztonsági szakterületről érkezik a vezető, fontos, hogy meghallja, megértse és érvényre is juttassa a szakág által támasztott igényeket a projekt valamennyi szakaszában.



1. ábra: Biztonsági központ létrehozása projekt
Forrás: a szerző szerkesztése

A megvalósítás alapkérdései:

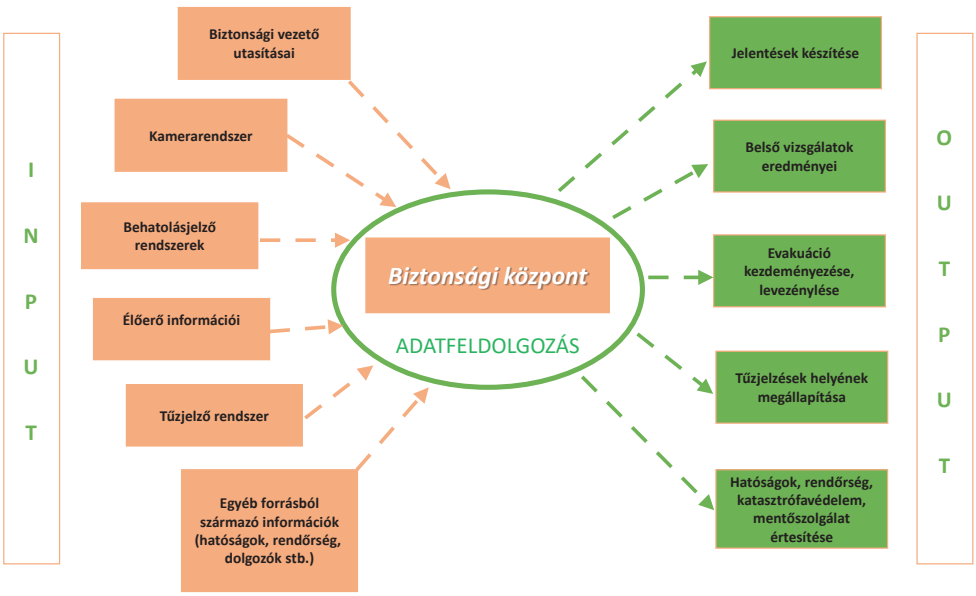
- A kivitelezési terv és az ahhoz használatos anyagok pontossága.
- A tervekben meghatározott és elfogadott elvárások megvalósításának fokozott ellenőrzése.
- Minőségi és garanciakérdések (a felhasznált anyagok és a kivitelezési munka minőségének garantálása a kivitelező által).
- Engedélyezési folyamatok (a létesítmény működéséhez szükséges hatósági engedélyek teljes körű beszerzése, illetve időszakos felülvizsgálatának intézése).[10]

Funkciók

A biztonsági központ létrehozása a biztonsági szolgáltatás, tevékenység keretbe foglalása, az adatok feldolgozásának központosítását is célozza. A bejövő információk jól detektálhatók, az egyes csatornákon érkező adatok fizikailag egy helyre érkeznek és összekapcsolhatók, összefüggéseikben értelmezhetők, kiértékelésük után pedig a válaszreakciók időben és adekvátan képződnek.

[10] Christián 2014b.

Az SOC az objektum védelmének központi eleme, amely működhet önállóan, de összekapcsolható, illetve egyfajta hierarchikus rendszerbe is állítható más biztonsági központtal vagy központokkal. A biztonsági központ földrajzi elhelyezkedése függ az üzemeltető telephelyi adottságaitól, a ráfordított anyagi erőforrásoktól, illetve szakmai döntésektől is.



2. ábra: A biztonsági központ információáramlása
Forrás: a szerző szerkesztése

A 2. ábra szemlélteti az információk gyűjtésének lehetséges forrásait, majd feldolgozás utáni „továbbküldését" intézkedések formájában, vagy akár az információ visszaküldését a forráshoz újabb adatigény megfogalmazásával, amennyiben döntés meghozatalához, illetve intézkedés kezdeményezéséhez az elsődleges információ kevésnek bizonyul.

Rendkívüli helyzetek

A napi operációval összefüggő biztonsági tevékenységen túlmenően adódhatnak rendkívüli helyzetek, amelyek eltérő reakciókat várnak az SOC személyzetétől. Tekintettel arra, hogy a biztonsági központban a nap 24 órájában szolgálatot látnak el, kézenfekvő, hogy a különböző váratlan helyzetek kezelésének is ez a központja, de legalábbis kulcsszerepet játszik azok megoldásában. A vállalat által megalkotott úgynevezett vészhelyzeti terv (ERP) rendelkezik az egyes feladatokról, szerepkörökről rendkívüli helyzetek esetén.

A stratégiai döntések nem az SOC-ban születnek meg, hanem az ilyen helyzetekben összeülő CMT[11] hozza meg azokat, amely a vállalatvezetés ide delegált tagjaiból tevődik össze, akik az általuk vezetett, a rendkívüli helyzetek kezelésében kulcsfontosságú területekért felelnek. A CMT elsődleges feladata az emberek, azon túlmenően pedig a vagyontárgyak mentése, ezek után pedig gondoskodni a helyreállításról és a termelés minél gyorsabb újraindításáról.

A biztonsági incidensek lehetnek ember által generáltak, illetve természeti eredetűek, jellegűek, amelyek bekövetkezésének esetén a detektálás és reagálás elsődlegesen a biztonsági központ feladata.

Váratlan helyezetek, amelyek kezelésében az SOC személyzetének kulcsszerepe van:

- időjárás okozta károk, meghibásodások kezelése,
- terrortámadás,
- bombafenyegetés,
- közlekedési katasztrófa,
- külső támadás,
- áramszünet,
- vízbetörés,
- epidéma, pandémia,
- földrengés,
- tűzeset.

A felmerülő kockázatokat figyelembe kell venni, majd ennek megfelelően kidolgozni az egyes esettípusokhoz kötődő lehetséges forgatókönyveket és folyamatokat. A felkészülés és a reagálási tervek kidolgozása a múltban bekövetkezett eseményeken alapul, de a vállalat alaptevékenységéhez kapcsolódó tipikus eseményekre is felkészülünk, kockázatelemzés segítségével. Az eseményspecifikus reagáláson túl szükség van eljárási rendre, amely tartalmazza az információs láncot, és definiálni kell döntési szinteket és jogosultságokat is. Az információs csatornák kijelölése a döntések és utasítások eljuttatásához a végrehajtó állományhoz elengedhetetlenek. A kommunikációs csatornákra van szükség a CMT, az SOC és az ERT[12] között. Az ERT a CMT által meghozott döntések végrehajtásában működik közre, és tagjait a CMT-tagok delegálják. Gondoskodni kell a helyettesítés rendjéről a CMT és ERT esetében. Az SOC-nak rendelkeznie kell személyzeti adatokkal, amelyek segítségével az evakuáció során meggyőződnek arról, hogy mindenki elhagyta az objektumot. A dolgozók legközelebbi hozzátartozói listájával is rendelkezni kell, hogy vészhelyzet esetén a családtagokkal fel tudjuk venni a kapcsolatot. Az adatok naprakészen tartása a kijelölt biztonsági személyzet/vezető feladata, felelőssége. Ennek érdekében folyamatos kapcsolattartás szükséges a Személyzeti Osztállyal.

[11] CMT: crisis management team (válságkezelő csapat).
[12] ERT: emergency response team (vészhelyzeti reagáló csapat).

Sérülékenységvizsgálat és a biztonsági központ fizikai pozicionálása

A megfelelő tervezés során a sérülékenységek a minimálisra csökkenthetők. Az olyan esetekben, amikor már meglévő objektumba telepítünk biztonsági központot, kénytelenek vagyunk az adottságainak megfelelő kompromisszumokat kötni. Közvetlenül, a dolgozók által frekventáltan használt területekről (például nagy forgalmú folyosó) ne legyen megközelíthető az SOC.

További tervezési szempontok

A biztonsági központot védő, megelőző infrastrukturális követelmények:

- a falazat és plafon kellően ellenálló kell legyen ipari baleset bekövetkezése és külső behatolás esetén is;
- a helyiségbe be- és kilépő kábelezés védelme;
- az informatikai rendszerek függetlenek az egyéb IT-rendszerektől;
- internetcsatlakozás nem lehetséges a használt eszközökön;
- vizesblokk ne legyen a közelben, illetve a hozzátartozó csővezeték ne menjen át a helyiségen, vízbetörés-védelem szükséges;
- friss levegő biztosítása;
- eszközök hűtésének biztosítása.

Mechanikai védelmi intézkedések:

- ellenálló falazat (például gipszkarton fal nem elfogadható) és plafon;
- megfelelő ellenállású ajtó;
- zárszerkezet az ajtóban;
- nincs ablak a helyiségen;
- ablakkal ellátott helyiségben gondoskodni kell a belátás korlátozásáról (fóliázás és függöny);
- a helyiségbe be- és kilépő kábelezés védelme.

Elektronikai védelmi intézkedések:

- beléptetővel ellátott ajtó;
- behatolásjelző rendszerbe integrálás;
- pánikgomb;
- interkom;
- UPS;[13]
- redundancia[14] biztosítása;
- elektromos ellátás;
- adatrögzítés (CCTV,[15] CAS,[16] intruder alarm[17]).

[13] UPS: uninterrupted power system (szünetmentes áramkör).
[14] Redundancia: erőforrások duplikálása a nagyobb rendelkezésre állás érdekében.
[15] CCTV: closed circuit television (zárt láncú kamerarendszer).
[16] CAS: centralized access system (beléptetőrendszer).
[17] Intruder alarm: behatolásjelző.

Kommunikáció:
- internet tiltva;
- független rádiókommunikáció, alternatív frekvenciával;
- mobiltelefon;
- vonalas telefon;
- közvetlen kommunikációs kapcsolat a rendőrséggel, katasztrófavédelemmel;
- privát kommunikációs eszközök és adathordozók bevitelének tiltása.

Rezsimintézkedések:
- belépések korlátozása;
- a belépési jogosultsággal rendelkezők körének rendszeres felülvizsgálata;
- sikertelen bejutások (fals kártyahúzások) rendszeres ellenőrzése és kivizsgálása;
- személyzet kiképzése, továbbképzése.

Humán faktor:
- személyzet kiválasztása;
- bizalmasság kérdése;
- titoktartási nyilatkozat;
- területismeret;
- képzés és továbbképzés;
- helyspecifikus ismeretek.

A biztonsági központ személyzetének és az IT-eszközöknek a védelme:
- az ipari tevékenység során esetlegesen felszabaduló, levegőben terjedő ártalmas gázoktól, részecskéktől és terjedésük irányától távol legyen;
- egyéni védelmi eszközök elhelyezése a helyiségben;
- önálló, megfelelő légcsere biztosítása;
- megfelelő hőmérséklet biztosítása.

A fenti szempontok szerinti megvalósítás mellett is fel kell készülnünk a biztonsági központ feladatainak ellátására alternatív megoldásokkal, amennyiben az elsődlegesen használt SOC-ból ez lehetetlenné válik. Célszerű létrehozni egy alternatív irányítási központot. Az alternatív központ biztosítására másik lehetőség, ha egy olyan központ veszi át a feladatok ellátását, amely a vállalatcsoporton belül egy másik objektum védelmében vesz részt. Ebben az esetben a tartalék központnak plusz személyzetre és eszközökre van szüksége úgy, hogy a megfelelő területismeret mellett az eszközök is alkalmasak legyenek a teljes értékű feladatellátásra. Az alternatív központ alkalmazásának akkor van realitása, ha egy vállalat egynél több telephellyel rendelkezik, amelyekből legalább kettő rendelkezik biztonsági központtal. A költség-haszon elv is szerepet játszik alternatív központ létrehozásában vagy már meglévő egység alkalmassá tételében a feladatok ellátására. Külföldön elhelyezkedő központban tevékenykedő személyzettől nem várható teljes értékű helyismeret, ugyanakkor ismerniük kell a helyi vészhelyzeti intézkedési terveket. Fontos, hogy közvetlen kapcsolatban legyenek a helyben szolgálatot teljesítő biztonsági személyzettel, illetve hogy szükség esetén a biztonsági központ legfontosabb funkcióit vegyék át, mint például a behatolásjelző

rendszer, a tűzjelző rendszer és CCTV-rendszer felügyelete. A kommunikáció a külföldi biztonsági központ személyzetével, a szükséges nyelvismeret szintén követelmény a biztonsági személyzet részére.

Jártasság biztosítása

A jártasság megszerzése, illetve fenntartása komoly erőfeszítést jelent az élőerős őrzést biztosító vagyonvédelmi cég oldaláról. Annak érdekében, hogy a biztonsági központ hatékonyan tudja ellátni feladatait az objektumvédelemben, illetve elsődleges irányító funkcióját betöltse, a technikai felszereltség mellett a személyzetnek rendelkeznie kell azzal a speciális tudással, amely biztosítja a működést az elvárt színvonalon. Az SOC-személyzet képzése iskolarendszeren belül és kívül sem megoldott, a szükséges ismereteket személyre, illetve telephelyre szabott formában kapják meg jelenleg a vagyonőrök. A biztonsági központban történő feladatellátás jóval több technikai jellegű kvalitást és alapvető IT-ismereteket igényel, mint amelyek a vagyonőri tevékenységhez szükségesek általában. Az ismeretek elsajátítása, illetve egy minimumszint meghatározása elengedhetetlen az SOC személyzete részére. Az SOC-ban a vagyonvédelmet szolgáló rendszereken kívül a tűzjelző rendszer központja is helyet kap, ezért szükséges a személyzet speciális, a beérkező tűzjelzésekhez kapcsolódó képzése, illetve az eljárásrend leoktatása rendkívüli, illetve vészhelyzetek eseteire. A személyzet létszámának meghatározása a feladatok jellegétől és mennyiségétől függ, de befolyásolja például a telephelyen telepített kamerák száma, milyen mennyiségűek a napi operáció során az élő időben követendő események, illetve a kivizsgálandó ügyek. Az éberség és a jártasság fenntartása érdekében a vészhelyzeti reagálást megfelelő időközönként gyakoroltatni kell, illetve nem szabad elfeledkeznünk az újonnan érkező személyzet képzéséről, valamint a meglévők továbbképzéséről sem. Fennelly szerint[18] a személyzetnek rendelkeznie kell az alábbiakban felsorolt készségekkel ahhoz, hogy hatékonyan tudja elvégezni a rábízott feladatot:

- biztonsági szabályzatok és eljárások ismerete,
- professzionalizmus,
- biztonsági tiszt jogosultsága,
- kapcsolatok a rendvédelmi szervekkel,
- járőrözési eljárások,
- megfigyelési technikák,
- kihívó technikák,
- vizsgálatok,
- jelentésírás,
- sürgősségi orvosi segítségnyújtás, elsősegélynyújtás,
- munkahelyi erőszak kezelése,
- biztonsági berendezések üzemeltetése.

[18] Fennelly 2013.

A fentieken túl azonban fontos, hogy a helyspecifikus szabályokat, eljárásokat tudják, illetve adaptálni legyenek képesek a megszerzett tudással a helyszíni adottságokhoz.

Összefoglalás

Az objektumvédelem során a védelmet ellátó biztonsági rendszerek központjának tervezése és kivitelezése létfontosságú. Az SOC esetében a rendelkezésre álló eszközök mind technikai, mind pedig élőerős oldalról hasonlók, mint amiket a teljes objektum védelméhez használunk. Az objektumvédelem célja nem kizárólagosan a periméter megóvása, hanem megfelelően kategorizálva és elhatárolva azokat, külön kisebb biztonsági zónák létrehozása és védelmi szintjük definiálása a kockázatelemzés eredményétől függően, hozzájuk rendelve a biztonsági rendszerelemeket. Ezeknek, az úgynevezett biztonsági zónán belüli szenzitív területeknek a felügyeletét is a biztonsági központba célszerű integrálnunk. Az SOC a szerepét akkor képes teljeskörűen betölteni, ha ott területismerettel, a biztonsági szabályokkal, az objektumon belüli munkafolyamatokkal, a technikai rendszerek kezelésével és megfelelő szakmai tudással rendelkező személyzet végzi a munkát, és képesek lekövetni az objektumon belüli folyamatváltozásokat is. A biztonsági központra úgy kell gondolnunk, mint a vállalatbiztonság agyközpontjára, ahol a bejövő információk feldolgozása zajlik, a megfelelő reagálás érdekében. Az SOC kialakításakor figyelembe vett környezeti adottságok, annak védelmi rendszere szavatolja a szolgáltatás folyamatosságának biztonságát. Az átgondolt kivitelezés, az érdekeltek bevonása a tervezéstől a megvalósulásig képesek garantálni azt, hogy olyan biztonsági központot alakítsunk ki, amely megfelel az előzetesen megfogalmazott feltételeknek, emellett alkalmasnak kell lennie arra is, hogy a későbbiekben – az igények esetleges változásához igazodva – képesek legyünk azt továbbfejleszteni. Az objektumvédelem kulcsfontosságú része az SOC, amelynek felépítése összehangolt munkát jelent több szakterület képviselőitől. Helye a komplex biztonsági rendszeren belül átgondolt koncepció eredménye. A biztonsági rendszeren belüli változásokat, fejlesztéseket képes lekövetni, illetve önálló egységként is továbbfejleszthető. A biztonságtechnika és az IT-terület fejlődése szorosan összefüggenek, az analóg rendszerek helyét egyre inkább átveszik a digitális megoldások, amelyekhez elengedhetetlen az IT-infrastruktúra fejlesztése. A rendszerek működéséhez szükséges személyzet tudását fejleszteni kell a megfelelő felkészültségi szint eléréséhez. A speciális tudás megszerzésére nem áll rendelkezésre iskolarendszerű vagy azon kívüli képzés, amelynek segítségével megfelelő alapokat kapnának az SOC-személyzet leendő tagjai. Az ismereteket munka közben, tapasztaltabb kollégáktól kapják meg, amihez hozzájárul még az objektumspecifikusan kidolgozott tréningtematika, amelyet a vagyonvédelmi vállalkozás vagy a megbízó vállalat biztonsági szakemberei dolgoznak ki. A vállalatbiztonsági kultúrával rendelkező cégek esetében a biztonsági folyamatok keretrendszere jobbára már adott, szerves része az átgondoltan megtervezett SOC.

Felhasznált irodalom

Christián László (2014a): *A magánbiztonság elméleti alapjai.* Budapest: NKE RTK.
Christián László szerk. (2014b): *Létesítményvédelem.* Budapest: Nemzeti Közszolgálati Egyetem.
Fennelly, Lawrence J. (2013): *Effective Physical Security.* Butterworth–Heinemann.
Garcia, Mary Lynn (2008): *The Design and Evaluation of Physical Security Systems.* Butterworth–Heinemann.
Horváth Tamás (2018): *Elektronikus megfigyelő- és ellenőrző rendszerek objektumorientált kialakítása különös tekintettel a biztonsági kockázatok rendszére.* Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola.

HADMÉRNÖK
BIZTONSÁGTECHNIKA

19. évfolyam (2024) 2. szám 17–28.
DOI: 10.32567/hm.2024.2.2

József Répás[1]

Examining the Application of Drone Forensics Methodology on Highly Automated Civil and Military Vehicles

Abstract

One of the aims of digital forensics investigations of modern civil and military vehicles traffic accidents or other crimes is to establish what kind of incident occurred, when, where, and under what circumstances. As the automation level of vehicles increases, connected solutions become more widespread (e.g. drone–vehicle cooperation), and an accurate timeline of events and credible evidence can be provided in vehicles and connected drones. The forensic examination of drones deals with the exploration, processing, interpretation, and analysis of data stored in drones and sent through the established communication channel, some of the examination steps of which may be applicable in the case of vehicle examination. This study aims to examine one of the areas of digital forensics, Drone forensics, to determine which of its steps or procedures can be applied in the expert examination of highly automated and increasingly autonomous vehicles (e.g. military vehicles).

Keywords: unmanned aerial vehicle, drone forensics, digital forensics, autonomous vehicles, autonomous vehicle forensics

Introduction

The increase in the level of vehicle automation means the collection, processing, and management of more and more data in both civilian and military applications. While in civilian use the protection of personal data is one of the key issues, in operational terms, the protection of operational information appears. In data storage units of vehicles, the information is retained for a longer or shorter period depending on the purpose of use. This can be data related to the operation, traffic, or environment of the vehicle,

[1] PhD student, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: repas.jozsef@uni-nke.hu

but it can also refer to the driver or passengers. The cooperative operation of vehicles in intelligent transport systems and advanced communication technologies allow them to coordinate their manoeuvres with nearby vehicles and gather a wide range of information about their surroundings. Direct or mobile communication is possible with infrastructure, vehicles, smart networks, devices, and pedestrians. This allows vehicles to extend their own perception and localisation. Another extension could be the addition of drones to the detection and navigation of vehicles, i.e., with a drone connected to the vehicles, additional information can be collected and processed by the vehicles. This could further expand the range of data generated, collected, stored, and processed in vehicles.

Drones, or Unmanned Aerial Vehicles (UAVs), are used for several purposes, including creating photos and videos of large areas, conducting military operations, and conducting environmental surveys. As a result of technological developments, UAVs now include many additional technologies, including high-performance cameras, thermal scanners, and even military weapons. As a result, from a military perspective, UAVs are now part of the Internet of Battlefield Things (IoBT) ecosystem. In addition to UAVs, the IoBT ecosystem includes components such as networks of sensors, wearable devices, and other Internet of Things (IoT) devices. This ecosystem is expected to generate large amounts of data, enabling military personnel to respond to various situations on the battlefield.

The use of drones extends beyond legal limits (e.g. recreational and corporate) to illegal and other violent operational applications. They are used in cyberattacks (e.g. unauthorised access and monitoring, surveillance, rouge access point, etc.), invasion of privacy, trespassing, damage, violation of no-fly zones, information gathering, international espionage, reconnaissance, smuggling, support for terrorism, or IED attack. The wide range application and functionality of UAVs increase the chances that forensics examination may be necessary to investigate an event (e.g. an accident or incident).[2]

Drone forensics

"Digital forensics is a significant domain that involves capturing and analyzing cybercrimes. It has many branches: database forensics, IoT forensics, cloud forensics, drone forensics, wireless forensics, malware forensics, mobile forensics, network forensics, and data forensics. These branches have numerous and redundant forensics models, frameworks, approaches, policies, procedures, and tasks."[3]

Regardless of the size, structure, and operation of drones, depending on their use, they collect and store large amounts of information about their users, as well as about the detected events and locations. Given that the use of drones may pose a threat to national safety and security, a post-mortem forensics examination of intercepted or crashed drones may be necessary. Their data, as vital pieces of evidence

[2] Hankó 2021; Studiawan et al. 2023; Krajnc 2018.
[3] Alotaibi et al. 2022.

during a forensics examination, can contribute to the achievement of the investigation goals and the answer to forensics questions. Digital forensics has several subdomains, drone forensics is the one. Drone forensics has a wide range of applications beyond law enforcement. It can be used in various fields, including:

- counter-terrorism (espionage or terrorist activities)
- accident investigations (determine the cause and prevent future incidents)
- privacy law compliance[4]

Figure 1: Drone forensics
Source: www.cyforce.in/images/Drone-Forensics-India.jpg

It is the responsibility of drone forensics to recover, obtain, process and analyse this information. Data generated by drones, such as ID's, geolocations, flight path and history, time, images, and videos greatly contribute to the reconstruction of the events.[5]

Drones operate on a principle similar to that of computers. They have a processor, a data storage unit, communication ports, sensors, a camera, and a unit that determines their geographical location. The control of the device, as well as the transmission of data, is carried out by wireless communication. Existing digital forensics methods and techniques can be used. The process steps for computer, IoT, or mobile forensics can also apply to drones.[6] Expert examination of drones serves three main purposes.

[4] Riaz 2023.
[5] Alotaibi et al. 2022; Gustafson 2024; https://qccglobal.com/drone-forensics-services/; Répás 2023; Répás et al. 2022; Tiwari 2022.
[6] Kovar–Bollö 2021.

- The first category is the identification of the affected persons (suspect, victim), which is primarily the user of the drone or the victim, so in this case the investigation is aimed at how the device was controlled. The method of control may vary from manufacturer to manufacturer. For example, a remote controller, a smartphone that transmits commands to the drone, or a smartphone that provides direct communication with the device via Wi-Fi or Bluetooth. Both control methods leave different traces of digital evidence.[7]
- The second category includes the analysis and interpretation of flight data. In such a case, information collected by the drone's sensors and navigation data is processed. By analysing this data, it is possible to find out where the drone took off from or calculate the time of the drone's failure from the battery level. The reconstruction and analysis of the flight path of the drone and the flight track may be important mainly in the investigation of crimes related to smuggling.
- The third category of the investigation is the extraction and processing of existing data on the drone's data carrier.

Figure 2: Future directions and main purposes

Source: https://media.licdn.com/dms/image/D4D12AQGjrcq6s2uFyg/article-inline_image-shrink_1500_2232/0/1700476063621?e=1720051200&v=beta&t=Yk5l4d-9BIGxjLAj6cFuQKJqjAM1CH6LpmR0WKYtzQ8

Drone forensics challenges

Millions of unmanned aerial vehicles (UAVs) are registered across the globe, with almost half of them being used for commercial purposes. Apart from the registered UAVs, there are a significant number of devices being used privately. These are used for various illegal activities such as smuggling of illegal drugs, unauthorised surveillance, potential attacks, carrying explosives, and disrupting aviation.

[7] Azhar et al. 2018.

Drones have become a popular technology because of their various uses. They store a lot of information about both the events they captured and their users. Drone forensics is responsible for recovering, obtaining, processing, and analysing this information. The data generated by UAVs, such as flight path, time, images, and videos, are extremely helpful in reconstructing the events.[8]

Although the examination of drones is carried out using a procedure and approach similar to that of computers, mobile phones, or IoT devices, there are still physical, legal, and technical challenges in investigating them.[9]

Due to the diverse drone manufacturers, standards, operating systems, and infrastructure-based networks, the forensic examination of drones is a complex and unclear field. Many drone forensics models and frameworks have been designed based on various peer-review processes and activities, as well as possible scenarios for drone-related incidents, and numerous models, frameworks, methods, approaches, tools, and algorithms have been offered in the literature to conduct investigations on different UAVs. However, there is still a lack of a structured and unified model for managing and facilitating forensics tasks and activities in digital forensics.

Due to the current drone expert examination procedures and the protection of assets, access to data is not easy. One of the challenges of trace recording that we are looking for answers to is drones as sources of evidence. In investigating a drone-related event, basic forensic questions[10] need to be answered:

- Who: the persons involved (suspect, victim, eyewitness), proof of use, linking the device and the person using it
- Why: the trigger, motivation of the event
- Where: the location of the event under investigation or related relevant locations
- When: date of the event under investigation and related events (flight history firmware, upgrade, maintenance, etc.)
- What: a compilation of a timeline of events, a description of the facts (what happened during the flight, what flights the drone made, what route it travelled, etc.)
- How: how the event occurred, how it was committed (how the drone was used)
- With whom: connecting to the stakeholders (who), and establishing the role of the participants or co-perpetrators (who, or what services are connected to the drone)

As usual, when examining drones, not all questions have answers, or they are not stored in one device, in one place, or in one way. While the images and videos taken by the camera are stored on the memory card, flight, navigation information and operating parameters are stored in the internal storage of the drone (sometimes with limited capacity), but the remote control also contains information about the connected/controlled drone, and the logically connected mobile device and the files

[8] Répás 2023; https://digitpol.com/drone-forensics/; Gustafson 2024; Singh 2022; www.qccglobal.com/drone-forensics

[9] Vízi 2019; Almusayli et al. 2024.

[10] Fenyvesi 2013.

related to the application running on it may also contain data related to the flight, communication or live broadcast by the drone.

A distinction should be made between known and unknown (constantly developing) factory- and custom-built devices. In the absence of standardisation, different manufacturers use different solutions (drone-specific hardware and databases) both technically and logically, and in the case of custom-built drones, additional individual solutions (data storage, data access, unknown communication, etc.). Some drones can be accessed via FTP and Telnet protocol, while others can be accessed via direct USB. In addition, access permissions to the drone are different. In most cases, access is limited to the media folder or system files only. That is, there are currently no consistent tools to carry out the process of obtaining data from drones.

The drone may be damaged during flight, landing, or interception. Storage may also be damaged, or (temporarily) stored flight data may be lost due to power failure. In the absence of off navigation, connection problems, and geographical coordinates, knowing the flight path of the drone becomes almost impossible. The linking of the unique identifiers of the drone, the remote control, the related services, and the identity of the owner also complicates the investigation. There may also be technical obstacles, such as incompatibility, lack of software, drivers, or appropriate cables, or failure to connect via the USB port. The encryption used by drones, and different file systems can cause incompatibility, even within the same device (different file systems are also used within the same drone).

The way in which data is extracted and analysed may also vary, taking into account the need to ensure data integrity and authenticity, or individual data storage solutions and logical access. The use of anti-forensics solutions (the use of solutions and procedures that make it difficult or impossible to perform the test effectively) can also be applied to drones, which pose an additional challenge for investigators. Various encryption and deletion solutions (e.g. remote or timed deletion), data hiding, and metadata modification make it difficult to obtain evidence. Determining the type of drone or its controller when the signal is scraped or removed can also be difficult.[11]

Extracting data from drones for forensic examinations presents a significant hurdle: creating a standardised and repeatable process that aligns with forensic peer-review principles while preserving data integrity. This issue parallels the challenges faced in expert examinations of highly automated civil and military vehicles, where a universal procedure has not yet been established.[12]

Drone data

The first step in answering the examinations questions is to identify the source of the data, the test object (in this case the drone), and the potential evidence (the

[11] Atkinson et al. 2020; Kovar–Bollö 2021; Kao et al. 2019; www.salvationdata.com/knowledge/what-is-drone-forensics

[12] Répás 2023; Al-Room et al. 2021.

data in the drone). In general, drone forensics has defined three main phases that fit into each step of digital forensics: preparation, data acquisition, and analysis phase.[13]

During the examination of the drone, the evidence can be divided into three categories:

- physical evidence, the device itself
- digital evidence, storage of drone data, data stored in the cloud or on other devices
- other/miscellaneous evidence, e.g. social media, purchase records, DNA, fingerprints

Compared to the examination of vehicles, it can be concluded that physical evidence can also be evaluated by the vehicle itself, since it can be both the target, object (contains evidence), and the means of the crime.

Digital and other categories of data can be stored in the internal memory of the drone, external memory card, remote controller, connected mobile device (e.g. mobile, tablet, notebook), cloud-based systems (social media, forums), or service providers (e.g. mobile phone company, web account). The data can be found on the drone's communication channel (in transit) for some examination. Compared to the examination of vehicles, it can be concluded that, similarly to drones, digital evidence connected to vehicles can be found in the vehicle itself (internal data storage, e.g. ECU, HDD, SSD, memory card, etc.), connected mobile device, manufacturer and service provider clouds, or in environmental and track elements.

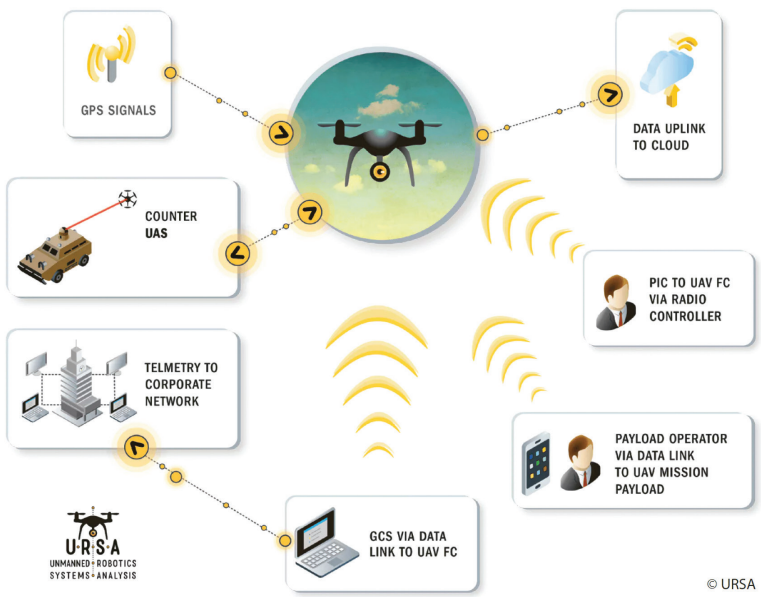


Figure 3: Drone connections
Source: www.japcc.org/wp-content/webp-express/webp-images/uploads/CUAS_Fig_19_1.png.webp

[13] Al-Dhaqm et al. 2021; Jain et al. 2017.

"Evidence from one source will lead you to evidence from other sources. Combined, they produce a compelling picture of the immediate flight, but also of operations, logistics and supply chain."[14] The stored data provides information about the identifiers of the drone and its components (e.g. remote controller, MAC, IMEI, IMSI), paired devices, software and firmware versions, and configurations. Flight track information includes landing, take-off, return locations (including frequent and preferred flight locations), and flight history (including known locations, home points, and routes travelled). Among operating parameters, GPS, telemetry, barometric data, state of the motor, and battery are recorded. The communication information about SSID, WiFi data, IP, and mobile communication (4G, 5G) connection. Information about payload, data recorded by sensors (photos, video recordings). In the case of vehicles, component identifiers, software, and firmware versions, or e.g., IMEI, IMSI numbers in connection with the Emergency call function are also stored. Flight track information in vehicles can be matched to track logs, and different flight parameters can be matched to the vehicle's operational and traffic parameters (see Figure 3).[15]

Drone forensics process

During the identification of evidence, if possible, the make, type, weight, and category of the drone should be determined, its individual characteristics (possible customisation, additional components) should be documented, and its physical condition assessed. For devices of well-known manufacturers, it is necessary to review the manufacturer's documentation, and in the case of drones developed individually and not known by expert software, obtaining and reviewing the controller manufacturer's documentation. Based on the documentation, the methods of accessing the data can be learned (e.g. API, interface, file system, operating system). If the device is unique or the control is not known and no information is available from documentation or other sources, physical or logical access to data can be achieved with individual solutions at considerable time and cost. Some manufacturers provide direct access to drone on-board logs via USB port, but there are also solutions where the information is stored on an SD card glued to the motherboard. Drone control applications can also provide an option for flight logs, however, this solution is not always stable, as the files can be corrupted, and do not contain all flight path information. In the case of a drone with severe electronic damage, data extraction can only be obtained by connecting to JTAG points or chip-off directly from the chip by removing the integrated media.[16]

The first step of the effective drone forensic process is preparation. In the preparation phase, data storage must be explored and identified, and the operability of devices must be checked. During a logical assessment, the drone's wireless network connections (Wi-Fi, Bluetooth, etc.), navigation, and data storage are checked.

[14] Kovar–Bollö 2021.
[15] Kovar–Bollö 2021; Tiwari 2022.
[16] Kovar–Bollö 2021.

In the acquisition phase, all steps, activities, and processes of obtaining and preserving relevant data from identified data sources should be documented. Create a Working Copy, or a physical or logical image of the data storage (in order to reduce the chance of damaging evidence, it should only be activated once).[17]

During the analysis phase, the data obtained should be examined and analysed to identify and uncover evidence. The analysis can be done manually or with the help of software using an automated method. In the practice of computer forensics, analysis is largely done with some kind of interactive tool, which must recognise and analyse the data structures and metadata embedded in the extracted data. In the case of drones, such solutions are implemented thanks to the expansion of the functionality of certain mobile forensics solutions. They have been supplemented with functions and options that make them suitable for examining drones as well. For example, the application can identify files by header or recover deleted files (in this case, it recovers individual entries in the file system and compiles the file afterward). It is extremely important to select and separate the wheat, i.e., relevant evidence.

If appropriate information is available about the device, such as a known factory device, some data can be accessed even with the help of free tools, which contribute to the achievement of the test purposes. During the compilation of the event itself and the timeline of the events, it is determined what kind of event occurred in which the investigated drone played a role.

The test shall ensure that subsequent remote manipulation of the data (erasing, modifying, or factory reset) is excluded. Therefore, if the drone is still operational, it must be switched off and data must be kept safe.

During the examination of drones, the interpretation of the extracted data also belongs to the analysis phase. There are several important aspects to evaluate, and interpret results, as well as elements that are likely to be overlooked, such as:

- the meaning of all relevant data has been properly interpreted
- whether the study was prevented (e.g. by anti-forensics solutions)
- timestamps are consistent
- how expert independence has been ensured

As a result of the analysis and interpretation, the answers appropriate to the purpose of the study, the event under investigation, and the supporting evidence are produced. The last phase of drone forensics is reporting.

Conclusions

Drones – unmanned aerial vehicles – are used for various purposes, including mapping, creating photos, and videos of large areas, managing environmental surveys, and conducting military operations. The increasing use and functionality of UAVs increase the chances that a digital forensics investigation may be required to examine the circumstances of an event. As a result, both industry and academia have issued

[17] Alhussan et al. 2022.

numerous guidelines and publications on expert testing of UAVs. However, survey results show the need for an enhanced digital forensic framework to support future expert investigations of these vehicles. In this study, the aim was to determine the common points of the investigation of UAVs and forensics for modern transport vehicles and to analyse which steps and elements of the drone forensics procedure can be applied during the examination of highly automated vehicles. In addition, data storage solutions for drones and vehicles and categories of stored data were compared. Reviewing the forensics examination of drones, it can be concluded that this is a continuously developing field with similar examination challenges. The devices, methods of use, and control show a mixed picture, therefore complex, flexible, easy-to-use solutions need to be applied. The test steps do not go beyond the general steps of digital forensics, they can be partially or fully applied to drones. The process steps listed in this study and their content are similar to those of vehicle-related tests, but in the case of vehicle testing, several process steps and specific characteristics need to be taken into account.

Acknowledgement

Prepared with the professional support of the Doctoral Student Scholarship Program of the Cooperative Doctoral Program of the Ministry of Innovation and Technology financed from the National Research, Development and Innovation Fund.

The author would like to especially thank the managing director and staff of Alverad Technology Focus Ltd. for their support for the research work.

References

Al-Dhaqm, Arafat – Ikuesan, Richard A. – Kebande, Victor R. – Razak, Shukor – Ghabban, Fahad M. (2021): Research Challenges and Opportunities in Drone Forensics Models. *Electronics,* 10(13), 1519. Online: https://doi.org/10.3390/electronics10131519

Al-Room, Khalifa – Iqbal, Farkhund – Baker, Thar (2021): Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models. *International Journal of Digital Crime and Forensics,* 13(1), 1–25. Online: https://doi.org/10.4018/IJDCF.2021010101

Alhussan, Amel A. – Al-Dhaqm, Arafat – Yafooz, Wael M. S. – Razak, Shukor Bin Abd – Emara, Abdel-Hamid M. – Khafaga, Doaa S. (2022): Towards Development of a High Abstract Model for Drone Forensic Domain. *Electronics,* 11(8), 1168. Online: https://doi.org/10.3390/electronics11081168

Almusayli, Asma – Zia, Tanveer – Qazi, Emad-ul-Haq (2024): Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology. *Technologies,* 12(1), 11. Online: https://doi.org/10.3390/technologies12010011

Alotaibi, Fahad Mazaed – Al-Dhaqm, Arafat – Al-Otaibi, Yasser D. (2022): A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. *Computational Intelligence and Neuroscience,* (1), 1–13. Online: https://doi.org/10.1155%2F2022%2F8002963

Atkinson, S. – Carr, G. – Shaw, C. – Zargari, Shahrzad (2020): Drone Forensics: The Impact and Challenges. In Montasari, Reza – Jahankhani, Hmaid – Hill, Richard – Parkinson, Simon (eds.): *Advanced Sciences and Technologies for Security Applications.* Springer, 65–124. Online: https://doi.org/10.1007/978-3-030-60425-7_4

Azhar, M. A. Hannan Bin – Barton, Thomas Edward – Islam, Tasmina (2018): Drone Forensic Analysis Using Open Source Tools. *Journal of Digital Forensics, Security and Law,* 13(1), 7–30. Online: https://doi.org/10.15394/jdfsl.2018.1513

Fenyvesi, Csaba (2013): A kriminalisztika alapkérdései. In Gaál, Gyula – Hautzinger, Zoltán (eds.): *Pécsi Határőr Tudományos Közlemények XIV.* Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, 341–349. Online: www.pecshor.hu/periodika/XIV/fenyvesics.pdf

Gustafson, Kimmy (2024): Modern Forensic Science Technologies. *Forensics Colleges,* 9 February 2024. Online: www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies

Hankó, Viktória (2021): A drónokkal kapcsolatos kockázatok és kezelési lehetőségeik. *Hadmérnök,* 16(3), 189–202. Online: https://doi.org/10.32567/hm.2021.3.11

Jain, Upasita – Rogers, Marcus – Matson, Eric T. (2017): Drone Forensic Framework: Sensor and Data Identification and Verification. In *2017 IEEE Sensors Applications Symposium* (SAS), Glassboro, NJ, USA, 1–6. Online: https://doi.org/10.1109/SAS.2017.7894059

Kao, Da-Yu – Chen, Min-Ching – Wu, Wen-Ying – Lin, Jsen-Shung – Chen, Chien-Hung – Tsai, Fuching (2019): Drone Forensic Investigation: DJI Spark Drone as A Case Study. *Procedia Computer Science,* 159, 1890–1899. Online: https://doi.org/10.1016/j.procs.2019.09.361

Kovar, David – Bollö, Joel (2021): Drone Forensics. *JAPCC.org,* January 2021. Online: www.japcc.org/chapters/c-uas-drone-forensics/

Krajnc, Zoltán (2018): Drónok, hibrid fenyegetés, terrorizmus a légtérből: A légi hadviselés privatizálása. *Hadmérnök,* 13(4), 358–369. Online: https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/3705

Riaz, Talha (2023): Digital Forensics on Drones: Tools, Techniques, and Real-World Applications. *Linkedin,* 20 November 2023. www.linkedin.com/pulse/digital-forensics-drones-tools-techniques-real-world-talha-riaz-qrilf/

Répás, József (2023): Definition of Forensic Methodologies for Autonomous Vehicles. *Hadmérnök,* 18(1), 125–141. Online: https://doi.org/10.32567/hm.2023.1.9

Répás, József – Schmidt, Miklós – Vitai, Miklós – Berek, Lajos (2022): *Mit árul el rólunk az autónk? – Modern járművek IT szakértői vizsgálatának kérdései és lehetőségei* [What Does Our Car Tell about Us? – Questions and Possibilities of Digital Forensic Analysis of Modern Vehicles]. Pécs: Szentágothai János Szakkollégiumi Egyesület.

Studiawan, Hudan – Grispos, George – Choo, Kim-Kwang Raymond (2023): Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unadd-

ressed. *Computers & Security,* 132, 103340. Online: https://doi.org/10.1016/j.cose.2023.103340

Tiwari, Ashwani (2022): Drone Forensics: An Unrevealed Dome. *Data Forensics,* 19 April 2022. Online: www.dataforensics.org/drone-forensics/

Vízi, Linda (2019): *A Computer Forensics jogi vonzata.* Online: https://netacademia.hu/courses/take/computer-jog/multimedia/8481853-figyelem-ez-egy-classic-tanfolyam

HADMÉRNÖK
HADITECHNIKA
19. évfolyam (2024) 2. szám 29–48.
DOI: 10.32567/hm.2024.2.3

Kovács Zoltán,[1] Daruka Norbert,[2] Dénes Kálmán,[3]
Ember István,[4] Vég Róbert[5]

Kitöltési mintázatok a 3D-nyomtatásban és azok hatása az alkatrész tulajdonságaira[6]

Infill Patterns in 3D Printing and Their Impact on the Properties of Parts

Absztrakt

A 3D-nyomtatás technológiája napjainkra széles körűvé vált, nagyon sok eljárás ismert, és az alapanyagok köre is bővül. Ez az additív gyártástechnológia már nemcsak a termékeket előállító vállalatok számára, hanem szinte mindenki számára elérhetővé vált. Egyre többen vásárolnak otthoni használatra, hobbicélokra valamilyen 3D-nyomtatót. A 3D-nyomtatás technológiája viszonylag egyszerűnek tűnik, egy megrajzolt vagy az internetről letöltött tárgy .stl formátumát kell feldolgozni egy szeletelőprogramban a nyomtató számára, majd elindítani a nyomtatást. Többféle szeletelőprogram ismert, viszont közös bennük, hogy számtalan paramétert lehet beállítani a megfelelő nyomtatás érdekében. Az egyik ilyen fontos paraméter a test belsejének kitöltési mintája, amely hatással van a nyomtatási időre,

[1] Egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Műveleti Támogató Tanszék, e-mail: kovacs.zoltan@uni-nke.hu
[2] Robbanóanyag-ipari szakmérnök, e-mail: daruka.norbi@gmail.com
[3] Építőmérnök, e-mail: denes.kalman.1975@gmail.com
[4] Tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Műveleti Támogató Tanszék, e-mail: ember.istvan@uni-nke.hu
[5] Egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Haditechnikai Tanszék, e-mail: vegh.robert@uni-nke.hu
[6] A 2022-2.1.1-NL-2022-00012 számú „Kooperatív Technológiák Nemzeti Laboratórium" projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával, a Nemzeti Laboratóriumok pályázati program finanszírozásában valósult meg.

a felhasznált alapanyag mennyiségére és a nyomtatott tárgy felhasználhatóságára. A cikk bemutatja a különböző kitöltési mintázatokat, jellemzőiket, ismerteti főbb felhasználási területüket.

Kulcsszavak: kitöltési minta, kitöltési tényező, 3D-nyomtatás

Abstract

3D printing technology is now widespread, with a large number of processes and a growing range of materials. This additive manufacturing technology is now available not only to companies that make products, but to almost everyone. More and more people are buying 3D printers for home use, for hobby purposes. The technology of 3D printing seems relatively simple, you have to process the .stl format of a drawn object, or an object downloaded from the internet, in a slicer program for the printer and then start printing. There are several types of slicing softwares, but what they have in common is that you can set a wide range of parameters to get the right print. One of these important parameters is the infill pattern inside the body, which affects the printing time, the amount of raw material used and the usability of the printed object. The article describes the different infill patterns, their characteristics and their main uses.

Keywords: infill pattern, infill factor, 3D printing

Bevezetés

A 3D-nyomtatás mint additív eljárás napjaink egyik leggyorsabban és legdinamikusabban fejlődő gyártástechnológiája. A 3D-nyomtatást akár gyűjtőfogalomként is felfoghatjuk, mivel nagyon sok különböző nyomtatási eljárást különböztethetünk meg (például szálhúzásos [FDM – *fused deposition modeling*], műgyantás [SLA – *stereolithography*] vagy poralapú [SLS – *selective laser sintering*]), amelyek számos alapanyagot használnak fel a nyomtatás során (például műanyagok, fémek, kerámia és akár fa is). Szilárdságukat vágott vagy folyamatos szálerősítéssel (szén- vagy üvegszál, kevlár) fokozhatják.[7]

A 3D-nyomtatást eleinte gyors prototípusok készítésére használták, de manapság már igen széles körű az alkalmazása. Az iparon belül az egyedi alkatrészek gyártása mellett már kisebb szériában is gyakran 3D-nyomtatási technológiákat használnak fel.[8] Az orvostudományon belül a fogászat és az implantátumok előállítása jellemző felhasználási forma, de már a csökkent beszerzési és üzemeltetési árak miatt a háztartásokban is megjelentek a hobbicélú 3D-nyomtatók. Mindeközben folyamatosan bővül a professzionális alkalmazások száma is. Számos helyen kutatják a technológia katonai felhasználásának lehetőségeit, sőt már a műveleti területen történő alkalmazására is vannak kísérletek.[9]

[7] Hegedűs 2023a: 62.
[8] Gyarmati 2023; Gyarmati–Hegedűs–Gávay 2022.
[9] Végvári 2023.

A 3D-nyomtatás során a nyomtatandó elem rétegről rétegre épül fel, ezáltal olyan komplex alakzatok hozhatók létre, amelyek más gyártási eljárással nehezen, egyáltalán nem, vagy pedig csak sok hulladék keletkezésével állíthatók elő. A 3D-nyomtatás fontos előnye, hogy optimális esetben nem termel hulladékot. Az FDM-nyomtatás során keletkező hulladék (például a támaszanyag) megfelelő eljárásokkal ismét nyomtatásra alkalmas anyaggá alakítható. A 3D-nyomtatás további előnye, hogy az alkatrész üregességét változtatni lehet. Gyártás szempontjából egy üreges alkatrész kevesebb időt és anyagfelhasználást igényel, mint egy tömör, ezáltal a teljes tömeg és a költség is csökken. A 3D-nyomtatás minősége sok paraméter megfelelő beállításától függ. A mechanikai igénybevételnek nem kitett nyomtatványok esetén a különböző beállítási paraméterek közül csak azokat szokták figyelembe venni, amelyek a nyomtatvány esztétikáját és az előállítási költségét befolyásolják, vagyis a rétegvastagságot és a kitöltést. Mechanikai igénybevételnek kitett nyomtatványok esetén a nyomtatás iránya és a nyomtatáskor használt kitöltési minta típusa is befolyásolja az előállított alkatrész használhatóságát.[10]

A nyomtatáshoz megválasztott kitöltési mintázat teljes mértékben meghatározza a nyomtatandó alkatrész belső szerkezetét, és ezáltal az alkatrész mechanikai tulajdonságainak egy jelentős hányadát is. A mechanikai igénybevétel esetén számításba kell venni azt a tényt is, hogy a kitöltési mintázat mennyire stabil és homogén az alkalmazott sűrűség esetén. Egyes kitöltési mintázatok csak bizonyos sűrűségig érhetők el ténylegesen, mivel egy adott érték fölött a nyomtató már nem tudja a tényleges mintát tökéletesen létrehozni.

Annak ellenére, hogy a 3D-nyomtatást gyakran gyors prototípusgyártásnak nevezik, valójában a nyomtatás többnyire sok időt vesz igénybe, főként egy jó minőségű nyomtatvány elkészítésekor. A nyomtatandó elemet az adott követelményeknek megfelelően nem feltétlenül tömör tárgyként nyomtatják, hanem üreges elemként, amelyet különféle geometriai alakzatokkal töltetnek meg az anyagfelhasználás optimalizálása és a nyomtatási idő csökkentése érdekében. Az üreges nyomtatott tárgyak gyakran nem elég erősek, teljesen tömör tárgyak nyomtatása viszont sok alapanyag felhasználásával jár. Az FDM-nyomtatással ritkán készítenek szilárd alkatrészeket, általában az elem belsejét kitöltik egy, a célnak megfelelő meghatározott mintával, adott sűrűséggel. Ez a sűrűség 0%-tól (teljesen üreges) 100%-ig (tömör tárgy) terjedhet. A 100%-os kitöltés esetén az erősség szempontjából nem igazán számít a kitöltési minta típusa, de a nyomtatási idő optimalizálása szempontjából igen.[11]

A kitöltési mintát a szeletelőprogramban lehet beállítani (például Cura vagy adott 3D-nyomtató gyári szeletelőprogramja), ahol a program különféle mintákat ajánl, amelyek mindegyikének megvannak a maga jellemzői, erősségei és fontosabb alkalmazási területei. A kitöltési mintákat külön-külön is lehet értékelni, de akár különböző szempontok alapján csoportosítani is lehet őket.

A Cura 5.2-es vagy újabb verziójában 14-féle kitöltési minta áll rendelkezésre, amelyeket felhasználhatóságuk szerint csoportosíthatjuk:

[10] Lennert–Sárosi 2021: 47.
[11] KREATE 2024.

- egyszerű és gyors 3D-nyomtatványokhoz (modellek, figurák): vonalak, cikcakk, villám;
- prototípusokhoz és közepesen erős alkatrészekhez: rács, háromszögek, három-hatszög;
- erős és funkcionális alkatrészekhez: kocka, osztott kocka, negyed kocka, oktett, giroid;
- rugalmas 3D-nyomtatványokhoz: körkörös, kereszt, 3D kereszt.[12]

Természetesen nem ilyen egyértelmű az adott kitöltési minta alkalmazási területe, mert egyes minták szélesebb körben használhatók. A nyomtatott elem erősségét nemcsak a kitöltési minta típusa határozza meg, hanem a kitöltési sűrűség és a kitöltési vonalak iránya is, mindezek együttesen nemcsak az alkatrész mechanikai tulajdonságait határozzák meg, de hatással vannak az utólagos megmunkálás lehetőségeire és az elérhető felületi minőségre is.[13]

Kitöltési minták egyszerű és gyors 3D-nyomtatványokhoz

Jellemző kitöltési sűrűségük 0–15% között van. Ezekkel az alacsony kitöltési értékekkel gyorsan elő lehet állítani a nyomtatványokat, amelyek nincsenek nagy erőhatásoknak kitéve (például modellek, különféle figurák).

Vonalak minta (lines)

A legismertebbnek nevezhető kitöltés a 3D-nyomtatásban a vonalak alkalmazása. Pontosan azt jelenti, amit a szó közöl, vagyis egyenes vonalak 3D-ben nyomtatva az x vagy y tengely mentén. A minta folyamatos vonalakat használ, amelyek egy irányban futnak, ezáltal töltve ki a 3D-nyomtatott test belsejét (1.a ábra). A kitöltő vonalak egymáshoz képest 90°-os szögben követik egymást, minden következő rétegben. Felülről nézve a minta rácsmintának tűnik, azzal a különbséggel, hogy minden rács két rétegből áll. Mivel a mintában a vonalak párhuzamosan futnak, így egyenletesebben osztják el a felső rétegek súlyát és feszültségét a test belsejében, megakadályozva a koncentrált nyomási pontok kialakulását. A minta segít elkerülni a 3D-nyomtatás „párnázottságát", amikor a nyomtatott test felső felületei egyenetlenek lesznek (párnaszerű megjelenés). A vonalak minta gyorsan nyomtatható, kevés alapanyagot használ fel, a szeletelőprogram számára könnyen számítható. Hátránya, hogy gyenge szilárdságot biztosít mind vízszintes, mind függőleges irányban. Jó választás olyan kicsi elemek nyomtatásához, amelyeknek nem kell túl erősnek lenniük.[14]

[12] Goldschmidt 2024.
[13] Zentay–Hegedűs–Végvári 2022.
[14] Pranay 2024.

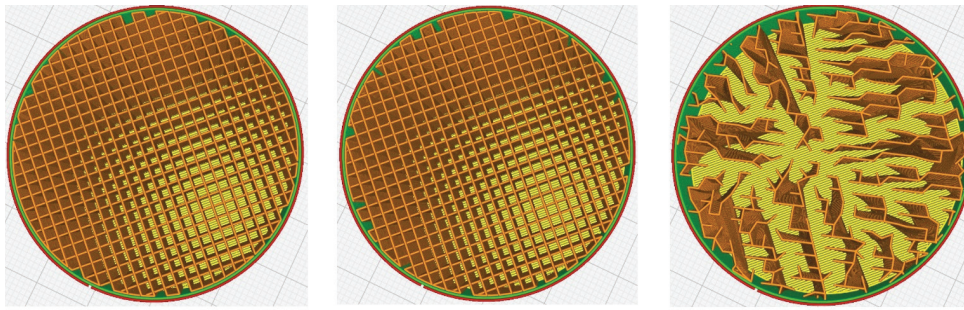
Cikcakkminta (zig zag)

A cikcakkminta részben hasonlít a vonalmintához, a különbség az, hogy egy rétegben váltakozó vonalak találhatók, amelyek ellentétes irányban haladnak, ami cikcakkmintát eredményez (1.b ábra). A minta csökkenti a filamentszál visszahúzásának szükségességét, így FDM-technológia mellett gyorsabb nyomtatást tesz lehetővé. Az egymást metsző átlós vonalak kellő erősítést adnak, ami a nyomtatvány belsejét megfelelően meg tudja támasztani. A kitöltési minta vezetése minden réteggel irányt változtat, ami szép nyomtatványt biztosít. A cikcakkminta egyszerű elemek nyomtatásához ideális, mivel kevesebb felső réteget igényel a kis hézagok miatt, rövidebb a nyomtatás ideje, és kevesebb az alapanyag-felhasználás is. A minta alkalmazásának hátránya, hogy az alkatrész z irányban csak kis igénybevétel elviselésére alkalmas.

Villámminta (lightning)

A villámkitöltés inkább külső támaszként működik, mint hagyományos kitöltésként, mivel olyan belső szerkezetet hoz létre, ami a tárgy nehezebben nyomtatható részeit támasztja alá, és alig, vagy egyáltalán nem támasztja meg azokat a részeket, ahol a nyomtatás anélkül is befejezhető. A villámkitöltéssel gyorsabb nyomtatás hozható létre, kevesebb anyagfelhasználással, mint az előző kettőnél. A villámkitöltés úgy működik, hogy azonosítja és támogatja a modell azon belső területeit, amelyeknek támasztékra van szükségük a nyomtatás során. A létrejövő támaszték egy elágazófa-szerű szerkezet lesz, ami villámcsapásra emlékeztet (1.c ábra). A villámkitöltés hatékonysága abból adódik, hogy a külső támaszokkal ellentétben, amelyeknek az építőlemezen kell kezdődniük, a villámtámaszok bárhol kezdődhetnek és végződhetnek a modell belső falán, így kevesebb anyagot használ fel, és a nyomtatott tárgy nagy része teljesen üreges maradhat. A villámkitöltés bonyolultsága miatt a szeletelési idő kismértékben megnő. Villámkitöltésnél a kitöltés százalékos aránya és a felhasznált anyag közötti kapcsolat nem lineáris, a kitöltés mennyisége a nyomtatandó tárgy geometriájától függ. Magas kitöltési százalékot nem célszerű alkalmazni a tárgy erősségének növelése érdekében, inkább másik kitöltési mintát kell választani. A villámkitöltés jól alkalmazható nem funkcionális tárgyak nyomtatására, például nagy belső felülettel rendelkező tárgyaknál (szobor). A nyomtatáshoz legalább 2-3 falréteget célszerű használni.[15] Igen gyakori az alkalmazása az SLA-nyomtatók esetében, ahol a technológia sajátossága miatt a támasztékok száma és kialakítása nem befolyásolja a nyomtatási sebességet.

[15] Lásd: https://ultimaker.com/learn/how-to-print-like-a-flash-with-lightning-infill/



a) b) c)

1. ábra: a) vonalak minta, b) cikcakkminta, c) villámminta
Forrás: a szerzők szerkesztése

Kitöltési minták prototípusokhoz és közepesen erős alkatrészekhez

Jellemző kitöltési sűrűségük 15–50% között van. Kis és közepes igénybevételeknek kitett alkatrészek nyomtatásához a rács, háromszög vagy három-hatszög kitöltési mintát kell alkalmazni, amelyek közepes erősséget biztosítanak. A vonalak mintához képest a nyomtatási idő például FDM-technológia esetében akár 25%-kal is nagyobb lehet.

Rácsminta (grid)

Rácsminta esetén a nyomtatófej keresztirányban mozog, az egymásra merőlegesen futó metsző vonalak rácsmintát hoznak létre (2.a ábra). A rácsmintának jobb a réteg-tapadása, mint az egyenes vonalú (vonalak minta) kitöltésnek. Azokon a helyeken, ahol a nyomtatási utak keresztezik egymást, az alapanyag felhalmozódik, ami a nyomtatás során zajt kelt, vagy akár nyomtatási hibát is okozhat, amikor a nyomtatófej átmegy rajta. A minta alakja a nyomtatás során végig ugyanaz marad, ezáltal minden irányban hasonló szilárdságot ad az alkatrésznek. A rácsminta viszonylag kis mennyiségű alap-anyag felhasználásával közepes szilárdságot nyújt. Egyenletes alátámasztást biztosít a felső felületnek, de a nagy terhelést nem képes elviselni.[16]

Háromszögek minta (triangles)

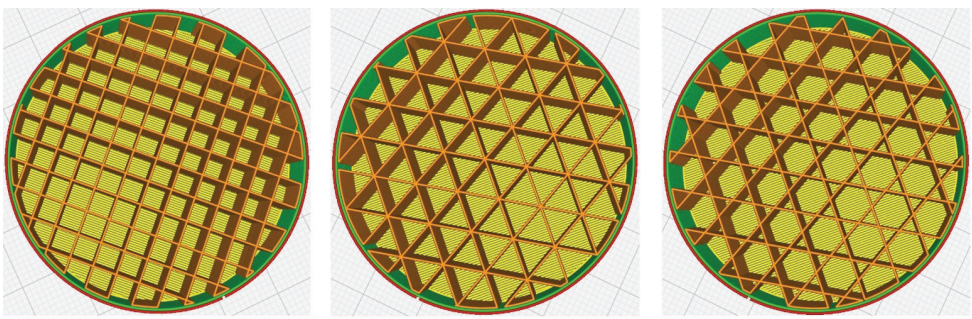
Hasonló a rácsmintához, mivel a nyomtatószál útjai egy rétegben keresztezik egy-mást, viszont három irányban nyomtatva háromszög alakú zsebek keletkeznek a 3D-nyomtatvány belsejében (2.b ábra). Mivel az egymásba illeszkedő háromszögek egyenletesebben osztják el az erőket a nyomtatvány belsejében, növekszik annak szilárdsága. A belső háromszögek erős szerkezetet hoznak létre, ezért a z irányú

[16] Omkar 2022.

erőhatároknak is képes nagyobb mértékben ellenállni. Különböző prototípusok előállítására kiválóan alkalmas a háromszögminta, mivel nagyobb nyomtatási sebességgel, jelentős szilárdságot biztosít, és jó nyírási ellenállással rendelkezik, viszont nyomtatás során a sok irányváltoztatás a nyomtatószál megszakadásához vezethet. A nyomtatási idő és anyagfelhasználás tekintetében szinte azonos a rácsmintával.[17]

Három-hatszög minta (tri-hexagon)

A három-hatszög minta a háromszögletű és hatszögletű minták keveréke, ahol a kitöltő vonalak egy rétegen belül keresztezik egymást. A kitöltő vonalak a háromszögmintához hasonlóak, de kissé el vannak tolva, így a minta minden rétegnél egyedi háromszög- és hatszögmintát hoz létre. A háromszögeket és a hatszögeket alkotó vonalak három irányban futnak, de nem találkoznak ugyanabban a helyzetben (2.c ábra). A háromszögek és a hatszögek együttműködése jó szilárdságot biztosít a minden irányból fennálló terhelésekkel szemben. A nyomtatás ideje a háromszögmintának megfelelő, a minta jól megtámasztja a felső rétegeket. Az azonos szilárdság vízszintes és függőleges irányban alkalmassá teszi a mintát prototípusok és közepes mechanikai szilárdságot igénylő alkatrészek nyomtatására.[18]



2. ábra: a) rácsminta, b) háromszögek minta, c) három-hatszög minta
Forrás: a szerzők szerkesztése

Kitöltési minták erős és funkcionális alkatrészekhez

Jellemző kitöltési sűrűségük 50% fölött van. Olyan alkatrészek nyomtatásához alkalmasak, amelyek több irányú terhelésnek vannak kitéve, valamint nagy szilárdságot igényelnek (például polctartó). Ezek a kitöltési minták biztosítják az erők egyenletes

[17] Rafiqul 2020.
[18] Ekaran 2023.

elosztását, iránytól függetlenül. Ezeknek a mintáknak a nyomtatása hosszabb időt vesz igénybe, de előnyük, hogy tartós, mégis könnyű alkatrészeket lehet általuk előállítani.[19]

Kockaminta (cubic)

A nyomtatás útvonalai egy rétegen belül keresztezik egymást, és a létrehozott minta olyan kockákat eredményez, amelyek egyik sarka lefelé néz (3.a ábra). A kocka alakú minta csökkenti a párnázás kialakulásának esélyét. A kitöltés belsejében légzsákok jönnek létre, amelyek hőszigetelésként szolgálnak, és ezáltal a nyomtatvány a vízen lebeghet. A kocka alakú kitöltés minden irányban jó szilárdságot és megfelelő esztétikát biztosít.

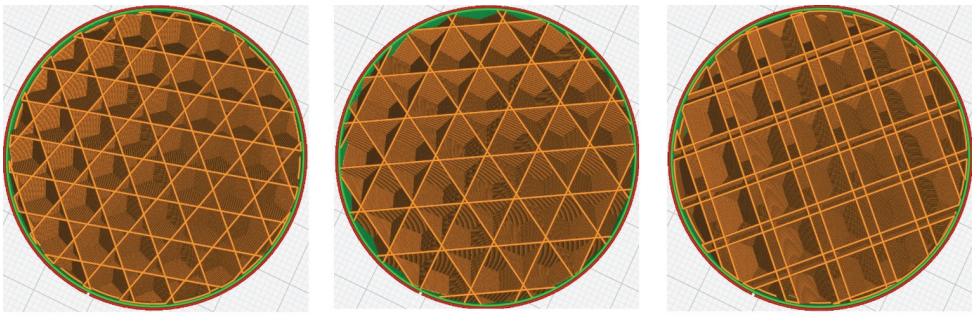
Osztottkocka-minta (cubic subdivision)

Az osztottkocka-minta hasonló a kockamintához, azzal a különbséggel, hogy a 3D-nyomtatvány középső része üreges. A nagyobb kockák a nyomtatvány közepén, a kisebbek pedig a szélén találhatók (3.b ábra). Alacsony kitöltési százalék esetén a nyomtatvány közepe teljesen üres lehet. A kockamintához képest a nyomtatási idő jelentősen lerövidül, javítja a szilárdság-tömeg arányt, mivel a kockák elég sűrűek ahhoz, hogy megfelelő erőt és tartást biztosítsanak, és elég könnyűek ahhoz, hogy ne eredményezzenek túl nagy súlyt. A minta hátránya, hogy nem alkalmas nagy terhelés elviselésére, a szeletelés számításigényes, így több időt vesz igénybe, és alacsony kitöltési százalék a felső réteg megereszkedését okozhatja.[20]

Negyedkocka-minta (qarter cubic)

A negyedkocka-minta kis kockákat és téglalap alakú formákat tartalmaz, amelyek rács alakban vannak elrendezve, ezáltal nagyobb anyagsűrűséget és jobb mechanikai tulajdonságokat tesz lehetővé (3.c ábra). Mivel a minta kis kockákat tartalmaz, hatékonyan osztja el a súlyt, jó szilárdságot biztosít kisebb falvastagság mellett. A kockák rácsszerű elrendezése esztétikusabbá teszi a nyomtatványt. A negyedkocka-minta alkalmas olyan alkatrészek előállítására, amelyeknek egyszerre kell erősnek és könnyűnek lenniük. Hátránya, hogy plusz réteget kell elhelyezni a nyomtatvány tetején a párnázottság elkerülése érdekében.

[19] Maker.io Staff 2021.
[20] Prusa 2024.



3. ábra: a) kockaminta, b) osztottkocka-minta, c) negyedkocka-minta
Forrás: a szerzők szerkesztése

Oktettminta (octet)

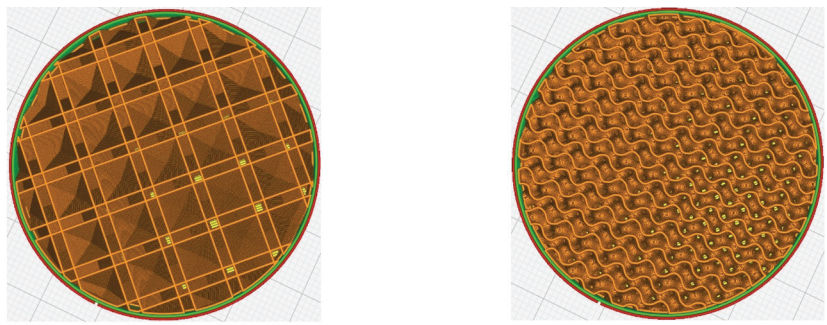
Az oktettminta 3D-kockákból és -tetraéderekből áll, így erős belső szerkezetet hoznak létre, főként ott, ahol a két forma találkozik (4.a ábra). Az oktettminta az alkatrésznek minden irányban jó nyírási ellenállást nyújt. A minta komplex formák 3D-nyomtatására alkalmas, mivel erős belső szerkezettel rendelkezik, csökkenti a párnázást, és kiváló szilárdságot biztosít. A minta hátránya, hogy a hosszabb kitöltési vonalak áthidalási és megereszkedési problémákat okozhatnak.[21]

Gyroidminta (gyroid)

A gyroidkitöltés viszonylag új, például a Cura esetében csak a 3.6-os verziójában, 2018-ban vezették be. A gyroidkitöltés az egyik legfejlettebb és legelőnyösebb kitöltési minta a nyomtatott alkatrész szilárdság/tömeg arányának szempontjából. A gyroid metsző 2D-hullámvonalakból álló 3D-geometria, amelynek nincsenek egyenes vonalai, és amely erős szerkezetet hoz létre. A gyroidmintával külső héj nélküli tárgyak is nyomtathatók. A kitöltési sűrűséget minimalizálni lehet változatlan nyírószilárdság mellett. A gyroidkitöltés hullámvonalak folyamatos nyomtatásával jön létre, ahol minden réteg különbözik az előzőtől, így hozva létre az összetett hullámos mintát. A gyroidkitöltéssel már 10%-os kitöltési tényezővel is jó szilárdság érhető el. A gyroidkitöltés egyik előnye, hogy lehetővé teszi közel izotróp tulajdonságú részek nyomtatását. Izotrópnak nevezzük azokat az anyagokat, amelyek ugyanolyan szilárdságot és anyagtulajdonságokat mutatnak függetlenül attól, hogy milyen irányú terhelésnek vannak kitéve. A gyroidkitöltés nem tökéletesen izotróp, de a köbös szimmetriája miatt hasonló tulajdonságokat biztosít.[22] A kinyomtatott 3D-s tárgy ellenállása mindhárom tengelyen hasonló. A gyroidkitöltésnek van az egyik legjobb

[21] Ekaran 2023.
[22] Boissonneault 2024.

sűrűség/szilárdság aránya a különböző minták közül. Ugyanolyan szilárdságú alkatrész előállításához kevesebb alapanyagra van szükség, mint más nagyobb sűrűségű kitöltési minták esetén. A nyomtatás sebessége a gyroidminta íves szerkezete miatt gyorsabb lehet a többi kitöltéshez képest. A minta hátrányaként lehet említeni, hogy mivel összetettebb, mint a 2D-s kitöltési minták, szignifikánsan hosszabb szeletelési időt igényel. Ha a kitöltési tényező túl nagy, és a kitöltő hullámok túl közel vannak egymáshoz, akkor a nyomtatófej mozgása rezgéseket kelthet a nyomtatóban, ami nyomtatási hibákat okozhat. Ezek a hibák elkerülhetők kisebb sűrűségű nyomtatás alkalmazásával. A kitöltőminta tetszetős geometriája miatt, illetve hogy héj nélkül is lehet nyomtatni, alkalmas esztétikus modellek (például lámpa, váza) előállítására. A gyroidminta a könnyű súly és a megfelelő szilárdság miatt jól alkalmazható a gépjármű- és repülőgépiparban, ahol az üzemanyag-felhasználás hatékonysága a súlycsökkentéstől nagymértékben függ.[23]



4. ábra: a) oktettminta, b) gyroidminta
Forrás: a szerzők szerkesztése

Kitöltési minták rugalmas 3D-nyomtatványokhoz

Kitöltési sűrűségük 0–100% között van, vagyis adott alkatrész igénybevétele, használati jellege határozza meg a kitöltés nagyságát. A kör-, kereszt- és 3D keresztminták biztosítják a legjobb rugalmasságot 3D-nyomtatott alkatrészeknek.

Körkörös minta (concentric)

A mintát koncentrikus körök sorozata hozza létre, ahol a kitöltés követi a modell kerületi vonalait, és a középpont felé kisebbíti azokat. Kocka nyomtatása esetén a kitöltés sok függőleges négyzetből fog állni, henger nyomtatása esetén a koncentrikus kitöltés koncentrikus köröket hoz létre a henger belsejében (5.a ábra). A körkörös minta esetén a kitöltés illeszkedik a nyomtatvány alakjához, ezáltal könnyen hajlíthatóvá

[23] Weyhaupt 2021; Chandler 2017.

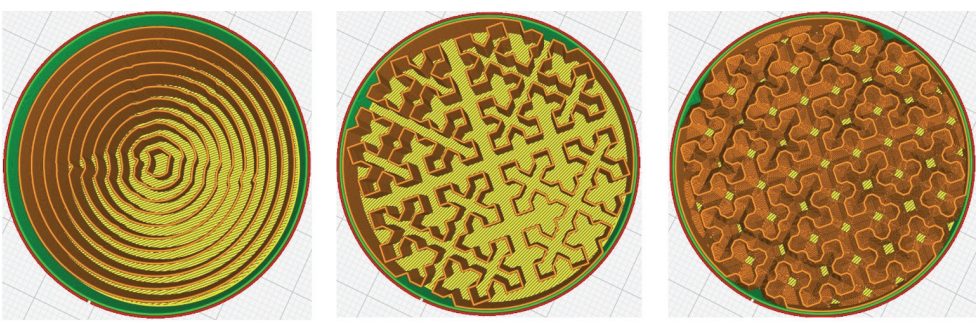
és rugalmasabbá teszi az alkatrészt. Olyan nyomtatványokhoz is alkalmas, ahol a belső szerkezetnek nem kell jelentős mechanikai igénybevételt elviselnie. A körkörös minta alkalmazása rugalmas alapanyag használatával optimális. A minta jellegzetes vizuális megjelenést hoz létre a nyomtatvány belsejében, ami áttetsző vagy félig áttetsző anyagon keresztül is látható. A minta gyorsabban nyomtatható, mivel létrehozása általában körkörös irányú folyamatos mozgást tartalmaz. A minta alkalmazásának előnye, hogy a sűrűség változtatásával szabályozható a merevség, vagyis a nyomtatvány rugalmassága, kevesebb az alapanyag-felhasználása és könnyen szeletelhető. A minta hátránya, hogy a felső rétegek könnyen megereszkednek a kitöltési sűrűség csökkentésével, valamint hogy ez az egyik leggyengébb kitöltési minta.[24]

Keresztminta (cross)

A minta keresztező vonalakat tartalmaz, amelyek keresztrácsot hoznak létre. A rács és a keresztek közötti hézag miatt rugalmas és sok hajlítást elvisel. A keresztminta jól alkalmazható olyan tárgyakhoz, amelyeknek hajlíthatónak kell lenniük (például telefontok). A kitöltő minta felülről nézve keresztre emlékeztet, ami áttetsző alapanyagnál dekoratív mintát nyújt (5.b ábra). FDM-nyomtatás során kevés szálvisszahúzást igényel, ami által a nyomtatási idő lerövidül. A minta alkalmazásának hátránya, hogy vízszintes (x–y) irányban nem nyújt kellő szilárdságot, míg függőleges (z) irányban nem elég rugalmas.

3D keresztminta (cross 3D)

A keresztminta 3D-s változata, amely a nyomtatandó tárgy belsejében összekapcsolt keresztekből álló 3D-rácsot tartalmaz (5.c ábra). A 3D keresztminta minden irányban azonos szilárdságot biztosít, kevesebb alapanyag-felhasználással jár, és átlátszó anyag használata esetén esztétikus megjelenést nyújt. A minta bonyolultabb, tovább tart a szeletelés.[25]



5. ábra: a) körkörös minta, b) keresztminta, c) 3D keresztminta
Forrás: a szerzők szerkesztése

[24] Prusa 2024.
[25] Pranay 2024.

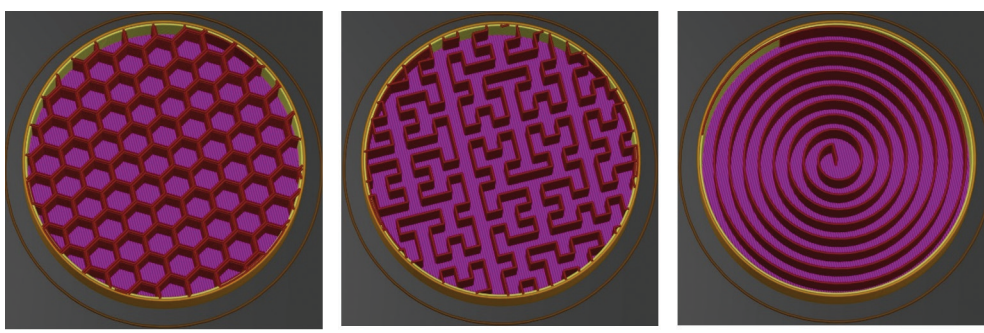
Egyéb kitöltési minták

Természetesen a Cura szeletelőprogramon kívül még sok egyéb, úgynevezett gyári szeletelőprogram létezik, amelyet a különböző gyártmányú 3D-nyomtatókhoz ajánlanak a forgalmazók. Ezekben a más típusú programokban megtalálhatóak a Cura-ban már látott kitöltési mintázatok, vagy azok valamilyen kisebb módosítással ellátott változatai, vagy pedig ezektől eltérő geometriát nyújtó mintázatok (például a SuperSlicer szeletelőprogramban megtalálható: méhsejt, Hilbert-görbe és az Arkhimédeszi akkord is).

A méhsejtkitöltés (6.a ábra) egy hatszögekből álló rácsot alkot, ahol a nyomtatási pályák nem keresztezik egymást, és amelynek fő előnye a nagy mechanikai ellenállása. Hátránya, hogy magas anyagfelhasználással jár, és a nyomtatási idő is jelentős mértékben megnő emiatt.

A Hilbert-görbe kitöltő minta (6.b ábra) egy téglalap alakú labirintust hoz létre a test belsejében. A minta előnye az esztétikus megjelenés, és mivel a test több nagy üregre van osztva, könnyen megtölthető a célnak megfelelően valamilyen folyadékkal. A kitöltő minta hátránya a hosszú nyomtatási idő.

Az Arkhimédeszi akkord (6.c ábra) egy spirál alakú minta, amely bizonyos fokú rugalmassággal rendelkezik, főként, ha rugalmas alapanyagból állítjuk elő. A spirális kitöltés megkönnyíti a folyadékkal feltöltést. Mivel egyszerű geometriáról van szó, mind anyagot, mind időt meg lehet takarítani a minta alkalmazásával.[26]



6. ábra: a) méhsejtminta, b) Hilbert-görbe minta, c) Arkhimédeszi akkordminta
Forrás: a szerzők szerkesztése

A kitöltési minta mellett jelentősége van a kitöltési vonal irányának is, amely alapértelmezésként 45°-ra van állítva, ezáltal FDM-technológia esetén mind az x irányú, mind az y irányú motor együttesen dolgozik a nagyobb nyomtatási sebesség érdekében. Adott esetben a megfelelő rugalmasság vagy szilárdság elérésére a kitöltési szöget célszerű lehet megváltoztatni. Ugyanakkor például SLA-technológia használata mellett a kitöltés tájolása nem befolyásolja a nyomtatási időt, azt szabadon lehet állítani például a várható mechanikus igénybevételnek megfelelően.

[26] SuperSlicerHu, lásd: https://szi-ga.gitbook.io/superslicerhu/konfig/print_settings/kitoeltesi-mintak

A kitöltés a legtöbb esetben egyenletes, de egyes programokban lehetséges állítani, hogy a kitöltés sűrűsége nagyobb legyen a kerület felé. A kitöltési sűrűség változtatásával az alkatrész szilárdságának és merevségének megtartása mellett kevesebb anyagot lehet felhasználni. A kitöltési sűrűség változtatásának másik módja, amikor a z tengely irányában változik a kitöltő minta sűrűsége, vagyis a kitöltés az alkatrész tetejének közelében sűrűbb lesz, mint az alján. Az általánosan használt szeletelőprogramok nem támogatják sem az egy alkatrészen belül, sem a nyomtatási meneten belül a kitöltési minták változtatását.

Kitöltési minták FDM-technológiás nyomtatási ideje és filamentfelhasználása

A kitöltési mintázatok általános jellemzése után célszerű megvizsgálni, hogy az egyes minták milyen nyomtatási időkkel és alapanyag-felhasználással járnak együtt a legáltalánosabban alkalmazott FDM-nyomtatók esetében. Mivel a nyomtatási idő azonos nyomtatási jellemzők és adott kitöltési mintázat esetén is különböző lehet más geometriájú modellek esetén, ezek összehasonlítása fontos. A kitöltési mintázatok jellemzőinek összehasonlításához három mintatestet választottunk ki, egy 50 x 50 x 50 mm-es kockát, egy 50 mm átmérőjű gömböt és egy funkcionális alkatrészt.

A kiválasztott mintatestek közül a kocka formája fogja legkevésbé befolyásolni a kitöltési mintázatot, mivel csak egy vékony héjjal rendelkezik, és a falai is merőlegesek, valamint a rétegek nagysága tetszőleges kitöltési minta mellett is közel azonos. A gömb forma is szabályos alakzat, azzal a fontos különbséggel, hogy az oldalfalak nem függőlegesek, és minden réteg különböző nagyságú. Mivel a 3D-nyomtatások alapvetően nem kockák és gömbök, hanem valós alkatrészek vagy egyéb tárgyak, amelyek formája szabálytalan, és akár szerteágazó lehet, valamint sok esetben könynyítésekkel vannak ellátva, szükséges egy ilyen tárgynál is elvégezni a vizsgálatot. A szabályos tárgyak eredményeihez hasonlítva egy komplexebb alkatrész eredményeit pontosabban meg lehet határozni, hogy melyik kitöltési minta mennyire befolyásolja a nyomtatási időt és a felhasznált alapanyag mennyiségét. Mivel számos szeletelőprogram van használatban, az összes ilyen programban található kitöltési mintázatot feldolgozni hatalmas munka lenne, ami nem feltétlenül volna célszerű, és a különböző programokban található minták között elég nagy átfedés tapasztalható. Ezért a széles körben használt Cura szeletelőprogramban található 14 darab kitöltési mintát hasonlítjuk össze egymással, mivel ez a program nemcsak széleskörűen felhasználható, de mivel ingyenes, mindenki számára elérhető is. A három különböző mintadarabot a rögzített főbb beállítási jellemzők mellett hat különböző kitöltési sűrűség változtatásával nyomtatjuk, miközben rögzítjük a nyomtatási időt és a szükséges filement hosszúságának nagyságát. A kapott eredményeket táblázatos formában közöljük, és vonjuk le a következtetéseket.

A nyomtatás során alkalmazott főbb beállítási jellemzők:

- nyomtató típusa: Ultimaker S3;
- filament: PLA;
- fúvóka mérete: 0,4 mm;

- rétegvastagság: 0,1 mm;
- falvastagság: 1 mm;
- alsó/felső vastagság: 1 mm;
- nyomtatási/kitöltési sebesség: 70 mm/s;
- nyomtatófej utazási sebessége: 150 mm/s;
- visszahúzási sebesség: 45 mm/s.

A nyomtatás során alkalmazott beállítási értékek közül csak a legfontosabbakat ismertettük, azokat, amelyeknek a legnagyobb hatása van a nyomtatási időre és a felhasznált alapanyag-mennyiségre. Természetesen számos egyéb jellemző van a Cura szeletelőprogramban, amelyek megváltoztatása lehetséges, de az alapbeállítások állandóra vételével, a kitöltési tényező megváltoztatásával összehasonlíthatók a különböző kitöltési minták alapanyag-felhasználásai és nyomtatási idői.

1. táblázat: Kitöltési minták nyomtatási idejének változása a kitöltési sűrűség változásának függvényében 50 x 50 x 50 mm-es kocka nyomtatása esetén

		Kitöltési sűrűség (%)					
Fsz.	**Kitöltési minta neve**	**10**	**30**	**50**	**70**	**90**	**100**
		kitöltési minta nyomtatási ideje (óra.perc)					
1	rács	5.10	7.21	9.39	11.58	14.14	15.24
2	vonal	5.00	7.18	9.36	11.55	14.13	15.20
3	háromszög	4.57	7.16	9.34	11.52	14.12	15.16
4	három-hatszög	4.54	7.11	9.30	11.47	14.10	15.13
5	kocka	4.58	7.16	9.33	11.51	14.10	15.19
6	osztott kocka	4.45	6.24	7.27	8.15	8.54	9.16
7	oktett	4.57	7.16	9.35	11.49	14.07	15.18
8	negyed kocka	4.59	7.14	9.35	11.50	14.07	15.18
9	körkörös	4.39	7.03	9.26	11.49	14.12	15.23
10	cikcakk	4.57	7.16	9.34	11.52	14.13	15.20
11	kereszt	4.54	8.32	12.10	17.08	22.32	24.33
12	3D kereszt	4.53	7.58	11.09	14.50	19.08	20.38
13	gyroid	5.01	8.11	13.03	18.01	23.13	25.53
14	villám	3.55	4.12	4.22	4.26	4.34	4.39

Forrás: a szerzők szerkesztése

Az 1. táblázatban látható, hogy a 14 db kitöltési mintából 9 db szinte teljesen azonos nyomtatásiidő-jellemzőkkel rendelkezik. Az osztottkocka-minta viszont lényegesen kisebb, a kereszt-, 3D kereszt- és gyroidminták pedig sokkal nagyobb nyomtatási idővel. A villámminta nyomtatási ideje alig mutat eltérést a kitöltési sűrűség változtatása

közben, ami betudható annak, hogy igazából a minta inkább alátámasztásként szolgál, és a test belsejének nagy része üreges marad. Mivel a test formája (kocka) adott, ezért a kitöltési sűrűség változtatásának alig van hatása a nyomtatási időre. A villámmintánál, miközben a kitöltés 10%-ról 100%-ra nő, a nyomtatási idő mindössze 19%-kal növekszik.

2. táblázat: Kitöltési minták nyomtatásához szükséges filament hosszúságának változása a kitöltési sűrűség változásának függvényében 50 x 50 x 50 mm-es kocka nyomtatása esetén

		Kitöltési sűrűség (%)					
Fsz.	**Kitöltési minta neve**	**10**	**30**	**50**	**70**	**90**	**100**
		nyomtatáshoz szükséges filament hosszúsága (m)					
1	rács	4,01	7,46	10,92	14,39	17,85	18,70
2	vonal	4,01	7,46	10,92	14,40	17,87	18,70
3	háromszög	3,98	7,47	10,93	14,39	17,85	18,71
4	három-hatszög	3,91	7,35	10,83	14,29	17,74	18,61
5	kocka	4,00	7,45	10,.89	14,36	17,85	18,70
6	osztott kocka	3,40	5,66	6,89	7,76	8,51	8,63
7	oktett	3,96	7,46	10,91	14,36	17,76	18,70
8	negyed kocka	3,98	7,42	10,91	14,35	17,80	18,70
9	körkörös	3,47	7,05	10,63	14,22	17,81	18,70
10	cikcakk	3,98	7,47	10,93	14,39	17,86	18,70
11	kereszt	3,60	6,49	9,17	12,06	14,81	15,31
12	3D kereszt	3,52	6,05	8,54	11,09	13,62	14,05
13	gyroid	4,01	7,43	10,72	14,14	17,47	18,31
14	villám	2,20	2,43	2,55	2,58	2,71	2,72

Forrás: a szerzők szerkesztése

A kitöltési minták nyomtatásához felhasznált filament hosszának a változásai láthatók a 2. táblázatban. A 14 db kitöltési mintából 10 db szinte azonos filamentfelhasználással rendelkezik. A gyroidminta érdekessége, hogy benne van az azonos felhasznált alapanyag csoportjában, ugyanakkor viszont az 1. táblázat szerint a legmagasabb nyomtatási idővel rendelkezik. Az osztottkocka-kitöltéshez használt anyagmennyiség a növekvő kitöltési százalékok esetén akár az 50%-os érték alá is csökkenhet a kocka- (rács- stb.) mintához képest. A kereszt- és 3D keresztminták sajátossága, hogy annak ellenére, hogy hosszú nyomtatási időkkel rendelkeznek, a felhasznált alapanyag mennyisége mégis csökken. A villámminta itt is egyenletes, alig növekvő emelkedést mutat, mivel a kitöltési százalék növekedése lényegesen nem befolyásolja a nyomtatási idő mellett a felhasznált alapanyag mennyiségét sem.

3. táblázat: Kitöltési minták nyomtatási idejének változása a kitöltési sűrűség változásának függvényében 50 mm átmérőjű gömb nyomtatása esetén

		Kitöltési sűrűség (%)					
Fsz.	**Kitöltési minta neve**	**10**	**30**	**50**	**70**	**90**	**100**
		kitöltési minta nyomtatási ideje (óra.perc)					
1	rács	2.55	4.08	5.20	6.32	7.43	8.20
2	vonal	2.56	4.08	5.20	6.32	7.43	8.19
3	háromszög	2.54	4.07	5.19	6.31	7.42	8.18
4	három-hatszög	2.53	4.06	5.18	6.30	7.41	8.17
5	kocka	2.54	4.07	5.19	6.31	7.42	8.18
6	osztott kocka	2.46	3.38	4.10	4.37	5.00	5.08
7	oktett	2.56	4.09	5.21	6.34	7.46	8.22
8	negyed kocka	2.57	4.09	5.21	6.34	7.46	8.22
9	körkörös	2.44	4.00	5.13	6.24	7.36	8.13
10	cikcakk	2.54	4.07	5.19	5.31	7.44	8.19
11	kereszt	2.59	4.40	6.54	9.23	12.05	13.29
12	3D kereszt	2.56	4.26	6.15	8.13	10.19	11.22
13	gyroid	2.56	4.39	7.10	9.45	12.30	13.53
14	villám	2.27	2.36	2.41	2.44	2.49	2.50

Forrás: a szerzők szerkesztése

4. táblázat: Kitöltési minták nyomtatásához szükséges filament hosszúságának változása a kitöltési sűrűség változásának függvényében 50 mm átmérőjű gömb nyomtatása esetén

		Kitöltési sűrűség (%)					
Fsz.	**Kitöltési minta neve**	**10**	**30**	**50**	**70**	**90**	**100**
		nyomtatáshoz szükséges filament hosszúsága (m)					
1	rács	2,16	3,97	5,77	7,56	9,36	9,80
2	vonal	2,21	3,99	5,78	7,58	9,37	9,80
3	háromszög	2,15	3,97	5,76	7,56	9,36	9,80
4	három-hatszög	2,12	3,94	5,74	7,54	9,32	9,77
5	kocka	2,15	3,95	5,76	7,55	9,34	9,78
6	osztott kocka	1,85	2,98	3,53	4,05	4,49	4,43
7	oktett	2,20	3,99	5,78	7,58	9,37	9,81
8	negyed kocka	2,20	3,98	5,78	7,57	9,37	9,81

		Kitöltési sűrűség (%)					
Fsz.	**Kitöltési minta neve**	**10**	**30**	**50**	**70**	**90**	**100**
		nyomtatáshoz szükséges filament hosszúsága (m)					
9	körkörös	1,87	3,73	5,59	7,45	9,32	9,78
10	cikcakk	2,15	3,97	5,76	7,56	9,38	9,81
11	kereszt	2,08	3,43	4,91	6,32	7,82	8,16
12	3D kereszt	1,98	3,23	4,55	5,83	7,18	7,49
13	gyroid	2,16	3,99	5,68	7,45	9,22	9,63
14	villám	1,27	1,40	1,05	1,51	1,59	1,55

Forrás: a szerzők szerkesztése

Gömb mintatest különböző kitöltési mintáinak változó kitöltési sűrűséggel történő nyomtatásakor hasonló tendenciákat kapunk, mint a kocka nyomtatásakor. A kockánál levont következtetések a gömb nyomtatásakor is alapvetően igazak, minimális számszerű eltérésekkel, ami abból adódik, hogy a gömb alakja meghatározza, hogy más és más nyomtatási rétegek alakulnak ki. Megállapítható, hogy mindkét elemi mintatest hasonló nyomtatási időkkel és filamentfelhasználási jellemzőkkel rendelkezik.

A harmadik elemzés egy valóságos alkatrész (váltókar gömbfej ágyazása) esetében történik, ahol többféle geometria előfordul, illetve a nyomtatás során alátámasztásokat is célszerű alkalmazni. Az alátámasztás jelen esetben egy második extruderrel valósul meg. PVA, vagyis vízzel oldható filament alkalmazásával. Az alapbeállítási jellemzők megegyeznek a kocka és a gömb beállításaival, kiegészítve a támasztékra vonatkozókkal:

- támasz elhelyezése: mindenhol;
- támasz túlnyúlási szöge: 45°;
- alátámasztás kitöltési sűrűsége: 50%;
- alátámasztás nyomtatási sebessége: 35 mm/s.

5. táblázat: Kitöltési minták nyomtatási idejének változása a kitöltési sűrűség változásának függvényében adott alkatrész nyomtatása esetén

		Kitöltési sűrűség (%)					
Fsz.	**Kitöltési minta neve**	**10**	**30**	**50**	**70**	**90**	**100**
		kitöltési minta nyomtatási ideje (óra.perc)					
1	rács	9.28	9.39	9.49	9.58	10.07	10.11
2	vonal	9.28	9.40	9.49	9.59	10.07	10.11
3	háromszög	9.28	9.40	9.49	9.58	10.07	10.12
4	három-hatszög	9.25	9.40	9.49	9.57	10.07	10.10
5	kocka	9.27	9.39	9.49	9.57	10.07	10.11
6	osztott kocka	9.14	9.32	9.47	10.02	10.15	10.21

		Kitöltési sűrűség (%)					
Fsz.	**Kitöltési minta neve**	**10**	**30**	**50**	**70**	**90**	**100**
		kitöltési minta nyomtatási ideje (óra.perc)					
7	oktett	9.26	9.39	9.48	9.58	10.07	10.12
8	negyed kocka	9.26	9.39	9.49	9.58	10.07	10.12
9	körkörös	8.54	9.03	9.19	9.35	9.51	9.57
10	cikcakk	9.28	9.40	9.49	9.58	10.08	10.13
11	kereszt	9.27	9.39	9.57	10.09	10.30	10.39
12	3D kereszt	9.28	9.39	9.52	10.03	10.22	10.29
13	gyroid	9.22	9.37	9.53	10.09	10.25	10.34
14	villám	8.58	9.05	9.09	9.11	9.14	9.14

Forrás: a szerzők szerkesztése

6. táblázat: Kitöltési minták nyomtatásához szükséges filament hosszúságának változása a kitöltési sűrűség változásának függvényében adott alkatrész nyomtatása esetén

		Kitöltési sűrűség (%)					
Fsz.	**Kitöltési minta neve**	**10**	**30**	**50**	**70**	**90**	**100**
		nyomtatáshoz szükséges filament hosszúsága (m)					
1	rács	4,90	5,06	5,21	5,36	5,52	5,53
2	vonal	4,90	5,06	5,21	5,36	5,52	5,53
3	háromszög	4,90	5,06	5,21	5,36	5,52	5,53
4	három-hatszög	4,86	5,06	5,20	5,36	5,50	5,52
5	kocka	4,90	5,05	5,21	5,37	5,51	5,53
6	osztott kocka	4,52	4,71	4,91	5,12	5,33	5,38
7	oktett	4,88	5,05	5,21	5,36	5,51	5,54
8	negyed kocka	4,89	5,05	5,21	5,36	5,51	5,54
9	körkörös	4,43	4,57	4,79	5,13	5,47	5,55
10	cikcakk	4,90	5,06	5,21	5,36	5,52	5,54
11	kereszt	4,85	4,96	5,13	5,21	5,41	5,41
12	3D kereszt	4,86	4,96	5,10	5,17	5,37	5,37
13	gyroid	4,84	5,01	5,17	5,33	5,49	5,50
14	villám	4,44	4,48	4,51	4,52	4,54	4,52

Forrás: a szerzők szerkesztése

Egy funkcionális alkatrész nyomtatása esetén a kitöltési minták nyomtatási idejének és a filament hosszának változási tendenciái megegyeznek a kocka és gömb mintatest nyomtatásáéval, különbség inkább a kitöltési sűrűség változásában látható. Amíg

a kocka és a gömb nyomtatásakor a 10% és a 100% kitöltés között háromszoros, négyszeres különbségek adódnak mind a nyomtatási idő, mind az alapanyag-felhasználás tekintetében, addig a funkcionális alkatrésznél ezek a különbségek alig 1,1–1,2-szeresek. Ezek a kicsi változások abból adódnak, hogy a funkcionális alkatrész alakja jelentősen eltér az elemi formáktól, nem nagy belső üreggel rendelkezik, hanem sok vékony fala van, ahol a falvastagság miatt kevésbé meghatározó a belső rész kitöltése. További idő- és anyagfelhasználással jár a támaszték elkészítése is, ami szintén megnöveli a nyomtatási időt és a felhasznált anyag mennyiségét. Amennyiben a kapott eredményekből levesszük a sok falvastagság és támaszték elkészítéséhez szükséges időt és anyagmennyiséget, akkor alapvetően hasonló értékeket kapunk, mint a kocka és a gömb esetében.

Összefoglalás

A cikk összefoglalta és felhasználásuk szerint (egyszerű és gyors nyomtatványokhoz, prototípusokhoz és közepesen erős alkatrészekhez, erős és funkcionális alkatrészekhez valamint rugalmas nyomtatványokhoz) csoportosította a különböző kitöltési mintákat, jellemezte azokat, és megfogalmazta az adott minták felhasználási lehetőségeit. Bemutatta alkalmazásuk főbb előnyeit és lehetséges hátrányait. Útmutatást nyújtott az egyes kitöltési minták 3D-nyomtatás során történő alkalmazására. Próbatestnyomtatásokkal hasonlította össze egymással a különféle kitöltési mintákat, és határozta meg az azok nyomtatásához szükséges időfelhasználást és alapanyag-mennyiséget. A vizsgálatokat három próbatest esetén végeztük el, egy kocka, egy gömb és egy tényleges funkcionális alkatrész esetén. A három próbatest nagymértékben különbözött egymástól, mert a kocka esetén csak függőleges és merőleges oldalakkal számolhattunk, a gömb esetén viszont minden réteg nagysága különböző és az oldalfalak is ferde felületekből álltak, a funkcionális alkatrész pedig egyesítette mindkét elemi próbatest jellemzőit. A mintadarabokat hat különböző kitöltési sűrűség változtatásával nyomtattuk, közben rögzítettük a nyomtatás időszükségletét és a felhasznált filament hosszúságát. A három különböző próbatest nyomtatása esetén a különböző kitöltési minták nyomtatási idejének és filamentfelhasználásának tendenciái hasonló jelleget mutattak, különbség a kitöltési sűrűség változásában tapasztalható.

Felhasznált irodalom

Boissonneault, Tess (2024): *Understanding the Gyroid Infill in 3D Printing.* Online: www.wevolver.com/article/gyroid-infill

Chandler, David L. (2017): *Researchers Design One of the Strongest, Lightest Materials Known.* Massachusetts Institute of Technology. Online: https://news.mit.edu/2017/3-d-graphene-strongest-lightest-materials-0106

Ekaran, Sammy (2023): *Which Infill Pattern Should You Use for 3D Prints?* Online: www.tomshardware.com/how-to/choose-infill-pattern-for-3d-prints

Goldschmidt, Benjamin (2024): *Cura Guide to the Best Infill Patterns.* Online: https://all3dp.com/2/cura-infill-patterns-all-you-need-to-know/#google_vignette
Gyarmati József (2023): Lánctalpas jármű kormányzása és ennek 3D modellezése. *Műszaki Katonai Közlöny,* 33(3), 51–61. Online: https://doi.org/10.32562/mkk.2023.3.5
Gyarmati József – Hegedűs Ernő – Gávay György (2022): Automata sebességváltóban alkalmazott kapcsolt bolygóművek – Wilson-váltó: Harckocsi-sebességváltó modell kialakítása 3D nyomtatással oktatási célból. *Műszaki Katonai Közlöny,* 32(3), 113–126. Online: https://doi.org/10.32562/mkk.2022.3.7
Hegedűs Ernő (2023a): Szálerősítéses anyagok 3D-s nyomtatásának hadiipari alkalmazási lehetőségei I. rész. *Haditechnika,* 57(4), 62–66. Online: https://doi.org/10.23713/HT.57.4.12
Hegedűs Ernő (2023b): Szálerősítéses anyagok 3D-s nyomtatásának hadiipari alkalmazási lehetőségei II. rész. *Haditechnika,* 57(5), 49–55. Online: https://doi.org/10.23713/HT.57.1.09
KREATE (2024): *Introduction.* Online: www.kreate3d.be/infill/
Lennert József Richárd – Sárosi József (2021): 3D nyomtatásnál alkalmazható kitöltési mintázatok hatása az ütőmunkára és annak szórására. *Jelenkori Társadalmi és Gazdasági Folyamatok,* 16(3–4), 47–56. Online: https://doi.org/10.14232/jtgf.2021.3-4.119-132
Maker.io Staff (2021): *Selecting the Correct 3D Printing Infill Pattern in Cura.* Online: www.digikey.com/en/maker/tutorials/2021/selecting-the-correct-3d-printing-infill-pattern-in-cura
Omkar, Kumbhar (2022): Different Infill Patterns in 3D Printing. *Medium,* 2022. december 13. Online: https://medium.com/@omkar.kumbhar20/assessment-of-different-infill-patterns-in-3d-printing-46f5bae71d99
Pranay, Gharge (2024): *Cura Infill Patterns: Which of the 14 Are Best, Fastest, and Strongest?* Online: https://clevercreations.org/cura-infill-patterns-best-fastest-strongest/
Prusa, Josef (2024): *Infill Types and Their Properties.* Online: https://help.prusa3d.com/article/infill-patterns_177130
Rafiqul, Islam (2020): Cura Infill Patterns |A Definitive Guide. *Medium,* 2020. április 8. Online: https://iamrafiqul.medium.com/cura-infill-patterns-6dd62be22d77
SuperSlicerHu: *Kitöltési minták.* Online: https://szi-ga.gitbook.io/superslicerhu/konfig/print_settings/kitoeltesi-mintak
Ultimaker: *How to Print Like a Flash with Lightning Infill.* Online: https://ultimaker.com/learn/how-to-print-like-a-flash-with-lightning-infill/
Végvári Zsolt (2023): A 3D nyomtatás felhasználási lehetőségei a műveleti logisztikában. *Katonai Logisztika,* 33(1–2), 177–198. Online: https://doi.org/10.30583/2023-1-2-177
Weyhaupt, Adam G. (2021): *Meet the Gyroid.* Online: https://plus.maths.org/content/meet-gyroid
Zentay Péter – Hegedűs Ernő – Végvári Zsolt (2022): A 3D-s nyomtatás és katonai alkalmazásának lehetőségei. 3. rész. *Haditechnika,* 57(2), 57–62. Online: https://doi.org/10.23713/HT.57.2.11

HADMÉRNÖK
KATONAI MŰSZAKI INFRASTRUKTÚRA

19. évfolyam (2024) 2. szám 49–62.
DOI: 10.32567/hm.2024.2.4

Hajós Bence[1]

Közúti hidak katonai és polgári terhelési osztályairól

Military and Civil Load Classes for Road Bridges

Absztrakt

A közúti hidak teherbírásának polgári és katonai osztályozása sok hasonlóságot mutat. A polgári és katonai eljárásokat összehasonlító tanulmány célja a STANAG 2021 magyarországi alkalmazásának elősegítése. A katonai besorolás gyors módszere lehet konverziós eljárások kidolgozása a polgári hidaknál már alkalmazott módszerhez hasonlatosan. Az elemzés javaslatokat ad a katonai besorolás egyes részletszabályaira, valamint egységes jelölésrendszert fogalmaz meg.

Kulcsszavak: STANAG 2021, híd, hídszabályzat, teherbírás, új jelölésrendszer

Abstract

Civilian and military classifications of the load capacity of road bridges show many similarities. The purpose of the study comparing civil and military procedures is to promote the application of STANAG 2021 in Hungary. A quick method of military classification of bridges can be the development of conversion procedures similar to the method already used for civilian bridges. The analysis gives suggestions for the rules of some details of the military classification, and this paper proposes a unified new signal system for the load capacity of bridges.

Keywords: STANAG 2021, bridge, bridge code, load capacity, new marking system

[1] Hidászmérnök, 2012-ben Az év hidásza, az Első Lánchíd Bt. ügyvezetője, e-mail: elsolanchid@elsolanchid.hu

Bevezetés

A katonai járművek és az ezek által használni kívánt hidak, átkelők teherbírási osztályozására a NATO Egységesítési Egyezményt adott ki (STANAG 2021). Az egyezmény és a mögöttes AEP-3.12.1.5 NATO szabvány címe: *Hidak, kompok, úszóművek és járművek katonai teherbírási besorolása.*[2]

Vizsgálódásom első részében röviden a polgári hídszabályzatok, hídtervezési előírások eddigi fejlődését és kétlépcsős rendszerét mutatom be, ami sok hasonlóságot mutat a katonai előírásokkal. Mivel a polgári hidak 1993-tól használt üzemi teherbírása és annak gyors bevezetése párhuzamba állítható az előttünk álló katonai MLC-besorolási feladattal *(military load classification)*, érdemes és hasznos ennek részletes bemutatása és megismerése.

Elemzésem második részében részletesebben foglalkozom a STANAG 2021 közúti hidakra vonatkozó teherbírási osztályaival. Javaslatokat fogalmazok meg a katonai hídteherbírás-szabvány egyes részleteivel kapcsolatosan. Végezetül a gyakorlatot nagymértékben segítő és nélkülözhetetlen, egységes jelölésrendszerre teszek javaslatot.

A téma aktualitását adja a STANAG 2021 alkalmazásának hazai elmélyítése mellett az is, hogy napjainkban folyamatban van a polgári hídtervezési előírások gyökeres megújítása, amiről külön tanulmányban számoltam be.[3]

Közúti hidak teherbírásának polgári osztályozása a hídtervezési előírásokban

A legelső, közúti hidak tervezésére vonatkozó magyarországi előírás 1910-ben jelent meg.[4] A jogszabályként kihirdetett hídszabályrendeletben háromféle terhelési osztály található.

1935-ben jelent meg a második közúti hídszabályzat „ideiglenes" jelzővel.[5] A hasznos terhek nem változtak, csak a budapesti közúti Duna-hidakra jelent meg egy külön terhelési osztály.

A sorrendben a harmadik szabályzatot, szintén ideiglenes jelzővel, 1950-ben adták ki, ötféle[6] terhelési osztállyal.[7]

Az 1956-ban megjelent szabályzat ágazati szabvány volt, négyféle terhelési kategóriával (A, B, C és D).[8] 11 évvel később szintén ágazati szabvány volt az 1967. évi hídszabályzat, amiben eggyel kevesebb, háromféle hasznos járműteher jelent meg.[9]

[2] A továbbiakban az egyezményre és a mögöttes szabványra együttesen STANAG 2021-ként hivatkozom, hasonlóan a szabvány saját szövegében található önhivatkozásokhoz.
[3] Hajós 2024.
[4] 33.034/1910 K.M. rendelet.
[5] KHSZ 1935.
[6] Ekkor bevezetett terhelési osztályok a legnagyobbtól a legkisebbig: I/A, I/B, II, III és IV.
[7] KHSZ 1950.
[8] KHSZ 1956.
[9] KHSZ 1967.

Ezt a szabványt 1979-ben módosították, ami jelentősen érintette a járműterhek intenzitását,[10] ezért teherbírási szempontból ez külön korszaknak tekintendő.

A polgári szabályozásban a következő váltás 1986–87-ben volt. Egyetlen előírás helyett fejezetenként külön szabványok jelentek meg, így a hídszabályzatból szabványsorozat lett.[11] Az egyes kötetek közül csak az általános szabályoknak jelent meg új változata 1991-ben (1. táblázat).

1. táblázat: Polgári hídtervezési magyar szabványok 1967-től napjainkig

1967	1986–87	1991	Szabvány címe	Hatályos?
MSZ-07-3201:1967	MSZ-07-3700:1987	MSZ-07-3700:1991	„Közúti hidak létesítésének általános szabályai"	érvényben
	MSZ-07-3701:1986		Közúti hidak erőtani számítása	2010. 12. 31-ig
	MSZ-07-3702:1987		Acélhidak tervezése	2010. 12. 31-ig
	MSZ-07-3709:1987		„Beton, vasbeton és feszített vasbeton közúti hidak tervezése"	2010. 12. 31-ig
	MSZ-07-3710:1987		Közúti öszvérhidak tervezése	2010. 12. 31-ig
	MSZ-07-3711:1986		Fahidak tervezése	2010. 12. 31-ig

Forrás: a szerző szerkesztése

Az európai uniós csatlakozással kötelezettséget vállaltunk az egységes európai méretezési szabványcsalád, az Eurocode bevezetésére és az ezzel ellentétes nemzeti szabványok kivezetésére. Az 1. táblázat szerinti szabványok egyszerre, 2010. december 31-én lettek visszavonva az általános szabályokat tartalmazó kötet kivételével, ami ma is hatályos. Helyettük a hídtervezési előírásokat a magyar hidásztársadalom átmenekítette az Útügyi Műszaki Előírásokba (ÚME). Az ÚME-k nem nemzeti szabványok, hanem a közútépítési ágazat saját műszaki normái.[12] Ezek az Eurocode-hoz képest „alacsonyabb" rangú „műszaki normák", amelyek használhatók az Eurocode alternatívájaként.[13] Az első hídtervezési ÚME-kötetsorozat 2002-ben jelent meg. A hat kötet első megújítása 2004–2005-ben volt, majd 2011-ben szintén egyszerre jelent meg hat új kötet, amelyek ma is hatályosak.[14]

[10] A két legfontosabb módosítás, hogy a kocsipálya egyenletes megoszló terhelését nem kell figyelembe venni a terhelési osztályhoz tartozó jármű által elfoglalt területen, és a nagyobb terhelésű járműveket a kocsipályán kereszt irányban nem kell teljesen a szegélyhez legközelebb (legkedvezőtlenebbül) elhelyezni.
[11] MSZ 07-3700, 3701, 3702, 3709, 3710, 3711.
[12] Hajós 2022.
[13] Hajós 2023.
[14] e-UT 07.01.12:2011.

Végigtekintve a polgári hídtervezési előírásaink megújításának gyakoriságát (1950, 1956, 1967, 1979, 1986, 2002, 2004, 2011), a leghosszabb érvényű előírás az 1986. évi volt, a legrövidebb pedig a 2002. évi első ÚME.

1910-től napjainkig összesen tízféle polgári hídtervezési előírás volt, összesen harmincféle ideális járműteherrel.

Közúti hidak üzemi teherbírásának bevezetése

Az előző fejezetben felvázoltam az egymást váltó hídszabályzatokat, kizárólag a hasznos közúti jármű alapértékének változását említve. Természetesen az egyes előírások különböznek a teherbírás igazolására vonatkozó szabályozásban, tükrözve a méretezéselmélet változását, amelyre itt nem térünk ki.

1988-ban megjelent egy új jogszabály,[15] amely szabadon engedélyezte a 40 tonna össztömeget meg nem haladó járművek közlekedését azok tengelyszámától függetlenül, amennyiben egyik tengely terhelése sem haladja meg a 10 tonnát. A jogi szabályozás jelentősen megelőzte ezen járművek tömeges elterjedését, így néhány évig a közúti hidak szabályozása, üzemeltetése érdemben nem rendezte ezt az új helyzetet.

Az országos közutak kezelési gyakorlata szerint egészen 1993-ig (!) a 20 tonna és annál nagyobb teherbírást a hidaknál tiltó táblákkal nem jelezték. Tiltó tábla hiányában pedig 1988-tól például egy 20 tonna teherbírású hídon szabadon és jogkövető módon közlekedhetett akár egy 40 tonna össztömegű jármű is!

A növekvő teherforgalom miatt az 1990-es évek elejére halaszthatatlanná vált a meglévő hidak súlykorlátozás-szabályozásának gyors kezelése, csak az országos közúthálózaton közel 6000 híd teherbírásának felülvizsgálata.

Megoldásként a dr. Tóth Ernő országos közúti főhidász vezetésével működő Hídszabályzat Bizottság kidolgozta és bevezette a hídtervezési előírásokban található teherbírási osztályok mellé az üzemi teherbírási osztályozást. Ezzel minden híd kettős teherbírás-besorolást kapott, egy tervezési eredetűt és egy egyszerűsített üzemi teherbírásit. Az üzemi teherbírási besorolás célja az volt, hogy áthidalja a hidak építési irataiból többnyire ismeretes tervezési teherbírás (mint láttuk, harmincféle) és a híd aktuális állapotából adódó eltéréseket. Az üzemi teherbírási kategóriákat úgy alkották meg, hogy az egyes üzemi teherbírási értéket nevesítő jelzőszám megfeleljen a hídon kitáblázandó össztömeg-korlátozásnak tonnában kifejezve. Az üzemi teherbírásjelzés perjel utáni része (/993) a bevezetés évére emlékeztet (1993). Azaz, ha az üzemi teherbírás 40/993, akkor a mindennapi közlekedésre mértékadó járműteher 40 tonna, így nincs szükség korlátozásra, mivel 40 tonna felett csak külön engedélyezéssel közlekedhet jármű. Ha pedig az üzemi teherbírás 16/993, akkor a hídon 16 tonna össztömeg-korlátozást kell kitáblázni.

A fenti üzemi teherbírás véletlenül sem keverendő össze a hidak tervezésére vonatkozó előírásokban szereplő járműterhek üzemi értékével. A járműteher üzemi értéke ugyanis a karakterisztikus érték (például 80 tonna) mellett egy olyan kisebb teher (például 32 tonna), amivel gyakori teherkombinációkhoz tartozó igazolásokat

[15] 10/1988. (XI. 24.) KM rendelet meghatározott járművek közúti közlekedésének feltételeiről.

kell végezni (például vasbeton szerkezet repedéskorlátozása). Sajnos a híd üzemi teherbírása emiatt nem a legszerencsésebb megnevezés, mégis ez terjedt el a szakmában.

A Hídszabályzat Bizottság 1993-ban kidolgozott egy segédletet az üzemi teherbírási értékek meghatározásához, nyolcféle üzemi ideális járművet alkotva (3, 6, 9, 12, 16, 22, 32 és 40 tonna), amelyek terhelései nagyon közel estek az akkor ténylegesen közlekedő járműtípusok tényleges terheléséhez. Ma már ez nem igaz, a közlekedő járművek több esetben azonos össztömeg mellett kedvezőtlenebb tengelyelrendezésűek a hidak szempontjából. Ez azonban már témánktól elkülönülő, de aktuális probléma, amivel a közeljövőben a közúti hídkezelőknek foglalkozni kell.

Közúti hidak üzemi teherbírásának konverziós meghatározása

Az országos közúthálózaton fekvő hidakra 1993-ban bevezetett üzemi teherbírás meghatározásához a Hídszabályzat Bizottság eljárásrendet készített, ami alapján a 19 megye közútkezelőjének hidászmérnöke elvégezhette a besorolást.

Az eljárásrend megadta a ténylegesen közlekedő járművekre nagyon hasonlító ideális járműveket, és előírta, milyen esetben kell a hídra egy vagy két járművet helyezni, valamint kell-e egyidejű megoszló terhelést is alkalmazni. A besorolás igénybevétel-összehasonlítással történt, jellemzően nyomatéki és nyíróerő-vizsgálattal, akárcsak a STANAG 2021 járműosztályozásánál.

A szakmapolitika részéről határozott igény volt, hogy a növekvő közúti teherforgalmat a lehető legkisebb mértékben korlátozzák a gyenge teherbírású hidak. A kritikus hidak erősítésére, felújítására alig volt forrás, ezért elfogadták a globális biztonsági szint kismértékű csökkentését, megengedve, hogy alapértéki igénybevétel-összehasonlításnál 10% túligénybevétel adódjon. Emellett lehetőségként bevezették, hogy további csökkentéseket is el lehet fogadni járulékos forgalomtechnikai intézkedés mellett (például sebességkorlátozás, követési távolság korlátozása, híd beszűkítése, váltakozó irányú forgalomirányítás).

Az országos közúthálózaton lévő mintegy 600 híd üzemiteherbírás-besorolását segítette egy egyszerű számítógépes program, ami támaszköz függvényében grafikusan megadta a kéttámaszú tartón értelmezett legnagyobb mezőközépi nyomatékot és a legnagyobb nyíróerőt. Emellett a budapesti központi Hídosztály további átváltási szabályokat is készített, amelynek számításait dr. Träger Herbert korábbi főhidász végezte (például 1910. évi 20 tonnás gőzekére méretezett híd 6,5 méter támaszközig megfelel 40/993 üzemi terhelésre, 6,5 és 9,0 méter támaszköz között pedig 32/993 üzemi terhelésre).

A besorolás lassan haladt, évekig elhúzódott. 1995–96 körül a hídnyilvántartásban már minden hídnak szerepelt az üzemi teherbírása, a 40 tonna alattiak helyszíni kitáblázása viszont a mai napig mutat még hiányosságot.

Közúti hidak szabályzati és üzemi teherbírásának jogállása és kölcsönös viszonya

Az 1993-ban bevezetett üzemi teherbírás meghatározása a bemutatott igénybevétel-összehasonlító módszer mellett részletes számítással is megengedett volt, néhány esetben ezt kellett alkalmazni. Az üzemi teherbírás egyértelmű gyors tájékoztatást adott, hogy a híd mekkora össztömegű járművet bír el biztonságosan.

1993-tól tehát minden országos közúti hídnak kétféle teherbírás-besorolását tartják nyilván, egy tervezési hídteherbírást (ez a fentebbi harmincféle) és egy üzemi teherbírást.

A kétféle teherbírás jogi megítélése, tulajdonsága eltérő. A tervezési teherbírást a híd tervezője, esetleg a hidat vizsgáló szakértő határozhatja csak meg. E tervezőnek, szakértőnek szakmagyakorlási jogosultsággal kell rendelkeznie, és a híd besorolásának szükséges dokumentuma hídterv, statikai számítás vagy szakvélemény. A tervezési teherbírás értéke lehet a hatályos és elmúlt idők hídszabályzatai szerinti teherosztály (említett harmincféle), és lehet az 1993-ban bevezetett üzemi teherosztály is. Főszabály, hogy a tervezési teherbírást tervvel, statikai számítással kell dokumentálni.

Sajnos vannak közúti hidak, amelyeknek elvesztek az építési tervei, iratai. Ekkor hiteles forrásnak tekinthetjük a régi nyilvántartási adatokat, amennyiben azokban ez az adat szerepel.

Különleges az 1950 előtt épült hidak esete, ha nincsenek meg sem a terveik, sem a nyilvántartási adataik. Tekintettel arra, hogy ezen hídcsoport tipikusan kis nyílású, többségében boltozat vagy kisebb nyílású vasbeton lemez, a hídnyilvántartásban ezek 1910. évi 20 tonnás teherbírással lettek felvéve. E hídcsoport esetében a becsült teherbírás tehát kellő óvatossággal kezelendő.

Az üzemi teherbírás meghatározása 1993-tól kezelői hatáskörben volt, tehát a besorolást többségében a közútkezelő hidászmérnöke végezte el szakmagyakorlási jogosultság nélkül. A besorolás kiinduló adata a tervezési hídteherbírás volt, a követendő eljárást pedig a Hídszabályzat Bizottság megadta. Különleges esetekben előfordult az üzemi teherbírás besorolásában tervező vagy szakértő közreműködése is, de ez csak ritka kivétel volt.

Az üzemi teherbírás emiatt egy rugalmasabb adat, amelynek módosításához nem kötelező tervezői erőtani számítás, szakvélemény, ellentétben a tervezési teherbírással. Így az üzemi teherbírás egyszerűbben, a közútkezelő saját hatáskörében is módosítható egy híd állapotromlásából fakadó teherbírás-csökkentés miatt, vagy akár hálózati forgalomszervezési okból.

A tervezési és üzemi teherbírás besorolása egymással szoros összefüggést kell mutasson, mivel az üzemi teherbírás alapvetően a tervezési teherbírásból származik, de nem kizárólagosan. Példának nézzünk egy B jelű[16] tervezési teherbírású hidat, aminek üzemi teherbírása 40 tonna, azaz nincs rajta össztömeg-korlátozás. Ha a híd kezelője olyan súlyos állapotromlást tapasztal, ami miatt szükségesnek látja kezelői hatáskörben össztömeg-korlátozás bevezetését, akkor egyszerűen módosíthatja az üzemi teherbírást 20 tonnára, miközben a tervezési teherbírása a hídnak marad B jelű, hiszen annak módosítása hídtervezői, hídszakértői kompetencia.

[16] A jelű teherbírási osztályban a hídra helyezendő jármű tömege 80 tonna, B jelű teherbírási osztályban 40 tonna, a kocsipálya maradék részeit pedig egyenletesen megoszló függőleges hasznos teherrel kell számítani.

STANAG 2021 szerinti hídteherbírási osztályok

A polgári és katonai méretezéselmélet alapjai azonosak, de a terhek jellemzői (karakterisztikus érték, gyakoriság, egyidejűség stb.) és a teherbírás-igazoláshoz szükséges parciális és dinamikus tényezők eltérők lehetnek. Jelen tanulmányban kizárólag a katonai hídteherbírás lehetséges különböző eseteit tekintem át, ezekhez tartozó tényezők és egyéb részletmegfontolások nem témái elemzésemnek.

A STANAG 2021 A melléklete megadja a 16 + 16 db ideális járművet lánctalpas és gumikerekes esetekre, amelyek a katonai terhelés alapját képezik. A teherbírás meghatározásának módját, ideértve a parciális tényezőket és dinamikus tényezőt is, alapvetően nemzeti hatáskörbe[17] utalja a szabvány, ezzel minden NATO-tagországnak az alkalmazásban mozgásteret adva. A szabványban lévő ideális járműterhek nem tartalmazzák a dinamikus hatást, szemben például az Eurocode járműterheivel.

A közúti hidaknak minden esetben kettős teherbírási minősítését kell elvégezni, megadva a besorolást külön lánctalpas és gumikerekes járművekre vonatkoztatva. Egyszerű kéttámaszú hídszerkezet esetén a hidak besorolásának számításához használhatók a járművek besorolására szolgáló táblázatok és grafikonok (B és C melléklet).

Tekintsük át a katonai forgalom egyidejűségi eseteit és a hídon való elhelyezését! Alapesetben, ha a híd hasznos kocsipálya-szélessége elegendő két forgalmi sávnak, akkor mindkét forgalmi sávban a legnagyobb ideális katonai járművel kell számolni. Ha kettőnél több forgalmi sáv átvezetésére alkalmas a híd, akkor a legfeljebb két forgalmi sávnyi katonai forgalmon felüli sávokon egyidejű polgári közlekedést kell feltételezni. A sávok előírt szélességét az MLC-besorolás függvényében a 2. táblázat tartalmazza. Többsávos hidak esetében vizsgálni kell azt a terhelési esetet is, amikor csak egy sávon van katonai forgalom, a híd többi szabad részén pedig egyidejű polgári közlekedés. A 5,50 méternél keskenyebb hidakat minden esetben egysávosnak kell tekinteni.

2. táblázat: A kocsipálya minimális szélessége egy- és kétsávos katonai közlekedéshez

Katonai besorolási osztály	Egy forgalmi sávos	Több forgalmi sávos
MLC4 - MLC12	2,75 m	5,50 m
MLC20 - MLC30	3,35 m	5,50 m
MLC40 - MLC70	4,40 m	7,30 m
MLC80 - MLC100	4,50 m	8,20 m
MLC120 - MLC150	5,00 m	nem megengedett

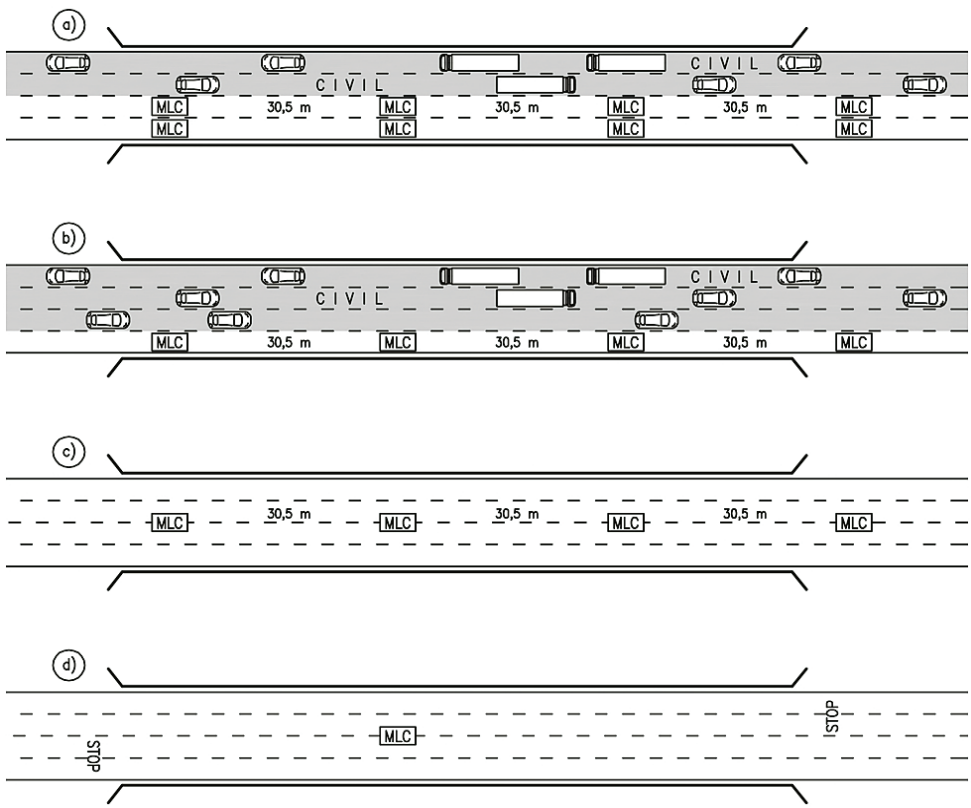
Forrás: a szerző szerkesztése STANAG 2021 6.1.8 pont nyomán

Normál terhelés esetén a katonai ideális járműveket konvojként kell modellezni, az egymást követő járművek között 30,5 méter távolságot hagyva. Ez lényeges különbség a polgári előírásokkal szemben. A katonai forgalmat azon sávokon vagy

[17] STANAG 2021: 6.1.5 és 6.1.6 pontok.

sávon kell figyelembe venni, ami a híd teherbírása szempontjából a legkedvezőtlenebb. A normál átkelés mellett a szabvány definiál két további esetet is, az óvatos *(caution)* átkelést és a kockázatos *(risk)* átkelést. Az óvatos átkelés esetén katonai konvoj helyett egyetlen jármű van a hídszerkezeten, nincsen egyidejű polgári forgalom, és az átkelés sebessége legfeljebb 5 km/h lehet. A kockázatos átkelés elrendezésében azonos az óvatossal, de ekkor megengedett a hídszerkezet kismértékű károsodása, ha az nem akadályozza az áthaladást.[18]

A STANAG 2021 szerinti teherbírás-értékelés a gyakorlatban sok nehézséget okozott, számos értelmezési kérdést felvetve. Ezért 2009-ben létrehozták a Katonai Hídértékelés (MBA – Military Bridge Assessment) szakértői csoportot (TOE – Team of Experts), amely az MCLSB Katonai Műszaki Munkacsoport (MILENG WG – Military Engineer Working Group) bizottságának jelent. A munkacsoport jelentései bekerültek a STANAG 2021 K mellékletébe. A szabvány nyolcadik kiadásában a tervezett 12 szakértői jelentésből már 7 megtalálható, az öt utolsó várhatóan a következő, 9. kiadásban fog megjelenni.



1. ábra: Katonai terhelési osztályokhoz tartozó jármű-egyidejűségi esetek
Forrás: a szerző szerkesztése

[18] STANAG 2021: H melléklet.

Az 1. ábrán négyféle jármű-egyidejűséget ábrázoltam.[19] Az ábrasorozat a) esete a normál átkeléshez tartozik, két sávon haladó katonai forgalommal.[20] Ez az eset csak legalább két forgalmi sávos hidaknál fordul elő, és ha van maradék forgalmi sáv, akkor ott egyidejű polgári terhelést kell feltételezni. Természetesen, ha a vizsgált híd éppen kétsávos, akkor csak katonai teher van a hídon, és nincs már maradék hely a polgári közlekedésre. Ez a terhelési egyidejűségi eset adja a legnagyobb terhelést a hidaknak.

A b) változatban csak egy forgalmi sávon halad a katonai forgalom, és a fennmaradó részen feltételezzük az egyidejű polgári közlekedést. Az egyes esetek gyakoriságának megítélése nem hidászmérnöki kompetencia, hanem katonai közlekedési kérdés, de talán kijelenthető, hogy ez a b) eset tekinthető békeidőben a legjellemzőbb katonai igénynek.

A c) esetben nincsen egyidejű polgári közlekedés, és egyúttal a katonai járművek konvoja a híd középvonalában halad, ami a hídszerkezet szempontjából kedvezőbb. Ilyen eset a szabvány alapszövegében nincsen, de a 2009-ben életre hívott szakértői csoport ajánlásában[21] ezt az egyidejűséget adják meg az óvatos *(caution)* átkelési esethez! Ezzel szemben a szabvány H melléklete az óvatos és a kockázatos *(risk)* átkeléshez egyaránt az 1. ábra szerinti d) esetet rögzíti (azaz nincs egyidejű polgári közlekedés, és a hídszerkezeten egyetlen jármű halad, legfeljebb 5 km/h sebességgel).

Ez az ellentmondás mindenképpen kezelendő, aminek érdekében javasolt a szabvány belső összhangját mielőbb megteremteni. Az ellentmondás továbbá kiterjed a járművek sebességére is. A hivatkozott K melléklet ugyanis a normál átkelésnél is korlátozza a katonai járművek sebességét, ami össztömeg függvényében 25, illetve 40 km/h, az óvatos átkelésnél pedig a H melléklet szerinti 5 km/h helyett szintén az össztömeg függvényében 15–25 km/h.

A katonai járművek közlekedésének egyidejűségi és sebességkorlátozási kérdése elsősorban katonai közlekedési kérdés, a katonai igényeket kell a hidak teherbírási rendszerében érvényre juttatni. A felsorolt esetek közötti fokozatok vonatkozásában viszont felhívom a figyelmet arra, hogy a sebességkorlátozás a helyváltoztatást jelentősen lassítja, miközben a kisebb sebesség okozta kedvezőbb dinamikus hatás a hídnak csak „kisebb" előnyöket okoz – már ha lehet az előnyöket és hátrányokat e tekintetben összehasonlítani.

Az egyes útszakaszokon lévő hídsűrűség tág határok között változik. Példának nézzük az M3-as autópálya Budapest és a miskolci elválási csomópont közötti szakaszát. Az önkényesen kiválasztott 140 kilométer hosszú úton 54 hídon kell áthaladni, ami 2,7 kilométer átlagos hidak közötti távolságot ad. Ha veszünk egy 25 járműből álló konvojt, akkor annak hosszúsága a követési távolságokkal akár 1 kilométert tesz ki. Ha a hidakon a konvojban haladó mértékadó jármű miatt sebességkorlátozást kell alkalmazni, könnyen belátható, hogy a konvoj mozgásdinamikája miatt szinte az egész 140 kilométeres szakaszt a hídon előírt sebességnél alig nagyobb átlagsebességgel lehet megtenni.

[19] A sematikus ábrán MLC betűkkel jelöltem az egyes teherbírási osztálynak megfelelő katonai lánctalpas vagy kerekes járművet.

[20] A két sávon haladó katonai forgalom lehet egyirányú és ellentétes irányú is, ennek nincs jelentősége a besorolás szempontjából.

[21] STANAG 2021: K melléklet, PoW 5.

A K melléklet szerinti sebességkorlátozás igen szigorúnak tűnik amiatt is, hogy a mai katonai járművek jelentős része alkalmas a megadottnál lényegesen nagyobb tartós sebességre. Emiatt indokolt a melléklet felülvizsgálata a sebesség szempontjából is.

A békeidőben legjellemzőbbnek vélhető 1. ábra szerinti b) eset mellett egy intenzív mozgósítás esetén talán a c) változat tekinthető egy fontos terhelési esetnek, mert az egyidejű polgári közlekedés terhelésének kizárása jelentékenyen növelheti a hidak MLC-besorolási szintjét, lehetővé téve a hatékony katonai mozgásokat. Emiatt javaslom az óvatos átkelés kritériumait a szabvány alapszövege szerint megtartani (csak egy katonai jármű, hídtengelyben), és egy újabb egyidejűségi eset bevezetését megfontolni a c) esetnek megfelelően.

A katonai járművek egyidejűségét természetesen mindig a statikailag összefüggő felszerkezeten kell értelmezni. Ha egy soknyílású híd statikailag kéttámaszú tartók sorozata, akkor az egyidejűség mindig csak egy nyílásra terjed ki. Ha a teljes híd egy közös folytatólagos felszerkezetből áll (például a Kőröshegyi völgyhíd 1872 méter hosszú szerkezete), akkor az egész hídra kell értelmezni. Van néhány összetett vagy egyedi hídszerkezet, ahol az egyidejűségre külön figyelni kell. A dunaújvárosi Pentele Duna-híd medernyílása egy önálló kéttámaszú felszerkezet, rajta összesen 2 + 2 forgalmi sávval és 1 + 1 műszaki biztonsági sávval. Ehhez a két oldalról csatlakozó ártéri szerkezetek viszont már irányonként is önállóak statikai szempontból, amelyek csak a saját irányuknak 2 forgalmi sávját és 1 műszaki biztonsági sávját hordozzák. Még összetettebb az M0-s budapesti körgyűrű Megyeri Duna-hídja, ami statikailag kilenc önálló felszerkezetből áll. Az egyedi eseteket tovább színesítik a változó szélességű hidak, kör alaprajzú hidak, elágazó felszerkezetek stb.

STANAG 2021 szerinti teherbírási besorolás megbízhatósága

A szabvány alapszövege tartalmaz megkülönböztető eseteket a besorolás megbízhatóságára vonatkozóan, ami egyrészt a híd teherbírását meghatározó személy képzettségétől, másrészt a besoroláshoz alkalmazott eljárásmódtól függ. Mindkét tényező széles skálán mozoghat, ami alapvetően kihat a hídteherbírási besorolás megbízhatóságára.

A 2009-ben elindított szakértői munkacsoport 3-as témája részletes ajánlást fogalmazott meg a hidak besorolásának megbízhatósági értékelésére.[22]

A besorolást végző személy minősítésére ötfokozatú osztályzást adtak meg: A szint: hídmérnöki képzettség nélküli személy; B szint: részleges hídmérnöki és katonai hídértékelési képesítésű személy, például mérnöktiszt; C szint: hídmérnök BA-diplomával és katonai hídértékelési képzéssel; D szint: építőmérnök MA-diplomával és katonai hídértékelési gyakorlattal; HN szint: honos nemzeti hatóság hiteles értékelése. A legutolsó, legmagasabb HN szintnek (HN – *host nation,* fogadó nemzet) tekinthetjük a híd kezelőjének minősítését is.

A besorolási eljárásrendre a hivatkozott mellékletben hét egymást követő, egyre szigorúbb fokozatot találunk, amelyet a 3. táblázatban foglaltunk össze. A legegyszerűbb,

[22] STANAG 2021: K melléklet, PoW 3.

leggyorsabb besorolási eljárás a 0. szint (gyors távoli felderítés), legrészletesebb a 6. szint, amihez részletes (kvázi kiviteli terv szintű) erőtani ellenőrzés és ezt kiegészítő helyszíni próbaterhelés (lehajlásmérés, önrezgésszámmérés) tartozik.

A meglévő közúti hidak MLC-besorolásának kívánatos megbízhatósági szintje az eljárás vonatkozásában a 3c szint. Ez az eljárás elveiben azonos a polgári üzemi teherbírás meghatározás általános menetével, azaz a híd tervezési teherbírásából származtathatjuk az MLC-besorolást. Konverziós eljárással gyors és kellően megbízható (3c) eredményt kaphatunk, de ehhez szükséges meghatározni az igénybevétel-összehasonlítás során alkalmazható parciális és dinamikus tényezőket, valamint a hazai közúti hídállomány ismeretében további iránymutatások rögzítése is szükséges (például járművek hídszerkezeten való effektív elhelyezése, egyidejű polgári közlekedést reprezentáló teher szabatos definiálása stb.).

3. táblázat: STANAG 2021, K melléklet szerinti teherbírás-besorolási eljárások

Értékelési szint	**Számítási modell**	**Szükséges adatok**	**Felderítés típusa**
0	Statisztikai eljárás	Korlátozott számú geometriai adat, véletlenszerűen kiegészítve a legnehezebb megfigyelt járművel	Gyors vagy távoli felderítés
1	Besorolási táblázatok vagy grafikonok használata	Korlátozott számú geometriai adat, véletlenszerűen kiegészítve a legnehezebb megfigyelt járművel	Gyors vagy távoli felderítés
2	Gerendamodell-számítás	Geometriai adatok és feltételezett anyagtulajdonságok	Gyors felderítés
3	Gerendamodell-számítás	Geometriai adatok + engedélyezett járműterhek (korrelációs módszer) 3a engedélyezett jármű 3b legnehezebb megfigyelt jármű 3c méretezésiteher-jármű	Gyors felderítés + 3b a tényleges forgalom megfigyelése (akár távolról is) 3c tervtári adatok
4	Gerenda- vagy részletesmodell-számítás	Részletes, de nem eléggé megbízható adatok (néhány adat feltételezett vagy pontatlan)	Részletes felderítés, alacsony pontosságú mérési technikák a hídon
5	Gerenda- vagy részletesmodell-számítás	Részletes és megbízható adatok	Részletes felderítés 5a nagy pontosságú mérési technikák 5b megbízható tervek és egyéb dokumentumok
6	Gerenda- vagy részletesmodell-számítás	Részletes és megbízható adatok a mért hídreakcióhoz igazítva	Mint az 5. pontban + mért sajátfrekvenciák vagy elhajlások a jól ismert járművek miatt

Forrás: STANAG 2021

Javaslat a STANAG 2021 szerinti hídteherbírási osztályok egységes jelölésére

A közúti hidak katonai teherbírási értékelése nem csupán egy érték: egyazon hídnak sokféle MLC-besorolása létezhet. Elkerülendő az egyes besorolásokhoz tartozó attribútumok keveredését, vagy a besorolástól való elszakadását, javaslom egy egységes jelölésrendszer bevezetését.

A teherszintet megtestesítő ideális katonai jármű MLC-besorolási számán kívül (például 100) öt-hat további alapvető tulajdonságot kell elválaszthatatlanul kezelni! Az alábbi javasolt jelölésrendszerhez a betonok szabványos jelölésrendszerét választottuk mintául. Beton esetében messze nem elégséges a szilárdság megadása (például C20), ami nyilván a legfontosabb tulajdonsága, hanem a jelölés többi része tartalmazza a környezeti kitéti osztályokat (például fagyálló vagy vízzáró), a szemnagyságot, a friss beton konzisztenciáját, az alkalmazandó cement típusát stb. (például C35/45–XC3–24–F3–CEM I 52,5 – 100 év – MSZ 4798:2016).

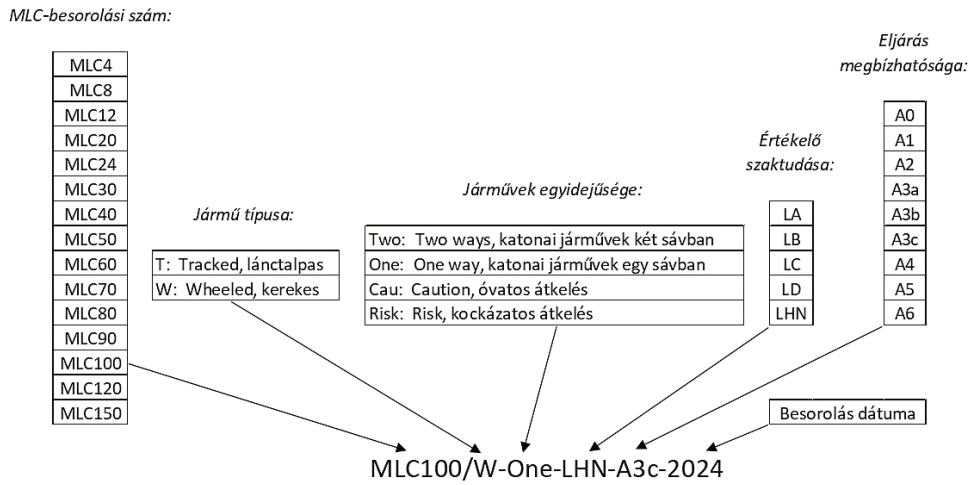
A hidak teherbírásánál jelölendők az alábbiak:

- A méretezési ideális jármű típusa: lánctalpas *(tracked)* vagy gumikerekes *(wheeled)*. Javasolt jelölés T és W.
- A járművek egyidejűségének négy esetét kell határozottan megkülönböztetnünk (fentebb ugyan felvetettem egy lehetséges és indokolt ötödik esetet is). Katonai forgalom két forgalmi sávon *(two ways – Two)* vagy csak egy sávon *(one way – One)*. Az egyidejű polgári közlekedést kizárja az óvatos átkelés *(caution – Cau)* és a kockázatos átkelés *(risk – Risk)*.
- A besorolás megbízhatóságának jelrendszerét a K melléklet vonatkozó táblázataiból vettem. A megbízhatósági szint az értékelő személytől és az alkalmazott eljárás mélységétől függ. Így az értékelő szaktudása lehet LA *(level A)*, LB, LC, LD és HN. Az alkalmazott eljárás pedig lehet A0 *(assessment level 0)*, A1, A2, A3, A4, A5 és A6.

A javasolt szabatos jelölés első tagja a besorolási főszám MLC előtaggal (2. ábra), amit perjellel követ a járműtípus, jármű-egyidejűség, az értékelő szaktudása és az eljárás megbízhatóságának megadása, egymástól hosszú kötőjelekkel elválasztva. A perjel utáni információk hiányában csupán a híd MLC-besorolási száma nem értelmezhető.

Egy hídnak tehát lehet a szabvány értelmében nyolcféle teherbírási besorolása (kétféle járműtípus és négyféle egyidejűség, 2 x 4 = 8), amihez összesen harmincötféle megbízhatósági index tartozhat (ötféle szaktudásszint, hétféle eljárási rend, 5 x 7 = 35).

Ha egy hídnak van ugyanazon értelmű hídteherbírás-besorolása két különböző megbízhatósági eljárásból, akkor a nagyobb megbízhatósági besorolást kell használni.



2. ábra: Javaslat a közúti hidak katonai teherbírásának szabatos jelöléséhez
Forrás: a szerző szerkesztése

A 2. ábrán lévő jelölést a végén indokolt a besorolás megállapításának évszámával kiegészíteni, ugyanis a híd teherbírása időben nem állandó, kezelni kell a híd leromlását éppúgy, mint egy felújításból, erősítésből származó javulást is. A besorolás évszáma tehát legalább olyan fontos besorolási tulajdonság, mint a megbízhatósági szintekre vonatkozó jelölések.

Egy híd lehetséges nyolcféle besorolása között pedig a polgári hidaknál bemutatott tervezési és üzemi teherbíráshoz hasonló belső összefüggések vannak. Így felállítható e nyolcféle besorolás „erősorrendje". Tipikusan egy híd gumikerekes besorolási száma nagyobb, mint a lánctalpas besorolás esetén. Hasonlóan az egyidejűségi eseteknél is felállítható egy sorrend: Two < One < Cau < Risk.

A megbízhatósági eljárásokra vonatkozó részletszabályokkal itt nem foglalkozom, de az ezek közötti összefüggés is leírható azzal, hogy ideális esetben a magasabb megbízhatósági szinthez tartozhat a magasabb teherbírási besorolás.

Összegzés

Láthattuk, hogy a polgári hídnyilvántartás szerinti üzemi teherbírás sok szempontból hasonlít a katonai előírás szerinti MLC-besorolásra, így a bevezetése során annak tapasztalatai hasznosíthatók.

A STANAG 2021 szerinti hídteherbírási osztályozást részletesen áttekintettem, bemutatva, hogy egyetlen hídnak akár nyolcféle besorolása is lehetséges, amelyek egymással párhuzamosan érvényesek.

Javaslatot adtam az „óvatos" és „kockázatos" átkelés egyidejűségi és sebességkorlátozási előírásainak felülvizsgálatára, megszüntetendő az egyes mellékletek közötti

ellentmondást. Szintén felvetettem a normál átkeléshez előírt sebességkorlátozás módosítását, ami szintén csökkenti a katonai mobilitást.

Az átkelési egyidejűségekre a szabvány alapszövege négyféle esetet különböztet meg. A választék bővítését javaslom, amikor nincsen polgári közlekedés a hídon, és a katonai konvoj a híd közepén haladhat, sebességkorlátozás nélkül.

Tanulmányom legfontosabb javaslata egy egységes jelölésrendszer bevezetése a STANAG 2021 szerinti hídteherbírás-értékekre. A teherbírásjelre adott javaslatomat szükség szerint tovább kell pontosítani és szabványosítani.

Felhasznált irodalom

33.034/1910 K.M. rendelet: Szabályrendelet a közúti hidak tervezéséről, forgalomba helyezéséről, próbaterheléséről és időszakos megvizsgálásáról (Közúti hídszabályzat). Online: https://hidak.hu/konyvek/KHSZ1910.pdf

AEP-3.12.1.5 NATO Standard Military Load Classification of Bridges, Ferries, Rafts and Vehicles. Edition A Version 1, September 2017.

e-UT 07.01.12:2011 Erőtani számítás közúti hidak tervezése (KHT) 2. Útügyi Műszaki Előírás. Online: https://ume.kozut.hu/dokumentum/745

Hajós Bence (2022): Az Útügyi Műszaki Előírások szerepe az útépítésre vonatkozó szabályrendszerben. *Útügyi Lapok,* 10(16), 10–17. Online: https://doi.org/10.36246/UL.2022.1.02

Hajós Bence (2023): Szempontok és javaslatok a közúti hídtervezés hasznos ideális jármű teherszintjének meghatározásához a készülő új Útügyi Műszaki Előírásban. *Útügyi Lapok,* 11(18), 30–43. Online: https://doi.org/10.36246/UL.2023.2.03

Hajós Bence (2024): Paradigmaváltás a közúti hídtervezésben a hasznos járműterhek vonatkozásában. Katonai alapterhek helyett polgári járműterhek bevezetéséről. *Műszaki Katonai Közlöny,* 34(2), 5–16. Online: https://doi.org/10.32562/mkk.2024.2.1

KHSZ (1935) A közúti hídszerkezetekre vonatkozó ideiglenes feltételek. M. Kir. Kereskedelemügyi Minisztérium. Budapest. Online: https://hidak.hu/konyvek/KHSZ1935idieglenes.pdf

KHSZ (1950) Ideiglenes küzúti hídszabályzat. Magyar Közlekedés- és Postaügyi Minisztérium. Budapest. Online: https://hidak.hu/konyvek/KHSZ1950ideiglenes.pdf

KHSZ (1956) KPM Sz. HI/1-56 R – G 82 Szakmai Szabvány. Online: https://hidak.hu/konyvek/KHSZ1956.pdf

KHSZ (1967) KPM SZ HI/1-67 – G 82 Szakmai Szabvány. Online: https://hidak.hu/konyvek/KHSZ1967_1r%C3%A9sz.pdf

STANAG 2021 Standardization Agreement, Military Load Classification of Bridges, Ferries, Rafts and Vehicles. Edition 8, 14 September 2018 NSO/1074(2017) MILENG/2021.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

19. évfolyam (2024) 2. szám 63–76.
DOI: 10.32567/hm.2024.2.5

Kátai-Urbán Maxim,[1] Mesics Zoltán,[2] Szakál Béla,[3] Cimer Zsolt[4]

A veszélyes üzemek környezeti kárelhárítási műszaki követelményeinek vizsgálata

Examination of the Technical Requirements for Environmental Damage Prevention of Dangerous Establishments

Absztrakt

A veszélyes anyagokkal foglalkozó üzemekben esetlegesen bekövetkező súlyos balesetek hatásai veszélyeztethetik a telephely környezetét. A környezeti hatások elhárítása vagy csökkentése fontos üzemeltetői és hatósági feladat. Jelen tanulmányban a szerzők elemzik és értékelik a veszélyes üzemekkel kapcsolatos környezeti kárelhárítás szabályozása üzemeltetői alkalmazásának tapasztalatait.

Kulcsszavak: ipari balesetek, környezeti károk, veszélyes üzem, kárelhárítás, Magyarország

Abstract

The effects of major accidents that may occur in dangerous establishments involving dangerous substances can endanger the surrounding environment of the site. Preventing or

[1] Osztályvezető, Semmelweis Egyetem Biztonságtechnikai Igazgatóság Biztonságszervezési Osztály, e-mail: katai.urban.maxim@semmelweis.hu
[2] Oktató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: zoltan.mesics@katved.gov.hu
[3] Oktató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: szakalbela1827@freemail.hu
[4] Dékán, Nemzeti Közszolgálati Egyetem Víztudományi Kar, e-mail: cimer.zsolt@uni-nke.hu

reducing related environmental impacts is an important task for operators and competent authorities. In the present study, the authors analyse and evaluate the experience of the operator's application of environmental damage prevention regulations related to dangerous establishments.

Keywords: industrial accidents, environmental impact, dangerous establishment, pollution prevention, Hungary

Bevezetés

A veszélyes anyagok jelenlétében bekövetkezett események más jelenségekhez hasonlóan gyakran súlyos következményekkel járnak a baleset helyszínére és környezetére nézve, és a hatás az országhatárokon túlra is kiterjedhet.[5] E hatások az emberi életet, egészséget és a vagyonbiztonságot egyaránt veszélyeztetik.[6] Földi László és Halász László véleménye szerint „a különféle veszélyes anyagokkal, technológiákkal foglalkozó üzemek tevékenysége potenciális környezeti veszélyforrásként értékelhető."[7]

A veszélyes anyagokkal foglalkozó üzemekben és a küszöbérték alatti üzemekben a veszélyes anyagok előállítása, feldolgozása vagy tárolása során bekövetkező súlyos balesetek esetenként katasztrofális hatással lehetnek az emberi egészségre, és szennyezhetik a felszíni és felszín alatti vizeket, a talajt vagy az épített környezetet.[8] Az ipari balesetek megelőzése mellett a veszélyes tevékenységek üzemeltetőinek fel kell készülniük az esetlegesen bekövetkező súlyos balesetek káros következményeinek elhárítására is.[9] Természetesen az üzemeltetők és a hatóságok, valamint az önkormányzatok közötti együttműködés is szükséges az esetlegesen bekövetkező események eredményes felszámolásához.[10] A súlyos balesetek elleni védekezés nagyszámú, a védekezésben részt vevő szervezet együttműködését igényli, hiszen „ez folyamatos és időszerű információcserét, valamint a feladatok időbeni és térbeli szinkronizálását igényli, hogy elkerülhető legyen az együttműködő szervezetek párhuzamos (és ezáltal felesleges) munkája."[11]

A veszélyes anyaggal foglalkozó üzemek üzemeltetőinek környezeti kárelhárítási tevékenységét a veszélyes üzemi szabályozás mellett a környezetvédelmi, illetve a vízügyi és vízvédelmi rendelkezések is érintik.[12] A rendszerváltást követően európai uniós mintára kidolgozott környezetvédelmi szabályozásban az egyik legfontosabb jogterület a felszíni és a felszín alatti vizek védelme (vízminőség-védelem).

Jelen cikkben a szerzők vizsgálják a környezeti kárelhárítási tevékenységhez tartozó katasztrófavédelmi, vízügyi és környezetvédelmi jogi szabályozást és a veszélyes üzemek által rendelkezésre bocsátott – az érintett telephelyekkel foglalkozó – üzemeltetői dokumentációban foglalt információt.

[5] Kátai-Urbán 2023.
[6] Nagy 2023.
[7] Halász–Földi 2014.
[8] Vince 2008: 46.
[9] Érces–Vass 2018.
[10] Teknős–Lakatos–Vass 2023.
[11] Berek–Földi–Padányi 2020.
[12] Cimer–Szakál 2015.

A környezetvédelmi és vízminőségi kárelhárítási szabályozás vizsgálata

A vízügyi és vízvédelmi hatósági és felügyeleti tevékenység

A vízügyi igazgatási és a vízügyi, valamint a vízvédelmi hatósági feladatokat ellátó szervek kijelöléséről szóló 223/2014. (IX. 4.) Korm. rendelet 11 vármegyei katasztrófavédelmi igazgatóságot és a Fővárosi Katasztrófavédelmi Igazgatóságot nevesíti vízügyi és vízvédelmi hatóságként. A vízvédelmi hatóságok a víz mint környezeti elem védelme tekintetében – a környezetvédelmi feladat- és hatáskör részeként – ellátják a *környezet védelmének általános szabályairól szóló 1995. évi LIII. törvényben* (Kvt.) meghatározott környezetvédelmi közigazgatási hatósági feladatokat. A rendelet országos vízvédelmi hatóságként a BM OKF-et adja meg, amelynek kijelölt vármegyei szervei látják el az elsőfokú vízügyi és vízvédelmi hatósági feladatokat. A BM OKF és a vízügyi igazgatási feladatokat ellátó országos vízügyi felügyelőség területi szerveinek illetékességi területe azonos. A Miniszterelnökség irányítása alatt működő szervezetek a területi Kormányhivatalok alárendeltségébe tartozó környezetvédelmi hatósági szervek és az általuk működtetett környezethasználati laboratóriumok. E laboratóriumok végzik többek között a katasztrófavédelem részére a vízminőség-védelmi kárelhárításhoz és kármentesítéshez kapcsolódó szaktevékenységet.

A környezetvédelmi hatóság a környezethasználattal járó tevékenységek esetében környezetvédelmi engedélyezési és felügyeleti tevékenysége keretében tesz eleget a Kvt.-ben rögzített feladat- és hatásköreiben meghatározottaknak. *A környezeti hatásvizsgálati és az egységes környezethasználati engedélyezési eljárásról szóló 314/2005. (XII. 25.) Korm. rendelet* (környezeti hatásvizsgálati rendelet) előírásai szerint a környezetvédelmi hatóság a rendelet hatálya alá tartozó tevékenységek részére egységes környezethasználati engedélyt (EKHE) ad ki.

A környezetvédelmi hatóság a környezeti hatásvizsgálat hatálya alá tartozó tevékenységek esetén környezetvédelmi engedélyt; az egységes környezethasználati engedélyezés hatálya alá tartozó esetekben egységes környezethasználati engedélyt; a környezetvédelmi felülvizsgálat hatálya alá tartozó tevékenységek esetén pedig környezetvédelmi működési engedélyt ad ki. A környezeti hatástanulmány elkészítésének tartalmi követelményei között – a rendelet 6. mellékletében foglaltaknak megfelelően – található az esetlegesen környezetterhelést okozó baleseteknek, meghibásodások lehetőségeinek, az ebből származó hatótényezőknek a bemutatása. A hatástényezők kiváltotta hatásfolyamatokat és azok hatásterületét környezeti elemenként és összességében kell vizsgálni. A várható közvetlen és közvetett környezeti hatások becslése és értékelése tekintetében be kell mutatni „a baleset-, üzemzavar-kockázat mértékét, különös tekintettel a felhasznált anyagokra és az alkalmazott technológiára". Az engedélyezési kérelemben foglalt létesítményben folytatott tevékenység hatásterületének meghatározásánál az üzemeltető figyelembe veszi az ipari baleseteknek és a természeti katasztrófáknak való kitettségből eredő várható hatásokat is, ahol a veszélyeztetett területet prognosztizálja az üzemeltető. A vizsgált rendelet 8. mellékletében találhatók az egységes környezethasználati engedélykérelem tartalmi követelményei, amelyek többek között a létesítmény kibocsátásainak forrásai, a kibocsátások minőségi

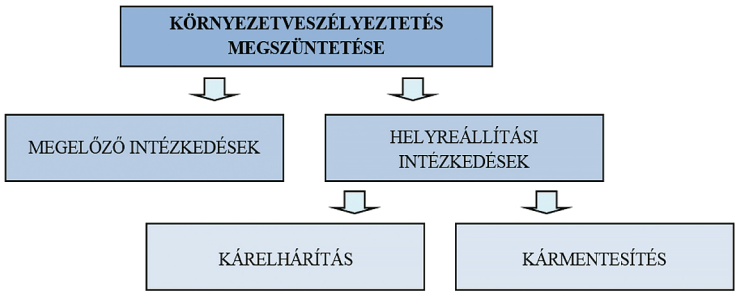
és mennyiségi jellemzői és várható környezeti hatásai, a hatásterület meghatározása, valamint kibocsátásmegelőzési vagy -csökkentési intézkedések leírása.

A hatásterület-értékelési folyamatban és a súlyos baleseti szabályozásban szereplő következményelemzési eljárás között hasonlóságok találhatók. Ennek is köszönhető, hogy az EKHE jelenleg is hatályos 8. melléklet B) része alapján „azon létesítmények esetében, amelyekre nem vonatkozik az 1999. évi LXXIV. törvény, mellékelniük kell az üzembiztonságra vonatkozó és havária esetén megteendő intézkedések bemutatását". Ez a követelmény – függetlenül attól, hogy a jelzett jogszabály már nem hatályos – azt jelenti, hogy a veszélyes anyaggal foglalkozó üzemek esetében a baleseti hatások megelőzésére, illetve a bekövetkező balesetek következményeinek csökkentésére vonatkozóan a biztonsági jelentésben, illetve elemzésben bemutatott rendszerek szolgálnak. A két engedélyezési eljárás nem helyettesíti, hanem kiegészíti egymást, ugyanis a hatósági vizsgálati szempontok különbözők. Természetesen az elkészített üzemeltetői dokumentációban vannak átfedések, ezáltal az egyes eljárások során elkészített dokumentumok közül bizonyos részeket a másik eljárásban is fel lehet használni. A súlyos baleseti és az EKHE szabályozás tárgyi hatálya alá eső tevékenységek köre alapvetően nem egyezik meg. Mégis vannak mindkét szabályozás hatálya alá tartozó tevékenységek, mint az energiaipar, a vegyipar, a hulladékkezelés, valamint egyes esetekben az élelmiszeripar és a bányászat tevékenységei. Az EKHE rendelet 9. mellékletében felsorolt, az elérhető legjobb technika meghatározásánál figyelembe veendő szempont annak igénye is, hogy megelőzzék a baleseteket, és minimálisra csökkentsék ezek környezetre gyakorolt hatását.

Vízminőség-védelmi kárelhárítás és kármentesítés szabályozásának értékelése

Az EKHE-hez kapcsolódó vízminőség-védelmi felügyeletet a vízvédelmi hatóság látja el, amelyhez kapcsolódóan a *használt és szennyvizek kibocsátásának ellenőrzésére vonatkozó részletes szabályokról* szóló *27/2005. (XII. 6.) KvVM rendelet* (kibocsátás-ellenőrzési rendelet) alapján a használt és szennyvizek kibocsátásának méréssel egybekötött helyszíni ellenőrzését is elvégzik. Ellenőrzik többek között az üzemeltetői önellenőrzéseket, a szennyezéscsökkentési ütemtervvel kapcsolatos feladatok megvalósulását.

A vízminőségben jelentkező környezetkárosodás megelőzésének és elhárításának rendjét a *vízgazdálkodásról szóló 1995. évi LVII. törvény* (Vgtv.) 18. § (2) bekezdése alapján, a környezet- és természetvédelmi követelményekre figyelemmel, a felszín alatti és a felszíni vizek mint környezeti elemek tekintetében környezeti kárelhárítási rendelet szabályozza. E tevékenységet a környezetveszélyeztetés megszüntetése érdekében végzik az állami, az önkormányzati és a gazdasági szereplők. Az 1. ábra mutatja be a környezetveszélyeztetés megszüntetésének kárelhárítási rendeletben alkalmazott összetevőit és azok fogalmi elemeit:



1. ábra: Vízminőség-védelmi kárelhárítás és kármentesítés fogalmi rendszerének felépítése
Forrás: a szerzők szerkesztése

A Kvt. 4. §-ban található fogalommeghatározása alapján a környezetveszélyeztetés a környezetkárosodás bekövetkezésének közvetlen veszélye, míg a környezetkárosodás a környezetben, illetve valamely környezeti elemben közvetlenül vagy közvetve bekövetkező, mérhető, jelentős kedvezőtlen változás, illetve valamely környezeti elem által nyújtott szolgáltatás közvetlen vagy közvetett, mérhető, jelentős romlása. A Kvt. rögzíti a megelőzés fogalmát is, amely a környezethasználat káros környezeti hatásai elkerülésének érdekében a leghatékonyabb megoldások, továbbá a külön jogszabályban meghatározott tevékenységek esetén az elérhető legjobb technika alkalmazása a döntéshozatal legkorábbi szakaszától. A helyreállítási intézkedés alatt pedig kárelhárítási vagy kármentesítési tevékenységet ért a jogszabály. A Kvt. 6. §-a értelmében a környezethasználatot úgy kell végezni, hogy többek között kizárja a környezetkárosítást. Az üzemeltető felelőssége és egyben kötelezettsége a kárelhárítás és kármentesítési tevékenység végrehajtása. Azonnali beavatkozást igénylő helyzetben – amikor a környezetkárosodás a közegészségügyet vagy a közbiztonságot veszélyezteti – az üzemeltető kárelhárítást végez, míg más esetben kármentesítést. A kárelhárítás során meg kell előzni más környezeti elem (a föld, a levegő, az élővilág, az épített környezet) károsodását és a környezetveszélyeztetést, továbbá minimalizálni szükséges a környezetterhelést. A felszíni és felszín alatti vizek szennyezése esetében a környezetveszélyeztetés helyéről, jellegéről és mértékéről bejelentés kell tenni a területi vízügyi hatóságnak és a területi vízügyi igazgatóságnak.

A környezethasználó gazdálkodó szervezetek a kárelhárításra való felkészülésben a vízügyi igazgatási és a környezetvédelmi szervekkel kötelesek együttműködni. A területi vízügyi szervek a területi vízgazdálkodási tervvel összefüggésben területi, míg a gazdálkodó szervezetek *a környezetkárosodás megelőzésének és elhárításának rendjéről szóló 90/2007. (IV. 26.) Korm. rendelet* 2. mellékletben felsorolt tevékenységek esetében üzemi kárelhárítási tervet kötelesek készíteni. Ezen túl a környezetvédelmi hatóság vagy a vízvédelmi hatóság bármely, a környezetet veszélyeztető technológiát üzemeltető gazdálkodó szervezetet kötelezhet tervkészítésre. A területi és az üzemi tervet a környezetvédelmi hatóság hagyja jóvá a vízügyi (vízvédelmi) hatóság szakhatósági közreműködésével.

A környezeti kárelhárítási rendelet szabályozásának értékelése

A környezeti kárelhárítási rendelet hatálya kiterjed a következő iparágakra: energiaipar, fémek termelése és feldolgozása, építőanyag-ipar, vegyipar, hulladékkezelés, papíripar, textilipar, bőripar, élelmiszeripar, állati anyagok feldolgozása, nagy létszámú állattartás, gépipar, bányászat, egyéb tevékenység. A súlyos baleseti szabályozás szempontjából alapvetően az energiaipar, vegyipar és hulladékkezelés létesítményei lehetnek érintettek, de találhatunk néhány közös veszélyes tevékenységet az élelmiszeripar, a bányászat vonatkozásában is.

A környezeti kárelhárítási rendelet 1. melléklete tartalmazza az üzemi kárelhárítási tervek tartalmi követelményeit. A rendelet szabályozza többek között a kárelhárítási anyagok és eszközök készletben tartását, az adatok nyilvántartását, a kárelhárítási gyakorlatokat, a környezetkárosodás észlelését, és felderítését és minősítését, a kárelhárítás végrehajtásának műveleti irányítását, a kárelhárítás készültségi fokozatait, annak elrendelését és megszüntetését. A környezetkárosodás minősítését a környezetvédelmi hatóság által működtetett laboratórium igénybevételével a vízügyi hatóság végzi, a vízügyi igazgatóság információt szolgáltat. A minősítés alapján a vízügyi igazgatóság kialakítja a lehetséges védekezés módozatait, és erről értesíti a vízügyi hatóságot. Beavatkozás szükségessége esetén a vízminőségi kárelhárítás végrehajtása műveleti irányításának a felelőse szintén a vízügyi igazgatóság. A környezeti kárelhárítási tevékenység a védekezésben részt vevő nagyszámú szervezet együttműködését igényli, hiszen „ehhez folyamatos és időszerű információcsere, valamint a feladatok időbeni és térbeli szinkronizálása szükséges, hogy elkerülhető legyen a partnerek párhuzamos (és ezáltal felesleges) munkája".[13]

A kárelhárítás feladatait – amelyet a vízügyi igazgatóság rendeli el a vízügyi hatóság bevonásával – a következő készültségi fokozatban kell ellátni:

- I. fokú készültség: a környezetkárosodás felderítése helyszíni műszaki szemle megtartásával;
- II. fokú készültség: a műveleti végrehajtást megelőző intézkedések megtétele, mint például a mintavétel, az elemzés és az értékelés;
- III. fokú készültség: a kárelhárítás műveleti végrehajtása: lokalizálás, közömbösítés, eltávolítás.

A készültség fokozatait meg kell szüntetni, ha az azt kiváltó ok megszűnt. A kárelhárítás kiadásainak viselésére a „szennyező fizet" elvet alkalmazzák. A víz mint környezeti elem tekintetében a vízvédelemért felelős miniszter szakmai irányítása mellett az illetékes hét kormányhivatal speciális környezetvédelmi (egyben vízvédelmi) igazgatási feladatként működtet regionális laboratóriumokat. A laboratóriumok – az immissziós, az emissziós, valamint a vízminőség-védelmi kárelhárításhoz és kármentesítéshez kapcsolódó monitoringrendszert működtetve – mintavétellel, laboratóriumi és egyéb műszeres vizsgálattal szolgálnak a közvetlen és közvetett vízgazdálkodási és vízvédelmi igazgatási feladatokat ellátó szervek részére.

[13] Berek–Földi–Padányi 2020.

A vízvédelmi igazgatási feladatokat ellátó szervek kijelöléséről, és egyes vízügyi tárgyú kormányrendeletek módosításáról szóló 366/2015. (XII. 2.) Korm. rendelet jelöli ki a vízügyi és vízvédelmi hatáskörrel rendelkező katasztrófavédelmi igazgatóságokat és a BM OKF-et a rendkívüli vízminőség-védelmi események közül az azonnali beavatkozást igénylő vízminőség-védelmi kárelhárítással kapcsolatos egyes vízminőség-védelmi közvetlen igazgatási feladatok ellátására, amelyek a következők:

- a környezeti kárelhárítási rendelet szerint állandó ügyelet tartása, a víz (felszíni és felszín alatti) és a földtani közeg esetében a károsodás felderítése;
- *a felszín alatti vizek védelméről szóló 219/2004. (VII. 21.) Korm. rendelet* (Fevir.) alapján a felszíni víz jelentősen kedvezőtlen állapota esetén a kivizsgálás lefolytatása;
- *a felszíni vizek minősége védelmének szabályairól szóló 220/2004. (VII. 21.) Korm. rendelet* (Favir.) alapján a földtani közeg, illetve felszín alatti víz rendkívüli terhelése, szennyezése vagy károsítása/károsodása, továbbá minőségének veszélyeztetése esetében a kivizsgálás lefolytatása.

A Fevir. alapján a szennyvízkibocsátással, a közcsatornába vezetéssel kapcsolatos környezetvédelmi követelmények a Kvtv. és a Vgtv. szerinti engedélyben jelennek meg. A rendelet önellenőrzési kötelezettséget határoz meg. A hatóság vízszennyezési és rendkívüli vízszennyezési bírságot szabhat ki, korlátozhat, felfüggeszthet vagy megtilthat.

Vízvédelmi szakhatósági tevékenység bemutatása

A környezet- és természetvédelmi hatósági ügyekben történő vízügyi és vízvédelmi szakhatósági eljárások *az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről szóló 531/2017. (XII. 29.) Korm. rendelet* (hatásköri rendelet) 1. melléklet 9. táblázatában adott felhatalmazás alapján folynak. A területi és az üzemi kárelhárítási terv jóváhagyására irányuló eljárásban a szakhatósági döntéshozatal a Vgtv., a környezeti kárelhárítási rendelet és hatásköri rendelet feljogosító rendelkezése alapján történik. A szakhatósági állásfoglalásnál a területi vízügyi és vízvédelmi hatóság szakemberei figyelemmel vannak továbbá *a vizek hasznosítását, védelmét és kártételeinek elhárítását szolgáló tevékenységekre és létesítményekre vonatkozó általános szabályokról szóló 147/2010. (IV. 29.) Korm. rendelet*re, a Fevir. és a Favir. rendeletekre is. A szakhatósági állásfoglalás *az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény* (Ákr.) 55. és 56. § figyelembevételével születik meg.

A katasztrófavédelmi igazgatóság szakhatósági eljárása során vízvédelmi szempontból a tevékenységnek, létesítménynek a felszíni és felszín alatti vizek védelmére, valamint a vizek állapotára gyakorolt hatását, vízügyi szempontból pedig a tevékenységnek, létesítménynek a vízbázisra, a vizek lefolyására, az árvíz és a jég levonulására gyakorolt hatását vizsgálja. A kérelem tartalmi követelményeit *a vízjogi engedélyezési eljáráshoz szükséges dokumentáció tartalmáról szóló 41/2017. (XII. 29.) BM rendelet* 4. számú melléklete határozza meg. A benyújtott dokumentáció vizsgálatánál a szakhatóság ellenőrzi, hogy a dokumentáció megfelel-e a környezeti kárelhárítási rendeletben meghatározott tartalmi követelményeknek.

Az üzemi környezeti kárelhárítási tervezés üzemeltetői gyakorlatának értékelése

A kutatás során a szerzők több üzemi kárelhárítási tervet vizsgáltak meg, amelyek között volt feldolgozóipari tevékenységek közé tartozó, veszélyes anyag kereskedelmi célú tárolására szakosodott üzem és szénhidrogén tárolásával foglalkozó létesítmény is.

Feldolgozóipari üzem környezeti kárelhárítási tervének vizsgálata

A feldolgozóipari üzemek területén tárolt veszélyes anyagok hasonló körülmények között vannak jelen, mint az általános tárolási funkcióval érintett logisztikai raktárakban. Jelen esetben egy gyógyszergyári telephelyen tűzveszélyes anyagokat raktározó alapanyag-tároló esetében végeztünk vizsgálatokat. A telephely üzemi kárelhárítási terve alapvetően követi a jogszabályi tartalmi követelményeket. Az általános tartalmi követelmények között található a telephelyre vonatkozó működési és üzemeltetési engedélyek nyilvántartása, amely kiváló lehetőséget ad a telephelyre vonatkozó engedélyek szakterületenkénti áttekintésére. Itt megtalálhatók az egységes környezethasználati engedély, a veszélyes anyaggal és készítménnyel végzett általános tevékenységi engedély, az izotópengedélyek.

A levegőminőség-védelmi engedélyek között van a helyhez kötött légszennyező pontforrások működési engedélye, valamint kibocsátási határértékeinek megállapítása; és a szén-dioxid üvegházhatásúgáz-kibocsátással járó tevékenység engedélyezése. A víz és szennyvíz vonatkozásában megemlíthető a telephely önellenőrzési tervének elfogadó határozata, az egyedi kibocsátási küszöbértékét megállapító engedély; a technológiai szennyvíz kezelése, a szenny- és csapadékvíz elvezetése tárgyú vízjogi üzemeltetési engedély; a szennyvíz- és oltóvíz-vezeték átvezetésének vízjogi üzemeltetési engedélye.

Talaj és felszín alatti víz vonatkozásában a folyamatban lévő kármentesítés vízilétesítményeinek vízjogi üzemeltetési engedélyét, valamint a telephely területén feltárt kátrányszennyezés kármentesítése, kármentesítési monitoring záródokumentáció elbírálása ügyében kármentesítési monitoring végzésére kötelezés megnevezésű engedélyeket említi meg a dokumentáció.

Hatósági szempontból ugyancsak hasznos a hatósági ellenőrzések és intézkedési tervek adatait tartalmazó rész, amely hatékonyan segíti a hatósági jogalkalmazó szervet feladatkörének ellátásában.

A következő alfejezetben található meg az alábbi információ: a telephely földrajzi elhelyezkedése, környezetének hidrogeológiai jellemzői, helyi és közeli kútadatok, különös tekintettel a potenciális szennyező forrásokra. A veszélyes tevékenység általános ismertetését követi az üzemi infrastruktúra bemutatása, ahol az ipari vízhálózatot és a tűzoltóvízrendszert, a közműveket is jellemzik. „A szennyvíz gyűjtő, kezelő és elvezető létesítmények, a kibocsátott szennyvíz jellemző mennyiségi és minőségi paraméterei" című fejezetben a terv külön tárgyalja a technológiai és kommunális, hűtő és csapadékvíz elvezetését, illetve a szennyvízkezelő létesítménnyel kapcsolatos információkat. A terv foglalkozik még a technológiai szennyvizek havária esetén

történő tárolási kérdéseivel, amikor az üzemeltető a veszélyes anyagokat tartalmazó technológiai szennyvíz elhelyezésére külön rendszert épített ki.

Megállapítható azonban, hogy az oltóvíztároló képessége ötször nagyobb, mint a vésztározó medence kapacitása. A kibocsátott szennyvíz jellemzőit az üzem minőségi és mennyiségi módon határozza meg. Külön alfejezet mutatja be a vegyi, biológiai anyagok mennyiségét, azok üzemen belüli tárolását.

A veszélyes áru szállítására az üzem közbiztonsági tervvel rendelkezik. A tervben melléklet képezi *a veszélyes folyadékok vagy olvadékok tárolótartályainak, tárolólétesítményeinek műszaki biztonsági követelményeiről, hatósági felügyeletéről szóló 1/2016. (I. 5.) NGM rendelet* hatálya alá tartozó tárolótartályok adatainak ismertetését. A keletkező veszélyes hulladékok sorsával kapcsolatos fejezet annak gyűjtésével, tárolásával és megsemmisítésre való továbbításával foglalkozik.

A kárelhárítási fejezet együttműködési tervvel kezdődik, amelyben szerepel az üzemen belüli figyelőhálózat (ellenőrzési rendszer), a riasztási rendszer, a kárelhárítási vezetők és a külső szervek adatai, a beléptetés rendje, a külső kárelhárítók (közművek, beavatkozók és együttműködő állami szervek) bevonásának rendje, részletes segítségkérési intézkedési terv. A szennyezés okának leírásánál (szinte minden hasonló üzemnél) általánosan alkalmazható események szerepelnek.

Az 1. táblázat tartalmazza a felderítésnél segítséget nyújtó információt.

1. táblázat: A veszélyesanyag-balesetnél történő felderítés alapinformációi üzemi példa alapján

Szembetűnő okok	**Rejtett okok**
Készülékek, gépek és szerelvények téves kezelése	Kezelői hibák, tévedések elhallgatása
Készülékek és gépek jól észlelhető meghibásodása	Készülékek, gépek be nem látható térben történő meghibásodása
Tömítetlenség miatti veszteségek	Rejtett anyaghibák, hajszálrepedések, tömítetlenségek
Csővezetékek, szerelvények meghibásodása	Föld alatti tartályok felszín alatti sérülései
Göngyölegek, tárolóedények sérülése	Hordótéri, raktári göngyölegsérülés
Baleset vagy egyéb rendkívüli esemény	Korróziós anyaghiba

Forrás: a szerzők szerkesztése

A veszélyesanyag-kibocsátásnál mértékadó üzemi adatoknál az átlagos reaktorméretnél kibocsátható veszélyesanyag-mennyiséggel számol az üzemeltető, azonban nem foglalkozik a nagyságrenddel nagyobb tárolókapacitású tartályparkokban tárolt anyagmennyiséggel. Semmilyen utalást nem ad a terv az üzemi veszélyes anyagokkal kapcsolatos súlyos baleseti szabályozáshoz tartozó belső védelmi tervben található súlyos baleseti eseménysorok adataira.

A lokalizációs terv rendeltetése a szennyezés továbbterjedésének megakadályozása, a szennyezés forrásainak megszüntetése. Az intézkedések szintén általánosak, de tartalmazzák a védekezés következő célkitűzéseit: az emberélet veszélyeztetettségének elhárítása, elsősegélynyújtás végzése, a szennyezés-utánpótlás megszüntetése,

a szennyezés csatornába, talajba kerülésének és szétterjedésének megakadályozása, a kárelhárító anyagok és eszközök rendelkezésre állása. A lokalizációs terv tartalmazza még a kárterület körülhatárolását, a potenciális veszélyforrásokat, a lokalizációs munka technológiai utasítását is. A veszélyforrásoknál a biztonsági elemzésre hivatkozik, de részletes eseménysorokat nem vázol fel. Ehelyett felsorolja az üzem területén található vízminőségi kárelhárítás szempontjából potenciális szennyező forrásokat, mint például a gyártástechnológia során felhasznált vegyi anyagokat; a gyártástechnológiát (emberi vagy műszaki hiba); a gyártási melléktermékeket és hulladékokat; a vegyi anyagok szállítását, tárolását, kezelését; vagy a keletkező szennyvizeket, illetve azok kezelését és elvezetését.

A lokalizációs tervben alkalmazott szennyeződés elleni védelem a felitató anyagok használata. A gyártástechnológiánál a szennyeződés kialakulásának okai lehetnek a gyártástechnológiai előírások megszegése; a téves emberi beavatkozás (ürítés, töltés, csapváltás stb.); az üzemen belüli hibás szállítás, szállításkori göngyölegsérülés, járművek meghibásodása; a készülékek, kiegészítő berendezések meghibásodása (törés, lyukadás stb.). Szállítás során csővezeték-meghibásodással, üzemi szállítási balesetekkel számolnak. A raktározás központi raktárakban és tartályparkokban történik. A tényleges kárelhárítási tevékenységnél kizárólag „a helyi kárelhárítási tervre" történő hivatkozás található. A terv foglalkozik a tartályok túltöltés elleni védelmével és időszakos felülvizsgálatával, a láng- és gőzérzékelők átjelzésével és a kármentőkkel. Mennyiségi jellemzést itt sem tartalmaz a terv. A szennyvíz- és csatornarendszer esetében a veszélyes anyagok bemosódásával számol a terv, azonban az oltóvízkezelés itt sem jelent veszélyforrást. „A lokalizáció személyi és tárgyi erőforrás szükséglete" című alfejezet szintén egy általános jellemzést tartalmaz.

A kárelhárítási műveleti terv fő fejezetében részletezik a kárelhárítás folyamatát és technológiai utasításait. Valamennyi veszélyes létesítményre üzemi vészhelyzeti utasítások készültek. Az egyes üzemi utasítások számba veszik az adott üzem területén bekövetkezhető vészhelyzeteket, ismertetik egy esetleges vészhelyzet idején szükséges teendőket, rögzítik az adott terület intézkedésre jogosult vezetőinek elérhetőségét. Az üzemi tervek és utasítások tartalmazzák a rendelkezésre álló kárelhárítási eszközök üzemen belüli elhelyezkedését, veszélyesanyag-kiömlés esetén szükséges intézkedések ismertetését. Az eseményeket két csoportra osztják, így a szilárd és folyékony anyag kikerülésére. A terv e része foglalkozik még a kárelhárítás során keletkező veszélyes hulladék összegyűjtésének, elszállításának, ártalmatlanításának módjával, illetve a kárelhárítási anyagok és eszközök meghatározásával.

„A rendkívüli szennyezés megelőzésének műszaki feltételei (kármentők, figyelő- és jelzőrendszerek), a kárelhárítás erőforrás szükséglete" című fejezetben megállapítják, hogy az 5 m^3-nél nagyobb tárolótartályok megfelelő műszaki védelemmel (például: kármentővel) rendelkeznek. Ezen túl intelligens tűzjelző rendszer is ki van építve, amelynek része a kézi jelzésadó, optikai füstérzékelő, ionizációs füstérzékelő, légelszívásos füstérzékelő, hősebesség-érzékelő, lángérzékelő, oldószergőz-érzékelő, vészkijárati elektronikus kulcsdoboz, vízérzékelő, oltóvízszivattyú és nyitásérzékelő.

A rendkívüli szennyezések megelőzésével kapcsolatban a vegyi anyagokat tároló, kezelő berendezések ellenőrzésével, a csatornarendszer felülvizsgálatával, a hulladékanyagok elhelyezésével és a karbantartási rendszerrel foglalkozó információkat

rögzítették. Megállapítható, hogy a szennyezett oltóvíz felfogásával és kezelésével ez a fejezet sem foglalkozik.

Veszélyes anyag kereskedelmi célú tárolására szakosodott üzem kárelhárítási tervének értékelése

Veszélyes anyag kereskedelmi célú tárolására szakosodott üzem kárelhárítási tervénél – mivel a jogszabályi követelmények elég világosak – a fenti értékelésen túl már csak a tevékenységspecifikus eltérő elemeket fogom kiemelni.

A telephelyi engedélyek között vízjogi engedélyek találhatók, mint a vízjogi létesítési engedély (monitoringkutak), a vízjogi üzemeltetési engedély (monitoringkutak) és a vízjogi üzemeltetési engedély (csapadékvíz-szikkasztók).

A főbb tevékenységek között szerepelnek a közúti és a vasúti folyékony veszélyesanyag-töltés, -lefejtés és -tárolás, valamint a csomagolt szilárd anyag kirakodása és raktározása. A technológiai szennyvízgyűjtő, -kezelő és -elvezető létesítmények zárt rendszerűek. A raktárépületekben esetleges elcsöpögést vagy kifolyást követő takarítás közben keletkező szennyezett mosóvizek a zsompokba folynak le, ahonnan konténerekbe kerül, majd veszélyeshulladék-tárolóban tárolják. A csurgalékvizek veszélyes hulladékként érvényes engedéllyel rendelkező ártalmatlanítóba kerülnek. A vészfelfogási mennyiség nincs részletezve. A padlószerkezetet kármentő medenceként alakították ki, amelyhez kármentő csatornák juttatják el a kifolyt anyagot, amelyet kisebb mennyiség esetén hordóznak. A raktárépület padozata kármentőként van kialakítva, amelynek 25–40 cm-es pereme van, ami a talajszinttől 10 cm-re emelkedik ki. A terv leírja, hogy a csurgalékvíz és a tűzoltáskor keletkező szennyezett oltóvíz kifolyását ez a műszaki megoldás meg tudja akadályozni. A tartálypark túltöltésbiztos, robbanásbiztos, nyomásmentes, és rendelkezik jelöléssel és gázlefejtő csatlakozással. Vészzuhanyok és szemlemosók is találhatók. Az épületen kívüli tartályok kármentőkkel rendelkeznek. A biztonsági berendezések között fel van sorolva a gázömlés-érzékelő és -jelző berendezés, illetve a hő- és füstérzékelő és -jelző berendezés.

A lokalizációs terv alapján a szennyező anyagok a technológiai tárolótartályok, üzemi vezetékek sérülése, a szivattyú sérülése, az átfejtés közben kerülhetnek a kármentőbe, azt követően pedig a talajvízbe.

A telephelyen belüli beavatkozási pontok az alábbiak: felszíni technológiai tárolótartályok közvetlen környezete, a technológiai vezetékrendszer szakaszoló elemei, a veszélyesanyag- és veszélyeshulladék-gyűjtőhely, a szivattyúterek, a csapadékvíz-elvezető csatorna telephelyen belüli víznyelő aknája. A lokalizálás felitatással, hordozható szivattyúval és kármentő edény helyszínre szállításával, vagy tartályautó helyszínre rendelésével lehetséges. Az útfelületre kifolyt veszélyes anyag esetében gátak elhelyezése történik. A kárelhárítási műveleteket az üzemeltető veszélyes létesítményenként külön-külön meghatározza. A terv része a belső védelmi terv, amely mellékletként tartalmazza a környezeti elemeket veszélyeztető súlyos baleseti eseménysorokat.

Szénhidrogén-származékokat tároló üzem kárelhárítási tervének áttekintő értékelése

Szénhidrogén-származékokat tároló üzemben bekövetkező súlyos baleset és üzemzavar esetében a szennyvízcsatornából felfogott szennyezett vizet összegyűjtik, és mechanikai úton (pihentetés, lefölözés) a szénhidrogén-összetevőket eltávolítják. Ez követően a szénhidrogéneket vagy újra feldolgozzák, vagy megsemmisítik a veszélyeshulladék-égetőműben. Az előtisztított vizet vegyszerrel kezelik, segítségével a maradék szénhidrogén is megköthető, lefölözhető. Végül a szénhidrogéntől mentesített víz a biológiai szennyvíztisztítóba kerül, amelyben baktériumok segítségével fémeket, foszfort, ammóniatartalmat távolítanak el.

Befejezés

A rendkívüli események környezeti következményeinek felszámolása napjainkban egyre nagyobb kihívás elé állítja a védelmi rendszer egészét. Az oltóvízszennyezés megelőzése a környezetbiztonság és az iparbiztonság határterületét jelentő szaktevékenység. Ezért hatással lehet rá a környezeti hatásvizsgálati, az egységes környezeti hatásvizsgálati, illetve a vízminőségi kárelhárítási tervezési szabályozás és a kapcsolódó környezetvédelmi és a vízvédelmi hatósági tevékenység.

A környezetvédelmi szabályozás alapján készülő környezeti vagy egységes környezeti hatástanulmány és a veszélyes üzemi biztonsági jelentés és elemzés közös tartalmi részeket tartalmaz. Ezen túl a szabályozások hatálya alá tartozó tevékenységek esetében is átfedések találhatók, amelyek nem helyettesítik, hanem kiegészítik egymást. Ezzel kapcsolatosan meggyőződésem, hogy a hatóságok közötti együttműködés szerepét (különös tekintettel például a supervisori közös hatósági ellenőrzésekre) a jövőben is magas szinten kell tartani.

A vízminőségben jelentkező környezetveszélyeztetés megelőzésének és elhárításának területén a környezeti kárelhárítási rendelet alapján készülő üzemi és területi kárelhárítási tervek elkészítése és alkalmazása a meghatározó, amelyek véleményem szerint hatással vannak a felszíni és felszín alatti vizek védelmére, különösen a vízbázis védelemre.

A vízügyi és vízvédelmi hatáskörrel rendelkező katasztrófavédelmi igazgatóságok szakhatóságokként működnek közre a hatásvizsgálati eljárásoknál, ahol vizsgálják a felszíni és felszín alatti vizek minősége védelmére vonatkozó szabályok érvényesülését. Ugyanez a helyzet az üzemi kárelhárítási tervek vízvédelmi szempontú szakhatósági vizsgálatánál is.

Az üzemi kárelhárítási tervezés és alkalmazás üzemeltetői gyakorlatára jellemző a változatosság, mivel a szabályozás hatálya alá tartozó tevékenységek üzemspecifikus jellemzőket hordoznak magukban.

Fő tanulság továbbá az is, hogy az üzemek többsége a veszélyes anyag kis mennyiségű kibocsátására és lokalizálására készül fel. A tárolóraktár létesítményeknél a padlózat szolgál felfogóhelyként, továbbá a tartályparkokat a veszélyes anyag mennyiségére méretezik. Az oltóvíz mennyiségét és elvezetését nem számszerűsítik.

A hazai iparbiztonsági felsőoktatásban, valamint a hagyományos iparbiztonsági tevékenységi területeken képzést kell biztosítani az ipari környezetszennyezés megelőzése területén.[14]

Felhasznált irodalom

Berek, Tamás – Földi, László – Padányi, József (2020): The Structure and Main Elements of Disaster Management System of the Hungarian Defence Forces, with Special Regard to the Development of International Cooperation. *AARMS,* 19(1), 17–26. Online: https://doi.org/10.32565/aarms.2020.1.2

Cimer, Zsolt – Szakál, Béla (2015): Control of Major-Accidents Involving Dangerous Substances Relating to Combined Terminals. *Science for Population Protection,* 7(1), 1–11. Online: www.population-protection.eu/prilohy/casopis/eng/21/98.pdf

Érces Gergő – Vass Gyula (2018): Veszélyes ipari üzemek tűzvédelme ipari üzemek fenntartható tűzbiztonságának fejlesztési lehetőségei a komplex tűzvédelem tekintetében. *Műszaki Katonai Közlöny,* 28(4), 2–22. Online: https://bit.ly/3TDnfBu

Halász László – Földi László (2014): *Környezetbiztonság.* Budapest: Nemzeti Közszolgálati Egyetem. Online: https://opac.uni-nke.hu/webview?infile=&sobj=9279&source=webvd&cgimime=application%2Fpdf%0D%0A

Kátai-Urbán Maxim et al. (2023): Veszélyes anyagok tárolása a logisztikai raktárakban. *Műszaki Katonai Közlöny,* 33(3), 63–75. Online: https://doi.org/10.32562/mkk.2023.3.6

Nagy Rudolf (2023): A munkahelyi kémiai ártalmak és az iparbiztonság. *Polgári Védelmi Szemle,* 15(19), 261–279.

Teknős, László – Lakatos, Bence – Vass, Gyula (2023): Possibilities for Further Development of the Disaster Management Authority System. *American Journal of Research Education and Development,* 1, 17–25. Online: www.red.devlart.hu/issues/2023_1.pdf#page=17

Vass, Gyula (2017): Industrial Safety Training in Disaster Management Higher Education in Hungary. *Pozhary i Chrezvychajnye Situacii: Predotvrashenie Likvidacia,* 8(2), 80–84. Online: https://doi.org/10.25257/FE.2017.2.80-84

Vince, Ivan (2008): *Major Accidents to the Environment: A Practical Guide to the Seveso II Directive and COMAH Regulations.* Oxford: Elsevier.

Jogi források

1995. évi LIII. törvény a környezet védelmének általános szabályairól

1995. évi LVII. törvény a vízgazdálkodásról

2016. évi CL. törvény az általános közigazgatási rendtartásról

223/2014. (IX. 4.) Korm. rendelet a vízügyi igazgatási és a vízügyi, valamint a vízvédelmi hatósági feladatokat ellátó szervek kijelöléséről

[14] Vass 2017.

314/2005. (XII. 25.) Korm. rendelet a környezeti hatásvizsgálati és az egységes környezethasználati engedélyezési eljárásról
90/2007. (IV. 26.) Korm. rendelet a környezetkárosodás megelőzésének és elhárításának rendjéről
366/2015. (XII. 2.) Korm. rendelet a vízvédelmi igazgatási feladatokat ellátó szervek kijelöléséről, és egyes vízügyi tárgyú kormányrendeletek módosításáról
219/2004. (VII. 21.) Korm. rendelet a felszín alatti vizek védelméről
220/2004. (VII. 21.) Korm. rendelet a felszíni vizek minősége védelmének szabályairól
531/2017. (XII. 29.) Korm. rendelet az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről
147/2010. (IV. 29.) Korm. rendelet a vizek hasznosítását, védelmét és kártételeinek elhárítását szolgáló tevékenységekre és létesítményekre vonatkozó általános szabályokról
27/2005. (XII. 6.) KvVM rendelet a használt és szennyvizek kibocsátásának ellenőrzésére vonatkozó részletes szabályokról
41/2017. (XII. 29.) BM rendelet a vízjogi engedélyezési eljáráshoz szükséges dokumentáció tartalmáról
1/2016. (I. 5.) NGM rendelet a veszélyes folyadékok vagy olvadékok tárolótartályainak, tároló-létesítményeinek műszaki biztonsági követelményeiről, hatósági felügyeletéről

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

19. évfolyam (2024) 2. szám 77–86.
DOI: 10.32567/hm.2024.2.6

Tóth Attila,[1] Tóth Levente[2]

Videóalapú tűzérzékelés

Video-Based Fire Detection

Absztrakt

A tűzesetek jelentős veszélyt jelentenek az emberi életre és a vagyonbiztonságra, ezért a korai észlelés kulcsfontosságú a potenciális károk mérséklése szempontjából. A hagyományos tűzjelző rendszerek többnyire füstérzékelőkre vagy hőérzékelőkre támaszkodnak, amelyek viszont bizonyos esetekben (például bonyolult kialakítású, tagolt környezetben) nem képesek a keletkező tüzet megfelelő korai stádiumban észlelni. Az elmúlt évek technológiai fejlődése azonban új lehetőségeket nyitott meg ezen a területen. A mesterséges intelligencia (MI) és a videóanalitika integrálása ígéretes megoldásnak bizonyult a tűzjelzési képességek javítására. Az MI-alapú videóanalitika alkalmazása lehetővé teszi, hogy a rendszerek sokkal gyorsabban és pontosabban észleljék a tüzeket, még azok korai stádiumában is. Az intelligens kamerák és a számítógépes látás technikáinak használata révén a tűzjelző rendszerek képesek felismerni a tűz különböző vizuális jeleit, mint például a füst, a lángok és a hőmérséklet-változások. A hagyományos tűzjelző rendszerekkel szemben az MI-alapú megoldások képesek folyamatosan tanulni és alkalmazkodni az új információkhoz, ami növeli az észlelés pontosságát, valamint az intelligens kamerák által gyűjtött adatok valós időben elemezhetők, ami lehetővé teszi a gyorsabb reagálást és beavatkozást. Szintén a rendszernek köszönhetően képesek különbséget tenni a valódi veszélyforrások és az ártalmatlan jelenségek között, így csökkentve a téves riasztások számát. Ez a cikk részletesen vizsgálja az MI-alapú videóanalitika fejlődését és alkalmazását a tűzjelzés területén. Emellett bemutatja a jelenlegi kihívásokat és a jövőbeli fejlődési irányokat ebben a szegmensben, hogy jobban megérthessük az MI és a videóanalitika potenciálját a tűzjelzés terén.

Kulcsszavak: kamera, mesterséges intelligencia, videóanalitika, korai tűzérzékelés

[1] PhD tanársegéd, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék, e-mail: toth.attila@uni-nke.hu
[2] PhD tanársegéd, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék, e-mail: toth.levente@uni-nke.hu

Abstract

Fire incidents pose a significant threat to human life and property security, making early detection crucial for mitigating potential damage. Traditional fire alarm systems predominantly depend on smoke detectors or thermal sensors, which may be insufficient in certain scenarios (such as intricate, compartmentalised settings) to promptly detect the emerging fire. However, technological advancements in recent years have opened new possibilities in this field. The integration of artificial intelligence (AI) and video analytics has proven to be a promising solution for improving fire detection capabilities. The application of AI-based video analytics allows systems to detect fires much faster and more accurately, even in their early stages. By using smart cameras and computer vision techniques, fire alarm systems can identify various visual signs of fire, such as smoke, flames, and temperature changes. Unlike traditional fire alarm systems, AI-based solutions can continuously learn and adapt to new information, enhancing detection accuracy. Additionally, the data collected by smart cameras can be analysed in real-time, enabling quicker response and intervention. These systems can also distinguish between real threats and harmless phenomena, reducing the number of false alarms. This article examines in detail the development and application of AI-based video analytics in fire detection. It also presents the current challenges and future development directions in this field to better understand the potential of AI and video analytics in fire detection.

Keywords: camera, artificial intelligence, video analytics, early fire detection

Bevezetés

Az épületekben és környezetükben egyre több kamerát használunk. A kamerákat túlnyomórészt vagyonvédelmi vagy munkavédelmi, esetleg munkafolyamat ellenőrzése céljából telepítjük.[3] A vagyonvédelmi rendszerek mellett használatosak a tűzmegelőzési célra telepített tűzvédelmi jelzőrendszerek, amelyek a tűzvédelmi oltórendszerekkel együtt látják el rendeltetésüket.[4] A tűzvédelmi jelzőrendszerek mellett különösen fontos az ipari környezetben, elsősorban tűzveszélyes és mérgező hatású veszélyes anyagok kimutatására szolgáló jelzőrendszerek alkalmazása is.[5] E rendszereket telepíthetik épületeken belül, mint például a kereskedelmi és logisztikai raktárépületekben, vagy a technológiai környezetben az épületen kívül is.[6] Az utóbbi években a technológiai fejlődés folytán előtérbe került e rendszerek egyszerűsítése és alkalmazásuk harmonizálása más célt szolgáló rendszerekkel. Utóbbiak lehetnek a vagyon- és munkavédelmi feladatok céljából telepített kamerarendszerek.

A felszerelt kamerák képeit emberek figyelik, akiknek a munkáját sok esetben különféle videóanalitikai eljárások támogatják.[7] Napjainkban jellemzően különálló

[3] Tóth 2017.
[4] Érces–Vass 2018.
[5] Cimer et al. 2021.
[6] Kátai-Urbán et al. 2023.
[7] Tóth 2018.

rendszereket telepítünk a fenti feladatokra. A rendszerek integrálásával és a felszerelt kamerák többcélú felhasználásával azonban jelentősen tudjuk csökkenteni a rendszerek összesített bekerülési költségét, a karbantartási költséget és az amortizációs költséget.

A kamerák többcélú felhasználása esetén a képeket figyelő emberek munkájának támogatása érdekében különféle videóanalitikai eljárások használata javasolt. Videóanalitikai eljárásokat használhatunk vagyonvédelmi célból, munkavédelmi célból, vagy akár munkafolyamat ellenőrzése céljából. Joggal merül fel a kérdés, hogy hogyan alkalmazhatnánk az épületen belüli és az épület környezetét figyelő kamerák képi információit tűzvédelmi célokra. A CCTV[8]-kamerák által szolgáltatott képek tűzvédelmi célú alkalmazásának kutatása napjainkra kulcsfontosságú kutatási területté vált.[9]

A hagyományos rendszerek hátrányai

Az automatikus tűzjelző rendszerek napjainkban túlnyomórészt optikai füstérzékelőket, hőmaximum-, illetve hősebesség-érzékelőket, szén-dioxid-érzékelőket, valamint ezek kombinációit használják a keletkező tűz hatására egy pont környezetében megjelenő különféle anyagi közvetítésű tűzjellemzők érzékelésére. Anyagi közvetítésű tűzjellemzők az égés során keletkező különféle aeroszolok, füstszemcsék és a hőmérséklet-emelkedés. Nagyobb területeket több pontszerű érzékelő telepítésével vagy vonali érzékelők használatával tudunk védeni. A vonali érzékelők alkalmazásával nagyobb érzékenységet tudunk elérni, így akár nagyobb belmagasságú épületeket is tudunk védeni. Az anyagi közvetítésű tűzjellemzőknek az érzékelése azonban viszonylag lassú, mivel az aeroszoloknak, a füstszemcséknek és a szállított hőnek el kell érnie a mennyezetre szerelt érzékelőt, ráadásul olyan koncentrációban vagy olyan mértékű hőmérséklet-emelkedést produkálva, amely már eléri a jelzési küszöbszintet. Tovább ronthatják a jelzési sebességet a nem megfelelő helyre tervezett vagy helytelenül telepített automatikus érzékelők, valamint az utólagosan beépített épületgépészeti elemek, világítótestek, vagy akár az utólag beépített nagy méretű bútorok, térelválasztók, ventilátorok.

A kültéren keletkező tüzek jelzése különösen nehézkes, mivel rendkívül korlátozott a kültéri körülmények között alkalmazható automatikus érzékelők köre. A korábban felsorolt pontszerű érzékelők csak beltérben használhatók, mivel kültéren csak fedett helyre lehetne őket telepíteni, de a nyitott kültéri tárolókban kialakuló nagy hőmérséklet-ingadozás, por, pára téves jelzést okozhatnak. Kültéren általában lángérzékelőket, esetleg hőérzékelő kábeleket használhatunk tűzjelzésre. Ezek az eszközök azonban kizárólag lángfázisban képesek érzékelni a keletkező tüzet. Ez komoly problémát jelent, hiszen az emberéletek megmentése és az anyagi károk minimalizálása érdekében kültéren is legkésőbb a füstképződés szakaszában kellene jeleznünk a keletkező tüzet. További probléma, hogy a füstérzékelők nem képesek megkülönböztetni a valódi

[8] CCTV: Az angol *closed circuit television system* szavak kezdőbetűiből képzett rövidítés, ami zárt láncú televízió-rendszert jelent. Gyűjtőnéven így nevezzük azokat a kamerarendszereket is, amelyek távoli hozzáféréssel is rendelkeznek, ezért nem tekinthetők zárt láncúnak.

[9] Cheong–Ko–Nam 2008.

tűzből származó füstrészecskéket és más forrásokból származó részecskéket, mint például a por vagy a sűrű vízgőz. Ez pedig magas téves riasztási eseményt produkál.[10] A lángérzékelők másik hátránya, hogy egyes természeti jelenségek, mint például a villámlás vagy a szikra, téves riasztást okozhatnak. Problémát jelenthet még ezen kívül az érzékelők elkoszolódás miatti „vakulása", amely rendszeres, gyakori karbantartással elkerülhető, azonban ez jelentősen megnöveli a rendszer üzemeltetési költségét.

MI-alapú videóanalitika a tűzjelzéshez

Az automatikus tűzjelző rendszerekkel szemben a CCTV-rendszer kameráinak tűzérzékelésre történő felhasználása nagymértékben növelheti a tűzbiztonságot. A kameraképek elemzésével sokkal rövidebb idő alatt észlelhető a keletkező tűz, mivel az égéskor keletkező különféle tűzjellemzőknek nem kell elérniük a kamerát ahhoz, hogy azokat a kamera észlelje, a beépített videóanalitika pedig jelzést generáljon. További előnye a képi látáson alapuló tűzérzékelésnek, hogy a képeket felügyelő élőerő távolról meg tudja állapítani, hogy valós tűzjelzés történt, vagy esetleg téves riasztás. Valós tűz esetén azonnal látja a tűz kiterjedését, annak terjedési irányát és sebességét, meg tudja állapítani, hogy mi van veszélyeztetve. Ezeknek az információknak a birtokában a kiérkező tűzoltó célirányosan tudja megkezdeni az oltást, és meg tudja gátolni a tűz továbbterjedését.

A mesterséges intelligencia (MI) az informatikai tudomány egy területe, amely az emberi gondolkodás és döntéshozatal mechanizmusait próbálja modellezni és szimulálni gépi rendszerek segítségével. Az MI fő célja az intelligens viselkedés utánzása, amely hasonló az emberi tevékenységekhez. A gépi tanulás, vagy más néven ML, az MI egyik alcsoportja, amelynek fő tevékenysége az adatokból tanuló algoritmusok fejlesztése, és ezek teljesítménye arányosan nő az adatok mennyiségével. Ezek az algoritmusok nem előre kódoltak egy adott feladatra, hanem az adatokból tanulva alakítják ki a feladatok végrehajtásának módját, és implicit szabályokat sajátítanak el a példákból. Az adatok alapján olyan becsléseket készítünk, amelyek lehetővé teszik a jövőbeli tevékenységek előrejelzését.

A mélytanulás, vagy DL *(deep learning),* az MI egyik területe, ami a biológiai neurális hálózatokon alapuló mesterséges neurális hálózatokkal foglalkozik. A mélytanulás fontos elemei a többrétegű neurális hálózatok, amelyek különböző matematikai műveleteket hajtanak végre a bemeneti adatokon, és ezzel progresszív módon magasabb absztrakciós szinteket hoznak létre. Ennek köszönhetően a rendszer képes megoldani olyan feladatokat, mint például a kép- és beszédfelismerés, a természetes nyelvfeldolgozás, az autonóm járművek vezérlése, az orvosi diagnózisok támogatása vagy az ipari minőség-ellenőrzés hatékonyságának növelése. Ezek a gépi tanulási modellek folyamatos fejlődésen mennek keresztül, és minél több adaton tanulnak, annál hatékonyabbá és megbízhatóbbá válnak a feladatok elvégzése során.

A mesterséges intelligencia képi jelfeldogozás céljára történő felhasználása mára már nem számít újdonságnak. A nagy teljesítményű és olcsó számítástechnikai

[10] Xu–Xu 2007.

hardverek elérhetősége, valamint a mesterséges intelligencia fejlődése következtében, a kezdeti pixelalapú mozgásérzékelést, vonalátlépést felváltották azok a nagy számítástechnikai kapacitást igénylő algoritmusok fejlesztései amelyek szükségesek egy hatékony, jól működő intelligens videómegfigyelő rendszer kialakításához. Ezek közé tartozik a már lassan húsz éves múlttal rendelkező tárgyak követése, az autóiparban is használt gyalogosok felismerése, a járáselemzés, a járműfelismerés, az arcfelismerés és a tömegszámlálás. A nanotechnológia térnyerésével lehetőség nyílik a gépi látás[11] kamerába történő integrálására és a lokális (végponti) vizuális tartalomelemzés megvalósítására. A gépi látás célja, hogy képessé tegye a számítógépeket az emberi látás alapvető elemeinek reprodukálására. Ezek lehetnek: mozgó objektumok, különösen emberi sziluettek felismerése, arcfelismerés, a megfigyelt személy életkorának és nemének meghatározása, rendszámfelismerés, terület- és határvédelem, mozgó objektumok számlálása, tömegek viselkedésének elemzése, tevékenységfelismerés és viselkedésmegértés, hirtelen, gyorsan végbemenő események észlelése (például rablás), szokatlan/rendellenes viselkedés felismerése (például verekedés, ájulás, elesés), objektumkövetés és pályaelemzés, járműkövetés és forgalomelemzés, elhagyott/elveszett tárgyak, vagy éppen a füst/tűz észlelése. Kültéren ezek a képelemző feladatok sokszor a változó időjárási és fényviszonyok miatt nem egyszerűek.

Az MI-alapú videóanalitika gépi látást és gépi tanulást alkalmaz a videófelvételek valós idejű elemzésére. Ezeket a rendszereket arra használják, hogy mintákat, rendellenességeket és adott tárgyakat vagy eseményeket ismerjenek fel a képi adatokban. A tűzjelzés kontextusában az MI-alapú videóanalitika képes lehet felismerni a tűz vizuális jellemzőit, mint a füst, a lángok, a hősugárzás és az égési folyamat egyéb jeleit.

Bár a mesterséges intelligencia témakör 2023. év végével, a nagy nyelvi modellek[12] elterjedésével kapott kiemelt figyelmet, a képtartalom-elemzés, ezen belül is a kamerák tűzérzékeléshez való használatának koncepciója a 20. század végére nyúlik vissza. 1996-ban a Washingtoni Állami Egyetem Gépészeti és Anyagtudományi Karán Plumb és munkatársa által készített tanulmány egy gazdaságos, videóalapú tűzérzékelő és helymeghatározó rendszer fejlesztésével foglalkozott.[13] A rendszer egy CCD-kamerát és egy számítógépet használt a tűz észlelésére és helyének meghatározására. A tanulmány kiemeli a rendszer gazdaságosságát, amely a videóalapú technológia alkalmazásának köszönhető. A videóalapú tűzérzékelés olcsóbb, mint a hagyományos érzékelők, és kevesebb karbantartást igényel.

A *video smoke detection,* azaz VSD-rendszer már a korai, analóg korszakában is annyira pontos volt a képi elemzésében, hogy különbséget tudott tenni a gőz és a füst között, és képes volt felismerni a kis mennyiségű füstöt és lángmintákat a videóképben. A VSD-rendszer szabványos CCTV-kamerákat használt, amelyek egy önálló feldolgozó rendszerhez kapcsolódtak.

[11] A gépi látás az ipari automatizálás egyik alaptechnológiája. A gépi látás során a kamerákkal készült képeket neurális hálózat segítségével dolgozzuk fel, és a mélytanulásnak nevezett folyamat végén osztályozással, klaszterezéssel segítjük az objektumfelismerést, -csoportosítást.

[12] A „nagy nyelvi modell" egy olyan mesterségesintelligencia-alapú rendszer, amely nagy mennyiségű nyelvi adatot használ fel a tanuláshoz és a nyelvi feladatok végrehajtásához. Ezek a modellek képesek szövegek feldolgozására, elemzésére és generálására, valamint nyelvi feladatok megoldására, például fordításra, szövegértésre és beszédfelismerésre.

[13] Plumb–Richards 1996.

Az azóta eltelt közel 30 év alatt sokat fejlődött mind a képalkotási, mind pedig a képfeldolgozási technológia. A fejlett gyártási technológiának és az ebből fakadó folyamatos miniatürizálódásnak köszönhetően a mai videókamera-alapú tűzérzékelő rendszerek képfeldolgozó algoritmusai nemcsak szerveroldali, hanem kamerába integrált módon is megtalálhatók. Ezek a kamerák fejlett képérzékelőkkel, nagy teljesítményű processzorral és MI-képes szoftverrel vannak felszerelve. Képesek valós időben elemezni a videófelvételeket, észlelni a potenciális tűzeseteket, és megfelelő riasztásokat kezdeményezni.

A lángok és a keletkező füstök alakja, sűrűsége és színe a tűzforrás méretétől, az éghető anyagok típusától és a környezeti feltételektől függően változik. Ennek megfelelően a videóalapú füstérzékelő algoritmusokat a felhasznált technológia szerint főként két kategóriára lehet osztani. A hagyományos füstérzékelő algoritmusokon alapuló rendszereknél először az előtér-kivonásos módszert használják a feltételezett füsttel borított terület kijelölésére. Ezután kivonják a füst jellemző vektorát a jelölt területről. Ez a lépés nagyban befolyásolja az ezt követő osztályozás teljesítményét. A legtöbb létező algoritmus statikus, szín-, alak-, textúra- és dinamikus, azaz mozgásjellemzőkön alapul. A lángok dinamikus jellemzői közé tartozik a villogás, az alakváltozások és a területváltozások, míg a füst dinamikus jellemzői közé tartozik a mozgás iránya és a kontúr változása. A kizárólag statikus jellemzők használatából eredő magas hamis-téves jelzések csökkentése érdekében célszerű a statikus és dinamikus jellemzők együttes kiértékelése.

A másik módszernél egy neurális hálózaton alapuló mélytanulásos füstérzékelési algoritmust használnak, amelyet nagyszámú füstadatkészlettel képeznek a végső füstérzékelési modell elkészítéséhez. A tanítási körülmények ismertetésére és a felmerülő kihívások kezelési módjára jó alapot szolgáltat Muhammad és társainak kutatása.[14] A betanítás és tesztelés céljára egy 2015-ben megjelent NVidia GeForce GTX TITAN X grafikus kártyát használtak 12 GB beépített memóriával. Az alapszámítógépen futó Ubuntu operációs rendszer Intel Core i5 CPU-val, 64 GB RAM-mal rendelkezett. A kísérletekben használt képek száma összesen 68 457 db volt, amelyeknek 20%-át betanításhoz, a fennmaradó 80%-ot pedig teszteléshez használták. Bizonyos kísérletekben az egyetlen képkockás kép statikus jellemzőinek felhasználása mellett a képkockák közötti mozgásinformációkat is felhasználják, amivel az érzékelés pontossága tovább növelhető. Ettől függetlenül a mélytanuláson alapuló módszer erősen függ az adatkészlettől, és sajnos ezen a területen nincs hivatalos, nyílt szabványú füstadatkészlet.

A technológia fejlődésének köszönhető a kameraképek növekvő felbontása, ami lehetővé teszi, hogy a videóalapú tűzérzékelést nemcsak kis területek megfigyelésére, hanem nagyobb, akár kültéri erdőtüzek észlelésére is alkalmazzuk.

Az észlelési megbízhatóság fokozása érdekében folyamatosak a kutatások. A képfeldolgozást alkalmazó tűzérzékelő algoritmusok jellemzően elemzik a lángok vagy a füst pixeltulajdonságait, olyan szempontokra összpontosítva, mint a szín, a láng és annak háttere közötti kontraszt, valamint a lángok villódzó viselkedése.

[14] Muhammad et al. 2018.

Sobel-szűrőt[15] használva pontosabban észlelhetjük az objektumszéleket, ezáltal megbízhatóbban meg tudjuk különböztetni a lángot a háttértől, ami kulcsfontosságú a hatékony lángérzékeléshez.[16] A lángszélek ismeretében következtethetünk a tűz nagyságára és a terjedés irányára és sebességére is. A lángérzékelő rendszerekben a Sobel-élérzékelést gyakran kombinálják színalapú szegmentációs módszerekkel. Ez a kombináció lehetővé teszi a rendszer számára, hogy mind a színinformációkat, mind az élinformációkat használja a lángok pontosabb azonosítására, javítva az érzékelőrendszer megbízhatóságát.

Nehézzé teszi a detektálást, hogy különösen a tűz kezdeti szakaszában a füst szinte átlátszó, alacsony kontrasztú, diffúz határokkal és gyorsan változó alakkal rendelkezik. A probléma akkor jelentkezik, amikor az időjárási feltételek (köd, eső, sűrű hóesés stb.) jelentősen módosítják az algoritmus képzésére használt körülményeket, mivel a legtöbb neurális hálózaton alapuló füstérzékelési módszert csak a normál időjárási környezetben készült tesztadatokkal tanítják. Ezek a zord környezeti elemek komoly képromlást, alacsony kontrasztot és részletek elvesztését okozzák, ami miatt a meglévő módszerek nem hatékonyak. Az ilyen események kezelésének egyik általános megközelítése a képek ködmentesítése.[17] A fejlettebb módszerek közé tartozik a köd szintetizálása a képeken, vagy füsttanító adathalmazok kifejlesztése ködös környezetben.[18]

Ígéretes kutatások folynak a YOLOv3[19] gépi tanulási algoritmus tűzterjedési vizsgálatokban történő alkalmazására. A modell alkalmazásával lehetőség van a pontos, valós időben történő tűzérzékelésre.[20] A különböző színmodelleket (HSV, RGB, YCbCr[21]) alkalmazva a lángok sajátos színjellemzőinek észlelésére, segít megkülönböztetni a tüzet más tárgyaktól, és tovább csökkenti a hamis riasztások számát.[22]

A megfelelő mesterségesintelligencia-algoritmus kiválasztása a technológia folyamatos fejlődése mellett nem egyszerű. Sanjana szerzőtársaival öt különböző neurális hálózatot tesztelt, hogy megállapítsa, melyik a leghatékonyabb a tűz érzékelésére.[23] Összességében a tanulmány arra a következtetésre jutott, hogy bár az összes tesztelt modell képes tüzek észlelésére, a tesztelt modellek közül a ResNet és a Mobile Net bizonyította a legnagyobb pontosságot a tüzek észlelésében. Mindkettő 83,06%-os pontossági arányt ért el, így azok megfigyelési rendszerekben történő megvalósítása jelentősen javíthatja a tűzérzékelést és a reakcióidőt. A többi modell, a GoogleNet,

[15] A Sobel-operátorok két mátrixból állnak, ha ezeket végigmozgatjuk a képen, kiszámítják a vízszintes és függőleges irányú gradienseket. A gradiensek nagysága és iránya alapján azonosítják az éleket.

[16] Riyadi–Aisyah 2018.

[17] Berman–Tali–Shai 2016.

[18] He et al. 2021.

[19] A YOLOv3 egy valós idejű objektumészlelő algoritmus, amelyet Joseph Redmon és Ali Farhadi fejlesztett ki. Ez a You Only Look Once (YOLO) algoritmus harmadik generációja, amely a sebesség és pontosság terén is jelentős javulást mutat az előző verziókhoz képest. A YOLOv3 egy Darknet-53 nevű mély neurális hálózatot használ a képek jellemzőinek kinyerésére. Ezután egy sor konvolúciós réteget és egy objektumészlelő réteget alkalmaz az objektumok észlelésére. A YOLOv3 architektúrája egyszerű és hatékony, ami hozzájárul a sebességéhez és pontosságához.

[20] Nagulan et al. 2022.

[21] A HSV a színeket árnyalat, telítettség és érték alapján írja le, míg az RGB egy vörös, zöld és kék színeken alapuló additív színmodell. Az YCbCr színmodell a fényerőt (Y) és a krominanciát (Cb és Cr) külön kezeli.

[22] Charoskar et al. 2023.

[23] Sanjana et al. 2022.

a RegNet és a testreszabott Feed Forward neurális hálózat alacsonyabb pontosságot mutatott.

A legfrissebb kutatásokban sikerült ezt a pontosságot is felülmúlni. A YOLOv8[24] modellekkel felépített tűzérzékelő rendszer közel 96%-os pontosságot ért el a tesztkörnyezetben.[25]

A kísérletek biztatók, bár a kültéri tűz és füst észlelése számos kihívást jelent. A füstcsóvák dinamikus és véletlenszerű szerkezete, valamint az összetett erdei tájat alkotó számos környezeti elem, mint például a felhőtakaró és a köd, megnehezíti az észlelési folyamatot. A számítógépes látástechnológia alkalmazása az emberi megfigyelés helyettesítésére rendkívül hatékony módszert kínál e kihívások megoldására.

Összegzés

A tűzoltás mielőbbi megkezdése érdekében, a tűz kialakulásának kezdeti szakaszában a pontos, hatékony és időben történő tűzérzékelés létfontosságú szerepet játszik. A hagyományos tűzérzékelési módszerek elsősorban érzékelőalapú technológiákra támaszkodnak, azonban fontos megjegyezni, hogy ezeknek vannak korlátaik és hiányosságaik. A mesterséges intelligencia és a különféle videóanalitikai módszerek az elmúlt években jelentős fejlődésen mentek keresztül, ezáltal forradalmasítva a tűzészlelést. Ezek a technológiák lehetővé teszik a korai szakaszban történő tűzészlelést, ami kulcsfontosságú a veszteségek minimalizálásában. A videóanalitikák kiértékelik a vizuális adatokat, például a videófelvételeket, hogy azonosítsák a tűzzel kapcsolatos jeleket, mint a füst, a hő vagy a lángok. A modern videóanalitika és a mesterséges intelligencia kombinációja nemcsak a tűzjelzést, hanem a teljes biztonságtechnikai rendszert is új szintre emeli. Az MI-alapú kamerarendszerek jelentősen javítják a tűzesetek azonosításának pontosságát. Ezek a rendszerek a viselkedéselemzés, hőmérsékletmérés és tűzdetektálás funkciókat is tartalmazzák, amelyekkel a tűzveszélyes helyzeteket még a kezdeti szakaszában lehet azonosítani. Bár még számos kihívást kell leküzdeni, a technológia folyamatos fejlődése azt sugallja, hogy az MI-alapú videóanalitika egyre elterjedtebbé válik a tűzbiztonság területén, hozzájárulva az emberi élet és a vagyonbiztonság védelméhez.

Az MI-alapú videóanalitika alkalmazása azonban nem mentes a kihívásoktól. Az egyik legnagyobb kihívás az adatok minősége és mennyisége. A rendszerek hatékonysága nagymértékben függ az általuk feldolgozott adatok pontosságától és relevanciájától. Ezenkívül az adatvédelem és a magánszféra kérdései is fontos szempontok, amelyeket figyelembe kell venni. Az adatbiztonság garantálása érdekében szigorú szabályozásokat és protokollokat kell bevezetni.

A jövőbeli fejlődési irányok között szerepel az MI-algoritmusok továbbfejlesztése, megfelelő tanító adatbázisok összeállítása, hogy még pontosabb és gyorsabb észlelést tegyenek lehetővé. Emellett fontos célkitűzés a rendszerek integrálása más

[24] A You Only Look Once (YOLO) algoritmus nyolcadik generációja.
[25] Chetoui–Akhloufi 2024.

biztonsági és épületfelügyeleti rendszerekkel, hogy egy átfogóbb és hatékonyabb védelmi hálózatot hozzanak létre.

Összességében elmondható, hogy az MI és a videóanalitika integrálása forradalmasíthatja a tűzjelző rendszereket, jelentősen növelve azok hatékonyságát és megbízhatóságát. Bár számos kihívás áll még előttünk, a technológiai fejlődési iránya ígéretes, és remélhetőleg hozzájárul majd a tűzbiztonság jelentős javulásához világszerte.

Felhasznált irodalom

Berman, Dana – Tali, Treibitz – Shai, Avidan (2016): *Non-Local Image Dehazing.* 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Las Vegas: IEEE. Online: https://doi.org/10.1109/CVPR.2016.185

Charoskar, Rohit et al. (2023): Fire Detection and Localization in Video Surveillance Application. *International Journal of Advanced Research in Science, Communication and Technology,* 3(1), 457–460. Online: https://doi.org/10.48175/IJARSCT-9066

Cheong, Kwang-Ho – Ko, Byoung-Chul – Nam, Jae-Yeal (2008): Automatic Fire Detection System Using CCD Camera and Bayesian Network. *Electronic Imaging,* SPIE6813. Online: https://doi.org/10.1117/12.764822

Chetoui, Mohamed – Akhloufi, Moulay A. (2024): Fire and Smoke Detection Using Fine-Tuned YOLOv8 and YOLOv7 Deep Models. *Fire,* 7(4), 135. Online: https://doi.org/10.3390/fire7040135

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

Érces Gergő – Vass Gyula (2018): Veszélyes ipari üzemek tűzvédelme ipari üzemek fenntartható tűzbiztonságának fejlesztési lehetőségei a komplex tűzvédelem tekintetében. *Műszaki Katonai Közlöny,* 28(4), 2–22. Online: https://bit.ly/3ZuWnaP

He, Lijun et al. (2021): Efficient Attention Based Deep Fusion CNN for Smoke Detection in Fog Environment. *Neurocomputing,* 434, 224–238. Online: https://doi.org/10.1016/j.neucom.2021.01.024

Kátai-Urbán, Maxim (2023): Identification Methodology for Chemical Warehouses Dealing with Flammable Substances Capable of Causing Firewater Pollution. *Fire,* 6(9), 345. Online: https://doi.org/10.3390/fire6090345

Muhammad, Khan et al. (2018): Convolutional Neural Networks Based Fire Detection in Surveillance Videos. *IEEE Access,* 6, 18174–18183. Online: https://doi.org/10.1109/ACCESS.2018.2812835

Nagulan, S. et al. (2022): An Efficient Real-Time Fire Detection Method Using Computer Vision and Neural Network-Based Video Analysis. In *Proceedings of Third Doctoral Symposium on Computational Intelligence,* 627–637. Online: https://doi.org/10.1007/978-981-19-3148-2_55

Plumb, O. Augustus – Richards, F. (1996): *Development of an Economical Video Based Fire Detection and Location System.* National Institute of Standards and Technology.

Riyadi, D. Slamet – Aisyah, Siti (2018): *Vision Based Flame Detection System For Surveillance Camera.* 2018 International Conference on Applied Engineering (ICAE), Batam. Online: https://doi.org/10.1109/INCAE.2018.8579405

Sanjana, S. et al. (2022): *Deep Learning Models for Fire Detection Using Surveillance Cameras in Public Places.* 13th International Conference on Computing Communication and Networking Technologies. Kharagpur: IEEE. 1–7. Online: https://doi.org/10.1109/ICCCNT54827.2022.9984601

Tóth Attila (2018): Az élőerő munkáját segítő technikai megoldások. *Hadmérnök,* 13(2), 29–36. Online: http://hadmernok.hu/182_03_toth.pdf

Tóth, Levente (2017): Resolution Limit of Small Image Sensors Size. *Acta Technica Corviniensis – Bulletin of Engineering,* 2, 39–44. Online: https://acta.fih.upt.ro/pdf/2017-2/ACTA-2017-2-05.pdf

Tóth Levente (2018): Kisformátumú képbontók határfelbontás korlátai. *Hadmérnök,* 13(3), 38–49. Online: http://hadmernok.hu/183_04_toth.pdf

Xu, Zhengguang – Xu, Jialin (2007): *Automatic Fire Smoke Detection Based on Image Visual Features.* 2007 International Conference on Computational Intelligence and Security Workshops (CISW 2007), Harbin. 316–319. Online: https://doi.org/10.1109/CISW.2007.4425500

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 2. szám 87–95.
DOI: 10.32567/hm.2024.2.7

Farkas Gábor[1]

SDR-adatfolyam feldolgozása korszerű módszerekkel

Modern Methods for Processing SDR Data Stream

Absztrakt

Napjainkban a félvezető technológia fejlettsége már lehetővé teszi, hogy SDR-ek segítségével rádiójeleket nagy sávszélességgel mintavételezzünk és rögzítsünk. Ennek számos előnye van, viszont a sávszélesség növekedésével a feldolgozandó adatmennyiség olyan mértékűre bővülhet, hogy azt hagyományos számítógéppel már nem lehet valós időben feldolgozni vagy letárolni. Így célszerűvé válik olyan programozható célhardverek alkalmazása, mint például az FPGA-k, amelyekkel a jelfeldolgozás hatékonysága jelentősen növelhető. Az ezekben az eszközökben rejlő lehetőségek kihasználásához mélyreható szakmai ismeretek szükségesek. Kutatásaim és tapasztalatom alapján nincs egységes módszer az FPGA-k témámhoz kapcsolódó funkcióinak kialakítására vonatkozóan, ezért szükségesnek látom, hogy a szakirodalom tanulmányozását követően olyan módszertant alakítsak ki, amellyel az FPGA-val történő nagy sebességű adatfogadást képesek lehetünk optimalizálni.

Kulcsszavak: SDR, FPGA, OSI-modell, jelfeldolgozás, gigabit Ethernet

Abstract

Today, the development of semiconductor technology makes it possible to receive and record radio signals with a high bandwidth using SDRs. This has many advantages, but as it grows, the amount of data to be processed can grow to such an extent that it can no longer be processed or stored in real time with a traditional computer. Thus, it becomes appropriate to use programmable target hardware such as FPGAs, which can be used to significantly

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: farkas.gabor.csp@gmail.com

increase the efficiency of signal processing. In order to take advantage of the potential of these tools, in-depth professional knowledge is required. According to my experience, there is no uniform method for developing the functions of FPGAs related to my topic. In this way, I see it as necessary, after studying the literature, to formulate a method that enables high-speed data reception with the FPGA in an optimal way.

Keywords: SDR, FPGA, OSI model, signal processing, gigabit Ethernet

Bevezetés

A szoftverrádiók (*software defined radio* – SDR) megjelenésével új perspektívák nyíltak a rádiókommunikációs eszközök területén. A modern, védelmi szféra számára fejlesztett rádió adó-vevők jellemzően SDR-alapon nyugszanak. A technológiával könnyebben megvalósíthatók olyan kommunikációs eljárások, mint például a kiterjesztett spektrumú vagy a frekvenciaugratásos jelátviteli módok, amelyeket lényegesen nehezebb zavarni vagy lehallgatni, így számottevő potenciált hordoznak a katonai felhasználás tekintetében.[2] Ezek az eszközök a NATO kognitív rádió fejlesztésére tett törekvései tekintetében is fontos szereplőnek számítanak, ahol szükséges a gyors hangolhatóság és a jelfeldolgozás rugalmas megvalósításának lehetősége.[3]

Számos SDR-típus érhető el, amelyek különféle frekvenciatartományokban működnek és más-más sávszélességgel rendelkeznek. Jellemzőjük, hogy USB- vagy Ethernet-csatlakozási lehetőséget biztosítanak az adatfolyam továbbításához. A drágább és jobb műszaki paraméterekkel rendelkezők általában az utóbbit használják. Ilyen például az Ettus Research által fejlesztett USRP N széria is, amelyet a MATLAB és a GNU Radio szoftverek egyaránt támogatnak.

1. ábra: Ettus Research USRP N200 szoftverrádió
Forrás: Ettus Research USRP N200 termékadatlap

[2] Haig et al. 2014: 74–75.
[3] Tang–Watson 2014: 3.

Az említett SDR-ek használatához egy számítógépre és egy azon futó szoftverre van szükség, amellyel a jelfeldolgozást, vizualizálást vagy rögzítést el tudjuk végezni. Az általam használt USRP N200 maximális mintavételi sebessége 50 MSps (*mega sample per second* – millió minta másodpercenként) 8 bites felbontás esetén.[4] Ebből jól látszik, ha mindössze egy csatornát veszünk figyelembe, és eltekintünk az átviteli protokoll miatt keletkező többletadattól, akkor is jelentős mennyiségű információt kell feldolgozni szoftver segítségével. Az átviteli rendszer minimális pufferelési lehetőséget biztosít, így a fogadó oldalon valós időben kell az adatokat kezelni a lehető legkisebb késleltetéssel, különben a csomagvesztés miatt a rögzíteni kívánt mintánk sérül.

Korábbi fejlesztési tapasztalataimra alapozva feltételezem, hogy a szoftveres adatfogadás sebességi korlátjaiból adódó problémákra bizonyos esetekben hatékony megoldást jelenthet egy FPGA-ra (*field programmable gate array* – programozható logikai hálózat) épülő jelfeldolgozó megoldás.

SDR-adatfolyam csatornakapacitási igénye

Az adatátvitelhez szükséges csatornakapacitást alapvetően a mintavételi sebesség, a felbontás és a csatornák száma határozza meg. Vegyük alapul a korábban említett USRP N200 típusú SDR-t, amely 1 Gbps Ethernet-csatlakozással rendelkezik az adatfolyam továbbítása érdekében. Jelen esetben csak a vételi adatáramlást vesszük figyelembe, mivel az adó irányba történő adatküldés független a vételi csatornától az Ethernet *full-duplex* jellege miatt. Az eszköz specifikációja szerint 50 MSps az átviteli kapacitás 8 bites felbontás mellett. 16 bites felbontás esetén 25 MSps-ra csökken ez az érték. Amennyiben összefoglaljuk a lehetséges kombinációkat a felbontás és a mintavételi sebesség tekintetében, jól látszik, hogy jelen esetben a korlátot az 1 Gbps-os Ethernet-csatlakozás jelenti. A mintavételezett jel eredménye 8 bites felbontás esetén két 8 bites értékből tevődik össze, mivel az IQ- (a komplex jel csatornái: képzetes és valós) formátumban továbbítódik. Ennek eredménye, hogy 8 bites mintavétel esetén 16 bit adatmennyiséggel kell számolnunk minden egyes minta esetén. A lehetséges mintavételi sebesség, felbontás és csatornaszám relációjában szükséges elméleti csatornakapacitás-igényt az 1. táblázat foglalja össze, amelyben zöld színnel jelöltem az 1Gbps Ethernet-csatlakozás által megvalósítható kombinációkat.

1. táblázat: Elméleti csatornakapacitás-igény a mintavételi sebesség, felbontás és csatornaszám függvényében

	8 bit, 1 csatorna	**16 bit, 1 csatorna**	**8 bit, 2 csatorna**	**16 bit, 2 csatorna**
25 MSps	400 Mbit/s	800 Mbit/s	800 Mbit/s	1600 Mbit/s
50 MSps	800 Mbit/s	1600 Mbit/s	1600 Mbit/s	3200 Mbit/s

Forrás: a szerző szerkesztése

[4] *USRP N200/N210 Networked Series* 2019.

Az adatátvitel megvalósításához szükséges információk miatt az elméleti átviteli sebesség ténylegesen soha nem érhető el. Az OSI (*open systems interconnection* – nyílt rendszerek összekapcsolása) modellt alapul véve megadhatók az adott réteg működéséből eredő konkrét veszteségek. A szóban forgó SDR UDP (*user datagram protocol* – felhasználói adatcsomag-protokoll) adatkapcsolatot valósít meg, amelynek adatrészébe VITA 49[5] szabvány szerinti protokollt ágyaz, amely előszeretettel alkalmazott ebben a szegmensben. Az eszköz nem támogatja a *Jumbo-frame* (óriás csomag) átvitelt, így a standard 1518 bájtos átviteli csomagmérettel kell számolni.

2. táblázat: Maximális átviteli csomagméret, veszteségek és az elérhető tényleges adatátviteli sebesség

Átviteli csomagméret – MTU (*maximum transmission unit* – maximális átviteli csomagméret)				**bájt**	**1518**
Veszteségek	Csomagközi szünet bájtban kifejezve (*inter-frame gap:* 96 ns@1 Gbps)		OSI level 2	bájt	12
	Ethernet-fejléc és CRC			bájt	18
	IP-fejléc		OSI level 3	bájt	20
	UDP-fejléc		OSI level 4	bájt	8
	VITA 49	Fejléc (ellenőrzés nélkül)	OSI level 5	bájt	4
Adat	**VITA 49**	Tényleges adat		bájt	1472
Ténylegesen elérhető adatátviteli sebesség				Mbit/sec	962

Forrás: a szerző szerkesztése

A csomagvesztés detektálása érdekében a VITA 49 protokollban lehetőség van egy számláló alkalmazására, amely minden egyes csomag kiküldését követően eggyel növekszik. Így a vevőoldali alkalmazásban detektálható, hogy mennyi csomag veszett el, feltéve, ha a kieső csomagok darabszáma nem nagyobb, mint a számláló körbefordulási értéke.
Amennyiben korszerű számítógéppel dolgozzuk fel az SDR-adatfolyamot, akkor az operációs rendszer vélhetően támogatja a munkánkat a hálózati adatforgalom gyors feldolgozása tekintetében. Ez igaz egészen az OSI 4 szintig, viszont a VITA 49 protokoll kibontását már nekünk kell valamilyen szoftveres módszerrel megoldani. Ezáltal ki vagyunk szolgáltatva az operációs rendszer feladat- és erőforrás-ütemezésének, amely egy közel 1 Gbps sebességű adatáramlás valós idejű megvalósításánál hamar problémát okoz. Példaként vegyük alapul, hogy a bejövő IQ-adatok demodulálásával amplitúdót számolunk az alábbi képlettel:

$$A = \sqrt{i^2 + q^2}$$

[5] *VITA Radio Transport Standard* 2018.

Amennyiben az USRP N200 szoftverrádió 50 MSps sebességgel mintavételez, az említett műveletet másodpercenként 50 millió alkalommal kell elvégezni. Önmagában már ez is jelentős erőforrást igénylő feladat, viszont a számítás elvégzését követően a kapott adatokkal még további műveleteket kell végezni, amelyek függenek az elérni kívánt céltól. Ilyen lehet például a vizualizáció vagy korrelációs függvények alkalmazása, amelyek további jelentős számítási kapacitásokat igényelnek.

További problémát okoz, hogy az átvitelre szolgáló hálózati kapcsolatban használt *flow-control* (adatáramlás-szabályozás) nem tud maradéktalanul megvalósulni. Feldolgozás során a vevőoldali hálózati eszköz egy úgynevezett *pause frame* (szünet kérése csomag) küldésével jelzi az adóoldalnak, hogy szüneteltesse a csomagok küldését. A jelen esetben alkalmazott 1 Gbps adatátviteli sebességnél a maximális szünet értéke 33,56 ms. Ebből következik, hogy az adóoldalnak, vagyis az USRP N200 készüléknek az ezen idő alatt keletkező mintát tudnia kell tárolni, mielőtt újrakezdi a csomagok továbbítását. Ez hozzávetőlegesen 4,2 MB adatot jelent. Az SDR-ben használt Xilinx Spartan 3A-DSP 1800 típusú FPGA belső BRAM (*block random access memory* – blokk tetszőleges hozzáférésű memória) memóriája használható fel az említett adatkumulálási feladatra. Ha feltételezzük, hogy ezt a memóriát kizárólag erre a célra használja fel, akkor az adatlapban megadott 1512 KB méretével jó közelítéssel egyharmadát tudja teljesíteni a szükséges áthidalásnak.[6] A rádiófrekvenciás jelek mintavételezése valós időben történik, így az említett bufferelési korlátból következik, hogy lesznek esetek, amikor csomagvesztés fog bekövetkezni. Bizonyos esetekben ez elfogadható, ugyanakkor például egy raszterező (monitorkép-visszaállító) alkalmazásnál a kieső adatok a kép szétesését okozzák.

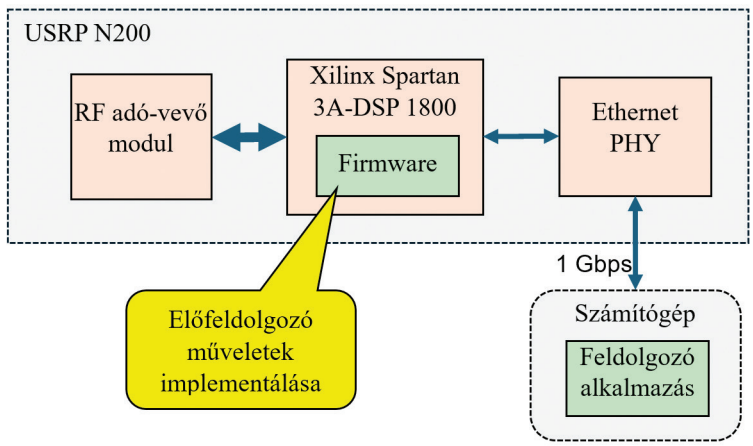
A fentiekből látható tehát, hogy a számítógéppel történő SDR-adatfolyam feldolgozása már viszonylag kis mintavételi sebesség esetén is problémát okozhat. Meg kell említenem, hogy a kereskedelmi forgalomban kapható *RFSoC 4x2* megnevezésű SDR-fejlesztőkártya vételi irányban, egyszerre négy csatornán, egyenként 5 GSps sebességgel képes mintavételezni.[7]

Nagy sebességű adatfeldolgozás FPGA segítségével

A felmerülő probléma leküzdése érdekében a számítógép irányába áramló adatok mennyiségét a lehető legkisebbre kell korlátozni. Amennyiben nem feltétlen szükséges számítógép használata – például látványos vizualizációs célokra –, úgy annak elhagyásával, célhardver segítségével valósítsuk meg a feldolgozást. Ebben nyújtanak segítséget az FPGA-eszközök, vagyis azok az integrált áramkörök, amelyek nagyszámú logikai kaput tartalmaznak, amelyek kapcsolatai kvázi szabadon programozhatók. Ilyen módon jól kézben tartható időzítésekkel és kiszámítható késleltetésekkel valósíthatjuk meg az adatok feldolgozását, teljes mértékben elkerülve a korábban vázolt adatvesztési jelenséget. Nem véletlenül találunk az USRP N200 SDR-ben is ilyen áramkört.

[6] *XA Spartan-3A DSP Automotive FPGA Family Data Sheet* 2011.
[7] *RFSoC 4x2 Overview.*

Egy lehetséges megoldás, hogy az SDR-ben lévő FPGA-konfigurációt *(firmware)* módosítjuk. Így nem szükséges további hardverelem, szoftveres megoldással kiegészíthetjük a meglévő eszközt olyan előfeldolgozási metódusokkal, amelyek redukálják a számítógép irányába továbbított adatmennyiséget. Például a korábban említett IQ-Amplitúdó demodulációt megvalósítva megfelezhetjük a szükséges csatornakapacitást. Hátulütője, hogy a meglévő eszköz hardveres adottságaihoz alkalmazkodnunk kell. Az alkalmazott Spartan 3A DSP (*digital signal processor* – digitális jelprocesszor) egy elavult széria, közel 20 évvel ezelőtt dobta piacra a gyártó. Számolnunk kell azzal, hogy az FPGA erőforrásainak jelentős részét lefoglalják az eredeti funkciók, így jelentősen korlátozottak a bővítési lehetőségek.



2. ábra: USRP N200 sematikus felépítése és az előfeldolgozó műveletek lehetséges implementálási helye
Forrás: a szerző szerkesztése

Egy másik megoldás, amely nagyobb mozgásteret enged, hogy az SDR-t érintetlenül hagyjuk, és egy külső FPGA-kártyával végezzük az előfeldolgozást, vagy akár a teljes folyamatot. Ez azért is előnyösebb, mert az SDR-ek konfigurációjának forráskódja nem minden esetben hozzáférhető, így előfordulhat, hogy a bővítéshez az eredeti funkciókat is le kellene programoznunk. Annak függvényében, hogy milyen bonyolultságú műveleteket kívánunk végezni, vagy milyen anyagi erőforrások állnak rendelkezésre, számos FPGA-típus közül választhatunk. Mivel az összeköttetéshez Ethernet-kapcsolatot használunk, így első körben az ehhez kapcsolódó paramétereket érdemes számításba venni. Vegyük alapul a Xilinx által gyártott FPGA-k nagy sebességű csatornáit, amelyeket fel lehet használni a kívánt célra.

3. táblázat: Xilinx FPGA-családok nagy sebességű csatornáinak maximális adatátviteli sebessége

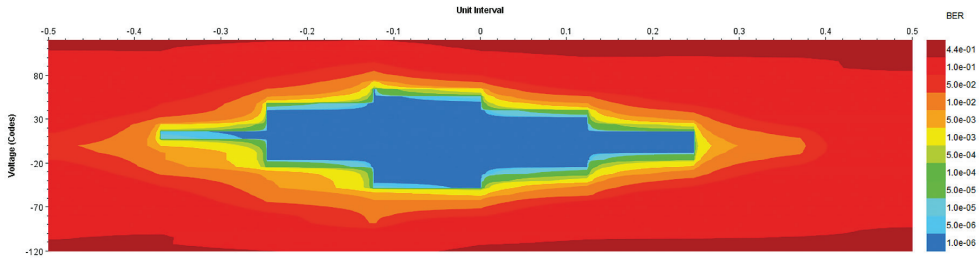
FPGA-család	Adó-vevő típus	Max. adatátviteli sebesség csatornánként (Gbps/csatorna)	Max. csatorna-szám	Max. adatátviteli sebesség eszközönként (Gbps/FPGA)
Vitrex UltraScale+	GTY/GTM	32,75/58,0	128/48	8384
Kintex Ultra-Scale+	GTY/GTM	16,3/32,75	44/32	3268
Vitrex UltraScale	GTH/GTY	16,3/30,5	60/60	5616
Kintex UltraScale	GTH/GTY	16,3	64	2086
Virtex 7	GTX/GTH/GTZ	12,5/13,1/28,05	56/96/16	2784
Kintex 7	GTX	12,5	32	800
Artix 7	GTP	6,6	16	211
Zynq UltraScale+	GTR/GTH/GTY	6/16,3/32,75	4/44/28	3268
Zynq 7000	GTX	12,5	16	400
Spartan 6	GTP	3,2	8	51

Forrás: a szerző szerkesztése a High Speed Serial alapján

Látható, hogy a felsorolt eszközök paraméterei jelentősen meghaladják a cikk írásakor hétköznapinak mondható számítógépekben elterjedt 1 Gbps sávszélességű hálózati csatolóképességet. Ez új perspektívákat nyit nagyobb mintavételi sebességet biztosító SDR-ek alkalmazásának irányába, mivel lehetőségünk nyílik a jelek gyorsabb feldolgozására.

Az Ethernet-kapcsolat létrehozásához az FPGA gyártója kínál előre elkészített konfigurációkat (IP Core), amelyek segítségével könnyen megvalósítható a feldolgozni kívánt adatok fogadása és továbbítása. Ezek magukba foglalják az OSI-réteg egyes és kettes szintjének kezelését is. A nagy sebességű adatkapcsolatnak a hardveres szempontoknak is meg kell felelni, így azok tesztelése javallott. Ehhez nyújt segítséget a Xilinx, hiszen a csatornák meghajtásához és bithiba rátájának meghatározásához elérhetővé teszi a szükséges konfigurációkat és szoftvereket (IBERT[8]).

[8] Integrated Bit Error Ratio Tester 7 Series GTX Transceivers v3.0 (2016).



3. ábra: A Xilinx IBERT-tesztelés után kapott 2D szemdiagramja, amely a csatorna fizikai jóságának megállapítására szolgál
Forrás: a szerző szerkesztése

Következtetések

Korábbi tapasztalataimra alapozva feltételeztem, hogy nagy mintavételi sebességű, SDR-ből származó adatfolyam feldolgozására hatékonyabb megoldást jelenthet egy FPGA-alapú rendszer, mint egy számítógépen futtatott szoftveres adatfeldolgozó. Az Ettus USRP N200 típusú SDR és az adattovábbításra használt Ethernet-csatorna elemzésével megállapítottam az adatvesztés lehetséges okait. Ezt követően javaslatot fogalmaztam meg, miszerint a probléma elkerülése érdekében érdemes célhardvert alkalmazni, hogy az időzítések és késleltetések kézben tarthatók legyenek, és az átviteli rendszer ne függjön a számítógépen futó operációs rendszer sajátosságaitól.

Két lehetséges megoldást vettem górcső alá, ami után megállapítottam, hogy az SDR-hez csatlakoztatott FPGA-kártya jelentheti az optimális megoldást, amelyek közül az aktuális feladatnak megfelelő ár/érték arányút választhatjuk a gyártók kínálatából. Ezen túlmenően, megvalósíthatunk olyan funkciókat is a kártyák segítségével, amelyek teljes egészében kiválthatják a végső feldolgozást vagy elemzést végző számítógépet. Ilyen lehet például AI- (*artificial intelligence* – mesterséges intelligencia) modell futtatása FPGA-n, amely jelentős perspektívákat rejt a SIGINT (*signal intelligence* – rádióelektronikai felderítés) területén is, biztosítva az eredmények gyors rendelkezésre állását.[9]

Felhasznált irodalom

Ettus Research USRP N200 termékadatlap. Online: www.ettus.com/all-products/un200-kit/

Haig Zsolt et al. (2014): *Elektronikai hadviselés*. Budapest: Nemzeti Közszolgálati Egyetem. Online: https://opac.uni-nke.hu/webview?infile=&sobj=9276&source=webvd&cgimime=application%2Fpdf%0D%0A

[9] Németh–Virágh 2023: 3.

High Speed Serial – Adaptive Computing Solutions Deliver the Highest Bandwidth, Superior Auto-Adaptive Equalization, and Industry-Leading Productivity Tools. Online: www.xilinx.com/products/technology/high-speed-serial.html#overview

Integrated Bit Error Ratio Tester 7 Series GTX Transceivers v3.0 (2016). Online: https://docs.amd.com/v/u/en-US/pg132-ibert-7series-gtx

Németh András – Virágh Krisztián (2023): Mesterséges intelligencia és haderő – További katonai alkalmazási lehetőségek VIII. rész. *Haditechnika,* 57(2), 2–5. Online: https://doi.org/10.23713/HT.57.2.01

RFSoC 4x2 Overview. Online: www.rfsoc-pynq.io/rfsoc_4x2_overview.html

Tang, Helen – Watson, Susan (2014): *Cognitive Radio Networks for Tactical Wireless Communications.* Kanada: Defence Research and Development. Online: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc198/p801238_A1b.pdf

USRP N200/N210 Networked Series (2019). Online: www.ettus.com/wp-content/uploads/2019/01/07495_Ettus_N200-210_DS_Flyer_HR_1.pdf

VITA Radio Transport Standard (ANSI/VITA 49) IF Data Packet Format (2018). Online: www.redrapids.com/images/whitepapers/TWP-000-001-R00.pdf

XA Spartan-3A DSP Automotive FPGA Family Data Sheet (2011). Online: https://docs.amd.com/v/u/en-US/ds705

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 2. szám 97–106.
DOI: 10.32567/hm.2024.2.8

Fazekas Gábor[1]

Oldalsávi információszivárgás mint valós fenyegetettség

Side-Channel Attack is a Real Threat

Absztrakt

Korunk védelmi iparának egyik kulcsfeladatköre az információbiztonság, amelynek emberi és technikai függései rendkívül sokrétűek. A vállalati és kormányzati szervek informatikai rendszerei folyamatos felügyeletet, fejlesztést és auditot igényelnek, amelyek kiterjednek az emberi munkaerőre is. Ennek egyik oka, hogy a mobil és egyéb szórakoztató elektronikai eszközök iránt a piaci kereslet már évekkel a koronavírus megjelenése előtt hatással volt az ipari ellátási láncokra, kezdve az elektronikai alkatrészek gyártásától a telekommunikációs protokollokon és a mesterséges intelligencián keresztül a fejlesztési módszertanokig. Ez az ipar folyamatos átalakulásához vezetett, ami maga után vonta az elektronikai eszközök fejlesztési idejének lerövidülését is. Végeredményképp olyan minőségű hardver-, szoftver- és módszertani eszközök váltak széles körben elérhetővé a civil lakosság számára, amelyek valós sebezhetőséggé emeltek egy addig mítoszként kezelt jelenséget. Kutatásomban a kisugárzásvédelem egy szegmensét, a passzív elektromágneses információszivárgást, illetve fenyegetettsége növekvő hatását és okait mutatom be. Kutatásom célja egy innovációs tevékenység során előállított saját fejlesztésű eszköz megvalósításán keresztül szemléltetni, hogy a civil lakosság által is hozzáférhető és megfizethető COTS (commercial off the shelf – kereskedelmi forgalomban elérhető) eszközök, szoftverek és a korszerű modellalapú fejlesztési gyakorlat segítségével mára valós fenyegetettséggé vált az elmúlt évtizedek során kizárólag az állami szereplők által alkalmazott megfigyelési technika.

Kulcsszavak: EMSEC, információbiztonság, MBD, SDR, TEMPEST

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: fazekg@gmail.com

Abstract

One of the key tasks of the defence industry of our time is information security, of which human and machine dependencies are extremely diverse. The IT systems of companies or government agencies require continuous supervision, development and audits, which also extend to the human resource. One of the reasons for this is that the market demand for mobile and other entertainment electronic devices subvert the industrial balance of power years before the emergence of the coronavirus, starting from the production of electronic components, through telecommunication protocols and artificial intelligence to development methodologies. This led to a continuous transformation of the industry, which entailed the shortening of the development time of electronic devices. As a result, high-quality hardware, software and methodological tools became widely available to the civilian population, which raised a phenomenon that had been treated as a myth to a real vulnerability. In my work, I present a segment of emission security, the leakage of passive electromagnetic information, and the growing trend and causes of the threat. The purpose of this publication is to illustrate through my own R&D, that with the help of COTS (Commercial Off the Shelf) devices, software and modern model-based development practices that are accessible and affordable to the civilian population, the observation techniques used exclusively by professional services in the 1950s, has now become a real threat.

Keywords: EMSEC, information security, MBD, SDR, TEMPEST

Bevezetés

Korunk társadalmában az információvédelem kiemelt fontosságú terület. Az információszivárgás témakörében a legritkább esetben említik az oldalsávi támadásokat *(side channel attack)*, vagyis a TEMPEST-et, amely napjainkra a civil szférát is érintő fenyegetettséggé vált. Az oldalsávi támadások olyan módszerek, amelyek fókuszában nem közvetlenül az információs csatorna áll, hanem az egyes informatikai rendszerek működéséből adódó egyéb fizikai jelenségek, például elektromágneses sugárzás, mechanikai rezgések vagy hőmérséklet-változás. Ezen jelenségek specifikus szenzorokkal detektálhatók és rögzíthetők, digitális jelfeldolgozási eljárásokkal pedig ezen csatornákon érzékeny adatokat nyerhetünk ki a célrendszerekből.

A vezeték nélküli telekommunikációs eszközök iránti piaci igény az ipart a nagy integráltságú, jó minőségű és tömeggyártott rádiófrekvenciás eszközök kutatása és fejlesztése felé terelte. Ennek, illetve a hatékony fejlesztést elősegítő MBD (*model based design* – modellalapú fejlesztés) módszertannak köszönhetően a polgári területeken is lehetséges az elektronikai eszközök elektromágneses felderítése és megfigyelése.

Kutatásom céljául tűztem ki, hogy polgári felhasználású komponensekből előállítsak egy olyan kísérleti eszközt, amely képes lehet LCD-monitorok oldalsávi elektromágneses sugárzásából származó információ, vagyis a megjelenített kép rekonstrukciójára. Ezzel rá szeretnék világítani a polgári lakosság esetleges fenyegetettségére, illetve a hazai TEMPEST-megfelelőségi kritériumok kidolgozásának fontosságára.

Az oldalsávi információszivárgás

Egy 1972-ben az amerikai Nemzetbiztonsági Szolgálat (NSA – National Security Agency) által írt, 2007-ben a titkosítás alól részben feloldott jelentés több, a témát érintő eseményről számol be. Az egyik ilyen eset a második világháború alatt történt a 131-b2 távíró rejtjelező géppel kapcsolatban, amelyet a Bell Laboratórium fejlesztett ki az Amerikai Egyesült Államok hadserege híradó csapatainak (USASC – United States Army Signal Corps) részére. Az eszköz már rendszeresítve volt a hadseregben, amikor egy Bell-mérnök észlelte, hogy a rejtjelező gép üzemszerű működésének indulásakor a laboratórium egy távoli részén található oszcilloszkóp kijelzőjén zavarok jelennek meg. A jelenséget vizsgálva kiderült, hogy a kilengések mértéke a rejtjelezendő üzenettől függően változik, tehát azok bizonyos mértékig visszafejthetők. Mivel az esetet a Bell biztonsági hiányosságként értékelte, tájékoztatták róla a híradó szervezeteket. A választ szintén tartalmazza a jelentés: „Nem veszed észre, hogy háború van? Egy kétes és ezoterikus laboratóriumi jelenségre alapozva nem állíthatjuk meg kriptográfiai műveleteinket. Ha ez valóban veszélyes, bizonyítsd be." Ennek megfelelően a Bell munkatársai elutaztak New Yorkba és a USASC rejtjelközpontjával szemben (Varick st.), attól 80 láb (24,4 m) távolságra települtek ki. Egy óra mérés alatt az üzenetek 75%-át sikerült visszafejteniük. Az esetet követően a hadsereg lefektetett néhány információvédelmi alapelvet a védelmi távolság, elektronikus árnyékolás és a zavarás tekintetében.[2]

Bár a háború rövidesen véget ért, a projekt bizonyosan tovább élt a hidegháborús környezetben. Az elektronikus adatfeldolgozó rendszerek kompromittáló kisugárzásának analízise tehát nagyságrendileg a második világháború óta képezi az információvédelem részét. Az 1980-as évek közepéig mértékadó publikus információ nem látott napvilágot e témában. Ezen változtatott Wim Van Eck holland számítógépmérnök 1985-ben megjelent cikke, amelyben a szerző egy CRT (*cathode ray tube* – katódsugárcső) monitor oldalsávi elektromágneses kisugárzását kihasználva rekonstruálta a monitoron megjelenő képet.[3] Markus Kuhn és társai több cikkben vizsgálták különböző eszközök elektromágneses kisugárzását mint biztonsági sebezhetőséget, majd 1998-tól Kuhn több cikket is publikált a monitorok lehallgathatóságáról.[4] Az eddigiek alapján kijelenthetjük, hogy az elektronikus eszközök hordoznak egyfajta lehallgathatósági rizikófaktort,[5] amelyet a besorolási szinthez mérten kell kezelni. Több terminológia is született a terület és a kapcsolódó eszközök vonatkozásában, úgymint: EMSEC (*emission security* – kisugárzásbiztonság), TEMPEST, illetve oldalsávi információszivárgás. Fontos megjegyezni, hogy jelen munka kizárólag az elektromágneses kisugárzással kapcsolatos, bár a jelenség nem csupán a nem szándékosan előállított elektromágneses hullámok detektálását érinti, hanem a hang-, optikai és egyéb kommunikációs tartományokat is.

[2] NSA 1972: 27.
[3] Eck 1985.
[4] Kuhn–Anderson 1998; Kuhn 2005.
[5] Kuhn 2003.

A TEMPEST magyarországi szabályozása

Magyarország TEMPEST-hatósága a Nemzeti Biztonsági Felügyelet (NBF), amely honlapján a következő definíciót használja:

„Minden elektromos eszköz bocsát ki magából elektromágneses jeleket. Ez a fizikai jelenség lehetővé teszi, hogy megfelelő eszközök alkalmazásával a kisugárzott jelekből reprodukálható legyen az eszközön kezelt eredeti adat. Minősített adat elektronikus úton történő kezelése esetén a kompromittálódás elleni fő feladat a minősített adatot tartalmazó kisugárzás minimális szintre történő csökkentése, ami megakadályozza az adat reprodukálhatóságát, annak illetéktelen kezekbe jutását. E módszer és a rá vonatkozó szabályok összefoglaló neve a TEMPEST."[6]

Magyarországon erre vonatkozó nyílt utalás mindössze a 41/2015. (VII. 15.) BM rendelet 3. mellékletének 3.3.10.14.4 Antennák alfejezetében található: „Az érintett szervezet olyan karakterisztikájú és teljesítményszintű antennákat és árnyékolási megoldásokat üzemeltet, vagy egyéb technikákat alkalmaz, amelyekkel csökkenti az érintett szervezet fizikai védelmi határain kívül a jelek észlelésének a valószínűségét."[7]

Az ezredfordulót követően a kisugárzásvédelmi témakörben folyamatosan növekvő kutatás-fejlesztési aktivitást óvatos kormányzati alkalmazkodás kíséri.[8] Erre a jelenségre a lehetséges magyarázatot a technológiai és a kutatás-fejlesztési tevékenységek módszertani fejlődésében kell keresnünk.

A fejlesztőkörnyezet

Az ezredfordulóig a széles sávú rádióvételnek jelentős költségvonzata volt. A mobilkommunikáció globális elterjedése és folyamatos fejlődése az egyre növekvő integráltságú rádiómodulok fejlesztését, gyártását vonta maga után. Az SDR-ek (*software defined radio* – szoftverrádió) (1. ábra) megjelenésével átalakultak a fejlesztői diszciplínák: a szoftveres alapsávi moduláció lehetősége közel hozta egymáshoz az informatikát és a rádiótechnikát.

Egy SDR kimenetéről érkező több MSps (*mega sample per second* – millió minta per másodperc) sebességű jelfolyam feldolgozása egy hagyományos PC-t (*personal computer* – személyi számítógép) használva valós időben nem megoldható. Bár az FPGA-k (*field programmable gate array* – programozható logikai hálózat) órajel-frekvenciájukat illetően elmaradnak a személyi számítógépekétől, azonban felhasználásukkal valódi párhuzamos művelet-végrehajtást érhetünk el, ezzel lehetővé téve a valós idejű jelfeldolgozást. A véges impulzusválaszú vagy FIR- *(finite impulse response)* szűrők neurális hálózatokon vagy egyéb nemlineáris dinamikus rendszereken alapuló adaptív szűrők. Ezek összességében egyszerű logikai alapelemekből felépíthető rendszerek,

[6] NBF.

[7] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

[8] Kuris 2010: 182–183.

amelyek esetében az FPGA egy ideális feldolgozóegység, mivel segítségével valós időben több, egyszerű művelet egyidejűleg hajtható végre. Ez a képesség szoftverrádiók alapsávi IQ- (a komplex jel csatornái: képzetes és valós) jeleinek kezelése során elengedhetetlen, ezért a valós idejű, széles sávú modulációs/demodulációs sémák alkalmazására és szűrésére jelenleg az FPGA optimális megoldást kínál.

1. ábra: LimeSDR szoftverrádió
Forrás: a szerző felvétele

Kutatásom során az egyszerű beszerezhetőség és az elérhető ár miatt az RTL-SDR szoftverrádiót használtam. Ezen eszközt eredeti rendeltetése szerint földfelszíni televízióműsor vételére fejlesztették, azonban alacsony ára miatt széles körben elterjedt a rádióamatőrök közrében is. Lényeges tulajdonságai:

- az alapsávi IQ-jelet USB-n keresztül továbbítja a számítógépnek;
- vételi frekvenciatartománya 100 kHz-től 1,7 GHz-ig terjed;
- maximális sávszélessége verziótól függően 1–3 MHz között van.

Népszerűsége miatt az eszközt számtalan rádiószoftver támogatja, mint például a GQRX, az SDRCube és a DAB Player. Ezen programok jellemzően kereskedelmi rádió- és televízióadások demodulációjára alkalmasak, ugyanakkor elérhetők olyan fejlesztői lehetőséget biztosító programok is, amelyek alkalmasak akár saját modulációs/demodulációs technológiák létrehozására, implementálására. Ilyenek például a GNURadio vagy a MATLAB.

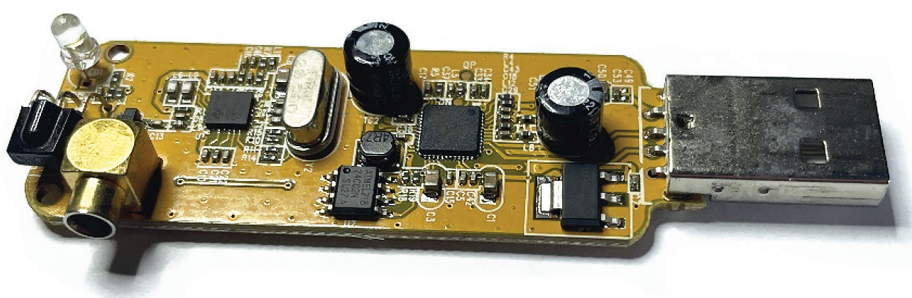
Felderíthetőség megállapítása

Jelenleg a NATO SDIP-27/2 szabványa rendelkezik az elektronikai eszközök kisugárzással szembeni védettségi szintjének megállapításáról az alábbiak szerint:[9]

- NATO SDIP-27 Level A – USA NSTISSAM Level I,
- NATO SDIP-27 Level B – USA NSTISSAM Level II,
- NATO SDIP-27 Level C – USA NSTISSAM Level III.

Az információszivárgással kapcsolatos határértékek, illetve mérési körülmények minősítettek, így számomra csupán relatív mérések elvégzésére nyílt lehetőség, amelyhez az eredeti kép közeltéri visszaállíthatóságának mértékével arányos saját kritériumokat állítottam fel. Bár a visszaállított kép felbontása arányos a vételi oldal sávszélességével, így a rádió sávszélességének növelésével a lehallgatott kép minősége is javul,[10] a visszaállított kép kontrasztossága kis sávszélességgel is biztosítható.

Jelen vizsgálat tárgya, hogy valóban jelenthet-e veszélyforrást a néhány ezer forintért beszerezhető RTL szoftverrádió (2. ábra).

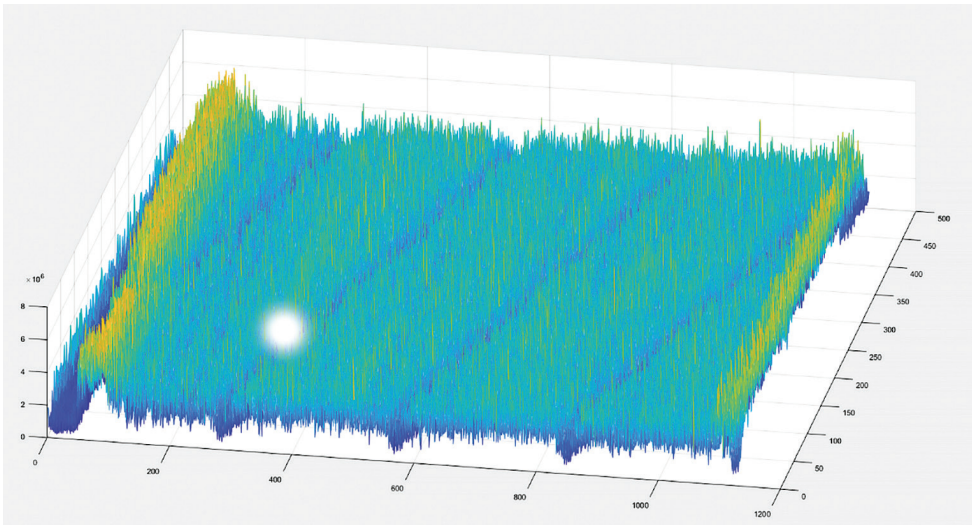


2. ábra: Pendrive méretű RTL-SDR szoftverrádió
Forrás: a szerző felvétele

Bár az eszköz sávszélessége kicsi, a modellalapú fejlesztési technikák alkalmazásával és saját demodulációs technika kifejlesztésével sikeresen detektáltam egy LCD-monitor szinkronjeleit (3. ábra).

A szoftverrádió mágnestalpas vevőantennáját ebben az esetben a vizsgált monitor közvetlen közelében helyeztem el, és a jelfeldolgozás offline volt, vagyis azt a szoftverrádió nyers alapsávi IQ-jeleinek rögzítése után, nem valós időben, MATLAB-bal végeztem. A mérés során több vivőfrekvencián mintavételeztem, majd ezeket az általam implementált raszterezésre is képes demodulátor-algoritmussal jelenítettem meg. Miután egyes frekvenciákon láthatóvá váltak a szinkronjelek, néhány MHz eltolással újabb jelrögzítést hajtottam végre. Ez hatásos stratégiának bizonyult a kompromittáló jelek felderítésében.

[9] Shopina 2020.
[10] Marinov 2014.



3. ábra: Monitor kisugárzásából visszaállított PAL szinkronjelek
Forrás: a szerző szerkesztése

A felderítés és képvisszaállítás hatékonyságának fokozásához a rendszer valós idejű jelfeldolgozási képességének kialakítása vált szükségessé. Mivel az RTL-SDR kis sávszélességű, egy személyi számítógép is elegendő a valós idejű jelek feldolgozására. A valós idejű mintavételezés és feldolgozás során a demoduláció módosításával, rádióspecifikus finomhangolással, illetve valós idejű feldolgozással elértem az eszköz képességeiből adódó határokat a hardver vonatkozásában (4. ábra), amely a rádió maximális mintavételi frekvenciájából adódó felbontási korlát volt.

4. ábra: Bal oldalon egy monitoron látható tesztkép, jobb oldalon az RTL-SDR szoftverrádióval visszaállított kép
Forrás: a szerző felvételei

A valós idejű feldolgozás egyik eredménye a nem szándékosan kisugárzott monitorkép felderítésével kapcsolatos folyamatok kialakítása. Bár jelenleg nem automatizált a módszer, mégis leírható folyamatok mentén, aminek szerves része a szinkronjelek időtartományban történő vizsgálata, illetve azok korrelációjának megjelenítése. Ezzel a módszerrel egy folyamatos, az RTL-SDR teljes vételi tartományában végrehajtott szkenneléssel felderíthetők a kompromittáló frekvenciák.

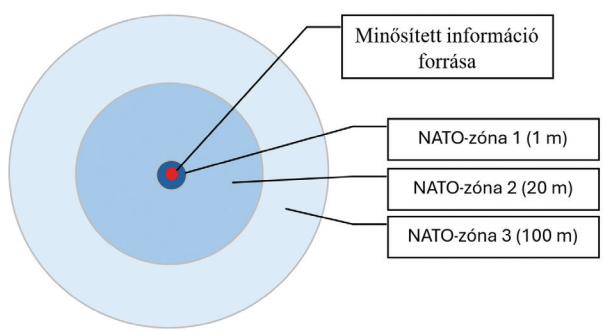
Másik eredményem a szoftverrádió korlátjainak meghatározása a visszaállított kép minőségének vonatkozásában. A közeg, a környezet és az eszközök jellegéből adódóan egy folyamatos, természetéből adódóan változó intenzitású zaj van jelen a visszaállított képen. Mivel ezen zavaró frekvenciák pixelszinten véletlenszerűen jelentkeznek, egyszerű átlagolással kiszűrhetők, ezzel jelentősen javítva a visszaállított kép minőségét. Jelen kutatás során a képek átlagolásán túl nem alkalmaztam a képminőség javítását célzó egyéb jelfeldolgozási eljárást. Bár az átlagolás hatékony megoldás, a visszaállított kép horizontális és vertikális futását a rádió feszültségvezérelt oszcillátorának hőmérsékleti stabilitása határozza meg. Az RTL-SDR esetében ezen alkatrész stabilitása csupán néhány képkockányi átlagolást tesz lehetővé. A folyamatos csúszásából eredendően a hosszabb átlagolások miatt elmosódottá válik a visszaállított kép.

A képminőség javítására további lehetőség a több vivőfrekvencián demodulált információ súlyozott összegzése,[11] illetve szoftveres jel- és képfeldolgozó algoritmusok, gépi tanulásos módszerek alkalmazása.

Felderíthetőség elleni védekezés

Védelem vonatkozásában a passzív TEMPEST-támadással szemben a minősítésnek megfelelő védőtávolság, illetve a körültekintő elektronikai tervezés jelenthet megoldást.

Ezeket az alapelveket már a második világháború végén is alkalmazták az USA híradó szervezetei, akkor a védőtávolságot 100, majd később 200 lábban határozták meg. Jelenleg Magyarországon a NATO SDIP-27 szerint szükséges a minősítésnek megfelelő zónákat meghatározni (5. ábra).[12]



5. ábra: Objektumon belüli védőtávolságok
Forrás: a szerző szerkesztése* SHOPINA *2020: 985 alapján

[11] KITAZAWA et al. 2022.
[12] SHOPINA 2020.

A védőzónák meghatározásán túl a veszélyeztetett eszköz gondos elektronikai tervezése jelenti az első védvonalat. Tervezéskor az EMC (*electromagnetic compliance* – elektromágneses megfelelőség) irányelveket érdemes szem előtt tartani, mivel a TEMPEST esetében is beszélhetünk kisugárzott, illetve a táp-, valamint vezetékes kommunikációs, illetve földelési vonalakon megjelenő nem kívánt információtartalomról. Fontos megjegyezni, hogy bár az elektromágneses vonatkozásban az EMC és a TEMPEST lényegüket tekintve azonosnak tűnhetnek, a két megfelelőség eltérő direktívák mentén működik.[13]

Az EMC kizárólag energiaszintekkel foglalkozik, a TEMPEST esetében viszont a kisugárzás információtartalmán van a hangsúly. Tehát ha van egy nagyintenzitású jelünk, ami miatt eszközünk nem teljesíti az EMC-megfelelőséget, ugyanakkor erre a nagyintenzitású jelre nincs érzékeny információt hordozó jel modulálva, a TEMPEST-megfelelőség teljesülhet az adott eszköz vonatkozásában. Másik esetet vizsgálva azonban, ha egy zavarjel megfelel az EMC-kritériumoknak, ugyanakkor intenzitása a TEMPEST-határvonalat túllépi, és védett információt tartalmaz, értelemszerűen beavatkozást tesz szükségessé a kiszivárgott jel intenzitásának csökkentése érdekében.

Ezen a ponton nem mindig jelentenek közvetlen megoldást az EMC-problémákkal kapcsolatos zajcsillapítási technikák. Jó példa erre az árnyékolás, amely bár hatékony az elektromágneses kisugárzások csillapításában, az árnyékolás kialakításának jellege, a tápellátás és egyéb áramköri megoldások, mint például az eszközök ESD- (*electrostatic discharge* – elektrosztatikus kisülés) védelme átalakíthatja a szivárgási csatornát kisugárzottról a vezetettre, amely elektronikai szempontból nehezebben kezelhető.[14]

Összegzés

Az információvédelem rendkívül szerteágazó terület, ahol a hatékonyság alapfeltétele a folyamatos kutatás és fejlesztés, hiszen az újabb technológiák hatékony kihasználásához megfelelő technikai megoldások is szükségesek. Kutatásom célja az volt, hogy bemutassam, a kereskedelmi forgalomban jelenleg bárki számára elérhető technológiák és technikai eszközök hatékony alkalmazásával belátható időtávon és költségvetéssel képessé válhatunk olyan minőségű berendezést előállítani, amely akár az oldalsávi elektromágneses kisugárzásból információ felderítésére és visszaállítására is alkalmas lehet. Éppen ezért tartom különösen fontosnak, hogy azokat az eljárásokat és irányelveket, amelyek mentén az eszközgyártók és az alkalmazók hatékonyan védekezhetnek az ilyen felderítési és lehallgatási eljárásokkal szemben, a lehető legkomolyabban vegyük figyelembe. Emellett rendkívül fontosnak tartom az ide vonatkozó jogszabályok frissítését, hazai TEMPEST-megfelelőségi kritériumok kidolgozását, illetve a polgári lakosság jövőbeni érintettségének vizsgálatát.

[13] Kinugawa–Fujimoto–Hajashi 2019.
[14] Pennesi–Sebastani 2005: 777–778.

Felhasznált irodalom

Eck, Wim Van (1985): Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk. *Computers & Security,* 4(4), 269–286. Online: https://doi.org/10.1016/0167-4048(85)90046-X

Kinugawa, Masahiro – Fujimoto, Daisuke – Hayashi, Yuichi (2019): Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure. *IACR Transactions on Cryptographic Hardware and Embedded Systems,* 2019(4), 62–90. Online: https://doi.org/10.46586/tches.v2019.i4.62-90

Kitazawa, Taiki et al. (2022): *TEMPEST Attack Against High-Resolution Displays Using Differences in the Transfer Function of EM Waves.* 2022 3rd URSI Atlantic and Asia Pacific Radio Science Meeting (AT-AP-RASC), Gran Canaria, Spain, 1–4. Online: https://doi.org/10.23919/AT-AP-RASC54737.2022.9814293

Kuhn, Markus G. (2003): *Compromising Emanations: Eavesdropping Risks of Computer Displays.* Technical Report 577. Cambridge: University of Cambridge. Online: www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf

Kuhn, Markus G. (2005): Electromagnetic Eavesdropping Risks of Flat-Panel Displays. In Martin, D. – Serjantov, A. (szerk.): *Privacy Enhancing Technologies.* PET 2004. Lecture Notes in Computer Science, 3424. Berlin–Heidelberg: Springer, 88–107. Online: https://doi.org/10.1007/11423409_7

Kuhn, Markus G. – Anderson, Ross J. (1998): Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. In Aucsmith, David (szerk.): *Information Hiding*. Lecture Notes in Computer Science, 1525. Berlin–Heidelberg: Springer, 124–142. Online: https://doi.org/10.1007/3-540-49380-8_10

Kuris Zoltán (2010): A komplex információvédelem új irányai a nemzeti minősített adatok védelmével összefüggésben. *Hadmérnök,* 5(4), 182–200. Online: https://real.mtak.hu/40796/

Marinov, Martin (2014): *Remote Video Eavesdropping Using a Software-Defined Radio Platform.* Cambridge: University of Cambridge.

National Security Agency (NSA) titkosítás alól feloldott *Tempest: A signal problem* című anyaga (1972). Online: www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf

Nemzeti Biztonsági Felügyelet (NBF): *TEMPEST*. Online: www.nbf.hu/hasznos-informaciok/tempest/

Pennesi S. – Sebastiani S. (2005): *Information Security and Emissions Control.* 2005 International Symposium on Electromagnetic Compatibility, Chicago, IL, USA, 777–781. Vol. 3. Online: https://doi.org/10.1109/ISEMC.2005.1513629

Shopina, Iryna et al. (2020): Cybersecurity: Legal and Organizational Support in Leading Countries, NATO and EU Standards. *Journal of Security and Sustainability,* 9, 977–992. Online: https://doi.org/10.9770/jssi.2020.9.3(22)

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 2. szám 107–121.
DOI: 10.32567/hm.2024.2.9

Gábor Horváth[1]

No Drone's Sky: Full Spectrum Drone Surveillance and Neutralisation Concept for Enhanced Counter-UAS Framework

(Part 2, Neutralisation)

Abstract

We are living in an era that is marked by the exponential growth of small Unmanned Aircraft Systems (sUAS), therefore the imperative for effective countermeasures against potential threats to public safety, national security, and individual privacy inherent in these airborne apparatuses has become increasingly pronounced. Following the foundational exploration of UAS surveillance in the first segment of the Counter-UAS (C-UAS) series, this second instalment shifts its gaze to the pivotal domain of drone neutralisation techniques. Investigating both soft and hard neutralisation methodologies, this study aims to unravel the intricate landscape of strategies devised to legally and securely incapacitate, disrupt, or assume control over sUAS threats. Drawing from a rich tapestry of existing literature and recent research endeavours, this paper embarks on an expedition through a spectrum of neutralisation approaches subjecting the aforementioned methodologies to rigorous scrutiny regarding their efficacy and other implications, in order to contribute substantively to the development of a resilient C-UAS framework. Moreover, this study lays the groundwork for the third part of this C-UAS series, where the author shall unfurl a vision of operation. Besides elucidating the challenges and opportunities inherent in the neutralisation of small drone threats, this study also aims to catalyse collaboration within the research community, dedicated to ensuring the secure coexistence within the airspace system.

Keywords: anti-drone, counter-UAS, drone sensing, drone neutralisation, drone surveillance

[1] Senior ATM Officer, Ministry of Defence, State Aviation Department, e-mail: horvath.gabor@uni-nke.hu

Introduction

The utilisation of small Unmanned Aircraft Systems (sUAS) is increasingly prevalent across a spectrum of malicious applications.[2] The escalating proliferation of these systems demands a re-evaluation of security measures for facilities in the foreseeable future. Traditional security protocols are anticipated to be inadequate due to the distinctive attributes of this emerging technology, facilitating swift circumvention of existing widespread systems and procedures.[3]

Consequently, numerous private, corporate and public entities find themselves inadequately equipped to mitigate threats posed by sUAS.[4] This paper categorises these threats as either *adversarial* or *unauthorised* based upon the operator's intentions, level of expertise, and the drone's operability. Both categories fall under the set of potentially harmful drone operations (Figure 1), which are defined below:

- *Adversarial sUAS (asUAS) threat* refers to the intentional and hostile use of small drones by individuals, groups, or entities with malicious intent. These threats may encompass activities such as surveillance, reconnaissance, sabotage, or direct attacks against targets of interest. Adversarial sUAS operators possess the necessary knowledge and expertise to deploy sUAS in a manner that poses risks to safety, security, and/or privacy, thereby constituting a deliberate threat to individuals, organisations, and/or critical infrastructure.
- *Unauthorised sUAS (usUAS) threat* involves the unlawful, malfunctioning, or illegal operation of small drones in violation of regulatory requirements, airspace restrictions, or established laws. These threats can arise from individuals or entities operating sUAS without proper certification, permits, or permissions, thereby posing risks to aviation safety, public security, or privacy. These activities include unauthorised, but not necessarily intended, flights in restricted airspace, interference with manned aircraft operations, and/or violations of privacy rights through unauthorised surveillance and/or data collection.

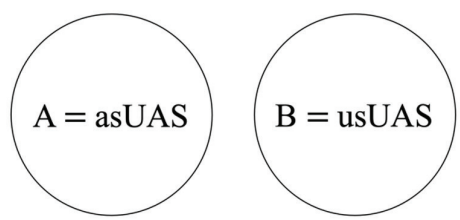


Figure 1: Presentation of potentially harmful drone operation sets
Source: compiled by the author

[2] Krajnc 2018.
[3] Jahangir–White 2021.
[4] Cline 2020.

The definitions given above play a crucial role within the confines of this study, as determining the appropriate intervention level of Counter-Unmanned Aircraft System (C-UAS) necessitates precise assessment of the extent of the small drone-induced threat. Therefore, the following sections introduce soft and hard mitigation techniques deemed most promising, then subsequently a mathematical formalisation of threat level determination is outlined, and finally conclusions are drawn to encapsulate the key findings.

Neutralisation methods

Neutralisation methods (NM) are triggered in order to counteract the threat posed by potentially harmful drone operations.[5] It is possible to activate multiple NMs simultaneously to enhance the efficiency of mitigation tactics. Additionally, these NMs may be situated on one or more distinct platforms, depending on the physical architecture of the Counter-Unmanned Aircraft System. During neutralisation C-UAS can execute the following actions:[6]

- controlling
- interrupting
- disabling
- destructing

These actions are facilitated through NMs, herein referred to as neutralisers, which have been categorised differently in different literatures,[7] but considering the aspects of set theory, the most scientifically founded solution might be the distinction between soft and hard neutralisation methods.

Soft neutralisation

Soft neutralisation (SN), within the context of C-UAS, denotes a particular approach wherein the neutralisation of a potentially harmful drone operation is achieved through methods that do not involve critical physical impact or destruction upon the targeted drone.[8] Instead, SN techniques focus on the disruption, interruption, or complete takeover of the drone's operation, effectively rendering it incapable of fulfilling its intended or unintended harmful mission. Soft neutralisation tactics are characterised by their emphasis on achieving operational success through subtle, non-destructive interventions, thereby minimising collateral damage, and preserving the integrity of the airspace environment. This multifaceted approach requires a comprehensive understanding of the target drone's capabilities, vulnerabilities, and operational context, as well as the development and deployment of sophisticated

[5] Csengeri 2019.
[6] Castrillo et al. 2022.
[7] Sander et al. 2018; Martins et al. 2020.
[8] Da Silva et al. 2023.

countermeasures tailored to neutralise its functionality while minimising the risk of unintended consequences. SNs encompass a diverse array of primarily non-kinetic means, including but not limited to electronic warfare techniques and cyber operations such as signal jamming, spoofing, hacking, while deploying countermeasures aimed at exploiting vulnerabilities in the drone's communication, navigation, or control systems.[9] Table 1 presents a comparative analysis of the key differences between various SN methods.

Table 1: Pros-cons comparison of UAS soft neutralisation methods

Method		Principle	Enabler	Pros	Cons
Jamming		Interfere with the communication system, prompting their evacuation or landing protocols.	Utilize an RF power amplifier and RF spectrum recognition technology.	Characterised by affordability, lightweight design, and compact dimensions, ensuring non-destructive interference. Suitable for concurrent application on multiple drones.	Effective solely against drones operating within the ISM[10] band, with potential interference to other ISM band devices.
Spoofing		Employ counterfeit positioning signals or simulated control commands to reroute drones.	Utilise signal analysis, data packet analysis, and decoding techniques.	Possess guidance and eviction capabilities without causing damage.	May disrupt other electronic devices. Limited effectiveness against encrypted communication channels.
Hacking		Acquire root privileges of drones' operating systems and execute requisite operations.	Engage in system penetration and analyse system vulnerabilities.	Characterised by cost-effectiveness and non-destructive capabilities.	Primarily compatible with specific operating systems and network-based protocols. May cause interference with other ISM band devices.

Source: compiled by the author

[9] Wentzel et al. 2024.

[10] ISM bands (industrial, scientific, and medical) are parts of the RF (radio-frequency) spectrum reserved for general use by, as the name suggests, scientific, medical, and industrial devices.

Jamming

A prevalent interrupting or disabling method for neutralising sUAS involves disrupting its sensors or systems using noise signals. In this paper, jamming is categorised into three main types: direct track deception, fusion, and protocol-aware, each targeting drone sensors and systems.[11] Researchers proposed a UAS team forming an air defence radar network to jam sensors, effectively tracking and jamming the targeted drones.[12] Another study utilised direct track deception and fusion to manipulate navigation and trajectory control systems, causing UAS to drift from the restricted areas.[13] Additionally, a software-defined radio (SDR)-based protocol-aware jamming system was introduced, outperforming tone and sweep methods.[14]

Researchers focused on long term evolution (LTE)-based UAS neutralisation, determining a jamming range of approximately 60 metres.[15] Furthermore, a system was developed to remotely neutralise explosive UAS in combat zones,[16] while a game theoretic approach was proposed for optimising jamming methods against UAS attackers.[17] Jamming offers non-damaging solutions to neutralise drones in restricted areas, functioning at various levels from hardware to software. However, its omni-directional effects and energy consumption pose challenges. Synthesising the studies referred above, the author suggest that jamming methods should be directional, controllable, and responsive.

Spoofing

Spoofing, as a controlling or interrupting neutraliser, involves generating fake signals to deceive the receiver of a potentially harmful drone, mimicking legitimate signals. The signals targeted for spoofing include those related to remote control, payload data, the Global Navigation Satellite System (GNSS), and sensors.[18] In order to execute spoofing, knowledge of communication protocol stacks is crucial. A study demonstrated a man-in-the-middle attack on UAS control systems, injecting control commands to interact with the UAS.[19] Another research utilized cracking software development kits (SDKs), reverse engineering, and GNSS spoofing to hijack UAS, comparing security performances of DJI and Parrot drones under exploitation attacks.[20]

Analyses were conducted on accessing internal sensors to neutralise sUAS in restricted areas that were largely successful.[21] A method to hijack the MAVLink

11 Sliti et al. 2018.
12 Zhao et al. 2009.
13 Li et al. 2018.
14 Pärlin et al. 2018.
15 Curpen et al. 2018.
16 Willner 2009.
17 Bhattacharya–Başar 2010.
18 Pistoia 2021.
19 Rodday et al. 2016.
20 Dey et al. 2018.
21 Esteves et al. 2018.

protocol on ArduPilot Mega 2.5 autopilot was presented, and a probabilistic attack model against UAS using denial of service attacks was proposed.[22] A physical-layer spoofing attack based on angle of arrival and path loss factors to recognise and locate UAS was suggested.[23]

Hacking

Drone hacking, as primarily a controlling or interrupting neutraliser, has been a subject of research for many years, focusing primarily on external interference, and networking methods referring to the exploitation of vulnerabilities in sUAS control systems or communication networks to disrupt or neutralise potentially harmful drone operations.[24] Outer interference methods require close proximity of interference devices to sUAS sensors such as inertial measurement units (IMUs) and GNSS, ensuring accurate data retrieval.[25] It is worth highlighting that sUAS rely primarily on Wi-Fi and cellular networks for communication, presenting vulnerabilities that malicious actors exploit to seize control of the drone. By infiltrating these networks, attackers can manipulate the autopilot, issuing directives for secure take-off or redirection.

A C-UAS may exploit network vulnerabilities to intercept communication packets, modify commands, or enforce authentication checks randomly. The sensory arsenal of a drone offers additional hacking opportunities for counteractivity.

Hard neutralisation

Hard neutralisation (HN), within the realm of C-UAS, delineates a methodology characterised by the direct physical incapacitation or destruction of a potentially harmful drone. In contrast to SN techniques, which focus mainly on non-kinetic means of neutralisation, HN methods entail the use of kinetic or electromagnetic force to eliminate the threat posed by the target drone.[26] The implementation of HN measures necessitates precision targeting, modern weapon systems, and effective command and control mechanisms to ensure accurate engagement and minimise collateral damage. Furthermore, the decision to employ HN techniques often requires careful consideration of the operational environment, potential legal implications, and the risk of unintended consequences.

Despite their effectiveness in neutralising immediate threats, HN methods may entail significant logistical, ethical, and diplomatic considerations, making them a subject of rigorous analysis and debate outside the broader framework of C-UAS operations.[27] HN measures include the utilisation of kinetic or direct energy weapons

[22] Ficco et al. 2022.
[23] Huang 2018.
[24] Rodday 2016.
[25] Balestrieri et al. 2021.
[26] Pistoia 2021.
[27] Arteche et al. 2017.

to interrupt, disable, or destroy the potentially harmful drone. Additionally, hard neutralisation tactics may involve the deployment of physical barriers, such as nets, or drones equipped with capture devices, to physically detain or capture the target sUAS.[28] Table 2 presents a comparative analysis of the various drone HN methods.

Table 2: Pros-cons comparison of UAS hard neutralisation methods

Method	Principle	Enabler	Pros	Cons
Kinetic Energy Weapons	Utilise physical impact to disable or destroy drones.	Projectile launcher platforms.	Highly effective HN method, relatively low cost per kill ratio.	High probability of collateral damage, limited range.
Direct Energy Weapons	Employ directed energy (e.g. lasers, microwaves) to disrupt or destroy drones.	Laser systems, microwave emitters, etc.	Precise targeting, rapid response, SN capability.	Limited range, high cost per kill ratio.
Physical Barriers	Utilise physical obstacles to prevent drone intrusion.	Fencing, nets, walls, barricades, drones, etc.	Minimal risk of collateral damage, relatively cheap, deterrent, SN capability.	Limited use due to deployment-specific, space consuming nature.

Source: compiled by the author

Kinetic energy weapons

Kinetic energy weapons (KEW) are designed to physically impede potentially harmful drones, necessitating precise targeting and tracking.[29] KEW must closely engage with the drone under attack to effectively neutralise it. There is a broad spectrum of KEW HN methods, involving even trained birds, through weaponised drones and relatively simple projectile launcher platforms.[30]

Kinetic based neutralisers, such as machine guns, guided missiles, and artillery, rely on physical munitions to incapacitate drones with certain guided missiles necessitating tracking systems while others utilise optical sensors for detection. These solutions are costly, primarily used in military settings, and can cause collateral damage upon impact, therefore not optimal against sUAS.[31] Collision drones represent another kind of KEW approach, where dedicated agile and highly manoeuvrable drones equipped with detection and tracking capabilities pursue and collide with the target sUAS. They utilise computer vision techniques for detection and may carry explosives to

[28] Rudys et al. 2022.
[29] Pistoia 2021.
[30] Chamola et al. 2020.
[31] Kang et al. 2020.

maximise impact. However, like projectile-based neutralisers, they can cause collateral damage and have longer neutralisation delays. Ultimately, collision drones are disposable systems, acting as a hybrid between drones and missiles.[32]

Direct energy weapons

Direct energy weapons (DEW) possess the capability to emit electromagnetic energy across a broad spectrum, affecting targeted drones' electronics either temporarily or permanently. These electromagnetic waves are classified into two categories: narrowband (or high-power microwaves) and wideband. Each category exhibits distinct characteristics. Narrowband electromagnetics operate on a single-tone frequency, demanding high power levels, while wideband electromagnetics distribute energy over a wider band with short pulses. Precise targeting of DEW is imperative for their effectiveness, as improper directionality can diminish lethality. Moreover, accurate assessment of neutralisation effectiveness post-usage is crucial.[33]

Laser-based neutralisers, on the other hand, can incapacitate or destroy sUAS by ionising their path and emitting an electric current. Lasers are categorised as low-power or high-power variants, and as such, require precise aiming and tracking. High-power lasers are capable of inflicting destructive damage.[34] However, challenges such as technological complexity, weather sensitivity, and accurate targeting persist. While effective in military settings, the deployment of DEWs in civilian environments is fraught with risks, including potential collateral damage and interference with general aviation operations. Additionally, their large size, weight, and power requirements limit their integration primarily to terrestrial platforms, rendering them unsuitable for deployment on low-altitude platforms like mini drones.

Physical barriers

Net capture, a physical approach, entails deploying nets to hinder sUAS mobility. C-UAS employ guns or specialised weapons to activate the net, immobilising the drone upon contact. A deployable net capture system was developed for installation on aircraft or authorised UAS, capable of apprehending unauthorised or unsafe drones.[35] Another novel idea presents a spin-launched UAS projectile engineered to deploy a capturing net, seamlessly integrated within the projectile's warhead and activated through conventional firearms.[36] Physical capture strategies prioritise the immobilisation of drones and their control systems, offering advantages such as ease of use, lightweight construction, and rapid assembly. Although physical capture approaches are efficient and cost-effective, they may pose risks to pilots as captured

[32] Brust et al. 2021.
[33] Borja 2023.
[34] Taillandier et al. 2023.
[35] Pistoia 2021.
[36] Blyskal 2019.

drones could sustain damage at varying levels. A drone interceptor, equipped with nets launched from firearms, adeptly detect and swiftly intercept moving targets, leveraging multispectral on-board sensing for remote or autonomous precision capture of potentially harmful sUAS.[37]

Threat level determination

A properly automated, optimally functioning C-UAS system can select the most practical NM with the best efficiency in any given situation as quickly as possible. The primary prerequisite for this is the precise determination of the threat level (TL). Taking this idea into account, the author presents a theory of logical connectivity based on binary mathematical foundations that, using the concepts discussed above, facilitates achieving the appropriate level of automation for C-UAS while simultaneously selecting the most effective NM. In formulating the theory, the methodological foundations were provided by the philosophical principle known as *Occam's razor,* resulting in an abductive heuristic model[38] that herein applied deriving from the smallest possible set of elements based on the binary values: *0* and *1*. When determining the threat level, three parameters, *intention, risk,* and *operability,* have been identified, each of which can assume values between 0 and 1 (Table 3), therefore a TL contains a 3-digit binary code.

Table 3: Threat parameters' binary values

Value	**0**	**1**
Intention	asUAS	usUAS
Risk	high	moderate (or lower)
Operability	high	moderate (or lower)

Source: compiled by the author

Intention

Intention embodies the purpose or objective behind the actions of sUAS. It encompasses the goals, motives, and planned behaviours of the drone operator or controlling entity. Understanding the intention behind drone activities is crucial for gauging the level of threat posed by the drone and devising an appropriate response strategy, where a value of *0* signifies an asUAS and *1* signifies usUAS intent.

Analysing the intention of a drone operation aids in assessing the severity of the threat it poses. Intention can reveal whether the drone's activities are benign (usUAS), such as aerial photography or surveying, or malevolent (asUAS), such as surveillance,

[37] Kang et al. 2020.
[38] McFadden 2021.

intrusion, or potential attacks. The evaluation combines factors like the drone's flight pattern, payload, and proximity to sensitive areas.[39]

Furthermore, comprehending the intention behind drone operations assists in selecting the most effective NM. For instance, if the operator's intention suggests hostile actions or potential harm, a HN method, like KEW or DEW, may be warranted to promptly eliminate the threat. Vice versa, if the intention seems non-threatening or the risk level is low, a softer approach, such as signal jamming or communication disruption, may be more suitable to neutralise the drone without causing undue damage or escalation. Thus, intention plays a pivotal role in guiding the decision-making process for choosing between hard or soft neutralisation methods in C-UAS operations.

Risk

Risk refers to the likelihood and potential consequences of harm or damage resulting from the presence or actions of potentially harmful drones. It entails assessing various factors, including the capabilities of the drone, its proximity to critical infrastructure or sensitive areas, and the intentions of the operator, to determine the level of threat posed by the drone.[40]

In the process of TL determination, risk analysis plays a crucial role in evaluating the severity of the threat posed by a drone and guiding the selection of an appropriate neutralisation method. Risk assessment involves considering the probability of a drone causing harm or disruption, as well as the potential impact of such events on security, safety, and operations. Factors such as the drone's flight path, altitude, speed, payload capability, and communication protocols are taken into account when determining the risk level associated with a drone. Additionally, the vulnerability of critical assets or personnel to drone-related threats is assessed to gauge the potential consequences of an incident.[41]

Based on the assessed risk level, decisions can be made regarding the deployment of HN or SN methods. If the risk is considered high (*0* value), indicating a significant threat to security or safety, hard neutralisation methods such as KEW or DEW may be necessary to swiftly eliminate the threat. Conversely, if the risk is moderate (*1* value) or the threat is less severe, softer approaches such as signal jamming or communication disruption may be sufficient to neutralise the drone without causing undue harm or escalation.

Operability

Operability refers to the operational capability and effectiveness of both the sUAS and its operators in responding to and neutralising drone threats. Within the confines

[39] Palik 2013.
[40] Sander et al. 2018.
[41] Jahangir–White 2021.

of this study it encompasses not only the technical capabilities of the drone but also the presumed knowledge, skills, and decision-making abilities of the operators responsible for its deployment.

The operability of a sUAS and its operators plays a critical role in assessing the appropriate response to a perceived threat posed by potentially harmful drones.[42] Determining operability involves the investigation of the drone's flight path, altitude, speed, payload capability, and communication protocols. In this context, operability is classified into two distinct levels: *0* representing high operability, and *1* indicating moderate or lower operability.

In short, operability, encompassing both technical capabilities and operator proficiency, is a fundamental aspect of TL determination of a sUAS operation, guiding the selection of appropriate neutralisation strategies to address varying threat scenarios.

Decision making

Based on the binary determination of the three threat parameters, a total of eight different scenarios (Table 4) can be envisioned, providing the simplest theoretical description using all accessible data and thus satisfying the criterion outlined above by *Occam's razor*.

Table 4: Recommended NM for each threat level

	Hard neutralisation			Soft neutralisation		
Parameter	**Intention**	**Risk**	**Operability**	**Intention**	**Risk**	**Operability**
Threat level	0	0	0	0	1	1
	0	0	1	1	0	0
	0	1	0	1	1	0
	1	0	1	1	1	1

Source: compiled by the author

As illustrated in Table 4, the highest conceivable threat arises when facing asUAS (intention = *0*) paired with high level of risk (risk = *0*) and operability (operability = *0*). Vice versa, the inverse scenario occurs when a usUAS (intention = *1*) is assigned alongside moderate risk (risk = *1*) and operability (operability = *1*) values within the system. While the choice of NM may seem obvious for options at the extremes of the spectrum, deliberation over whether to opt for hard or soft neutralisation becomes more contentious, particularly around the median values. It is essential to emphasise that while the recommendations outlined in Table 4 can be considered as general guidelines, they may vary for a specific system (e.g. '*0 1 1*' could be addressed with HN since it has malevolent intention, if the environment otherwise allows this method).

[42] Arteche et al. 2017.

Conclusion

The examination of neutralisation methods for countering drone threats underscores the critical need for effective strategies to safeguard public safety, national security, and individual privacy. This study has explored a spectrum of soft and hard neutralisation methodologies, shedding light on their efficacy and other implications within the broader framework of C-UAS operations. By delving into soft neutralisation techniques such as jamming, spoofing, and hacking, as well as hard neutralisation methods including kinetic energy weapons, direct energy weapons, and physical barriers, this paper has provided a comprehensive analysis of the diverse approaches available for mitigating sUAS threats.

The genuine theory unfolded of this research, guided by the principle of Occam's razor, emphasises the importance of a minimalist, logical yet easily streamlined approach to threat level determination in C-UAS operations. By distilling complex threat scenarios into binary parameters of intention, risk, and operability, this study has facilitated the development of an abductive heuristic model for selecting the most appropriate neutralisation method. Through the application of this model, decision-makers can efficiently assess threat levels and deploy the optimal neutralisation method, whether soft or hard, to address the specific context of each situation.

Addressing possible opposing viewpoints, it is acknowledged that the choice between soft and hard neutralisation methods may be subject to debate, particularly in scenarios where threat parameters fall within intermediate values. However, by prioritising simplicity and efficiency in threat level determination, the proposed model offers a pragmatic framework for navigating such complexities and making informed decisions in C-UAS operations.

Furthermore, it is imperative to recognise that this study represents Part 2 in a series of papers on C-UAS, laying the groundwork for the final paper currently in progress. As such, the findings and methodologies presented herein pave the way for Part 3, which will focus on the vision of operation for comprehensive UAS surveillance and neutralisation frameworks. By building upon the insights gained from this study, the forthcoming paper will further elucidate the challenges and opportunities in the evolving landscape of C-UAS technologies and strategies.

In summary, the investigation conducted in this paper underscores the multifaceted nature of UAS threats and the importance of adopting innovative and adaptive approaches to counter them effectively. By embracing the principles of Occam's razor and logical connectivity, decision-makers can navigate the complexities of C-UAS operations with clarity and precision, ultimately enhancing the resilience and security of our airspace systems.

Acknowledgement

This paper was prepared with the professional support of the Doctoral Student Scholarship Program of the Co-operative Doctoral Program of the Ministry of Culture and Innovation financed from the National Research, Development and Innovation Fund.

National Research, Development and Innovation Office

References

Arteche, David – Chivers, Kenneth – Howard, Bryce – Long, Terrell – Merriman, Walter – Padilla, Anthony – Pinto, Andrew – Smith, Stenson – Thoma, Victoria (2017): *Drone Defense System Architecture for US Navy Strategic Facilities.* Naval Postgraduate School, Monterey, USA.

Balestrieri, Eulalia – Daponte, Pasquale – Vito, Luca de – Lamonaca, Francesco (2021): Sensors and Measurements for Unmanned Systems: An Overview. *Sensors,* 21(4), 1518. Online. https://doi.org/10.3390/s21041518

Bhattacharya, Sourabh – Başar, Tamer (2010): Game-Theoretic Analysis of an Aerial Jamming Attack on a UAV Communication Network. In *Proceedings of the 2010 American Control Conference,* Baltimore, MD, USA, 2010, 818–823. Online: https://doi.org/10.1109/ACC.2010.5530755

Blyskal, Tomasz – Fong, Richard – Thompson, LaMar (2019): *Scalable Effect Net Warhead.* US Patent (Application Number: 10,197,365).

Borja, Lauren (2023): High-Energy Laser Directed Energy Weapons: Military Doctrine and Implications for Warfare. In Gruszczak, Artur – Kaempf, Sebastian (eds.): *Routledge Handbook of the Future of Warfare.* London: Routledge, 353–363. Online: https://doi.org/10.4324/9781003299011-37

Brust, Matthias – Danoy, Grégoire – Stolfi, Daniel – Bouvry, Pascal (2021): Swarm-Based Counter UAV Defense System. *Discover Internet of Things,* 1(2). Online: https://doi.org/10.1007/s43926-021-00002-x

Castrillo, Vittorio – Manco, Angelo – Pascarella, Domenico – Gigante, Gabriella (2022): A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones. *Drones,* 6(3), 65. Online: https://doi.org/10.3390/drones6030065

Chamola, Vinay – Kotesh, Pavan – Agarwal, Aayush – Naren – Gupta, Navneet – Guizani, Mohsen (2020): A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques. *Ad Hoc Networks,* 111, 102324. Online: https://doi.org/10.1016/j.adhoc.2020.102324

Cline, Travis (2020): *Mitigating Drone Attacks for Large High-Density Events.* PhD Thesis. Purdue University. Online: https://doi.org/10.25394/PGS.13341860.v1

Curpen, Radu – Bălan, Titus – Micloş, Ioan Alexandru – Comănici, Ionut (2018): Assessment of Signal Jamming Efficiency against LTE UAVs. In *2018 International*

Conference on Communications (COMM), Bucharest, Romania, 2018, 367–370. Online: https://doi.org/10.1109/ICComm.2018.8484746

Csengeri, János (2019): Counter-Drone Activity as a System. *Security & Future,* 3(1), 31–34.

Da Silva, Douglas – Machado, Renato – Coutinho, Olympio – Antreich, Felix (2023): A Soft-Kill Reinforcement Learning Counter Unmanned Aerial System (C-UAS) with Accelerated Training. *IEEE Access,* 11, 31496–31507. Online: https://doi.org/10.1109/ACCESS.2023.3253481

Dey, Vishal – Pudi, Vikramkumar – Chattopadhyay, Anupam – Elovici, Yuval (2018): Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study. In *31st International Conference on VLSI Design and 17th International Conference on Embedded Systems* (VLSID), Pune, India, 2018, 398–403. Online: https://doi.org/10.1109/VLSID.2018.97

Esteves, José Lopes – Cottais, Emmanuel – Kasmi, Chaouki (2018): Unlocking the Access to the Effects Induced by IEMI on a Civilian UAV. In *International Symposium on Electromagnetic Compatibility,* (EMC EUROPE), Amsterdam, Netherlands, 2018, 48–52. Online: https://doi.org/10.1109/EMCEurope.2018.8484990

Ficco, Massimo – Palmiero, Raffaele – Rak, Massimiliano – Granata, Daniele (2022): MAVLink Protocol for Unmanned Aerial Vehicle: Vulnerabilities Analysis. In *2022 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress,* (DASC/PiCom/CBDCom/CyberSciTech), Falerna, Italy, 2022, 1–6. Online: https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927895

Huang, Ke-Wen – Wang, Hui-Ming (2018): Combating the Control Signal Spoofing Attack in UAV Systems. *IEEE Transactions on Vehicular Technology,* 67(8), 7769–7773. Online: https://doi.org/10.1109/TVT.2018.2830345

Jahangir, Mohammed – White, Daniel (2021): Good Practices and Approaches for Counter UAV System Developments – An Industrial Perspective. In Clemente, Carmine – Fioranelli, Francesco – Colone, Fabiola – Li, Gang (eds.): *Radar Countermeasures for Unmanned Aerial Vehicles.* E-book. Online: https://doi.org/10.1049/SBRA543E_ch12

Kang, Honggu – Joung, Jingon – Kim, Jinyoung – Kang, Joonhyuk – Cho, Yong Soo (2020): Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems. *IEEE Access,* 8, 168671–168710. Online: https://doi.org/10.1109/ACCESS.2020.3023473

Krajnc, Zoltán (2018): A drónok elleni stratégia és eljárások. *Repüléstudományi Közlemények,* 30(3), 139–148.

Li, An – Wu, Qingqing – Zhang, Rui (2018): UAV-Enabled Cooperative Jamming for Improving Secrecy of Ground Wiretap Channel. *IEEE Wireless Communications Letters,* 8(1), 181–184. Online: https://doi.org/10.1109/LWC.2018.2865774

Martins, Bruno – Holland, Arthur – Silkoset, Andrea (2020): *Countering the Drone Threat: Implications of C-UAS Technology for Norway in an EU and NATO Context.* PRIO Paper, Peace Research Institute Oslo.

McFadden, Johnjoe (2021): *Life Is Simple: How Occam's Razor Set Science Free and Unlocked the Universe.* New York: Basic Books.

Palik, Mátyás (2013): A pilóta nélküli légijárművek katonai alkalmazása. In *Pilóta nélküli repülés profiknak és amatőröknek.* Budapest: Nemzeti Közszolgálati Egyetem, 281–298.

Pärlin, Karel – Alam, Muhammad – Moullec, Yannick (2018): Jamming of UAV Remote Control Systems Using Software Defined Radio. In *2018 International Conference on Military Communications and Information Systems* (ICMCIS), Warsaw, Poland, 2018, 1–6. Online: https://doi.org/10.1109/ICMCIS.2018.8398711

Pistoia, Daniela (2021): Counter UAS Systems Overview. In Clemente, Carmine – Fioranelli, Francesco – Colone, Fabiola – Li, Gang (eds.): *Radar Countermeasures for Unmanned Aerial Vehicles.* Scitech Publishing, 21–43. Online: https://doi.org/10.1049/SBRA543E_ch1

Rodday, Nils – Schmidt, Ricardo – Pras, Aiko (2016): Exploring Security Vulnerabilities of Unmanned Aerial Vehicles. In *NOMS 2016 – 2016 IEEE/IFIP Network Operations and Management Symposium,* Istanbul, Turkey, 2016, 993–994. Online: https://doi.org/10.1109/NOMS.2016.7502939

Rudys, Saulius – Laučys, Andrius – Ragulis, Paulius – Aleksiejūnas, Rimvydas – Stankevičius, Karolis – Kinka, Martynas – Razgūnas, Matas – Bručas, Domantas – Udris, Dainius – Pomarnacki, Raimondas (2022): Hostile UAV Detection and Neutralization Using a UAV System. *Drones,* 6(9), 250. Online: https://doi.org/10.3390/drones6090250

Sander, Jennifer – Kuwertz, Achim – Mühlenberg, Dirk – Müller, Wilmuth (2018): High-Level Data Fusion Component for Drone Classification and Decision Support in Counter UAV. In *Proceedings of Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation,* Orlando, SPIE 10651. Online: https://doi.org/10.1117/12.2306148

Sliti, Maha – Abdallah, Walid – Boudriga, Noureddine (2018): Jamming Attack Detection in Optical UAV Networks. In *20th International Conference on Transparent Optical Networks* (ICTON), Bucharest, Romania, 1–5. Online: https://doi.org/10.1109/ICTON.2018.8473921

Taillandier, Maximilian – Peiffer, Richard – Darut, Gabriel – Verdy, Charles – Regnault, Reneé – Pommies, Miles (2023): Duality Safety – Efficiency in Laser Directed Energy Weapon Applications. In *Proceedings of SPIE, High Power Lasers: Technology and Systems, Platforms, Effects,* Amsterdam, Netherlands, 2023. Online: https://doi.org/10.1117/12.3001871

Wentzel, Alexander – Cornils, Jan – Valentin, Marco – Heynicke, Ralf – Scholl, Gerd (2024): *Compact Counter-UAS System for Defeating Small UAV in Complex Environments, Detection, Tracking, ID and Defeat of Small UAVs in Complex Environments.* (STO-MP-SET-315).

Willner, Byron (2009): *Methods and Apparatuses for Detecting and Neutralizing Remotely Activated Explosives.* US Patent (Application Number: 12/126,570).

Zhao, Chen – Wang, Xuesong – Xiao, Shilin (2009): Cooperative Deception Jamming against Radar Network Using a Team of UAVs. *IET International Radar Conference,* Guilin, China, 2009. Online: https://doi.org/10.1049/cp.2009.0418

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 2. szám 123–148.
DOI: 10.32567/hm.2024.2.10

Katona Gergő[1]

Kiberbiztonsági stratégiák, szabályozások és ajánlások az okosrepülőterek számára: fenyegetések és megoldások

Cybersecurity Strategies, Regulations and Recommendations for Smart Airports: Threats and Solutions

Absztrakt

Az okosrepülőterek digitális és hálózati integrációja miatt a kiberbiztonság kulcsfontosságú. A repülőtéri folyamatok digitalizálása, az automatizálás és a személyre szabott utasélmény iránti igény új kiberbiztonsági kihívásokat teremt. Az USA, az EU és nemzetközi légi közlekedési szervezetek jogszabályokkal és ajánlásokkal segítik a repülőterek információbiztonsági szintjének növelését, hogy jobban ellenálljanak a kibertámadásoknak. A kutatás célja, hogy azonosítsa az okosrepülőterek specifikus rendszerelemeit és az ezekre leselkedő kiberbiztonsági fenyegetéseket. Nemzetközi dokumentumok elemzésével a cikk feltérképezi, az Európai Unió, az Egyesült Államok és nemzetközi légi közlekedési szervezetek által közzétett, a szektorral kapcsolatos publikációk milyen mélységgel foglalkoznak a kiberbiztonsággal, illetve milyen szinten adnak választ az azonosított fenyegetésekre. A kutatás eredményei hozzá tudnak járulni az okosrepülőterek biztonsági szintjének javításához és a kiberfenyegetésekkel szembeni védelemük megerősítéséhez.

Kulcsszavak: okosrepülőtér, kiberbiztonság, IoT, érettség, Alverad

[1] Junior kutató, Nemzeti Közszolgálati Egyetem, e-mail: katona.gergo@uni-nke.hu

Abstract

With the digital and network integration of smart airports, cyber security is key. The digitalisation of airport processes, automation and the need for a personalised passenger experience are creating new cyber security challenges. The US, the EU and international aviation organisations are helping airports improve information security through legislation and recommendations to make them more resilient to cyberattacks. The aim of this research is to identify the specific system components of smart airports and the cybersecurity threats they face. Through an analysis of international documents, the article explores the depth to which publications published by the European Union, the United States and international aviation organisations on the sector address cybersecurity and the level of response to identified threats. The results of this research can contribute to improving the security level of smart airports and strengthening their defences against cyber threats.

Keywords: smart airport, cybersecurity, IoT, maturity, Alverad

Bevezetés

Az okosrepülőterek korszakában, ahol a digitális technológiák és a hálózatok kapcsolata határozza meg a működés minden aspektusát, a kiberbiztonság kérdése kiemelten fontos. Az egyes tényezők, mint például a repülőtéri folyamatok egyre nagyobb mértékű digitalizálódása és automatizálása, a személyre szabott utasélmény kialakításának igénye, valamint a légi közlekedés mint azonosított kritikus infrastruktúra ágazat jelentős kihívásokat rejt magában kiberbiztonsági területen. Az USA, az EU szervezetei, valamint a nemzetközi légi közlekedési szervezetek érzékelik a repülőterek és a légi közlekedés kiberbiztonsági kihívásait, ezért jogszabályokkal, ajánlásokkal és tervekkel segítik a szereplők információbiztonsági érettségi szintjének növelését. Az ilyen szabályozások és iránymutatások célja, hogy erősítsék a szervezetek ellenálló képességét a kibertérből jövő fenyegetésekkel szemben.

A tudományos probléma meghatározása

Az okosrepülőterek számos különböző típusú rendszerekből állnak, amelyek folyamatosan hatással vannak egymásra. A rendszerek egymástól való magas fokú függése az egyes rendszerelemek kiberbiztonsági sebezhetőségének értékét felerősítheti. Ezen sebezhetőségek kihasználása a légi közlekedésben hatalmas anyagi károkat tud okozni, és akár emberéleteket is veszélyeztet. Ezért fontos, hogy az ilyen típusú rendszerekkel rendelkező repülőterek rendszer-, fenyegetés- és követelménykörnyezetét azonosítsuk és kiértékeljük.

Módszertan

A kutatás során a szerző *state-of-art* analízissel vizsgálja meg, hogy milyen specifikus rendszerelemeket lehet azonosítani egy okosrepülőtér esetében, illetve ezek milyen kiberbiztonsági fenyegetéssel néznek szembe. Ezen nemzetközi dokumentumvizsgálattal térképezi fel a szerző azokat a szabályozásokat, irányelveket, stratégiákat, ajánlásokat, amelyekkel az egyes európai uniós vagy egyesült államokbeli, illetve nemzetközi légi közlekedési szervezetek publikáltak a légi közlekedés kiberbiztonságával kapcsolatban. Illetve a feltérképezett dokumentumokat csoportosítom az alapján, hogy milyen részletességgel vizsgálják a kiberbiztonságot. Azokat a dokumentumokat is elemzem, amelyekben a legrészletesebben fejtik ki a légi közlekedés kiberbiztonságát. A szerző azt vizsgálja, hogy az előzőleg azonosított fenyegetésekkel kapcsolatban milyen szintű segítséget tudnak nyújtani a dokumentumok.

Kutatási hipotézisek

A szerző a kutatás kezdetén az alábbi hipotéziseket fogalmazta meg:

H1: Az Egyesült Államok szervezetei több és részletesebb dokumentumot publikálnak a légi közlekedés kiberbiztonságával kapcsolatban, mint az Európai Unió intézményei.

H2: A nemzetközi módszertanok, dokumentumok implementálásával az azonosított kiberbiztonsági fenyegetések bekövetkezési kockázata csökkenthető az okosrepülőterek esetében.

A kutatás célkitűzése

A kutatás célja átfogó képet nyújtani az okosrepülőterek fogalmáról és az azt megalkotó rendszerekről. Azonosítani azokat a kihívásokat, amelyekkel szembe kell néznie az okosrepülőteret üzemeltetőnek. További célja a kutatásnak egy átfogó elemzés, amely megvizsgálja, hogy az Egyesült Államok, illetve az Európai Unió egyes szervezetei és a nemzetközi légi közlekedési szervezetek milyen mélységgel foglalkoznak a szektor kiberbiztonságával, és milyen szintű választ adnak ezek a dokumentumok az előzőleg azonosított biztonsági fenyegetésekre.

Repülőtér-generációk

A repülőterek osztályozása egy folyamatosan fejlődő terület, amely az utóbbi években kiemelt figyelmet kapott a légi közlekedési iparágban. Az osztályozási rendszer nem csupán a repülőterek fizikai infrastruktúráját és elhelyezkedését veszi alapul, hanem egyre inkább a technológiai fejlettséget, az utasokkal való interakció minőségét és az üzemeltetési hatékonyságot is figyelembe veszi. Ahogy a világ digitalizálódik, úgy válnak a repülőterek is egyre „okosabbá", integrálva a legújabb technológiai

innovációkat nemcsak az operatív hatékonyság, de az utasélmény javítása érdekében is. Ebben a kontextusban a repülőterek osztályozása átfogó keretrendszert nyújt, amely bemutatja, hogyan fejlődhetnek és alkalmazkodhatnak a repülőterek az új kihívásokhoz és technológiákhoz. Az osztályozás négy fő kategóriába sorolja a repülőtereket az 1.0-tól a 4.0-ig, ahol az 1.0 a legkevésbé fejlett, míg a 4.0 a legmodernebb, okosrepülőtereket jelöli.

Az 1.0-s besorolású repülőterek az alapvető szolgáltatások biztosítására összpontosítanak, mint amilyen a biztonságos és hatékony repülőgép-működtetés, áruszállítás, utasfelvétel, biztonság, poggyászkezelés, miközben igyekeznek minimalizálni a késéseket és az operatív zavarokat. „A repülőterek fejlettebb műveleteket végeznek, de nem fordítanak kellő figyelmet az utasok igényeire" – állítják Alansari és munkatársai kutatásukban.[2] A repülőtéri érdekeltek csak minimális adatot osztanak meg, és a lehető legalacsonyabb szintű együttműködést valósítják meg.

A 2.0-s besorolású repülőterek a modern technológiák alkalmazásával képesek az operatív változásokra reagálni, az adatok megfelelő mennyiségének jelenléte és az érdekelt felek közötti gyors információcsere révén. A repülőterekben megjelennek automatizmusok, de az egyes rendszerek főleg szigetszerűen, egymástól elszigetelten működnek. Ezeken a repülőtereken az egyes bérlők például olyan technológiákat vehetnek igénybe, mint wifi, széles sávú internet és videómegfigyelési szolgáltatások, anélkül, hogy saját megoldásaikat kellene szervezniük és karbantartaniuk.[3]

A 3.0-s besorolású repülőterek modern technológiákkal és jellemzőkkel rendelkeznek. A Cisco Smart Airports tanulmánya[4] szerint a rendszerek egy „digitális rács" köré épülnek, amely lehetővé teszi a magas sebességű széles sávú adatforgalmat az egész ökoszisztémában, beleértve az egyes szereplők között, például repülőtér-üzemeltető, légitársaságok, légiforgalom-irányítás. Az egyes folyamatok hatékonyságát az információ és adatok valós idejű cseréje javítja, amely során az egyes rendszerek folyamatos és nagyszámú adatkapcsolatokkal operálnak,[5] így lehetővé válik jobb és gyorsabb döntések meghozatala. A 3.0-s besorolású repülőterek az utasélményre koncentrálnak, ahol az utasok profitálnak az utasadatok cseréjéből, lehetővé téve számukra, hogy személyre szabott szolgáltatásokat kapjanak.

A 4.0-s besorolású repülőtér koncepciója az Open Data és a Linked Data elveken nyugszik. Az adatoknak integrálódniuk kell egymással, hogy kompatibilis struktúrával rendelkezzenek. A biztonság az egyik legfontosabb szempont. Az adatokat a hatályos jogszabályoknak megfelelően kell védeni. Az érzékeny adatokhoz csak a rendszer jogosult felhasználói férhetnek hozzá. Az Open Data elv alapgondolata az adatok bővítésének és megosztásának lehetősége a jogosult felhasználók között, így mindenki számára elérhetővé téve azokat.[6]

A SITA felmérése[7] alapján is látható, hogy a repülőterek folyamatos beruházásokat hajtanak végre az IT-megoldásaik terén. Az elemzésből jól kiolvasható, hogy a repülőterek

[2] Alansari–Soomro–Belgaum 2019.
[3] Fattah et al. 2009.
[4] Fattah et al. 2009.
[5] Blondel–Zintel–Suzuki 2015.
[6] Nau–Benoit 2017.
[7] SITA 2023.

technológiai fejlődése dinamikus és folyamatos, ahol az IT-kiadások jelentős növekedése az innováció iránti elkötelezettség fokát mutatja. Az utóbbi években megfigyelhető, hogy az üzemeltetési *(opex)* és a tőkeberuházási *(capex)* költségek egyensúlyba kerültek, ami a repülőtéri iparág fejlődési és beruházási hajlandóságát jelzi, nem csupán a meglévő infrastruktúra fenntartását célozzák meg a repülőterek. Különösen 2022-ben az IT-költségek túlszárnyalták az előrejelzéseket, elérve a repülőtéri bevételek 7,17%-át, ami jelzi a tőkeberuházások intenzív növekedését. Ez a tendencia folytatódhat, 2023-ra az elemzésbevételek még nagyobb, 7,45%-os részét kitevő IT-kiadásokra számítottak. A repülőterek stratégiailag fontosnak tartják az adattárházakba, üzletiintelligencia-szoftverekbe, biometrikus azonosító rendszerekbe, valamint az 5G kommunikációs technológiákba történő befektetést. A határellenőrzési folyamatban a legelterjedtebb a biometrikus azonosítás, de a közeljövőben a repülőterek tervezik ezen technológiát más repülőtéri folyamatokba is integrálni. Ezzel párhuzamosan a mesterséges intelligencia és üzleti intelligencia területén a repülőterek stratégiailag fontosnak tartják a startupvállalkozásokkal való együttműködést.

Okosrepülőterek főbb rendszerei és azok kihívásai

Rendszerelem-áttekintés

Az okosrepülőterek rendszereinek azonosítása során azokat elemezzük, amelyek a légi közlekedéssel kapcsolatos specifikus célokat és funkciókat szolgálnak ki. Jelen vizsgálat hatóköréből kikerülnek azok az általános rendszerek, amelyek nem szektorspecifikus feladatokat látnak el, mint például vállalatirányítási rendszerek, épületüzemeltetési rendszer, általános IT-infrastruktúra-rendszerek, mivel a cikk célja az, hogy mélyreható és releváns ismereteket nyújtson egy szűkebb, de kritikus területről. Az általános használatú rendszerek kizárása lehetővé teszi a szerzőnek, hogy fókuszáltabb elemzést végezzen az okosrepülőterek információs rendszereiről.

A repülőterek esetében két fő területet tudunk megkülönböztetni, a légi tevékenységekkel összefüggő részleget *(airside)* és a földi tevékenységeket magában foglaló részleget *(landside)*.

Airside

- Légiforgalom-irányítási rendszer. A légiforgalom-irányítási rendszer kulcsfontosságú eleme a repülőtér rendszereinek, mivel alapvető szerepet játszik a légi közlekedés biztonságának, hatékonyságának és zavartalanságának biztosításában. E rendszer felelős a repülőgépek földi mozgásainak és légi útvonalainak koordinálásáért, a légtér és a repülőtéri létesítmények optimális kihasználásáért, valamint a forgalom folyamatos és biztonságos áramlásának fenntartásáért. Ezen a területen is léteznek magasabb szinten automatizált rendszerelemek. Ilyen rendszerelem lehet a pályaelőrejelzés-technológia, ami lehetővé teszi a repülőgépek útvonalának térbeli és időbeli előrejelzését, növelve a repülési

tervek pontosságát és a biztonságot. Ilyen technológia a középtávú konfliktusfelismerés is, ami 0–60 perces időhorizonton belül azonosítja a lehetséges légtérkonfliktusokat.[8]

- Repülőgépek földi kiszolgálása. A földi kiszolgálási feladatokat általában a légitársaság és a szolgáltató közötti szolgáltatási szintű megállapodások határozzák meg, amelyek rögzítik a kívánt terjedelmet, árat, minőségi szintet és kulcsfontosságú teljesítménymutatókat. A földi kiszolgálási tevékenységek két fő kategóriába sorolhatók, úgymint a „szárnyon felüli" és „szárny alatti" tevékenységek. A „szárnyon felüli" tevékenységek a repülőgép utasterével kapcsolatosak, és magukban foglalják az utasok beszállását és leszállását, az étkeztetést, a kabin tisztítását és előkészítését, valamint szükség szerint a biztonsági és védelmi ellenőrzéseket. A „szárny alatti" tevékenységek a rakomány (konténeres és ömlesztett) kirakodására és berakodására, valamint egyéb földi tevékenységekre összpontosítanak, mint például az áramellátás (*ground power unit,* GPU), a kabinhőmérséklet beállítása, a futóművek rögzítése, az üzemanyag-utántöltés, az ivóvíz- és WC-kiszolgálás, a vontatás és visszatolatás, valamint az utasok feljutásának biztosítása lépcsőkön, rámpákon vagy utasfelszállási hídon keresztül. Azonban ezek automatizálása nem egyszerű, mivel az egyes repülőgépek fizikai adottságai, az automatizált és manuális folyamatok összehangolása mind nagy kihívást tud jelenteni ezen a területen.[9]
- Repülőtéri járművek nyomon követése. Ez a rendszer lehetővé teszi a repülőtéri üzemeltetők számára, hogy valós időben lássák a járművek jelenlegi és korábbi helyzetét, és nyomon kövessék az erőforrások felhasználását. A rádiófrekvenciás azonosítás (*radio frequency identification,* RFID) címkékkel ellátott vészhelyzeti járműveket is figyeli, ami hozzájárul a gyorsabb válaszidőkhöz, mivel az incidensparancsnokok és a mentőegységek azonnal információt kapnak a leggyorsabb útvonalakról.[10]

Landside

- Okosbecsekkolás. Az utasok a check-in során többféle módszert is használhatnak, többek között weboldalas megoldást, mobiltelefonos applikációt és számítógépes kioszkokat. Ezekkel a megoldásokkal csökkenteni lehet a földi kiszolgáló személyzet emberi közreműködését, és ezáltal a légitársaságok képesek csökkenteni a költségeiket, illetve a személyzet által elkövetett hibákat. Az okosrepülőterek összekapcsolták a működő légitársaságok összes kioszkját, és az utasok a terminálon elhelyezett bármelyik közös kioszkon keresztül bejelentkezhetnek.[11]
- Önálló beszállás. A beszállási folyamat számos manuális részből áll, amelyben személyzeti interakció szükséges. A beszállást segítő és ellenőrző rendszerek

[8] Bestugin et al. 2020.
[9] Tabares – Mora-Camino 2019.
[10] Marks–Rietsema 2014.
[11] Wittmer 2011.

segítik ezen folyamat automatizálását úgy, hogy a kapuknál elhelyezett beszállókártya-olvasók lehetővé teszik, hogy az utasok saját maguk olvassák be a beszállókártyájukat. Így emberi ellenőrzés nélkül, az RFID-olvasási technológiát használva szállhatnak fel a repülőgépre. A beszállókártya beolvasása után a kapuk automatikusan kinyílnak, és az utasok beléphetnek a repülőgépbe. Emberi beavatkozás csak a földi személyzet által végzett felügyelet során szükséges.[12]

- Beltéri navigálás és további utaskezelés. A mobilapplikációk segíthetnek az utasoknak a repülőtéren belüli navigálásban,[13] illetve csatorna lehet az utas és a terminál személyzete között az egyes fontos információk átadására, mint például járatkésés.[14]
- Határellenőrzés. A kézipoggyász ellenőrzésére szolgáló robbanóanyag-felderítő rendszerek (*explosive detection systems for cabin baggage screening,* EDCSB) röntgensugaras technológiát és mesterséges intelligenciát használnak a robbanóanyagok azonosítására és elkülönítésére a poggyász röntgenfelvételein. Az EDCSB-rendszerek automatikusan meg tudják határozni, hogy a poggyász tartalmaz-e veszélyes anyagokat.[15]
- Az e-kapuk használata során az utasok személyzeti beavatkozás nélkül képesek személyazonosságukat validálni. Az útlevél-azonosító megadását, illetve a biometrikus azonosítást követően lehet áthaladni.[16]
- Poggyászkezelés. A rádiófrekvenciás azonosítás (RFID) és a vezeték nélküli érzékelőhálózatok integrációja lehetővé teszi egy olyan rakományfelügyeleti rendszer létrehozását, amely a zökkenőmentes működés elősegítése érdekében valós idejű nyomon követést és a repülőtéri rakomány helymeghatározását képes megvalósítani. Az RFID a poggyászok címkézésére is használható, az összegyűjtött információkat pedig egy IoT-felhőszerverben tárolják, hogy az adatok a különböző repülőtereken könnyen visszakereshetők legyenek. Mobilalkalmazásokkal integrálva az utasok mobilkészülékeik segítségével pontosan nyomon követhetik csomagjaik helyét, és csökkenthetik az elveszett poggyászok számát.[17]
- AODBS *(Airport Operations Database System)*. A repülőtéri adatbázis operációs rendszer egy speciális szoftverplatform, amelyet a repülőterek használnak különféle adatok kezelésére, tárolására és feldolgozására. Ezek az operációs rendszerek központi szerepet játszanak a repülőtér működésében, mivel lehetővé teszik az adatok hatékony és biztonságos kezelését, és támogatják a különféle repülőtéri szolgáltatások integrációját. Egy ilyen rendszerben a következő adatok jelenhetnek meg:

[12] Rajapaksha–Jayasuriya 2020.
[13] Mantouka et al. 2018.
[14] AlMashari et al. 2018.
[15] Hättenschwiler et al. 2018.
[16] del Río et al. 2016.
[17] Wang 2018.

a) Repülési információk kezelése: az AODBS tárolja a járatokkal kapcsolatos összes fontos információt, beleértve a járatmenetrendeket és a járatok kapuhoz rendelését. Ez a rendszer biztosítja, hogy a járatok időben és hatékonyan legyenek kezelve.
b) Erőforrás-kijelölés: az AODBS felelős a repülőtéri erőforrások, mint például a kapuk, check-in pultok és beszállókapuk kijelöléséért és kezeléséért. Ez segít optimalizálni a repülőtér működését, és biztosítja az erőforrások hatékony felhasználását.
c) Diagramok és statisztikai jelentések készítése: az AODBS lehetővé teszi különböző diagramok és statisztikai jelentések készítését, amelyek segítenek a repülőtér üzemeltetésének elemzésében és optimalizálásában.[18]

Látható, hogy az okosrepülőterek főbb ismérve a különböző rendszerek közötti magas szintű interoperabilitás. A magas szintű kapcsolódás alapja a rendszerek rendszere (*system of systems,* SoS) koncepciójának a megléte. Az SoS a rendszerek összességét egyesíti egy olyan feladathoz, amelyet egyik rendszer sem képes egyedül elvégezni. Az egyes rendszerelemek megtartják saját kezelésüket, céljaikat és erőforrásaikat, miközben az SoS-on belül együttműködnek, és alkalmazkodnak az SoS céljainak eléréséhez.[19]

Okosrepülőterek kiberbiztonsági kihívásai

Az ENISA tanulmánya,[20] illetve a Georgia Lykou és társai[21] által publikált tanulmány azonosította azokat a fenyegetési kategóriákat, amelyek hatással lehetnek az okosrepülőterekre:

- Hálózati és kommunikációs támadások. A hálózatok rosszindulatú forrásokból érkező támadásoknak vannak kitéve, amelyek passzív és aktív kategóriákba sorolhatók. A passzív támadások esetén az adatokat lehallgatják, míg az aktív támadások során a hálózat normál működését zavarják meg, és hozzáférést szereznek a hálózati eszközökhöz. Annak ellenére, hogy az egyes protokollok megpróbálják megakadályozni a kommunikáció lehallgatását, az intelligens repülőterek még mindig vonzó célpontok a manipulációs vagy hálózati támadásokhoz. A vezeték nélküli kommunikáció, a légi forgalmi irányítás rádiójelei is veszélyeztetettek lehetnek, amelyeket zavaró eszközökkel befolyásolnak. A szolgáltatásmegtagadási támadások (*denail of service,* DoS) további kockázatot jelentenek, mivel megzavarhatják az információs rendszereket és a hálózatokat, ami komoly hatással lehet a repülőtéri rendszerekre és az utasokra.
- Rosszindulatú szoftverek. A rosszindulatú szoftverek, amelyek megfertőzhetik az általános információs rendszereket, veszélyeztethetik az intelligens eszközöket, beleértve az utasok és a személyzet mobil eszközeit, valamint a repülőtéri

[18] Yang 2010.
[19] Sharkov 2017.
[20] ENISA 2018.
[21] Lykou–Anagnostopoulou–Gritzalis 2018.

infrastruktúra rendszereit. Az ilyen szoftverek rosszindulatú viselkedést mutatnak, visszaélve a környezeti jogosultságokkal, és súlyos hatással lehetnek a repülőtéri rendszerekre. Az intelligens repülőtéri rendszerekben fennálló sebezhetőségek miatt a rosszindulatú szoftveres támadások potenciális veszélyt jelentenek.

- A repülőtéri eszközök manipulációja. A repülőtéri eszközök manipulálásának különféle módjai veszélyeztethetik a repülőtéri infrastruktúrát. A központi foglalási rendszerek, az adminisztrációs informatikai rendszerek és a tárolt érzékelőadatok manipulálása súlyos következményekkel járhat, beleértve a fizikai biztonság megsértését is.
- A jogosultsággal való visszaélés. A hozzáférés-ellenőrzések ellenére a támadók képesek lehetnek hitelesítő adatokat megszerezni és jogosultsági jogokat kiterjeszteni. Még a bennfentes fenyegetésként fellépő alkalmazottak vagy vállalkozók is visszaélhetnek jogosultságaikkal, például hitelesítő adatok lopásával vagy social engineering technikákkal.
- Social engineering és adathalász-támadások. A social engineering módszereivel az embereket lehet manipulálni vagy félrevezetni, ami átjutást biztosít a rendszerbe. Az e-mail továbbra is az elsődleges módszer a támadók számára, lehetővé téve számukra az áldozatok fiókjainak, személyazonosságának és jogosultságának megszerzését.

A Georgia Lykou és társai[22] által publikált cikkben egy kérdőíves felmérést ismertettek, amelyben 34 európai, illetve amerikai repülőteret elemeztek. A cikk egy felmérést is tartalmazott, hogy az okosrepülőterek esetében az IoT-eszközök alkalmazása a SCADA-rendszereken keresztül, az air- és landside területeken át mindenhol megtalálható. A cikkből az is látható, hogy az okosrepülőtereket érintő fenyegetések az airside és landside rendszerek esetében is megjelennek, tehát a legtöbb repülőtéri rendszerre hatással vannak. Ez azért lehetséges, mert az okosrepülőterek esetében a rendszerintegráció igen nagy számban jelenik meg a legkülönbözőbb szinteken az IoT-eszközök segítségével, így létrehozva az SoS-architektúrát. Az SoS-ökoszisztéma elemeiben egyetlen sebezhetőség kihasználásával akár az egész összekapcsolt architektúrát veszélyeztetni lehet, így akár egy poggyászkezelő rendszerben megjelenő IoT-eszköz sérülékenysége kihatással lehet a repülőgép berakodására is.[23]

A légi közlekedés kiberbiztonságát érintő nemzetközi dokumentációk áttekintése

Jelen fejezetben megvizsgálom azokat a dokumentumokat, amelyeket az Egyesült Államok és az Európai Unió szervezetei bocsátottak ki. Ezenfelül azokat a dokumentumokat is, amelyeket valamely nemzetközi szervezet publikált a polgári légi közlekedés kiberbiztonságával kapcsolatban.

[22] Lykou–Anagnostopoulou–Gritzalis 2018.
[23] Sharkov 2017.

Azért az Egyesült Államokat, illetve az Európai Uniót választottam mint elemzésem célpontjai, mivel e két terület tagállamai rendelkeznek a legnagyobb utasforgalmat kiszolgáló repülőterekkel. A Nemzetközi Polgári Repülési Szervezet 2022-es légi közlekedési statisztikai eredményeiből az látható, hogy a világ utasfogalom alapján 25 legnagyobb repülőteréből 19 reptér vagy az USA-ban, vagy az Európai Unióban található.[24]

Az egyes dokumentumokat az alapján értékeltem, hogy milyen szinten jelennek meg bennük kiberbiztonsági követelmények/ajánlások. Az alábbi értékelési módszert alkalmaztam:

- Érintőleges: olyan dokumentum, amely megemlíti a kiberbiztonság fontosságát, azonban azon belül nem jelöl meg specifikus területet.
- Alapszintű: olyan dokumentum, amely a kiberbiztonsági szabályozás valamelyik aspektusát kifejti, azonban csak irányelveket, illetve magas szintű szabályozásokat/ajánlásokat tartalmaz.
- Átfogó: a kiberbiztonság legtöbb területével kapcsolatosan határoz meg magas szintű szabályozásokat/ajánlásokat.
- Részletes: olyan dokumentum, amely a kiberbiztonság legtöbb területével kapcsolatosan részletes szabályozást/ajánlásokat tartalmaz. Ezen felül azon dokumentumok, amelyek a kiberbiztonság valamelyik területével kapcsolatban fogalmaznak meg részletes követelményeket/ajánlásokat. Alapul véve ezeket, részletes szabályokat lehet kialakítani az információbiztonság területén.

Az 1. táblázatban jogszabályi szinten csak hatályban lévő dokumentumok jelennek meg, mivel csak azoknak a tartalma kötelező érvényű.

1. táblázat: A légi közlekedés kiberbiztonságával kapcsolatos nemzetközi dokumentumok vizsgálatai

Szabályozás /Szabvány/ Ajánlás neve	**Leírás**	**Követelmények absztrakciós szintje**	**Dokumentum típusa**	**Hatókör/ Kiadó**
Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete[25]	Polgári légi közlekedés területén alkalmazandó közös szabályok meghatározása.	Érintőleges	jogszabály	Európai Unió/ Európai Parlament és a Tanács

[24] ICAO 2022a.

[25] Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete (2018. július 4.) a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
Az Európai Parlament és a Tanács 376/2014/EU rendelete[26]	A polgári légi közlekedésben előforduló események jelentéséről, elemzéséről és nyomon követéséről.	Érintőleges	jogszabály	Európai Unió/ Európai Parlament és a Tanács
A Bizottság (EU) 2022/1645 felhatalmazáson alapuló rendelete[27]	Az (EU) 2018/1139 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról a potenciális hatással járó információbiztonsági kockázatok kezelésére vonatkozó követelmények.	Átfogó szintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács
Az Európai Parlament és a Tanács (EU) 2022/ 2555 irányelve (NIS 2)[28]	A NIS 2 irányelv két kulcsfontosságú területre összpontosít: a kiberbiztonsági felügyeletre és a kiberbiztonsági tanúsításra. Ezek a területek az Európai Unióban a kiberbiztonság magas szintjének biztosítását és a digitális szolgáltatások iránti bizalom növelését szolgálják. Kiberbiztonsági Felügyelet: Az irányelv előírja a kiberbiztonsági felügyeletért felelős nemzeti hatóságok létrehozását. Ezek a hatóságok felügyelik a kiberbiztonsági követelményeknek való megfelelést. Az alapvető és fontos szervezetek kategóriákba sorolása alapján történik a felügyelet. Az alapvető fontosságú szervezetek, ilyenek például a repülőterek, szigorúbb felügyelet alá esnek. Kiberbiztonsági szabályozás terén átfogó, magas szintű követelményeket fogalmaz meg a hatálya alá eső szervezetekkel szemben. Jelen jogszabály terméktanúsítási része nem érvényes a légi közlekedési ágazatra.	Átfogó szintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács

[26] Az Európai Parlament és a Tanács 376/2014/EU rendelete (2014. április 3.) a polgári légi közlekedési események jelentéséről, elemzéséről és nyomon követéséről, valamint a 996/2010/EU európai parlamenti és tanácsi rendelet módosításáról és a 2003/42/EK európai parlamenti és tanácsi irányelv, valamint az 1321/2007/EK bizottsági rendelet és az 1330/2007/EK bizottsági rendelet hatályon kívül helyezéséről EGT-vonatkozású szöveg.

[27] A Bizottság (EU) 2022/1645 felhatalmazáson alapuló rendelete (2022. július 14.) az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek a 748/2012/EU és a 139/2014/EU bizottsági rendelet hatálya alá tartozó szervezetekre vonatkozó, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésével kapcsolatos követelmények tekintetében történő alkalmazására irányadó szabályok megállapításáról, valamint a 748/2012/EU és a 139/2014/EU bizottsági rendelet módosításáról.

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

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
Az Európai Parlament és Tanács (EU) 2018/1139 rendelete[29]	A légiközlekedési tanúsítás a NIS 2 hatálya alól kivételt képez, mert ezen területet jelen rendelettel tervezik lefedni a jogalkotók. Az IKT-rendszerek tanúsítása magában foglalja annak biztosítását, hogy ezek a rendszerek megfeleljenek a szigorú biztonsági és védelmi előírásoknak a balesetek, incidensek és a légi forgalmi műveletek zavarainak megelőzése érdekében. A rendelet hangsúlyozza az IKT-rendszerek, termékek és komponensek alapos értékelésének fontosságát a biztonsági követelményeknek való megfelelés ellenőrzése és a repülési tevékenységekben való alkalmazásukkal kapcsolatos potenciális kockázatok mérséklése érdekében. Viszont a kiberbiztonság csak magas szinten jelenik meg a dokumentumban.	Alapszintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács
A Bizottság (EU) 2015/1998 végrehajtási rendelete[30]	A légiközlekedés-védelmi közös alapkövetelmények végrehajtására vonatkozó részletes intézkedések megállapításáról szóló jogszabály, amely közvetlenül nem azonosít specifikus kiberbiztonsági követelményt. Azonban számos olyan kontrollt határoz meg, amelyet egy IKT-eszköz biztosít, illetve fizikai biztonsági követelmény is szerepel ezen jogszabályban.	Alapszintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács
A Bizottság (EU) 2019/1583 végrehajtási rendelete[31]	A 2015/1998 végrehajtási rendeletet bővíti ki külön kiberbiztonsági követelményekkel.	Alapszintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács

[29] Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete (2018. július 4.) a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről.

[30] A Bizottság (EU) 2015/1998 végrehajtási rendelete (2015. november 5.) a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról.

[31] A Bizottság (EU) 2019/1583 végrehajtási rendelete (2019. szeptember 25.) a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról szóló (EU) 2015/1998 végrehajtási rendeletnek a kiberbiztonsági intézkedések tekintetében történő módosításáról.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
A Bizottság (EU) 2017/373 végrehajtási rendelete[32]	A rendeletben magas szinten jelenik meg kiberbiztonság. A dokumentumban a védelemirányítási rendszer előírja, hogy a légi navigációs szolgáltatók, a légi forgalmi áramlásszervezés szolgáltatói és a hálózatirányítók megtegyék a szükséges intézkedéseket rendszereik, rendszerelemeik és adataik védelme érdekében az olyan információ- és kiberbiztonsági kockázatokkal szemben, amelyek jogosulatlan beavatkozást jelenthetnek a szolgáltatás nyújtásában.	Érintőleges	jogszabály	Európai Unió/ Európai Parlament és a Tanács
A Bizottság (EU) 2023/203 végrehajtási rendelete[33]	Potenciális hatással járó információbiztonsági kockázatok kezelésére vonatkozó követelmények tekintetében.	Alapszintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács
A Bizottság (EU) 2023/1769 végrehajtási rendelete[34]	A légi forgalmi irányítási/légi navigációs szolgálati rendszerek és rendszerelemek tervezésében vagy gyártásában részt vevő szervezetek jóváhagyására vonatkozó műszaki követelmények és igazgatási eljárások megállapításáról.	Alapszintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács

[32] A Bizottság (EU) 2017/373 végrehajtási rendelete (2017. március 1.) a légiforgalmi szolgáltatást/léginavigációs szolgálatokat és más légiforgalmi szolgáltatási hálózati funkciókat és azok felügyeletét ellátó szolgáltatókra vonatkozó közös követelmények meghatározásáról, valamint a 482/2008/EK rendelet, az 1034/2011/EU, az 1035/2011/EU és az (EU) 2016/1377 végrehajtási rendelet hatályon kívül helyezéséről, továbbá a 677/2011/EU rendelet módosításáról.

[33] A Bizottság (EU) 2023/203 végrehajtási rendelete (2022. október 27.) az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU és az (EU) 2015/340 bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet hatálya alá tartozó szervezetek, valamint a 748/2012/EU, az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU, az (EU) 2015/340 és a 139/2014/EU bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet hatálya alá tartozó illetékes hatóságok tekintetében a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésére vonatkozó követelmények tekintetében történő alkalmazására vonatkozó szabályok megállapításáról, valamint az 1178/2011/EU, a 748/2012/EU, a 965/2012/EU, a 139/2014/EU, az 1321/2014/EU és az (EU) 2015/340 bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet módosításáról.

[34] A Bizottság (EU) 2023/1769 végrehajtási rendelete (2023. szeptember 12.) a légiforgalmi szolgáltatási/léginavigációs szolgálati rendszerek és rendszerelemek tervezésében vagy gyártásában részt vevő szervezetek jóváhagyására vonatkozó műszaki követelmények és igazgatási eljárások meghatározásáról, valamint az (EU) 2023/203 végrehajtási rendelet módosításáról.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
Elsődleges, könnyen hozzáférhető szabályok az információbiztonságért[35]	Ez a dokumentum részletes követelménykatalógust tartalmaz a légi közlekedés szereplőinek. Ennek alapja ezen ágazat esetében megjelenő jogi szabályozás. Azonban a jogszabályok csak főbb követelményeket határoznak meg. Ezzel a dokumentummal biztosítani lehet a magasan megfogalmazott elvárásoknak való megfelelést.	Részletes	ajánlás	Európai Unió/ Európai Unió Repülésbiztonsági Ügynökség
A légi forgalmi irányítás kiberbiztonsági érettségi modellje[36]	A dokumentum az Eurocontrol által meghatározott érettségi rendszert írja le. Ez alapján pontosan azonosítható, hogy az adott szervezet az információbiztonság egyes területét milyen érettségi szinten üzemelteti.	Részletes	felmérő módszertan	Európai Unió/ Eurocontrol
Okosrepülőterek biztonsága[37]	Az ENISA dokumentuma átfogó elemzést nyújt az okosrepülőterek felépítéséről és azon fenyegetésekről, amelyeket számításba kell vennie ezen létesítményeknek. Azonosít különböző szcenáriókat, amelyek az egyes fenyegetések bekövetkezéséhez köthetők. Illetve tartalmaz egy követelménykatalógust is, amely azonosítja a kiberbiztonság egyes területeinek főbb követelményeit.	Részletes	publikáció	Európai Unió/ Európai Unió Kiberbiztonsági Ügynöksége
Repülési kiberbiztonsági stratégia[38]	A Nemzetközi Polgári Repülési Szervezet (ICAO), az Egyesült Nemzetek Szervezetének ügynöksége kiadott 2019-ben egy kiberbiztonsági stratégiát. A stratégia a következő hét pillérre épülő keretrendszer: nemzetközi együttműködés; irányítás; hatékony jogszabályok és szabályozások; kiberbiztonsági politika; információmegosztás; incidenskezelés és vészhelyzeti tervezés; és kapacitásépítés, képzés és kiberbiztonsági kultúra.	Alapszintű	stratégia	Nemzetközi/ Nemzetközi Polgári Repülési Szervezet

[35] EASA 2023.
[36] Eurocontrol 2019.
[37] ENISA 2018.
[38] ICAO 2019.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
Kiberbiztonsági cselekvési terv, 2. kiadás[39]	A dokumentum az EASA által kiadott útmutató, amely az Európai Unió 2023/203 és 2022/1645 rendeletei alapján készült. Célja az információbiztonsági kockázatok kezelése a légi közlekedési szektorban, tartalmazza az ISMS bevezetésének és fenntartásának követelményeit, incidens kezelésére vonatkozó irányelveket, valamint példákat a fenyegetési forgatókönyvekre. Emellett részletezi az egyes információbiztonsági feladatokat, az azok ellátásához szükséges személyzeti követelményeket és képzettségi elvárásokat, segítve ezzel a biztonság fenntartását és növelését.	Átfogó	cselekvési terv	Nemzetközi/ Nemzetközi Polgári Repülési Szervezet
Kiberbiztonsági kultúra a polgári repülésben[40]	A dokumentum útmutatást nyújt a tagállamok és az érdekelt felek számára a polgári légi közlekedési ágazat szervezetein belül a szilárd kiberbiztonsági kultúra kialakításához. A dokumentum hangsúlyozza a szervezeti kultúra jelentőségét a kiberbiztonságban, valamint a személyzet folyamatos képzését és támogatását a kiberbiztonsági kockázatok kezelésében és az ágazat ellenálló képességének fokozásában.	Részletes	útmutató	Nemzetközi/ Nemzetközi Polgári Repülési Szervezet
Kiberbiztonsági stratégiai iránymutatás[41]	A dokumentum célja egy átfogó globális kiberbiztonsági stratégia megalkotása a polgári repülés területén. Az ICAO (International Civil Aviation Organization – Nemzetközi Polgári Repülési Szervezet) felismeri a kibertámadások növekvő fenyegetését, amelyek különböző területeken egyszerre hathatnak és gyorsan terjedhetnek. Az új stratégia célja, hogy a polgári repülési szektor ellenálló legyen a kibertámadásokkal szemben, és világszerte biztonságos és megbízható maradjon, miközben tovább fejlődik és növekszik. E cél elérése érdekében az ICAO hangsúlyozza az államok közötti együttműködés fontosságát, a megfelelő törvényhozás és szabályozás megteremtését, az információmegosztást, valamint az incidens kezelését és a vészhelyzeti tervezést. A stratégia további kulcselemei közé tartozik a képességfejlesztés, a képzés és a kiberbiztonsági kultúra erősítése.	Átfogó	útmutató	Nemzetközi/ Nemzetközi Polgári Repülési Szervezet

[39] ICAO 2022b.
[40] ICAO 2022c.
[41] ICAO 2022d.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
Útmutató a jelzőlámpás eljáráshoz[42]	A Nemzetközi Polgári Repülési Szervezet ezen dokumentumban egy olyan jelzőrendszer alkalmazását írja le, amely segítségével a kibertérben kezelt, továbbított adatokra a szenzitivitásuk és értékük alapján kell szabályokat kialakítani.	Átfogó	útmutató	Nemzetközi/ Nemzetközi Polgári Repülési Szervezet
Elnöki szakpolitikai irányelv – létfontosságú infrastruktúrák biztonsága és ellenálló képessége[43]	Azonosítja a közlekedési ágazatot mint kritikus infrastruktúrát, és magas szintű irányelveket tartalmaz. Tehát a légi közlekedés csak közvetetten jelenik meg benne.	Érintőleges	irányelv	Egyesült Államok/ Fehér Ház
H.R.302 – Az FAA 2018. évi újbóli felhatalmazásáról szóló törvény[44]	Intézkedéseket tartalmaz a repülési szektor kiberbiztonságának a fejlesztésére az alábbi pontokban: légi forgalmi irányítási rendszerben azonosított kiberbiztonsági sebezhetőségek megszüntetése; a kiberbiztonságnak az okosrepülőtér kezdeményezés alapelemének kell lennie; pilóta nélküli légi járművek kiberbiztonsága; a Szövetségi Légügyi Hivatal integrált tesztkörnyezetet alakítson ki a légi forgalmi irányítás modernizációs technológiáinak kutatására, fejlesztésére, értékelésére és validálására.	Alapszintű	jogszabály	Egyesült Államok/ Kongresszus
AC 119-1A – A légijármű-hálózat biztonsági program működési engedélyezése[45]	Tanácsadó körlevél, részletesen leírja, hogyan lehet megszerezni a repülőgépek üzemeltetési engedélyét, amelyek a fedélzeti számítógépes hálózat biztonságával kapcsolatos különleges feltétel alapján kaptak tanúsítványt. Ezen dokumentumban az információbiztonságok elleni védelem, illetve az eseménykezelés is megjelenik mint szempont.	Alapszintű	tanácsadói körlevél	Egyesült Államok/ Szövetségi Légi Közlekedési Hatóság

[42] ICAO 2022e.
[43] Presidential Policy Directive/PPD-21 – Critical Infrastructure Security and Resilience.
[44] H.R.302 – An act to provide protections for certain sports medicine professionals, to reauthorize Federal aviation programs, to improve aircraft safety certification processes, and for other purposes.
[45] AC 119-1A – Operational Authorization of Aircraft Network Security Program.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
A Közlekedésbiztonsági felügyelet kiberbiztonsági ütemterve[46]	A Közlekedésbiztonsági felügyelet kiberbiztonsági ütemterve a Belbiztonsági Minisztérium kiberbiztonsági stratégiájához közvetlenül igazodó keretrendszert biztosít, amely alapján a Közlekedésbiztonsági felügyeletnek a következő öt évben végre kell hajtania kiberbiztonsági feladatait. A felügyelet évente felülvizsgálja és frissíti az ütemterv végrehajtási tervét. A dokumentum a következő pilléreken alapszik: kockázatazonosítás, sebezhetőség csökkentése, fenyegetés csökkentése, következmények enyhítése.	Átfogó	ütemterv	Egyesült Államok/ Közlekedésbiztonsági felügyelet
Szövetségi légi közlekedési hatóság Kiberbiztonsági stratégiája[47]	A dokumentum a (Federal Aviation Administration – FAA) 2018-as Reauthorization Act 509. szakasza alapján készült jelentés, amely áttekinti és frissíti az FAA kiberbiztonsági stratégiáját. A jelentés kiemeli a stratégia öt alappillérét, amelyek célja az FAA hálózatainak és rendszereinek védelme, az adatvezérelt kockázatkezelési képességek fejlesztése, a munkaerő kiberbiztonsági képességeinek építése, valamint a kormányzati és ipari partnerekkel való együttműködés fenntartása és fejlesztése. A dokumentum bemutatja a 2019-es felülvizsgálat eredményeit, az azóta történt fejlesztéseket, és az új technológiák, például a felhőszolgáltatások integrálását a stratégiába.	Alapszintű	stratégia	Egyesült Államok/ Szövetségi Légügyi Hivatal
Közlekedési rendszerek ágazatspecifikus terv[48]	Megjelenik a légi közlekedési ágazat mint kritikus infrastruktúra, és azonosítja azok résztvevőit, többek között a repülőtereket is. Azonosítja a biztonsági kihívásokat, megjelenik a kiberbiztonsági fenyegetés mint fogalom. Azonosítja a célokat és prioritásokat is a biztonsággal kapcsolatban.	Alapszintű	terv	Egyesült Államok/ Amerikai Kibervédelmi Ügynökség

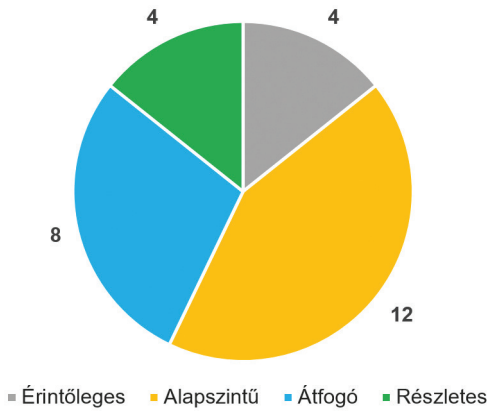
[46] TSA 2018.
[47] FAA 2020.
[48] CISA 2015.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
CANSO kiválósági szabvány a kiberbiztonság terén[49]	A Polgári Légiforgalmi Szolgálatok Szervezete (Civil Air Navigation Services Organization, CANSO) Biztonsági Állandó Bizottságának kiberbiztonsági munkacsoportja (Cyber Safety Task Force, CSTF) készítette. Célja egy átfogó kiberbiztonsági érettségi keretrendszer biztosítása a navigációs szolgáltatóknak. A keretrendszer az információbiztonság területeit átfogó módon írja le és egyes értettségi szinten értékeli azokat.	Átfogó	szabvány	Nemzetközi/Polgári Légiforgalmi Szolgálatok Szervezete
Légiforgalom-irányítási kiberbiztonsági szabályzat sablon[50]	Alapot biztosít a légi forgalmi irányítóknak, amely alapján egy minden információbiztonsági területre kiterjedő szabályozási rendszert lehet elkészíteni.	Alapszintű	útmutatás	Nemzetközi/Polgári Légiforgalmi Szolgálatok Szervezete
Repülési kiberbiztonsági iránymutatás[51]	Két része van. Az első része kifejezetten a szervezeti kultúrával és hozzállással kapcsolatban fogalmaz meg átfogó követelményeket. Míg a második a repülőgépek kiberbiztonságával és kockázatával fogalmaz meg átfogó szabályozást.	Átfogó	útmutatás	Nemzetközi/Nemzetközi Légi Szállítási Szövetség
Biztonsági irányítási rendszer (SeMS) kézikönyv[52]	Átfogó kockázatmenedzsment, illetve biztonsági keretrendszer kialakítását segíti elő, azonban a kiberbiztonsági területtel érintőlegesen foglalkozik.	Átfogó	szabvány	Nemzetközi/Nemzetközi Légi Szállítási Szövetség

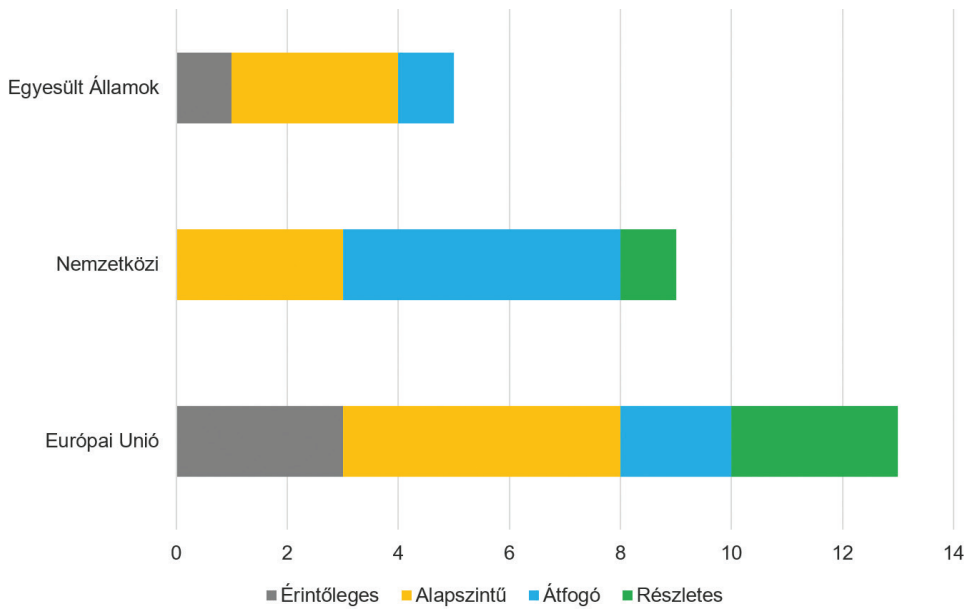
Forrás: a szerző szerkesztése

Összesen 28 dokumentum. Absztrakciós szintjeik vizsgálata során az látható, hogy a legtöbb publikált forrás (12 db) alapszintű szabályokat/ajánlásokat fogalmaz meg a légi közlekedés kiberbiztonságával szemben. Ezt a csoportot követik az átfogó szintű dokumentumok (8 db), majd a részletes (4 db) és az érintőleges (4 db) jelenik meg.

[49] CANSO 2020.
[50] CANSO 2021.
[51] IATA 2021.
[52] IATA 2024.



1. ábra: A dokumentumok absztrakciós szintjeinek megoszlása
Forrás: a szerző szerkesztése



2. ábra: Absztrakciós szint megoszlása területi hatókör szerint
Forrás: a szerző szerkesztése

Ha megvizsgáljuk hatókörszinten az egyes dokumentumokhoz tartozó követelményi absztrakciós szintet, akkor az látható, hogy az Egyesült Államok egyes szervezetei darabszám alapján kevés anyagot bocsátottak ki a témában. Illetve ezen dokumentumok főleg alapszintű követelményeket/ajánlásokat tartalmaznak. Kiemelhető az Európai Unióhoz köthető dokumentumok mennyisége, illetve részletessége. Az EU

számos jogi szabályozásban foglalkozik a légi közlekedés kiberbiztonságával. Szervezetei részletes elemzést, illetve útmutatást nyújtanak a légi közlekedési szereplők, így az okosrepülőterek üzemeltetői számára is. Iránymutatásai nemcsak a legfőbb kockázatokkal foglalkoznak, hanem segítséget nyújtanak egy szervezetszintű információbiztonsági irányítás kialakításához és fenntartásához is. Megállapíthatjuk tehát, hogy az Európai Unió szervezetei több és részletesebb dokumentumot publikáltak a témában. Első hipotézisemet megcáfoltam.

Okosrepülőterek kiberbiztonsági kihívásainak csökkentése a nemzetközi dokumentumok alapján

Vajon az előzőleg megjelölt, okosrepülőterekkel kapcsolatos kiberbiztonsági kihívásokra az azonosított és részletesnek értékelt nemzetközi dokumentumok képesek-e releváns útmutatást adni?

A légi közlekedés kiberbiztonságát érintő nemzetközi dokumentumokat különböző kategóriákba soroltuk. A besoroláskor azt a hatékonyságot vizsgáltuk, hogy a dokumentumok milyen mértékben segítenek az adott fenyegetés kezelésében.

A következő értékelési kategóriákat állítottuk fel:

- Kielégítően segít: a dokumentum teljes mértékben lefedi az adott fenyegetést, beleértve annak felismerését, megelőzését, az azonnali válaszintézkedéseket, valamint a helyreállítási folyamatokat. Minden releváns aspektust részletesen tárgyal, és konkrét, gyakorlati útmutatást nyújt.
  - A következő jellemzőkből többet is tartalmaz az adott dokumentum:
    - Részletes előírások a fenyegetésanalízissel és azonosítással kapcsolatban.
    - Pontosan meghatározza, hogyan lehet hatékony megelőzési és védelmi stratégiát kialakítani.
    - Pontosan meghatározza, hogyan lehet hatékony és azonnali válaszintézkedéseket kialakítani.
    - Pontosan meghatározza, hogyan lehet helyreállítási tervet és folyamatokat kialakítani.
    - Példák és esettanulmányok bemutatása.
- Részben segít: a dokumentum csak részlegesen fedi le az adott fenyegetéseket. Egyes aspektusokat jól kezel, de hiányosságok vannak a fenyegetésazonosítás, a megelőzés, a válaszintézkedések vagy a helyreállítási folyamatok terén. A dokumentum hasznos, de önmagában nem nyújt teljes körű támogatást.
  - A következő jellemzőkből többet is tartalmaz az adott dokumentum:
    - Alapvetések azonosítása a fenyegetésanalízissel kapcsolatban.
    - Felsőbb szintű meghatározása a megelőzési és védelmi stratégia kialakításának.
    - Általános követelmények leírását tartalmazza a válaszintézkedések kialakításával kapcsolatban.
    - Kevésbé részletes példák és esettanulmányok.
- Nem segít: a dokumentum nem nyújt megfelelő segítséget az adott fenyegetés kezelésében. Hiányoznak a releváns információk, a megelőzési stratégiák

és a válaszintézkedések. A dokumentum nem ad gyakorlati útmutatást, és nem járul hozzá hatékonyan a fenyegetés kezeléséhez.
– A következő jellemzőkből többet is tartalmaz az adott dokumentum:
  ° Hiányos vagy nem létező követelmények a fenyegetésanalízis témájában.
  ° Nincsenek vagy minimálisak a követelmények a megelőzési stratégiával kapcsolatban.
  ° Hiányzó vagy minimális követelmények a válaszintézkedésekkel kapcsolatban.
  ° Nincs gyakorlati példa vagy esettanulmány.

Ezek az értékelési kategóriák segítenek az egyes dokumentumok hatékonyságának meghatározásában és az okosrepülőterek számára releváns információk, anyagok kiválasztásában, hogy hatékonyan kezelhessék az adott fenyegetéseket.

2. táblázat: Részletes absztrakciós szinttel rendelkező dokumentumok vizsgálata az azonosított fenyegetések tükrében

Forrás-dokumentum	**Hálózati és kommunikációs támadás és DDoS-támadás**	**Rosszindulatú szoftver**	**Repülőtéri eszközök manipulációs támadásai**	**Engedéllyel való visszaélés támadása**	**Social engineering és adathalász-támadások**
Elsődleges, könnyen hozzáférhető szabályok az információbiztonságért[1]	Kielégítően segít	Kielégítően segít	Kielégítően segít	Kielégítően segít	Kielégítően segít
Okosrepülőterek biztonsága[2]	Kielégítően segít	Kielégítően segít	Kielégítően segít	Kielégítően segít	Kielégítően segít
A légi forgalmi irányítás kiberbiztonsági érettségi modellje[3]	Részben segít	Részben segít	Részben segít	Részben segít	Részben segít
Kiberbiztonsági kultúra a polgári repülésben[4]	Részben segít	Részben segít	Részben segít	Részben segít	Kielégítően segít

Forrás: a szerző szerkesztése

[1] EASA 2023.
[2] ENISA 2018.
[3] Eurocontrol 2019.
[4] ICAO 2022c.

Mindkét dokumentum, amely egészében lefedi az egyes kihívásokat, olyan részletes és átfogó kontrollkörnyezetet tartalmaz, amelyek együttes alkalmazása csökkenteni tudja az egyes fenyegetések kockázatát, mivel fő céljuk egy kockázatokkal arányos védelem kialakítása a szervezeten belül. Ezért ezen dokumentumok olyan információbiztonsági folyamatok kialakítását teszik lehetővé, amelyekkel az egyes összekapcsolt rendszerek sebezhetőségeit, az azokat kihasználó fenyegetéseket már a kezdetekkor azonosítják. Így fel lehet mérni, kezelni lehet, illetve folyamatosan figyelemmel lehet kísérni a fenti fenyegetések kockázatát.

A légi forgalmi irányítás kiberbiztonsági érettségi modellje dokumentum célja a kiberbiztonsági érettségi szint vizsgálata; hasznos és részletes dokumentum, de egy okosrepülőtér inkább csak a meglévő folyamatai értékelésére tudja használni, nem pedig azok kialakítására. Csak részben tud segítséget nyújtani az azonosított kihívásokkal szemben.

A *Kiberbiztonsági kultúra a polgári repülésben* dokumentum hatókörében megemlíti a kockázatok és fenyegetések csökkentésének támogatását. Illetve azokat a főbb alapelveket fejti ki, amelyek alapján működtetni kell az információbiztonságot. Részben tud segíteni az egyes fenyegetések elkerülésében vagy gyors felismerésében. A social engineering és adathalász-támadások esetében megtörtént a lefedés, mivel ezen dokumentum a személyi állománnyal foglalkozik, és részletesebben taglalja a tudatosítás és oktatás fontosságát.

A vizsgálatok igazolják H2 hipotézisemet: Az okosrepülőket érő kiberbiztonsági fenyegetésekre léteznek olyan nemzetközi dokumentációk, amelyek tudnak segíteni a létesítmények üzemeltetőinek, hogy felkészüljenek a kihívásokra, illetve azok hatékony elhárítására.

Összegzés

A cikk azonosítja, hogy pontosan mit is nevezhetünk okosrepülőtérnek, leírja a létesítmények főbb funkcióját és az azokat kiszolgáló rendszerelemeket. A rendszerelemek esetében látható volt a nagyobb fokú összekapcsolódás és az IoT-eszközök szerepe. Azonosítottuk azokat a fenyegetési kategóriákat, amelyekkel szembe kell néznie egy okosrepülőteret üzemeltető személyzetnek. A fenyegetéseket elemezve az látható, hogy az SoS-architektúra miatt egy rendszer sérülékenysége hatással van az egész összekapcsolt architektúrára. Ez alapján a fenyegetések mind *airside,* mind *landside* oldali rendszerekben megjelennek. A kutatás azon témakört is vizsgálta, hogy az USA, az EU és nemzetközi szervezetek viszonylatában milyen dokumentumok reflektálnak a légi közlekedés kiberbiztonságára. 28 dokumentumot azonosítottunk, amelyek jogszabályokat, ajánlásokat, stratégiákat tartalmaznak. Az elemzésből kiderült, hogy a kiberbiztonság milyen absztrakciós szinten jelenik meg ezen dokumentumokban. A legtöbb azonosított dokumentum alapszintű, ezt követik az átfogó publikációk, az érintőleges, valamint részletes leírások azonos megoszlást mutattak. Ha az Egyesült Államok és az Unió viszonylatában vizsgáljuk meg a kérdéskört, az látható, hogy utóbbi jóval több és részletesebb dokumentumot bocsátott ki. Megvizsgáltuk a dokumentumok használhatóságát az egyes azonosított fenyegetésekkel kapcsolatban.

Az elemzésből az látható, hogy vannak olyan publikációk, amelyek teljes mértékben segítséget tudnak nyújtani az azonosított fenyegetések kezelésére. Mindezt egy olyan információbiztonsági menedzsmentrendszer kialakításával, amelyben minden biztonsági eljárás, legyen az folyamatbéli, fizikai vagy technológiai, középpontjában a kockázatokkal arányos védelem áll. Tehát a fent azonosított fenyegetéstípusokat az okosrepülőtereknek a kezdetektől figyelembe kell venniük a működésük során, így azok bekövetkezési kockázatát alacsonyan tudják tartani.

A TKP2021-NVA-16 számú projekt a Technológiai és Ipari Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP2021-NVA pályázati program finanszírozásában valósult meg. A publikáció az I. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencia előadása alapján készült.

Felhasznált irodalom

AC 119-1A – Operational Authorization of Aircraft Network Security Program.

Alansari, Zainab – Soomro, Safeeullah – Belgaum, Mohammad Riyaz (2019): Smart Airports: Review and Open Research Issues. In Miraz, Mahdi H. et al. (szerk.): *Emerging Technologies in Computing*. International Publishing: Springer, 136–148. Online: http://dx.doi.org/10.1007/978-3-030-23943-5_10

AlMashari, Reema et al. (2018): *IoT-based Smart Airport Solution.* 2018 International Conference on Smart Communications and Networking, 1–6. Online: http://dx.doi.org/10.1109/SMARTNETS.2018.8707393

Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete (2018. július 4.) a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről.

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

Az Európai Parlament és a Tanács 376/2014/EU rendelete (2014. április 3.) a polgári légi közlekedési események jelentéséről, elemzéséről és nyomon követéséről, valamint a 996/2010/EU európai parlamenti és tanácsi rendelet módosításáról és a 2003/42/EK európai parlamenti és tanácsi irányelv, valamint az 1321/2007/EK bizottsági rendelet és az 1330/2007/EK bizottsági rendelet hatályon kívül helyezéséről EGT-vonatkozású szöveg.

A Bizottság (EU) 2015/1998 végrehajtási rendelete (2015. november 5.) a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról.

A Bizottság (EU) 2017/373 végrehajtási rendelete (2017. március 1.) a légiforgalmi szolgáltatást/léginavigációs szolgálatokat és más légiforgalmi szolgáltatási hálózati funkciókat és azok felügyeletét ellátó szolgáltatókra vonatkozó közös követelmények meghatározásáról, valamint a 482/2008/EK rendelet, az 1034/2011/EU, az 1035/2011/EU és az (EU) 2016/1377 végrehajtási rendelet hatályon kívül helyezéséről, továbbá a 677/2011/EU rendelet módosításáról.

A Bizottság (EU) 2019/1583 végrehajtási rendelete (2019. szeptember 25.) a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról szóló (EU) 2015/1998 végrehajtási rendeletnek a kiberbiztonsági intézkedések tekintetében történő módosításáról.

A Bizottság (EU) 2022/1645 felhatalmazáson alapuló rendelete (2022. július 14.) az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek a 748/2012/EU és a 139/2014/EU bizottsági rendelet hatálya alá tartozó szervezetekre vonatkozó, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésével kapcsolatos követelmények tekintetében történő alkalmazására irányadó szabályok megállapításáról, valamint a 748/2012/EU és a 139/2014/EU bizottsági rendelet módosításáról.

A Bizottság (EU) 2023/203 végrehajtási rendelete (2022. október 27.) az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU és az (EU) 2015/340 bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet hatálya alá tartozó szervezetek, valamint a 748/2012/EU, az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU, az (EU) 2015/340 és a 139/2014/EU bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet hatálya alá tartozó illetékes hatóságok tekintetében a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésére vonatkozó követelmények tekintetében történő alkalmazására vonatkozó szabályok megállapításáról, valamint az 1178/2011/EU, a 748/2012/EU, a 965/2012/EU, a 139/2014/EU, az 1321/2014/EU és az (EU) 2015/340 bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet módosításáról.

A Bizottság (EU) 2023/1769 végrehajtási rendelete (2023. szeptember 12.) a légiforgalmi szolgáltatási/léginavigációs szolgálati rendszerek és rendszerelemek tervezésében vagy gyártásában részt vevő szervezetek jóváhagyására vonatkozó műszaki követelmények és igazgatási eljárások meghatározásáról, valamint az (EU) 2023/203 végrehajtási rendelet módosításáról.

Bestugin, A. R. et al. (2020): Advanced Automated ATC Systems. In *Air Traffic Control Automated Systems.* Singapore: Springer, 25–123. Online: https://doi.org/10.1007/978-981-13-9386-0_2

Blondel, Mathieu – Zintel, Michael – Suzuki, Hiroto (2015): *Airports 4.0: Impact of Digital Transformation on Airport Economics.* Online: www.adlittle.com/sites/default/files/viewpoints/2015-05-Arthur_D_Little_T_T-Impact_of_Digital_on_Airport_Business_Model.pdf

CANSO (2020): *CANSO Standard of Excellence in Cybersecurity.* Online: https://canso.fra1.digitaloceanspaces.com/uploads/2021/04/canso_standard_of_excellence_in_cybersecurity.pdf

CANSO (2021): *Air Traffic Management Cybersecurity Policy Template.* Online: https://canso.fra1.digitaloceanspaces.com/uploads/2021/04/air_traffic_management_cybersecurity_policy_template-EN.pdf
CISA (2015): *Transportation Systems Sector-Specific Plan – 2015.* Online: www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems
EASA (2023): *First Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645).* Online: www.easa.europa.eu/en/document-library/easy-access-rules/first-easy-access-rules-information-security-regulations-eu
ENISA (2018): *Securing Smart Airports. Available.* Online: www.enisa.europa.eu/publications/securing-smart-airports
Euorcontrol (2019): *ATM Cybersecurity Maturity Model Level 1.* Online: www.eurocontrol.int/sites/default/files/2019-09/atm-cybersecurity-maturity-model.pdf
FAA (2020): *Cybersecurity Strategy.* Online: www.faa.gov/sites/faa.gov/files/FAA_Cybersecurity_Strategy_PL_115-254_Sec509.pdf
FATTAH, Amir et al. (2009): *Smart Airports: Transforming Passenger Experience To Thrive in the New Economy.* Cisco Internet Business Solutions Group (IBSG). Online: www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf
HÄTTENSCHWILER, Nicole et al. (2018): Automation in Airport Security X-Ray Screening of Cabin Baggage: Examining Benefits and Possible Implementations of Automated Explosives Detection. *Applied Ergonomics, 72*, 58–68. Online: https://doi.org/10.1016/j.apergo.2018.05.003
H.R.302 – An act to provide protections for certain sports medicine professionals, to reauthorize Federal aviation programs, to improve aircraft safety certification processes, and for other purposes
IATA (2021): *Aviation Cyber Security Guidance Material Form.* Online: www.iata.org/en/programs/security/cyber-security/aviation-cyber-security-guidance-form/
IATA (2024): *Security Management System Manual (SeMS).* Online: www.iata.org/en/publications/store/security-management-system-manual/
ICAO (2019): *Aviation Cybersecurity Strategy.* Online: www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx
ICAO (2022a): *Presentation of 2022 Air Transport Statistical Results.* Online: www.icao.int/sustainability/WorldofAirTransport/Documents/ARC_2022_Tables_final_12032024.pdf
ICAO (2022b): *Cybersecurity Action Plan.* Online: www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx
ICAO (2022c): *Cybersecurity Culture in Civil Aviation.* Online: www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Culture%20in%20Civil%20Aviation.EN.pdf
ICAO (2022d): *Cybersecurity Policy Guidance.* Online: www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf
ICAO (2022e): *Guidance on Traffic Light Protocol.* Online: www.icao.int/aviationcybersecurity/Documents/Guidance%20on%20Traffic%20Light%20Protocol%20Policy.EN.pdf

Lykou, Georgia – Anagnostopoulou, Argiro – Gritzalis, Dimitris (2018): Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors,* 19(1), 19. Online: https://doi.org/10.3390/s19010019

Mantouka, Eleni et al. (2018): Gamification in Mobile Applications: The Case of Airports. *Journal of Intelligent Transportation Systems,* 23(5), 1–10. Online: https://doi.org/10.1080/15472450.2018.1473157

Marks, Adam – Rietsema, Kees (2014): Airport Information Systems—Airside Management Information Systems. *Intelligent Information Management,* 6(3), 149–156. Online: https://doi.org/10.4236/iim.2014.63016

Nau, Jean Baptiste – Benoit, Franck (2017): *Smart Airport: How Technology is Shaping the Future of Airports.* Online: https://wwa.wavestone.com/app/uploads/2017/12/Smart-Airport-2017.pdf

Presidential Policy Directive/PPD-21 – Critical Infrastructure Security and Resilience.

Rajapaksha, Aruna – Jayasuriya, Nisha (2020): Smart Airport: A Review on Future of the Airport Operation. *Global Journal of Management and Business Research,* 20(3), 25–34. Online: https://doi.org/10.34257/GJMBRAVOL20IS3PG25

del Río, José Sánchez et al. (2016): Automated Border Control E-Gates and Facial Recognition Systems. *Computers & Security,* 62, 49–72. Online: https://doi.org/10.1016/j.cose.2016.07.001

Sharkov, George (2017): A System-of-Systems Approach to Cyber Security and Resilience. *Information & Security,* 37, 69–94. Online: https://doi.org/10.11610/isij.3706

SITA (2023): *Air Transport IT Insights 2023.* Online: www.sita.aero/resources/surveys-reports/air-transport-it-insights-2023/

Tabares, Diego – Mora-Camino, Felix (2019): Aircraft Ground Operations: Steps Towards Automation. *CEAS Aeronautical Journal,* 10(3), 965–974. Online: https://doi.org/10.1007/s13272-019-00390-5

TSA (2018): *TSA Cybersecurity Roadmap.* Online: www.tsa.gov/sites/default/files/tsa_cybersecurity_roadmap.pdf

Wang, Le (2018): Application of Wireless Sensor Network and RFID Monitoring System in Airport Logistics. *International Journal of Online and Biomedical Engineering (iJOE),* 14(1), 89–103. Online: https://doi.org/10.3991/ijoe.v14i01.8058

Wittmer, Andreas (2011): Acceptance of Self-service Check-in at Zurich Airport. *Research in Transportation Business & Management,* 1(1), 136–143. Online: https://doi.org/10.1016/j.rtbm.2011.06.001

Yang, Shen (2010): *Architecture of Airport Operation Database System.* 2009 First International Conference on Information Science and Engineering, 2278–2281. Online: https://doi.org/10.1109/ICISE.2009.346

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 2. szám 149–163.
DOI: 10.32567/hm.2024.2.11

Surányi Zsolt Mihály,[1] Ollári Viktor Szilárd[2]

A medikai rendszer használatának infokommunikációs lehetőségei az első ellátás helyszínén

Information Communication Options for Using the Medical System at the Point of First Care

Absztrakt

A harctéri és katasztrófaelhárítási műveletek során kiemelten fontos a sérültek hatékony ellátása, amihez a műveleti területen alkalmazható medikai rendszerek nyújtanak nehezen helyettesíthető támogatást az egészségügyi állomány számára. Az újgenerációs IKT-technológiák integrálása nemcsak a medikai rendszerek alkalmazhatóságát növelhetik meg, de lehetőséget biztosítanak valós idejű, pontos és releváns metaadatokkal kiegészíteni a C2/C4ISR által generált információkat. A vonatkozó szakirodalom és szabályozók elemzése segítségével rámutatunk ezen technológiák fúziójának szükségességére, kitérve egyes alkalmazási és jövőbeni fejlesztési lehetőségekre.

Kulcsszavak: harcmező, kommunikáció, C4IS, digitalizáció, IT-hálózat

Abstract

Effective casualty care is of crucial importance in combat and disaster relief operations, and medical systems deployed in the field provide a vital support to medical personnel. The integration of next-generation ICT technologies not only enhances the operational utility of medical systems, but also enables the provision of real-time, accurate and relevant metadata

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: suranyizsolt1980@gmail.com
[2] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola.

to augment the information produced by C2/C4ISR. By analysing the relevant literature and regulators, the necessity of merging these technologies will be highlighted, together with specific possible future opportunities for their application and development.

Keywords: battlefield, communications, C4IS, digitalisation, IT network

Bevezetés

Napjainkban egyre több ország hadserege elkötelezett amellett (nem kivétel a NATO[3] sem), hogy a 21. századra jellemző technikai vívmányok okozta versenyben megtartsa a lépéselőnyt. Siposné és Szenes professzorok szerint 2014-ben lépett a Szövetség a negyedik fejlődési szakaszába, amely periódust *NATO 4.0*-ként neveztek el. Ezen időszakban a hidegháborús időszakhoz hasonló katonai védelmi és elrettentési feladatokkal kell(ett) szembenéznie a NATO-nak, ami az ukrán válság kialakulásához és az Iszlám Állam felemelkedéséhez köthető.[4]

A *NATO 2030 – Együtt egy új korszakért* című tanulmányban a Szövetség jelenlegi helyzetét értékelik, javaslatokat fogalmaznak meg a következő évtizedre várható kihívásokra, hogy azokra a Szövetség koncepcionális és tudatos választ adhasson mint katonai és politikai szervezet. Ebben a tanulmányban kijelentik, hogy az új technológiák egyértelműen megváltoztatják a hadviselés természetét, lehetségessé válnak a hiperszonikus támadások[5] és a hibrid hadműveletek.[6]

A 21. században nemcsak a civil oldalon, de a katonai területen is érezhető az információs eszközök dinamikus fejlődése. Kijelenthető, hogy egy modern szemléletű hadsereg működése elképzelhetetlen modern információtechnológiai (IT-) eszközök nélkül. Jobbágy szerint „a személyi állomány korszerű ismeretekkel történt kiképzése és felkészítése nélkül egy modern haderő nem képes megfelelő módon reagálni az újtípusú kihívásokra és fenyegetésekre, melyek a klasszikus hadszíntér helyett egyre inkább a digitális hadszíntéren öltenek testet."[7]

A digitális világban a katonák egészségügyi adatainak folyamatos elérése megkerülhetetlen igényként jelenik meg.

Jelen tanulmányban bemutatjuk a Magyar Honvédség által használt medikai rendszert (MedWorkS), rávilágítva annak harctéri/katasztrófaelhárítási műveletekben való alkalmazásának és az újgenerációs mobiltechnológiák integrálásának szükségességére, kitérve a medikai rendszerek és a C2/C4ISR megoldások fúziójában rejlő egyes lehetőségekre.

[3] North Atlantic Treaty Organization – Észak-atlanti Szerződés Szervezete.
[4] Szenes–Siposné 2019: 18–23.
[5] Hiperszonikus sebességgel (a hangsebesség többszöröse) repülő támadóeszköz, amelynek elfogása a hagyományos légvédelmi rendszerekkel rendkívül nehéz.
[6] NATO Secretary General 2020.
[7] Jobbágy 2017a: 203–213.

A harcmezőn történő digitális betegellátás alapjai

Már a 2000-es években megjelentek olyan mobil számítástechnikai megoldási kezdeményezések, amelyekkel csökkenteni lehet a harctéren végzett egészségügyi ellátások során vétett hibákat, egyúttal növelve a beavatkozások minőségét.

A BMIST[8] mobilalkalmazási csomag lehetővé teszi a felhasználók számára a kritikus egészségügyi információkhoz való hozzáférést, hatékony klinikai döntéstámogató eszközökkel segítve. Az ellátás megkezdésekor generálódik egy EHR,[9] amely szinkronizálódik az amerikai hadügy-minisztérium[10] által üzemeltetett egészségügyi felügyeleti és orvosi információs rendszerekkel az ellátás legkorábbi szakaszától kezdve a veterán adminisztráció[11] által nyújtott krónikus gondozásig. A fejlesztés konkrét célok alapján valósult meg: PDA[12] és vezeték nélküli interfész integrációja; a helyi alkalmazás és felhasználói felület fejlesztése; kommunikációs infrastruktúra és az adattároló, valamint visszakereső rendszer fejlesztése. Így a komplett rendszer messzemenően támogatja a longitudinális egészségügyi nyilvántartást a katonai egészségügyi rendszer minden elemében, annak teljes időspektrumán keresztül.[13] Török Péter[14] bemutatta, hogy több NATO-tagállam hadseregében jelenleg is zajlik a „digitális katona" eszközrendszereinek fejlesztése, amelyben már megjelenhet az egyéni harcos életfunkcióinak különböző módon történő monitorizálása és azon adatok továbbítása.

Jelenleg – a Magyar Honvédség által – használt medikai rendszer

A Magyar Honvédség Egészségügyi Központ szervezetéből 2023. január 1-jével kivált a Honvédkórház, így megszűnt hadrendi elem lenni. Új megnevezése: Észak-Pesti Centrumkórház-Honvédkórház, irányító szerve a Belügyminisztérium, fenntartó szerve pedig az Országos Kórházi Főigazgatóság lett.[15] A galvanikus szétválás lehetővé tette, hogy az addig medikai és STN-hálózati[16] tartományban üzemelő egészségügyi informatikai rendszer hálózati elérhetőségét egységesíteni lehessen.

A Magyar Honvédség egészségügyi szolgálata az Asseco Zrt. (Globenet üzletága) által – több mint 20 éve – kifejlesztett és azóta is folyamatosan megújuló MedWorkS medikai rendszerét használja, amely az Oracle adatbázis-technológián alapul.[17] Az integrált egészségügyi informatikai rendszer moduláris felépítésű, akár a felhasználó igényeire is szabható.

[8] Battlefield medical information system-tactical – BMIST (harctéri medikai információs rendszer).
[9] Electronic health record – EHR (elektronikus egészségügyi adatmezők együttese).
[10] U.S. Department of Defence – DoD (Amerikai Egyesült Államok Védelmi Minisztérium).
[11] U.S. Department of Veterans Affairs – VA (Amerikai Egyesült Államok Veteránügyi Minisztérium).
[12] Personal digital assistant – PDA (személyes digitális asszisztens – kisméretű mobil eszköz).
[13] Morris et al. 2006.
[14] Török 2021.
[15] 1997. évi CLIV. törvény (Eütv.) 244/C. §.
[16] Stacioner network – STN (kiépített, stacioner hálózat).
[17] Lásd: https://portal.vik.bme.hu/files/00003024.pdf

A MedWorkS alkalmazás nemcsak az egészségügyi ellátáshoz szükséges specifikus modulokkal rendelkezik (például labordiagnosztika, mikrobiológia, gyógyszertári, védőoltás-nyilvántartás stb.), hanem az egészségügyi intézmény adminisztratív működéséhez szükséges háttérmunkákhoz kapcsolódó rendszerekkel (például pénzügy, minőségirányítás, gazdálkodás, anyagigénylés) is képes együttműködni.

2023 decemberétől a MedWorkS alkalmazás kizárólag az STN-tartományban érhető el a megfelelő kliens segítségével. Ennek előnye, hogy a Magyar Honvédség jelenlegi külszolgálatainak helyszíneiről (Koszovó, Bosznia-Hercegovina) is lehetséges a medikai rendszerben az egészségügyi események rögzítése, vagy a beteg anamnéziséhez történő hozzáférés.

A missziókból a nagy távolságra telepített (tábori) vezetési pont – VSAT[18]-technológia – teszi lehetővé a stacioner hálózathoz vagy egyéb, a meghatározott rendszerekhez történő csatlakozást. Fizikai kialakításuk révén a műholdas rendszerek gyorsan, egyszerűen kiépíthetők. A tábori rendszerek mindezek eredményeképpen kormányzati és egyéb hálózatokra is tudnak csatlakozni, támogatva a hatékony harci vezetést és irányítást.[19]

Infokommunikációs kitekintés

A katonai és katasztrófavédelmi műveletek során egyaránt fontos, hogy a vezetési és irányítási feladatokért felelős entitások mindenre kiterjedő, időszerű, célirányosan szűrt és strukturált információkkal rendelkezzenek, beleértve az érintett műveletben részt vevő állomány bevethetőségét is. A harctéri egészségügyi ellátás infokommunikációs háttere *(is, az AJP-6-nak megfelelő)* stabil, mindemellett a műveleti helyzet (sok esetben volatilitású) változásaihoz adaptívan alkalmazkodó hírközlési ökoszisztémán kell hogy alapuljon. Mindemellett a katonai erők alkalmazása jelentős természeti és egyéb katasztrófák, terrorcselekmények következményeinek elhárítása során szükségszerűen indukálja a civil és katonai hírközlési rendszerek esetleges és célspecifikus összehangolhatóságát/irányított átjárhatóságát a válságkezelés hatékonyságának biztosítása érdekében.[20] Hazai környezetben a kormányzati kommunikációs rendszerek *(NTG, EDR, ZRH, Köznet, K-600/KTIR),* a Magyar Honvédség (MH KCEHH[21]), valamint a Vbö.[22] által szabályozott esetekben a BM szervezetek és a civil szféra infokommunikációs ökoszisztémái biztosíthatják a javasolt telemedicina-megoldás adatforgalmi igényének kiszolgálásához és vezetési és irányítási rendszerekhez történő integrálásához szükséges elektronikus hírközlési hátteret.[23] Nemzetközi vonatkozásban a TETRA alapú EDR, a már említett VSAT és adott missziók vonatkozásában az AJP-6 szerinti honvédelmi rendszerek biztosíthatják a szükséges együttműködési szintet.

[18] Very small aperture terminal – VSAT (nagyon kis átmérőjű antennával működő terminál).
[19] Szeleczki–Farkas 2022.
[20] Összhangban az AJP-3.19 és AJMedP-6 doktrínákkal.
[21] Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata, lásd Jobbágy 2017b.
[22] 2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról.
[23] Farkas 2020: 42–44.

5G mint lehetőség

Az 5G katonai alkalmazásának lehetőségeit aktívan vizsgálják úgy szövetségi, mint tagállami szinten a NATO érintett szervezetei. A NATO Szövetséges Transzformációs Parancsnokság 2023. évi TIDE Sprint[24] konferenciáján kifejezetten fókuszba kerültek az 5G egészségügyi és C2 *(vezetés és irányítás)* támogatási lehetőségei.[25] Kétségtelen, hogy a technológia szabványokban és a szabványosító testületek (például 3GPP, ETSI) által kibocsátott ajánlásokban lefektetett paraméterei alapján – *az ismert és lehetséges (kiber-) kockázatok kezelése mellett*[26] – optimális hatékonysággal támogathatja a hon-, rend-, katasztrófavédelem jelenleg alkalmazott infokommunikációs technológiai (IKT) ökoszisztémájának modernizálását. Az 5G-technológia támogathatja, egyebek mellett, a reziliens tábori hírközpontok és rádiós vezetési komplexumok kialakítását, de egyidejűleg a műveleti állomány „jóléti" szolgáltatásainak biztosítását is.[27] Mindemellett az 5G szerves interoperabilitást biztosíthat a polgári és katonai hírközlési rendszerek között úgy itthon, mint a missziók során; természetesen, figyelembe véve a műveleti körülményeket, valamint a fogadó ország(ok) egyes sajátosságait (például frekvenciakiosztás).[28]

Tekintettel az 5G integráló jellegére, nemcsak a válság- és katasztrófahelyzetek kezeléséért felelős vezetés támogatásában játszhat szerepet, de a jövőbeni harcállás-pontokkal szemben megfogalmazott követelmények (megnövelt ellenálló képesség, agilitás, adaptációs képesség) megvalósítását, valamint a Magyar Honvédség harcászati szintű képességei fejlesztését *(például interoperabilitás, C2, digitális katona)* is támogathatja.[29]

5G-technológiai áttekintés

A mobil IKT-k a 4G óta – amely globálisan tömegek számára tette lehetővé az internet közel helyfüggetlen elérését – jelentős, egyre növekvő potenciált képviselnek a kibertér ökoszisztémájában. Ahhoz, hogy az 5G-technológia jelentőségéről képet alkothassunk, tekintsük át röviden főbb jellemzőit! Szükséges az elején kiemelni, hogy az újgenerációs mobilkommunikációs hálózatok már inkább az informatikai hálózatok körébe sorolhatók, kiegészítve mindezt a szoftverizáció[30] és a virtualizáció[31] funkcióival.[32]

[24] A TIDE (think-tank for information decision and execution – információs döntéshozatal és végrehajtás agytröszt) Sprint a Szövetséges Transzformációs Parancsnokság éves rendezvénye, amelynek célja a védelmi, tudományos és ipari szféra képviselőinek bevonása a jövőbeni kihívások, az ezekre adható lehetséges válaszok, az interoperabilitást támogató megoldások feltérképezésébe. Alapvető cél a szervezet K+F+I-folyamatainak felgyorsítása, hatékonyságának növelése, a szövetségesek együttműködési kompetenciáinak erősítése.

[25] NATO TIDE Sprint 2023.

[26] ENISA 2019: 11–24; Pernik et al. 2021: 17–25; Lee et al. 2023: 17–22.

[27] Jobbágy 2017b: 233–235.

[28] Lee et al. 2023: 16, 31–33.

[29] Tóth–Farkas 2023: 62; Szeleczki–Farkas 2022: 78.

[30] Dedikált/célhardverek kiváltása szoftveres megoldásokkal.

[31] Hálózati funkciók szoftveres megsokszorozása, egy hardvererőforrás többszörös kiaknázása – azaz 5G esetében logikailag elkülönített hálózatok létrehozása egyazon hardveres alapon (Lásd ITU-T Y.3011 ajánlás).

[32] Tóth 2023: 79.

A mobilhálózatok kapcsán alkalmazott főbb mérőszámok (KPI)[33] megközelítéséből a 4G és az 5G közötti jelentős különbség az adatátviteli sebesség (egységnyi idő alatt átvitt adatmennyiség, mértékegysége: bit/másodperc) növekedésében, valamint a késleltetési idő (a hálózat két végponti készülékén megvalósuló akció és reakció közti időintervallum) csökkenésében érhető tetten; harmadik mérőszámként az 1 km^2 területen kiszolgált eszközök maximális száma jelenik meg.[34] Ezen képességek egyik alapja a „masszív MIMO technológia";[35] illetve az ezt kiaknázó, a mm-es tartományban *(Ka sávtól)*[36] értelmet nyerő úgynevezett nyalábformázás *(beamforming)*, amely a MIMO antennaelemek fizikai elmozgatása nélkül képes hullámnyalábok képzésére és ezek célirányos továbbítására a végponti (felhasználói) készülékek felé úgy, hogy adott tartományon belül annak mozgását is leköveti. Az 5G és utódgenerációi esetében a nagy pontosságú helymeghatározás, nagy sebességgel és/vagy nagy magasságban mozgó végponti készülékek kiszolgálása is jelentős szerepet kap. Az 1. táblázat kivonatos jelleggel mutatja be a generációváltások kvantitatív *(és utalás szinten kvalitatív)* jellemzőit.

1. táblázat: 5G- és 6G-mérőszámok összehasonlítása

	4G	**5G**	**6G**
Adatátviteli sebesség	1 Gbps	20 Gbps	1000 Gbps
Felcsatlakoztatható eszközök száma	100 000/km^2	1 000 000/km^2	100/m^3
Késleltetési idő	10 ms	1 ms	0,1 ms
Stabilitás *(rádiójel-átvitel)*	n/a	$1–10^{-5}$	$1–10^{-7}$
Mobilitás *(eszközkövetés)*	350 km/h	500 km/h	1000 km/h
Horizontális helymeghatározási pontosság	50 m	0,2 m	0,01 m
Vertikális lefedettség	n/a	300 m	10 000 m

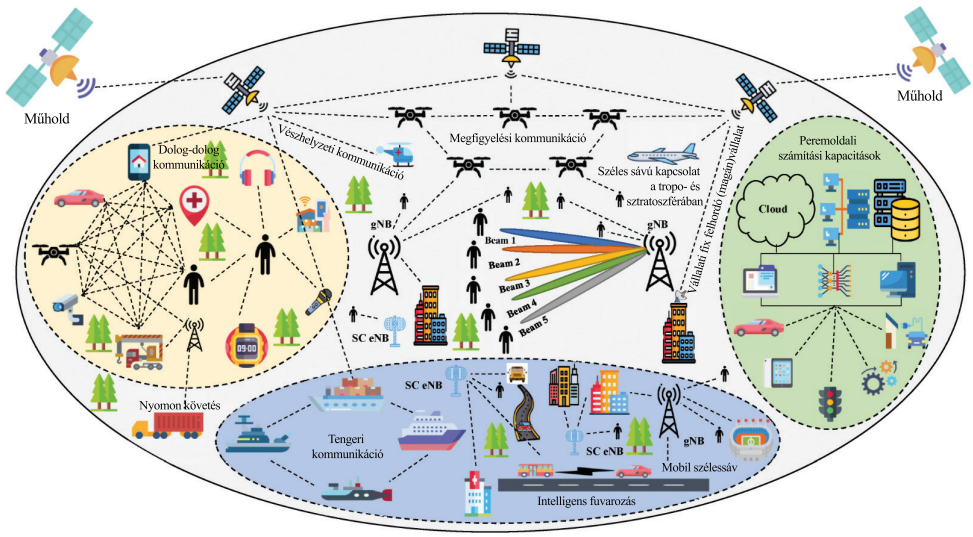
Forrás: 3GPP Műszaki jelentés 2022: 3GPP TR 21.916 V16.1.0. Lásd: www.3gpp.org/ftp/Specs/archive/21_series/21.916/21916-g10.zip

Mint az 1. táblázatból kitűnik, az újgenerációs mobil IK-technológiák képességportfóliója három jellemző köré csoportosítható:[37]

- nagyszámú felcsatlakoztatott IKT-megoldás *(idesorolva a gép-gép és IoT-kommunikációt)* kiszolgálása (mMTC),[38]
- nagysebességű adatátvitel (eMBB),[39]
- megbízható és egyben rövid késleltetési idejű kommunikáció (uRLLC).[40]

[33] Key performance indicators – KPI (kulcsfontosságú teljesítménymutatók).
[34] Tóth 2023: 54.
[35] Multiple-input multiple-output – nagyszámú antennaelem integrálása egy 5G-antennába.
[36] 26,5–40 GHz.
[37] Tóth 2023: 57.
[38] Massive machine-type communications – mMTC (masszív gépi típusú kommunikáció).
[39] Enhanced mobile broadband – eMBB (továbbfejlesztett mobil szélessáv).
[40] Ultra reliable low latency communications – uRLLC (ultramegbízható, alacsony késleltetésű kommunikáció).

Az újgenerációs mobil IKT-k szabványosítási folyamatai alapvetően olyan hálózat-topológiai megoldások kialakítását célozzák meg, amelyek a kommunikáció megszakítás nélküli továbbítását, a szolgáltatás „mindenütt jelen lévő" voltát biztosítják. Ezért a szabványalkotók alapvető elemként számoltak az üvegszálas gerinchálózatokkal,[41] a műholdas[42] és nagymagasságú *(18–22 km)* platformrendszerekkel (HAPS),[43] valamint a szolgáltatófüggetlen (MESH-jellegű ad hoc) hálózatokkal, WiFi-technológia integrálásával.



gNB = 5G bázisállomás (Next-Generation Node B)
SC eNB = kiscellás 4G bázisállomás (Evolved Node B)
BEAM = rádiónyaláb

1. ábra: 5G/6G ökoszisztéma

Forrás: www.mdpi.com/electronics/electronics-11-00121/article_deploy/html/images/electronics-11-00121-g001.png

Az újgenerációs mobilkommunikációs technológiák fejlődésének irányt szabó technológiai ajánlások *(például 3GPP, ETSI)* fejlődése, a szoftverfejlesztéshez hasonlatosan, mára egy kvázi „szerves", a verziók eredményeinek egymásra épülő fejlődési folyamatává vált. A vonatkozó szabványcsomag 18. verziójával kapcsolatos fejlesztések 2024 első negyedévében zárultak le. A 18-as verzió (Rel-18) fő irányai közt szerepelt, a teljesség igénye nélkül:

- a geostacionárius műholdak felvivőhálózati *(a végponti eszközök és a gerinchálózat közti adatátviteli platform)* alkalmazása;
- a nem földi IoT-kommunikáció kiszolgálásának fejlesztése;

[41] Farkas 2023: 24.
[42] Tóth 2023: 55.
[43] High altitude platform systems – HAPS (jellemzően drónokra/léghajókra telepített bázisállomások. Towers in the Skies 2021).

- az „IoT-magánhálózatok"[44] kialakításának lehetősége;
- az L *(1–2GHz)* és S *(2–4 GHz)* sávok alkalmazási lehetőségének integrálása az 5G-műhold-kommunikációba;
- az MI alkalmazási lehetőségeinek elemzése a szolgáltatásminőség/stabilitás és a helymeghatározás területein;
- a helymeghatározás centiméter-pontosságú *(vivő-fázis alapú)* technológiáinak integrálása – beleértve két végponti eszköz (mobiltelefon, jármű) relációkat is;
- az 5G-kommunikációban kiemelt jelentőségű időszinkronizáció ellenállóbbá tétele;
- kiterjesztett és kiegészített valóság (XR/AR) technológiák támogatásának megalapozása – beleértve a haptikus *(fizikailag megérinthető)* internet megvalósítását támogató immerzív, valós idejű kommunikáció alkalmazhatóságát;
- a (masszív) MIMO-funkció továbbfejlesztését (többek között) annak érdekében, hogy adott végponti eszköz kommunikációs igényét egyidejűleg több bázisállomás-antenna is kiszolgálhassa.[45]

Medikairendszer-specifikus 5G-lehetőségek

Úgy a katonai, mint a katasztrófavédelmi műveletek során egyaránt alapvető fontosságú, hogy az első ellátás helyén alkalmazott medikai rendszert kiszolgáló kommunikációs hálózat akkor is jelen legyen, ha a „békeidőszaki" hálózatokra az érintettek nem támaszkodhatnak. Az 5G „natív" és széles körű lehetőséget biztosít a műveleti területet például az STN-nel összekötő ad hoc hálózatok kialakítására, amely támaszkodhat a helyszínen tartózkodók *(5G-kompatibilis)* mobil földi és légi drón (UGV, UAV) egységeire, de akár HAPS és műholdas elemeket is bevonva az ökoszisztémába.

A drónok alkalmazásának lehetséges előnyei között említhető, hogy egyéb hasznos teher mellett *(hő-/kameramodul, radar, LiDAR akusztikus és egyéb szenzorok)* nemcsak rádiófrekvenciás, de például komplementer technológiaként az akár 100 Gbps adatátviteli sebességet biztosító, fényalapú kommunikációs (LiFi)[46] csatornán is kommunikálhatnak egymással, illetve a földi *(megfelelő kiegészítővel ellátott)* medikai rendszerrel. A jelenlegi technológiák mellett lehetséges olyan tanuló algoritmust futtató drónrajok alkalmazása, amelyek képesek akár önállóan is feltérképezni a műveleti területet, és önmagukat az optimális – *LiFi, illetve a mm hullámhosszú 5G-kommunikáció szempontjából kiemelten fontos* – rálátást és távolságot biztosító pozícióba manőverezni és ezt dinamikusan fenntartani.[47]

A földi műveleti egység követése biztosítható a medikarendszert futtató eszköz virtuális integrálásával a rajba mint „masterdrón";[48] illetve járművön/ruházaton/felszerelésen elhelyezett, kisteljesítményű gépilátás-technológiák segítségével, magas

[44] A felhasználó által létrehozott, az általa üzemeltetett eszközökből (okosotthon, testen hordott megoldások stb.) hálózat.
[45] 3GPP TR 21.918 V0.2.0 (2024-02).
[46] Light Fidelity, IEEE 802.11bb szabvány.
[47] Leichenko et al. 2024.
[48] Phadke–Medrano 2022.

hatékonysággal azonosítható vizuális azonosító *(például QR-kód)* alkalmazásával. Utóbbi esetben a drónraj „mindenkor aktuális master eleme"[49] azonosítja, és követi a vizuális azonosítóval *(például QR-kód, AprilTag,*[50] *ChromaTag*[51]*)* ellátott objektumot.[52] Katonai műveletek estében szükséges biztosítani, hogy a drónok mozgása kellően sztochasztikus legyen, nehezítve az ellátási hely beazonosítását, az optimális minőségű adatkapcsolat fenntartása mellett.

A lehetséges alkalmazási forgatókönyvek részletezésétől most eltekintve, szükséges hangsúlyozni, hogy amennyiben nem katonai művelet keretében alkalmazzák a katonai 5G-ökoszisztémát és/vagy nem katonai kommunikáció bevonása válik szükségessé, a megfelelő adatbiztonságot garantáló interfész és az adott műveleti környezetnek megfelelő egyéb intézkedések meghozatala, védelmi megoldások alkalmazása szükséges.[53]

Infokommunikációs összefoglaló

Az 5G szabványokban és műszaki ajánlásokban foglalt paraméterei alapján olyan kommunikációs ökoszisztéma kialakítását teszi lehetővé, amely ellenálló és adaptációs képességeit tekintve meghaladja az 1. táblázatban megjelenített KPI-ket, és interoperabilitás tekintetében jelentősen felülmúlja elődgenerációit; így *(szabványszinten)* megfelel az AJP6 doktrínában megfogalmazott tíz fő CIS[54] karakterisztikának. Az előző fejezetben említett, „LiFi" kompatibilis drónrajon alapuló ad hoc hálózati opció nemcsak a fényalapú kommunikációt, de a mm hullámhosszú *(nyalábképzésen alapuló)* jeltovábbítást is támogatja; mindkét eljárás magasabb *(de nem kikezdhetetlen)* védelmet biztosít az akaratlan és szándékos zavarások, illetve az adatszivárgás ellen. A vázolt, dinamikus 5G-ökoszisztéma stabil, biztonságos infokommunikációs alapot biztosíthat a medikai rendszerek kiszolgálásához, illetve az ebből származó adatok továbbításához a C2 megoldások számára.

Figyelembe véve, hogy jelen írás fókusza a katonai mellett kiterjed a katasztrófavédelmi és egyéb műveletek hírközlési támogatására – *amely szükségessé teheti egyéb szervezetek és kiemeleten civil mobilhálózatok bevonását* –, szükséges elmondani, hogy jelenünk globális 5G-ökoszisztémáját vizsgálva többen megállapítják, hogy az 5G bevezetése nem az előzetesen elvárt ütemben halad, jelentős „rés" alakult ki a szabvány szerinti lehetőségek/előírások és a felhasználók által tapasztalt szolgáltatásminőség között. Ennek okai között keresendő a „konzervatív" (4G-t utánzó) hálózatfejlesztés, amely nem biztosítja az 5G alapvető támogató technológiájának

[49] Misra et al. 2021.

[50] Az AprilTag vizuális azonosító (referenciaábra) rendszert kifejezetten a kiterjesztett valóság (XR) és a robotika sajátos igényeihez igazítva fejlesztették ki. A QR-kódhoz hasonló, de annál egyszerűbb azonosító ábrák gyorsan előállíthatók, és a kis számítási igényű (akár mobiltelefonon is futtatható) AprilTag érzékelőszoftver biztosítja a detektált címkék pontos 3D-pozíciójának meghatározását és a megjelölt eszköz/entitás azonosítását.

[51] A ChromaTag az AprilTag-hez hasonló elvet követ, de a színkontraszt folyamatba emelésével csökkenti a téves detektálások számát, lehetővé téve a „címke" jobb rejtését, diszkrét elhelyezését.

[52] Liang et al. 2020.

[53] Park 2024.

[54] Communication and information system – CIS (kommunikációs és információs rendszer).

(mm hullámhossz) alkalmazhatóságát; illetve az említett frekvenciatartomány jogi szabályozása a legtöbb államban kevéssé rendezett.[55] A 3,5 GHz környéki tartományok alkalmazása problematikus egyes Oroszországgal szomszédos országokban (például Litvánia), mivel a Föderáció továbbra is katonai (műholdas) kommunikációra használja azt. Az ukrán–orosz konfliktus, illetve a 2019-es Norvégiában megtartott Óramű hadgyakorlat idején tapasztalt GPS „anomáliák" ráirányítják a figyelmet arra, hogy a pusztán GPS-időszinkront alkalmazó 5G-hálózatok/annak egyes elemei megbéníthatók a GPS-jel kompromittálásával is.[56] Ezen körülményeket, különösen külföldi feladat-végrehajtások során, a hálózatbiztonság egyéb kérdései mellett, szükséges szem előtt tartani.

Jövőbe tekintés, mit hozhat a jövő…

A harcmezőn megjelenő – tableteken kezelhető – digitális egészségügyi alkalmazások használata nem csupán fikció manapság. A 2023 októberében kirobbant és azóta is tartó gázai konfliktusban már bizonyítottan használja az IDF egészségügyi szolgálata[57] ezen innovatív alkalmazást, amelynek célja, hogy forradalmasítsa a sérült katonákról szóló orvosi információk megosztását a csatatérről az egészségügyi ellátást végző kórházak irányába.

Az új alkalmazás tavaly novemberi bevezetése kiváltotta az eddig megszokott, az első ellátó által kézzel kitöltött űrlapokat és dokumentációkat. A terepen dolgozó egészségügyi személyzet által használt táblagépekre telepített alkalmazás lehetővé teszi a sérült egészségi állapotának és a megkezdett ellátás (kimentés, akut sürgősségi beavatkozás) tényének digitális rögzítését. Ezeket a létfontosságú adatokat azután NFC-kártyákon keresztül zökkenőmentesen továbbítják a sérült kiürítését végzőknek, majd a további ellátást végrehajtó egészségügyi intézmény irányába. Így biztosítva, hogy részletes és pontos egészségügyi információk kísérjék végig a sérült katonát az evakuálási folyamat során. Ez a digitális megoldás nemcsak a létfontosságú egészségügyi adatok átvitelét egyszerűsíti, egyben elősegíti a sérültek állapotváltozása miatt megkövetelt folyamatos osztályozást is, ezzel is növelve az ellátás hatékonyságát.[58]

A MedWorkS palettájában már megtalálható a MobiWorkS[59] vizittámogató alkalmazás, amely tableten keresztül kapcsolódik az integrált informatikai rendszerhez. A betegellátás során rögzített adatok folyamatosan frissülnek az ellátásra kerülő személy rekordjában, így minden egészségügyi esemény dokumentálása naprakész. Az alkalmazás megfelelő kiindulási alapot jelenthetne további fejlesztésre.

Ezen irányban elindulva megfontolandó lenne – az előre meghatározott igények alapján – egy konkrétan katonai vagy katasztrófavédelmi felhasználásra kifejlesztett modul létrehozása, amelyet az első ellátáskor használna a Magyar Honvédség vagy valamelyik társszervezet egészségügyi szolgálata.

[55] Koziol 2023.
[56] Lee et al. 2023: 11, 38.
[57] Israel Defense Forces Medical Corps – IDF (Izraeli Védelmi Erők egészségügyi hadtest/szolgálat).
[58] Yeshiva World News 2024.
[59] Lásd: https://asseco.hu/egeszsegugy/termekek/mobiworks/

A minél szélesebb körben történő felhasználás miatt nemcsak katonai műveletekre kellene szűkíteni a használhatóságát, hanem katasztrófavédelmi helyzetek vagy tömeges sérülésekkel járó káresemények felszámolására is alkalmassá kellene tenni a rendszer ezen elemét.

Infokommunikációs közeljövő

A középtávú infokommunikációs jövőkép (6G) alapvető elemei a műholdas[60] és nagymagasságú *(18–22 km)* platformrendszerek (HAPS),[61] a szolgáltatófüggetlen (MESH-jellegű ad hoc) hálózatok, a WiFi- és egyéb vezeték nélküli hálózatok, valamint az úgynevezett intelligens jeltükröző, -továbbító felületek (IRS[62]). A 6G, az ITU *(Nemzetközi Telekommunikációs Szövetség)* 2023 novemberében kibocsátott ajánlása *[ITU-R M.2160-0 (11/2023)]* szerint egy olyan elektronikus hírközlési ökoszisztéma, amely egyértelműen épít a jövő IT/IKT-megoldásainak szinergiájára. A vízió egy olyan (technológiai) világ képét vázolja fel, amelyben a Föld népességének túlnyomó része képes kapcsolódni egy fenntartható módon, magas biztonsági szint fenttartása mellett üzemeltetett kibertérhez.[63]

Mindezt egy olyan hálózat segítségével, amely transzparens, szabvány szerinti interfészekkel rendelkező rendszerelemekből épül fel, így biztosítva annak gyártófüggetlen kialakíthatóságát; valamint képes integrálni a korábbi generációk *(4G, 5G)* és egyéb kommunikációs technológiák hálózati szegmenseit is. Az ajánlásban prognosztizált technológiai trendek – *XR, ember-gép kooperáció, multiszenzoros (hang-, kép-, haptikus [például virtuális „fizikai" kezelőfelület], mozgásmintát azonosító) interfészek* – egy, a valós és virtuális világ szimbiotikus létezésén és egymásra hatásán alapuló jövőképet vetítenek elénk. A jelentős kiberbiztonsági kockázatok kezelése esetén megvalósítható az a műveleti helyzet, amelynél az adott műveletben részt vevő állomány testén, ruházatán, környezetében lévő IoT-megoldások (érzékelők), illetve a környezetét leképező megoldások (RADAR, LiDAR, audio érzékelők és vizuális képalkotók) révén valamennyi, az adott művelet szempontjából releváns személy azonnali, teljes körű, 3D-információt szerezhet az aktuális műveleti helyzetről. Mindezt úgy, hogy valójában a Föld bármely pontján tartózkodhat, a vizsgált eseménytől akár több tízezer kilométerre is. A 3D-jelleg azt is magában foglalja, hogy a megfelelő eszközökkel „testközelből" szemlélheti az eseményeket, saját élete, testi épsége veszélyeztetése nélkül. A medikai rendszerek vonatkozásában ez magával hozhatja azt is, hogy az ellátást a legjobb traumatológusok végezhetik, enyhe túlzással egy másik kontinensről irányítva egy megfelelő kialakítású medikai ellátó drónt. A hálózatok menedzselését túlnyomórészt (annak kiterjedése és komplexitása okán) az MI fogja

[60] Tóth 2023: 55.
[61] Liu et al. 2024.
[62] Intelligent reflecting surface – IRS (intelligens jeltükröző/továbbító felület).
[63] Security by design, blockchain alapú adatvédelem, natív védelmi kapacitások a DDOS és man-in-the-middle támadások ellen; automatikus önjavító kapacitások a természeti és ember okozta szolgáltatási zavarok azonnali kezelésére stb.

végezni; mindemellett a hálózat lehetőséget kínál MI-alapú szolgáltatások üzemeltetésére, igénybevételére.

Ez természetesen feltételezi az 5G-nél megkezdett, az ökoszisztéma felhőalapokra helyezésének kiteljesedését annak érdekében, hogy lehetséges legyen a számítási kapacitások allokálása fizikailag a lehető legközelebb a felhasználóhoz – kvázi „mindenhol jelen lévő" számítási kapacitást biztosítva számukra. Mindezek az ipar számára olyan erőforrást/lehetőséget kínálnak, amelyben az „éppen időben" *(just in time)* logisztikai stratégia minőségileg más értelmet nyer; hiszen az információ valós idejűen juthat el az azt igénylő entitáshoz/folyamathoz egy magas hatékonyságú, (végletekig) személyre szabott kiszolgálást biztosítva a megcélzott/igénylő végfelhasználó számára. A tervezett 3D-pozicionálás és leképezés *(integrált kommunikáció és érzékelés)* úgy az ipar, mint a közigazgatás entitásai és a végfelhasználók számára egyaránt a felhasználási lehetőségek széles körét kínálhatják fel. Szükséges rámutatni, hogy mindezen technológiák megvalósításának egyik elengedhetetlen feltétele a THz frekvenciák igénybevétele és hatékony alkalmazása; hasonlatosan az 5G-hez, amelynél a mm hullámhosszú spektrum[64] szerves alkalmazása elvárt lenne a szabvány szerinti minőségi elvárások optimális teljesítéséhez. Hasonlóan elkerülhetetlen az új típusú antennatechnológiák (extrém MIMO – E-MIMO) és antenna-ökoszisztémák (újrakonfigurálható intelligens felületek – RIS[65]) kifejlesztése és alkalmazása a 6G valós kapacitásainak biztosításához.[66]

Az ITU 6 kiemelt felhasználási szcenáriót vázol fel az ITU-R M.2160-0 (11/2023) ajánlásában. Ebből három az 5G-nél megjelenített forgatókönyvek továbbfejlesztett változata: *eMBB-ből Immerzív Kommunikáció (IC), uRLLC-ből hiperstabil és alacsony késleltetési idejű kommunikáció (HRLLC), mMTC-ből nagytömegű kommunikáció (MC); amelyeket kiegészít három új csoport: integrált MI és kommunikáció (IAAC), mindenhol jelen lévő kapcsolat (UC), integrált érzékelés és kommunikáció (ISAC)*.[67] Az egyes forgatókönyvek részletes ismertetését mellőzve, a 2. táblázat összefoglalóan bemutatja az IMT-2030 felhasználási forgatókönyveinek főbb sajátosságait.

Az ISAC vonatkozásában egyes jelenleg folyó kutatások, a „hagyományos" (időjárás, behatolás, elárasztás/árvíz stb.) érzékeléseken felül olyan információk begyűjtését is megelőlegezik, mint a „ruhán és takarófelületen átlátó" objektumdetektálás (fegyverérzékelés), autonóm (földi/légi/vízi) járművek közlekedésének monitorozása és irányítása (ütközési pályák detektálása), gyalogos és járműforgalom megfigyelése és menedzselése stb.[68]

[64] 30 GHz-től felfelé; frekvenciagazdálkodási gyakorlatban már ide sorolják az EU által kijelölt 24 GHz feletti tartományokat is.
[65] Reconfigurable intelligent surfaces – RIS (újrakonfigurálható intelligens felületek).
[66] ITU-R M.2160-0 (11/2023): 5–10.
[67] Singh et al. 2024.
[68] Strinati et al. 2024

2. táblázat: IMT-2030 forgatókönyvek

IMT-2030 (6G) forgatókönyv	**Főbb jellemzők**
Immerzív kommunikáció (IC)	A kommunikáció teljes spektrumát felöleli, a hangátviteltől a holografikus és/vagy multiszenzoros távoli jelenlétet biztosító szolgáltatásokig, beleértve a virtuális és valós objektumokkal folytatott interakciókat.
Hiperstabil és alacsony késleltetési idejű kommunikáció (HRLLC)	Elsődlegesen ipari és kritikusinfrastruktúra-menedzsment, egészségügyi felhasználások (stb.) stabil, extrém rövid késleltetési időt (lásd 1. táblázat) igénylő igényeinek kiszolgálását célozza.
Nagytömegű kommunikáció (MC)	Az IoT-megoldások számának drasztikus emelkedésére reagáló forgatókönyv (lásd 1. táblázat).
Mindenhol jelen lévő kapcsolat (UC)	Az elektronikus hírközlési technológiák teljes körének integrálását célzó forgatókönyv.
Integrált MI és kommunikáció (IAAC)	MI-képességek integrálása, valamint a számítási és MI-kapacitások hatékony, dinamikus allokálása, az ezekre épülő szolgáltatások (például autonóm járművek) támogatása.
Integrált érzékelés és kommunikáció (ISAC)	Multidimenzionális érzékelésen alapuló térinformációk biztosítása, hálózathoz nem csatlakozó objektumok/entitások vonatkozásában is, beleértve a mozgási/viselkedési sajátosságok detektálásának opcióját.

Forrás: ITU-R M.2160-0 (11/2023) alapján a szerző fordítása és szerkesztése

Mint a fent vázoltakból kitűnik, az újgenerációs mobilkommunikációs technológiák egy olyan komplex ökoszisztémát testesítenek meg, amely szinte korlátlan mennyiségű, közel teljes körű, számos dimenzióból megközelített/feldolgozott, releváns információ közel azonnali elérését biztosíthatja a felhasználó entitások számára. Mindezen képességek a medikai rendszerek teljesen új generációit alapozhatják meg, ahol már nemcsak az érintett központi adatbázisok válnak elérhetővé, de a kezelt személy testén (testében), ruháján elhelyezett érzékelők folyamatosan frissülő információkkal láthatják el úgy az egészségügyi állományt/mentést végzőket, mint a C2/C4ISR megoldásokat.

Összefoglaló

A tanulmány bemutatta a medikai rendszerek alkalmazásának jelenlegi formáit, szükségességét, jövőbeni lehetőségeit. Rámutatott arra, hogy az 5G-jellegű ökoszisztémák alkalmazása olyan rugalmasságot tehet lehetővé, ami biztosíthatja a vonatkozó doktrínákban lefektetett elvárosoknak való megfelelőséget.

Az újgenerációs mobilkommunikációs technológiák (5G/6G) teljesítik az AJP6 doktrínában megfogalmazott előírásokat. A megemlített kommunikációs technológiák (WiFi, LiFi, műhold stb.) integráló jellegükből fakadóan magas szintű rugalmassággal, egyes sajátosságaik révén magas (de nem kikezdhetetlen) védelmi szinttel rendelkeznek. Az 5G/6G olyan komplex ökoszisztémát képezhetnek, amelyek szinte korlátlan mennyiségű, közel teljes körű, számos dimenzióból megközelített/feldolgozott, releváns információ közel azonnali elérését biztosíthatják a felhasználó entitások számára,

továbbá lehetőséget nyújthatnak medikai rendszerek újgenerációinak kifejlesztésére, integrálva testen/testben/ruhaszövetben lévő érzékelőket az arra alkalmas rendszerekbe. Mindezekből fakadóan biztonságos infokommunikációs alapot biztosíthatnak a medikai rendszerek kiszolgálásához, illetve az ebből származó adatok továbbításához a C2/C4ISR megoldások számára.

Felhasznált irodalom

ENISA (2019): *EU-Wide Coordinated Risk Assessment of 5G Networks Security*. Online: https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

Farkas Tibor (2020): Védelmi infokommunikációs hálózatok és rendszerek – szakmai felkészítés. *Hadtudomány Szemle,* 13(1), 37–48. Online: https://doi.org/10.32563/hsz.2020.1.3

Farkas Tibor (2023): A kommunikációs és információs rendszerek értelmezése napjainkban: Követelmények és kihívások. In Tóth András (szerk.): Új típusú kihívások az infokommunikációban. Budapest: Ludovika, 11–30.

Jobbágy Szabolcs (2017a): A negyedik generációs hadviselés infokommunikációs aspektusai – fogalmi kitekintő. *Hadmérnök,* 12(1), 203–213. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/20888/171_16_jobbagy.pdf?sequence=1&isAllowed=y

Jobbágy Szabolcs (2017b): A Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata. *Hadmérnök,* 12(3), 223–236. Online: http://hdl.handle.net/20.500.12944/20889

Koziol, Michael (2023): 5G Networks Are Performing Worse, What's Going on? *IEEE Spectrum,* 2023. május 6. Online: https://spectrum.ieee.org/5g-rollout-disappointments

Lee, Mary et al. (2023): *Opportunities and Risks of 5G Military Use in Europe.* RAND National Security Research Divison. Online: https://doi.org/10.7249/RRA1351-2

Leichenko, Kyrylo et al. (2024): Deployment of a UAV Swarm-Based LiFi Network in the Obstacle-Ridden Environment: Algorithms of Finding the Path for UAV Placement. *Radioelectronic and Computer Systems,* 1, 176–195. Online: https://doi.org/10.32620/reks.2024.1.14

Liang, Xiao (2020): Moving Target Tracking Method for Unmanned Aerial Vehicle/Unmanned Ground Vehicle Heterogeneous System Based on AprilTags. *Measurement and Control,* 53(3–4), 427–440. Online: https://doi.org/10.1177/0020294019889074

Liu, Hongshan et al. (2024): Near-Space Communications: The Last Piece of 6G Space-Air-Ground-Sea Integrated Network Puzzle. *arXiv:2401.00283 [cs.IT].* Online: https://doi.org/10.48550/arXiv.2401.00283

Misra, Sudip et al. (2021): Dynamic Leader Selection in a Master-Slave Architecture-Based Micro UAV Swarm. *IEEE Global Communications Conference (GLOBECOM),* 1–6. Online: https://doi.org/10.1109/GLOBECOM46510.2021.9685538

Morris, Tommy J. et al. (2006): Battlefield Medical Information System-Tactical (BMIST): The Application of Mobile Computing Technologies to Support Health

Surveillance in the Department of Defense. *Telemedicine Journal and E-health,* 12(4), 409–416. Online: https://doi.org/10.1089/tmj.2006.12.409

NATO Secretary General (2020): *NATO 2030: United for a New Era – Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General.* Online: www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

NATO TIDE Sprint 2023. Online: www.act.nato.int/article/allied-command-transformation-hosts-2023-tide-sprint-events-to-promote-interoperability-between-allies/

Pernik, Piret et al. (2021): *Research Report Supply Chain and Network Security for Military 5G Networks.* Tallin: NATO CCDCOE. Online: https://ccdcoe.org/uploads/2021/10/Report_Supply_Chain_and_Network_Security_for_Military_5G_Networks.pdf

Phadke, Abhishek – Medrano, F. Antonio (2022): Towards Resilient UAV Swarms—A Breakdown of Resiliency Requirements in UAV Swarms. *Drones,* 6(11), 340. Online: https://doi.org/10.3390/drones6110340

Park, Hyun-A (2024): Secure Proxy Re-Encryption Protocol for FANETs Resistant to Chosen-Ciphertext Attacks. *Applied Sciences,* 14(2), 761. Online: https://doi.org/10.3390/app14020761

Singh, Rohit et al. (2024): Towards 6G Evolution: Three Enhancements, Three Innovations, and Three Major Challenges. *arXiv:2402.10781*. Online: https://doi.org/10.48550/arXiv.2402.10781

Strinati, Emilio Calvanese et. al (2024): Towards Distributed and Intelligent Integrated Sensing and Communications for 6G Networks. *arXiv:2402.11630.* Online: https://doi.org/10.48550/arXiv.2402.11630

Szeleczki Szilveszter – Farkas Tibor (2022): A Magyar Honvédség harcászati infokommunikációs hálózatainak korszerűsítési irányelvei. *Hadtudomány,* 32(1), 74–92. Online: https://doi.org/10.17047/HADTUD.2022.32.1.74

Szenes Zoltán (2021): Merre tovább, NATO? *Honvédségi Szemle,* 149(6), 3–19. Online: https://doi.org/10.35926/HSZ.2021.6.1

Szenes Zoltán – Siposné Kecskeméthy Klára (2019): *NATO 4.0 és Magyarország. 20 év tagság, 30 év együttműködés*. Budapest: Zrínyi.

Tóth András (2023): Az 5G-technológia jellemzői és a kialakításában rejlő kihívások. In Tóth András (szerk.): Új típusú kihívások az infokommunikációban. Budapest: Ludovika, 51–98. Online: https://real.mtak.hu/175140/

Tóth András – Farkas Tibor (2023): Opportunities and Directions for the Evolution of Command and Control Systems in the Context of Multi-domain Operations. *Vojenské reflexie,* 18(3), 59–73. Online: https://doi.org/10.52651/vr.a.2023.3.59-73

Török, Péter (2021): A Brief Overview of Digital Military Systems Used in the Armies of NATO Member Countries. *Nemzetbiztonsági Szemle,* 9(1), 56–70. Online: https://doi.org/10.32561/nsz.2021.1.4

Yeshiva World News (2024): IDF Launches Innovative App to Streamline Battlefield Medical Data Transfer to Hospitals. *Yeshiva World News,* 2024. február 4. Online: www.theyeshivaworld.com/news/israel-news/2258650/idf-launches-innovative-app-to-streamline-battlefield-medical-data-transfer-to-hospitals-see-dramatic-footage.html

HADMÉRNÖK
FÓRUM
19. évfolyam (2024) 2. szám 165–174.
DOI: 10.32567/hm.2024.2.12

Fári Márton[1]

Fenyegetés és elrettentés, különös tekintettel a kommunikációra az emberiség hajnalán

Threat and Deterrence, with Special Reference to Communication at the Dawn of Mankind

Absztrakt

Napjainkban a modern fenyegetési, elrettentési és kommunikációs eljárások ismerete és alkalmazása mind stratégiai, mind pedig taktikai szinten egyaránt természetesnek mondható hadművészeti szempontból. Ugyanakkor a szerző szerint fontos és érdekes tanulmányoznunk az emberiség hajnalán a fenti területeken eddig napvilágra került tudományos eredményeket, mivel azok számos tanulsággal szolgálhatnak napjainkban is.

Kulcsszavak: elrettentés, fenyegetés, őskor, kommunikáció, technológia, áttekintés, hadművészet

Abstract

Nowadays, the knowledge and application of modern threat, deterrence and communication techniques at both strategic and tactical levels can be taken almost for granted from a military-operational point of view. At the same time, the author believes that it is important to study the scientific results that have come to light in these fields since the dawn of mankind, as they can provide many lessons for today.

Keywords: deterrence, threat, prehistory, communication, technology, overview, art of war

[1] Okleveles történész, e-mail: fari.marton@spartan.hu

Bevezetés

Napjaink technológia uralta környezetében talán hajlamosak lehetünk csak a szuperszámítógépekre, a közösségi médiára[2] és – különösen napjaink biztonsági kihívásait vizsgálva – az egyes fegyveres konfliktusokban rejlő fenyegetésekre, valamint az elrettentésre gondolni. Könnyen belátható azonban, hogy a technológia[3] és bizonyos kommunikációs eljárások már *az emberiség hajnalán* kritikus szerepet játszottak a túlélésben és a társadalmi struktúrák, illetve a kultúra kialakulásában. Ez a tanulmány az emberi viselkedés, valamint a nyelvi készségek fejlődésének és a társadalmi rend fenntartásához szükséges fenyegetési és elrettentési mechanizmusoknak az összefüggéseit vizsgálja azzal a céllal, hogy egyrészt a magyar hadtudomány kultúrantropológiai területén meglévő eddigi ismereteket tovább gazdagítsa,[4] másrészt annak érdekében, hogy egy vonatkozó kutatás első elemeit megfogalmazza. Hadtudományi szempontból az is hangsúlyozandó, hogy Füzi szerint[5] az egyetemes és magyar hadművészet megismerő és feltáró jellegű törekvése alapján az ókortól napjainkig vizsgálja a katonai fenyegetés és elrettentés vonatkozó kérdéseit. De ha csak rövid történeti idősávokban gondolkozunk, akkor is könnyen találhatunk az előbb említett témakörökre számos példát az elmúlt másfél évszázadban. Megközelítésem módszertana és sarokköve multi- és interdiszciplináris jellegű, nemcsak azért, mert szakmai ismereteim is megkövetelik ezt, hanem azért is, mert elismert szakírók[6] is rögzítették már ennek szükségességét, de nehézségeit is. Az előbb említett szakember egy másik publikációjában[7] pedig azt mutatja be plasztikusan, hogy hogyan váltak az egyes technológiai, de különösen kommunikációs vívmányok napjaink hadviselésének szerves részeivé. Módszertanom az elérhető hazai és nemzetközi források elemzését csakúgy magában foglalja, mint azok kritikáját, így döntően megismerő, azaz kvalitatív. Az így kinyert ismereteket igyekszem lényegi csomópontokba rendezni, majd levonni a következtetéseket.

[2] Bányász 2020: 127.

[3] Technológia: Mindazon módszereknek és eszközöknek az ismertetése, amelyeknek segítségével a nyersanyag használati tárgyakká dolgozható fel. Lásd A magyar nyelv értelmező szótára, https://bit.ly/3MUktEh
Érdekes adalék, hogy a kifejezés az ókori görögöktől eredeztethető, ugyanis τεχνολογια < τεχνη „mesterség" + λογος „tan" + toldalék ια) az ember által készített olyan célszerű, az egyéni (emberi) képességeit megnövelő eszközökről (például gépek, anyagok és eljárások), valamint azok alkalmazásáról szóló ismeretek összefoglaló neve, amelyek segítségével az emberiség egyre többet tud megismerni, megváltoztatni, megőrizni stb. az őt körülvevő világból. Bérczi 1985. Az ókori görögök számára a technológia a művészetek és a kézművesség megvitatását jelentette. Woods–Woods 2000.

[4] Bakos–Jobbágy 2015; Jobbágy 2015.

[5] Füzi 1986.

[6] Németh 2019.

[7] Németh 2013.

Az emberiség hajnala[8]

Az emberi evolúció tudományterületének kétségtelenül leghíresebb képviselője a 19. században élt és alkotott angol természettudós, Charles Robert Darwin (1809–1882), akinek 1859-ben jelent meg *A fajok eredete* című munkája, amely bár nem lelt bizonyos körökben lelkes fogadtatásra, napjainkra az általa végzett alapkutatások alapozták meg azt, hogy a későbbi tudományos kutatások az „emberiség hajnala" koncepcióját megalkossák és az alábbiak szerint osszák fel.

A homininek megjelenése Wood és Lonergan szerint:[9] Az emberiség hajnala a hominin (azaz az emberfélék, beleértve az ember modern formáit és közvetlen ősét) megjelenésével kezdődik, ami körülbelül 6-7 millió évvel ezelőtt történt Afrikában. Ezek az ősi lények kezdetben hasonlítottak a mai nagy emberszabású majmokhoz, de két lábon jártak.

A Homo nemzetség fejlődése Antón, Potts, Aiello szerint:[10] Az emberiség hajnala fogalmába beletartozik a Homo nemzetség, beleértve a *Homo habilis* és *Homo erectus* fajokat, amelyek körülbelül 2,5 millió évvel ezelőtt jelentek meg. Ezek a fajok már fejlettebb eszközhasználatot és társadalmi viselkedésformákat mutattak.

A korai modern ember *(Homo sapiens)* megjelenése Hublin és társai szerint:[11] A korai modern *Homo sapiens* körülbelül 300 000 évvel ezelőtt jelent meg Afrikában, és azóta terjedt el világszerte, végül kiszorítva vagy beolvadva más, olyan korai emberfajokba, mint a neandervölgyi ember.

A kulturális innovációk időszaka McBrearty és Brooks szerint:[12] Az emberiség hajnala időszakát kulturális innovációk is jellemezték, mint például az eszközkészítés, tűzhasználat, nyelv és művészetek megjelenése, amelyek mind hozzájárultak az emberi társadalmak bonyolultabb szerveződéséhez.

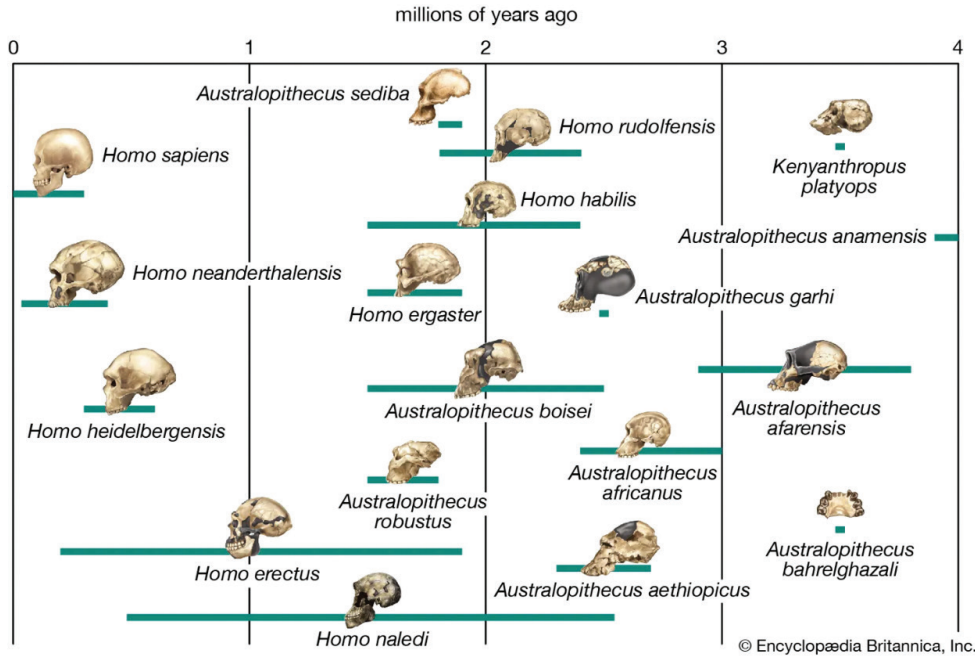
[8] Bár az „emberiség hajnala" kifejezés pontatlannak tűnhet, mégis ezt a kifejezést tartom célravezetőnek használni, tekintettel a területen jelenleg is zajló kutatásokra és a szinte naponta újabb archeológiai felfedezésekre. Úgy gondolom, hogy ez a megfogalmazás elég tág keretet biztosít számomra ahhoz, hogy a meglévő szakmai vitákat figyelembe véve legyen arra elegendő kutatási időintervallumom, hogy a már létező és elfogadott eredményeket bedolgozhassam publikációmba. Hozzáteszem, hogy az MTA Tudományági nómenklatúra besorolása szerint a Természettudományok területén belül a Biológiai Tudományok tudományág Evolúcióbiológia kutatási területéről beszélünk.

[9] Wood–Lonergan 2008.

[10] Antón–Potts–Aiello 2014.

[11] Hublin et al. 2017.

[12] McBrearty–Brooks 2000.



1. ábra: Az emberiség hajnalának időszakonkénti vizuális megjelenése az eddig feltárt fosszíliák alapján
Forrás: https://cdn.britannica.com/92/392-050-14244BE2/scheme-evolution-human-lineage-hominin-species-bars.jpg

Az emberi kommunikáció kialakulása

Ennél a témakörnél fontos előrebocsátanunk az Ausztráliai Múzeum munkatársának néhány fontos megállapítását:[13]

- Mivel a nyelv nem tud „megkövesedni", a tudósoknak pusztán közvetett bizonyítékokra kell támaszkodniuk, amikor megpróbálják meghatározni őseink nyelvi és beszédkészségét. A nyelv kialakulásának idejéről két fő nézet létezik:
  - Egyes tudósok úgy vélik, hogy a nyelv hirtelen alakult ki, és csak a saját fajunkra korlátozódik.
  - Mások azt állítják, hogy a nyelv lassan fejlődött ki az elmúlt 2 millió év során, és nem korlátozódott a saját fajunkra.

Az előbbi nézetet támogatók a nyelvhasználattal kapcsolatos viselkedés régészeti bizonyítékaira összpontosítanak. E bizonyítékok nagy része csak az elmúlt 40 000 évre nyúlik vissza, és magában foglalja a rendkívül összetett eszközök gyártását, a szimbolikus művészet előállítását és a kiterjedt kereskedelmi rendszerek létezését. A másik nézetet támogató szakemberek azt állítják, hogy a nyelv lassan fejlődött ki,

[13] Dorey 2020.

és a csontvázmaradványokra, illetve a beszédprodukcióval kapcsolatos szerkezetek bizonyítékaira alapozzák érvelésüket. A beszélt nyelvvel kapcsolatos bizonyos fizikai jellemzők, mint például a hangszalagok elhelyezkedése, az agy szerkezete és a gerincvelő mérete, fokozatosan alakultak ki a modern emberi formává. Ezek a bizonyítékok a nyelv és a beszéd képességének idővel történő növekedésére utalnak.

Az emberi kommunikáció története az ősi időkben kezdődött, amikor a korai emberek először kezdtek jelzéseket és gesztusokat használni, hogy ötleteket és érzéseket közvetítsenek egymásnak. Ezek a korai kommunikációs formák elsősorban nonverbális eszközök voltak, amelyek kritikus szerepet játszottak az emberi csoportok együttműködésében és túlélésében is. Ezek a kommunikációs formák segítették az egyedek közötti együttműködést és a konfliktusok elkerülését, valamint a csoporton belüli hierarchia kialakítását. Ezek a kommunikációs formák akkor így jelenhettek meg:

- A mimika, testtartás és a különböző hangok használata alapvető szerepet töltöttek be az érzelmek és szándékok kifejezésében. Ekman és Friesen szerint[14] az arckifejezések egyetemesek és kulturális határokon átívelően értelmezhetők, ami arra utal, hogy ezek a kommunikációs formák mélyen gyökereznek az emberi evolúcióban, ahogyan *a gesztusok* is, hiszen a kézmozdulatok és a test pozíciói segítettek bonyolultabb üzenetek átvitelében még a beszéd kialakulása előtt. McNeill szerint[15] a gesztusok szerves részét képezik az emberi kommunikációnak, és elengedhetetlenek voltak az első nyelvi rendszerek kialakulásához.
- A korai emberi kommunikációban a hangok és intonációk használata is kulcsfontosságú volt.[16] A hangmagasság és a hangerő változtatása segített az üzenetek sürgetőségének vagy fontosságának hangsúlyozásában. Andrew kutatásai[17] rámutattak, hogy a primátok kommunikációs technikái között szerepelnek a specifikus hangképzési minták, amelyek hasonló funkciókat látnak el, mint az emberi intonációs minták.

Őseink művészete mint lehetséges bizonyíték

A 2. ábrán látható barlangrajzon jól kivehetők az őseink által használt, zsákmányállatok elejtésére szolgáló kézifegyverek. Álláspontom szerint ez nemcsak azt bizonyítja, hogy képesek voltak összehangoltan tevékenykedni, amihez a hatékony kommunikáció elengedhetetlen, hanem azt is, hogy ismerték és használták azokat a technikákat, amelyek az állatok elejtéséhez és húsuk feldolgozásához nélkülözhetetlenek voltak. Ráadásul az eszközökhöz szükséges ragasztóanyagok elkészítése és összetételük szükség szerinti módosítása is olyan komplex kognitív készségekre és képességekre világít rá,[18] ami alapján joggal feltételezhetjük, hogy őseink e technológiai folyamatok szerves részeként is képesek voltak kommunikációra.

[14] Ekman–Friesen 1969.
[15] McNeill 1992.
[16] Ti. az intonáció a természetes emberi nyelv legbonyolultabb eszköze, amelynek jellemzőit Péter 1991 szerint számos vita övezi.
[17] Andrew 1963.
[18] Schmidt 2024.

2. ábra: Korai őseink egyik fennmaradt barlangrajza
Forrás: www.discovermagazine.com/the-sciences/did-ancient-humans-ever-go-to-war-with-neanderthals

A fenyegetés[19] mint kommunikációs eszköz

A fenyegetési viselkedés az emberi kommunikációs stratégiák között különleges helyet foglal el. Különösen így volt ez az emberiség hajnalán, amikor a verbális nyelv még nem volt teljesen kifejlett. Fenyegetési viselkedések révén az egyedek képesek voltak erőforrásokat megszerezni, dominanciát kialakítani és társadalmi konfliktusokat rendezni. Az általam vizsgált szakirodalom alapján a korai emberi csoportokban a fenyegető viselkedésre vonatkozóan az alábbi csoportosítás funkcióit és formáit a rangsor és az erőforrások elosztásának szabályozására használták. Az antropológiai kutatások, mint amilyen Blurton Jones munkája is,[20] bemutatják, hogy a fenyegetési magatartás hogyan játszott szerepet a társadalmi hierarchiák kialakításában és fenntartásában. Ezeket alapvetően két nagy csoportba sorolhatjuk.

[19] „A fenyegetés a lehetséges veszélyek legmagasabb megnyilvánulási szintjét képviselő helyzetek, állapotok és folyamatok összessége". *Közszolgálati Online Lexikon,* https://lexikon.uni-nke.hu/szocikk/fenyegetes/
[20] Blurton Jones 1987.

Dominancia kialakítása és fenntartása

A dominancia kialakításában a fenyegetési viselkedés az egyik legfontosabb eszköz volt. Az egyedek, akik képesek voltak hatékonyan fenyegető viselkedést bemutatni, gyakran szereztek magasabb státuszt a csoportban. A 2006-os Sapolsky-kutatás szerint ezek a viselkedések korrelálhatnak a stresszhormonokkal, ami befolyásolja az egyedek fiziológiai állapotát és társadalmi kapcsolatait.

A fenyegetés és az alárendeltség jelei

A fenyegetési viselkedés nemcsak a dominancia kialakítására szolgált, hanem az alárendeltség jeleinek kommunikálására is. Az alárendelt egyedek gyakran használtak specifikus gesztusokat és testhelyzeteket, hogy elkerüljék a konfliktust és csökkentsék a támadás esélyét. Keddy-Hector szerint[21] az alárendeltség jeleinek megértése kulcsfontosságú az állati viselkedés és az emberi szociális dinamikák tanulmányozásában.

Az elrettentés[22] mint viselkedési forma az emberiség hajnalán

Az őskorban az elrettentés mint viselkedési forma már jelen volt, bár megjelenésének módjai és mechanizmusai eltértek a későbbi, fejlettebb civilizációs formáktól. Ezek a korai elrettentési formák gyakran összefüggtek az alapvető túlélési ösztönökkel és a társadalmi struktúrák kezdetleges kialakulásával. Idesorolhatók Earle, valamint Vanhaverbeke, Hartley és Kennedy, továbbá O'Shea és McHale Milner munkái,[23] akik szerint az alábbiakról beszélhetünk.

Területi elrettentés. Az ősemberközösségek gyakran használtak területi jelzéseket, például faágak vagy kövek elrendezését, hogy megjelöljék saját területeiket, és elrettentsenek más csoportokat a behatolástól. Ez a viselkedés nemcsak az emberekre, hanem számos más állatfajra is jellemző, amelyek szintén területi határokat hoznak létre, és védik azokat.

Fizikai megjelenés és „mutasd magad nagyobbnak". Az őskori emberek és elődeik, mint például a neandervölgyiek, gyakran alkalmazták a „mutasd magad nagyobbnak" stratégiát ellenséges csoportok vagy ragadozók elrettentésére. Ez magában foglalhatta a testük felfújását, hangos kiáltásokat vagy csoportos megjelenést, hogy nagyobbnak és fenyegetőbbnek tűnjenek.

[21] Keddy-Hector 1992.

[22] Az elrettentést a biztonságpolitikai tudományterület, így a hadtudomány is számontartja. Amennyiben azt a katonai hatalomhoz sorolja, akkor „A katonai hatalom mások magatartásának befolyásolása fegyveres erő alkalmazásával vagy az azzal való fenyegetéssel. A fegyveres erőszak alkalmazásának lényege a másik magatartására gyakorolt hatás, nem pedig az erőszakkal okozott veszteség vagy kár. A kívánt hatást a további erőszak kilátásba helyezése éri el, társulva azzal a biztosítékkal, hogy az erőszakot alkalmazó fél akaratának teljesítése esetén az erőszak elkerülhető. A katonai erő funkciói közül az elrettentés és a kényszerítés gyakorol hatást az ellenség szándékaira. A védelem nem az ellenség szándékaira, hanem képességeire irányul: az elrettentés célja, hogy az ellenség tartózkodjon a cselekvéstől." In *Közszolgálati Online Lexikon.*

[23] Earle 2000; Vanhaverbeke 2005; Hartley–Kennedy 2013; O'Shea – McHale Milner 2002.

Agresszív demonstrációk. Az őskori csoportok néha demonstratív agressziót alkalmaztak, hogy elijesszék az ellenségeket vagy versenytársakat. A taktika magában foglalhatta a fegyverek, mint kőbalták és lándzsák bemutatását, ami szimbolizálta a csoport harci készségét és képességét az erőszak alkalmazására.

Szociális szabályok és tabuk. Bár kevésbé dokumentáltak, bizonyos szociális szabályok és tabuk, amelyeket az őskori emberi csoportok követtek, szintén funkcionálhattak elrettentési eszközként. Ezek a szabályok segíthettek a belső csoporton belüli rend fenntartásában, és elrettentették az egyéneket a tiltott viselkedéstől, amely veszélyeztetheti a csoport túlélését.

Pszichológiai elrettentés. Az ősemberközösségekben a pszichológiai elrettentés is jelen lehetett, például a hiedelmeken és spirituális gyakorlatokon keresztül. A természeti jelenségekhez és a halálhoz kapcsolódó mítoszok és rítusok révén a csoportok képesek lehettek fenntartani a rendet és elrettenteni az egyéneket a szociális normák megsértésétől.

Összegzés

A fentieket összegezve úgy vélem, hogy a jelenlegi tudományos ismereteink tükrében kijelenthető, hogy mind a kommunikáció, mind az ezekhez kapcsolódó technológia csírái megjelentek az emberiség hajnalán. Az is megállapítható, hogy ezek más-más ütemben fejlődhettek az egyes történeti időszakokban, azonban az nagy bizonyossággal kijelenthető, hogy őseink felhasználták ezeket aktuális céljaik, de összességében véve a túlélésük és fennmaradásuk érdekében. A tárgyalt témát övező archeológiai viták teljesen természetesnek mondhatók, bár ezen a területen is szinte naponta jelennek meg jelentős, új felfedezések és tudományos eredmények, különös tekintettel az ultramodern archeológiai technológiák fejlesztésének és alkalmazásának köszönhetően. A fentiek alapján észszerű és megalapozott következtetésem az is, hogy őseink ebben a kritikus fejlődéstani időszakban is alkalmazták a kommunikáció egyes formáit a túlélés érdekében, ami megnyilvánulhatott az elrettentés és a fenyegetés egyes korai formáiban és eljárásaiban is. Mivel korai őseink kisebb csapatokba verődve vándoroltak, így akár az is elképzelhető, hogy egyes csoportok idővel összehangolták kommunikációs és elrettentési képességeiket. Ugyanakkor hiba lenne a mai hadtudományi gondolkodásunk egészét kivetíteni a tárgyalt időszakra, hiszen az akkori tér- és időérzékelés teljesen más volt, mint napjainkban. Vélhetően a kis csoportokban mozgó őseink adott esetben jobbnak láthatták a direkt konfrontáció elkerülését, hiszen ehhez egyrészt elegendő tér állt rendelkezésükre, másrészt a túlélés elsődleges szempontjai vezérelték őket. Ez persze nem jelenti azt, hogy nem kerültek egymással valamilyen kapcsolatba.

Felhasznált irodalom

Andrew, R. J. (1963): The Origin and Evolution of the Calls and Facial Expressions of the Primates. *Behaviour,* 20(1–2), 1–107. Online: https://doi.org/10.1163/156853963X00220

Antón, Susan C. – Potts, Richard – Aiello, Leslie C. (2014): Evolution of Early Homo: An Integrated Biological Perspective. *Science,* 345(6192):1236828. Online: https://doi.org/10.1126/science.1236828

Bakos Csaba – Jobbágy Zoltán (2015): Explaining the Evolutionary Dynamics of an Insurgency: T. E. Lawrence and the Art of Tribal Warfare. *AARMS,* 14(1), 91–99. Online: https://doi.org/10.32565/aarms.2015.1.8

Bányász Péter (2020): *Közösségi média és közszolgálat.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet. Online: https://bit.ly/4gCkMRE

Bérczi Szaniszló (1985): *Anyagtechnológia I.* Egyetemi jegyzet. Budapest: Tankönyvkiadó.

Blurton Jones, Nicholas G. (1987): *Társadalom, konfliktus és az emberi viselkedés evolúciója.* Cambridge University Press.

Dorey, Fran (2020): *How Do We Know if They Could Speak?* Australian Museum. Online: https://australian.museum/learn/science/human-evolution/how-do-we-know-if-they-could-speak/

Earle, Timothy (2000): Archaeology, Property, and Prehistory. *Annual Review Of Anthropology,* 29, 39–60. Online: https://doi.org/10.1146/annurev.anthro.29.1.39

Ekman, Paul – Friesen, Wallace V. (1969): *Az arckifejezések nemzetközi repertoárja.* Prentice-Hall.

Hartley, Ralph J. – Sharon, L. Kennedy (2013): *Claiming/Re-claiming Space with Place-marking in Rural and Urban Landscapes.* XXV Valcamonica Symposium Papers. Online: www.ccsp.it/web/SITOVCS2013/programma%20e%20pdf%20vari/PDF%20x%20sito%20web/Hartley%20&%20Kennedy.pdf

Hublin, Jean-Jacques et al. (2017): New Fossils From Jebel Irhoud, Morocco and the Pan-African Origin of Homo Sapiens. *Nature,* 546, 289–292. Online: https://doi.org/10.1038/nature22336

Jobbágy Zoltán (2015): A háború antropológiája: primitív hadviselés, gerilla hadviselés és a szövetséges összhaderőnemi műveletek sikere. *Hadtudomány,* 25(e-szám), 67–78. Online: https://doi.org/10.17047/HADTUD.2015.25.E.67

Keddy-Hector, A. (1992). Alárendeltség és szociális stressz. *Annual Review of Ecology and Systematics,* 23, 231–253.

McBrearty, Sally – Brooks, Alison S. (2000): The Revolution That Wasn't: A New Interpretation of the Origin of Modern Human Behavior. *Journal of Human Evolution,* 39(5), 453–563. Online: https://doi.org/10.1006/jhev.2000.0435

McNeill, David (1992): *Hand and Mind: What Gestures Reveal about Thought.* University of Chicago Press.

Németh József Lajos (2013): A (stratégiai) kommunikáció és a háború kapcsolata napjaikban. *Hadtudomány,* 2013(1–2), 129–139. Online: www.mhtt.eu/oldsite/hadtudomany/2013/1_2/HT_2013_1-2_Nemeth_Jozsef.pdf

Németh József Lajos (2019): A stratégiai kommunikáció interdiszciplináris megközelítésben. *Hadtudományi Szemle,* 12(1), 167–174. Online: http://dx.doi.org/10.32563/hsz.2019.1.11

O'Shea, John M. – McHale Milner, Claire (2002): Material Indicators of Territory, Identity, and Interaction in a Prehistoric Tribal System. In Parkinson, William A. (szerk.): *The Archaeology of Tribal Societies.* Berghahn Books, 200–226. Online: https://doi.org/10.2307/j.ctv8bt29z.15

Péter Mihály (1991): Az érzelemkifejező intonáció nyelvi státusáról. In *Studia in Honorem Andreae O. Vértes Oblata a Collegis et Discipulis.* Magyar Fonetikai Füzetek 23. Budapest: MTA nyelvtudományi Intézete, 132–140. Online: https://adt.arcanum.com/hu/view/MTA_MagyarFonetikaiFuzetek_1991_23/?pg=2&layout=s

Sapolsky, Robert M. (2006): A stressz, az állapot és a fenyegető viselkedés kapcsolata. *Hormones and Behavior,* 50(4), 539–550.

Schmidt, Patrick et al. (2024): Ochre-Based Compound Adhesives at the Mousterian Type-Site Document Complex Cognition and High Investment. *Science Advances,* 10(8). Online: https://doi.org/10.1126/sciadv.adl0822

Vanhaverbeke, H. Waelkens (2005): Territoriality and Social Change in Prehistoric Communities. A Case-Study From the Burdur Plain (Anatolian Lake District). *Aegean Archaeology,* 7, 13–37.

Wood, Bernard – Lonergan, Nicholas (2008): The Hominin Fossil Record: Taxa, Grades and Clades. *Journal of Anatomy,* 2008. április 1. Online: https://doi.org/10.1111/j.1469-7580.2008.00871.x

Woods, Michael – Woods, Mary B. (2000): *Ancient Communication: From Grunts to Graffiti. (Ancient Technology).* Runestone Publishing.

Tartalom