HADMÉRNÖK

Katonai műszaki tudományok online folyóirata

14. évfolyam 3. szám • 2019

IMPRESSZUM

Hadmérnök
Katonai műszaki tudományok online folyóirata
ISSN 1788-1919

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: http://hadmernok.hu

Kiadó
Ludovika Egyetemi Kiadó Nonprofit Kft.
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu
A kiadásért felel: Koltányi Gergely ügyvezető igazgató
Olvasószerkesztő(k): Balla Nóra, Gergely Zsuzsanna

Tartalom

HADMÉRNÖK
BIZTONSÁGTECHNIKA

14. évfolyam (2019) 3. szám 5–11.
DOI: 10.32567/hm.2019.3.1

Berek Lajos,[1] Hódosi Viktória[2]

Veszélyes objektumok biztonsági rendszereinek ellenőrzése

Inspection of the Security Systems of Dangerous Facilities

Jelen cikk a személy- és vagyonvédelem területén a veszélyes objektumok vagyonvédelmi rendszereinek ellenőrzési módszereit vizsgálja. A veszélyes objektumok besorolásuk – azaz funkciójuk, elhelyezkedésük, veszélyeztetettségi fokuk – alapján különbözők lehetnek.

Kulcsszavak: **veszélyes objektumok, vagyonvédelmi rendszer, ellenőrzés**

A good working security system needs all its components to work perfectly. After a design process, the system maintenance takes place. In some special facilities, the security systems need more attention. The inspections and maintenance can be different.

Keywords: **security, inspection, maintenance**

Bevezetés

A vagyonvédelem egyik meghatározó területe az objektumvédelem. Az objektumok fajtái, funkciói, elhelyezkedésük, veszélyeztetettségük különbözők lehetnek. Az objektumoknak van egy olyan része, amely veszélyeztetett, tehát azért kell őrizni és védeni, hogy az biztonságosan elláthassa rendeltetésszerű feladatát. Ugyanakkor ezeknek van egy olyan csoportjuk, amely amellett hogy veszélyeztetett, önmaga is veszélyeztethet. Ez utóbbi az objektumok közül kevesebb, azonban mivel az ott lévő anyagok, eszközök, maga a rendeltetésszerű működés sérülése jelentős – gyakran

[1] Óbudai Egyetem, egyetemi tanár, e-mail: berek.lajos@uni-nke.hu, ORCID: https://orcid.org/0000-0003-1705-1173
[2] Óbudai Egyetem, Biztonságtudományi Doktori Iskola, doktorandusz, e-mail: viktoria.hodosi@gmail.com, ORCID: https://orcid.org/0000-0002-4932-6939

környezeti – hatást válthat ki, ezért kiemelt fontossággal kezelendő. Ezek a létesítmények speciális vagyon- és életvédelmi megoldásokkal kötelesek szavatolni az emberi élet, egészség és környezet sérülésmentességét. Ezért rendszereik tervezése, kialakítása valamint karbantartása kiemelt figyelmet kell, hogy kapjon. A cikkemben a veszélyes objektumok biztonsági rendszereinek ellenőrzésével kívánok foglalkozni.

Veszélyes objektumok

A személy- és vagyonvédelem vonatkozásában elmondható, hogy léteznek olyan speciális objektumok, amelyeket bizonyos paramétereiknél fogva veszélyes objektumok közé sorol a szakirodalom. „Személy és vagyonbiztonság szempontjából objektumok az épületek, létesítmények, bekerített vagy nyitott területek, melyek valaki, vagy valami által veszélyeztetettek és azt biztosítani kell" [1]. Ez előbbi definíció alapján a veszélyes objektumokat három nagy csoportba sorolhatjuk.

Első csoport

Az első csoport, azok a veszélyes objektumok, amelyek a működésükből kifolyólag tartoznak a veszélyes objektumok kategóriába. Ilyen lehet például egy vegyi üzem, gyógyszergyár, olajfinomító. Ezek az üzemek rendeltetésszerű működésüktől eltérő állapotukban tartoznak a veszélyes objektumok közé.

Második csoport

Második csoportba tartoznak azok a veszélyes objektumok, amelyek betöltött feladatukból, elhelyezkedésükből, valamint befogadóképességükből fakadóan kiemelt célpontok lehetnek egy esetleges támadás kapcsán. Ilyenek lehetnek a kritikus infrastruktúraelemek, kiemelt létesítmények közelében elhelyezkedő nagyobb objektumok, vagy például stadionok.

Harmadik csoport

Harmadik csoportba tartoznak azok a veszélyes objektumok, amelyek kiemelkedően nagy értéket képviselnek vagy tárolnak. Ilyen lehet egy kincstár, bank vagy múzeum.

Általánosságban minden objektum őrzésénél és védelménél ugyanazok az alapvető eszközök, technikák, technológiák, módszerek és eljárások jelentkeznek. Azonban a veszélyeztetés és a veszélyesség arányában ezek mennyisége, minősége jelentősen különbözhet. Minden objektumnál akkor optimális és hatékony a vagyonvédelem, amennyiben az alkalmazott erőforrások komplexek. A komplex vagyonvédelmet a mechanikai védelem, elektronikai jelzőrendszer, élőerő valamint ezeket egybefogó megelőző biztonsági rendszabályok építik fel. Ezek a vagyonvédelmi rendszerelemek

a tervezéstől a kivitelezésen át a karbantartásig bezárólag együttesen alkotják a komplex vagyonvédelmet. A tervezési szakaszt, majd a kivitelezést követően az üzemeltetett rendszer karbantartása kiemelten fontos feladat. Minden részegység együttes működése esetén beszélhetünk megfelelő védelemről, működő rendszerről. Kiemelt fontosságú létesítmények esetében ezekkel a részegységekkel szemben támasztott követelmények nagyobbak, szigorúbbak lehetnek, ezzel garantálva azok üzemszerű működését. Kiemelt fontosságú lehet például egy veszélyes objektum is.

Veszélyes objektumok karbantartása

A veszélyes objektumok komplex vagyonvédelmi rendszerei abban az esetben hatékonyak és működnek rendeltetés szerint, amennyiben azok minden részegysége karbantartott, ellenőrzött. Ebből kifolyólag a technikai rendszerek folyamatos karbantartása kiemelten fontos feladat. A karbantartásokat csoportosíthatjuk aszerint, hogy milyen időközönként kerül sor rájuk. Így például éves, negyedéves, havi vagy akár heti rendszerességgel is történhet karbantartás. Ennek megválasztása számos különböző rendszertechnikai paramétertől függ. Figyelembe kell venni a működés jellegét, meghibásodás valószínűségét, műszaki részegységes munkaóráinak számát, valamint a komplex rendszer becsült élettartamát is. A karbantartás csoportosításának másik lehetséges metódusa arra alapoz, hogy egy feltételezett vagy várható hiba bekövetkezik-e. Azaz egy várható eseményt kíván megelőzni vagy bekövetkezés esetén orvosolni. Ebben az esetben a csoportosítás az alábbiak szerint határozható meg:

Megelőző karbantartás

Ebben az esetben nem egy konkrét hiba kijavítása a cél, hanem egy lehetséges megelőzése. A számítások alapján, amelyek a rendszer minden egyes működési mechanizmusát tartalmazzák, készül egy kivonat, amely azokat a rendszerelemeket veszi sorra, amelyek meghibásodása valószínűségi sorrendben bekövetkezhet. Ezeket az egységeket besorolják, kategorizálják, majd karbantartáskor ezek figyelembevételével vizsgálják az egész rendszert. Ebben az esetben a karbantartást végző személyzet a rendszerelem üzemszerű működésével összhangban, illetve arra tekintettel végzi a megelőző karbantartási munkát.

Javító karbantartás

Második karbantartástípusról, a javító karbantartásról akkor beszélünk, amennyiben egy konkrét hiba elhárítása a karbantartás célja. A szerződésben foglalt karbantartási munka – megállapodás szerinti – részét képezi a meghibásodások javítása. Például a vagyonvédelmi karbantartási szerződésekben gyakori kikötés a javítás elvárt ideje, azaz a hiba észlelését követően a szerződött cég hány órán beül vállalja a hiba elhárítását és az eredeti üzemszerű állapot visszaállítását. Adott helyszínre történő kiérkezés

időbeliségét a szerződő partnerek egyéni igényeinek megfelelően alakítják. További vagyonvédelmi szemléletű karbantartási szerződések lényegi pontja a tartalékképzés kérdése. Azaz a rendszerelemeket, amelyek működésükből kifolyólag kopóalkatrésznek minősülnek, vagy meghibásodásuk a rendszer teljes üzemképtelenségét vonhatja maga után, milyen darabszámban raktározzák. Ebben az esetben – a megoldás költségvonzata miatt – általában a megrendelő fél halmozza fel a szükséges alkatrészeket, tartozékokat. Ezek az előre betárolt tartalékok meghibásodás esetén azonnal felhasználhatók, így az üzemszerű működés a javítást követően folytatódhat, rövid időn belül. A javító-karbantartás esetében egy váratlan meghibásodásról beszélünk, így a munka elvégzése nem kötött olyan paraméterhez, mint az időbeli ismétlődés, rendszeresség vagy az üzemszerű leállás, illetve műszak kezdete és vége. A javító karbantartás esetében a cél a hiba lehető legrövidebb időn belüli javítása, ezzel csökkentve a kiesés okozta mindennemű veszteséget. Abban az esetben, amikor a karbantartást nem külső szerződéssel megbízott cég végzi, hanem a létesítmény saját hatás- és felelősségi körben azt képes és szándékozik ellátni, a tartalékképzés kérdése értelemszerűen megoldott.

Utólagos karbantartás

Harmadik csoportba sorolhatók azok a karbantartások, amelyek egy konkrét hibajavítást követnek. Az utólagos vagy helyreállító karbantartás célja az, hogy a javító karbantartást követően ellenőrizze, hogy minden részegység újból megfelelően működik. Megbizonyosodjon arról, hogy az elvégzett munka szakszerű volt, a rendeltetésszerű működés visszaállt, valamint minden része a rendszernek megfelelően működik. Ebben a karbantartási csoportban a dokumentumok ellenőrzése is kiemelt feladat, hiszen minden rendszerben történt változtatást, így a javításokat is, megfelelően dokumentálni kell.

Veszélyes objektumok ellenőrzése

A veszélyes objektumokban a kötelező karbantartási munkálatokon túl, besorolásukból fakadóan felügyeleti szervek (vagy a létesítmények saját hatáskörükben is) tarthatnak ellenőrzést [2]. Ezek az ellenőrzések több szempont alapján vizsgálhatók.

Ellenőrzési dimenzió

Ebben az esetben két ellenőrzést említhetünk. Az egyik a komplex átfogó ellenőrzés, amely során a teljes vagyonvédelmi rendszert tesztelik. Így a teljes technikai eszköztár, mint elektronikai berendezések, mechanikai védelmet ellátó egységek, valamint az élőerős állomány revíziója is megtörténik. Komplett, átfogó ellenőrzés időben egy hosszú folyamat, így lehet akár többnapos is. Gyakorisága ebből kifolyólag általában éves vagy kétéves intervallumokban ismétlődik. Ezzel szemben a rutinellenőrzések sokkal gyakoribbak. A rutinellenőrzések alkalmával egy adott, kisebb egységet ellenőriznek.

Előzetes terv alapján újabb és újabb területek mellett, adott visszatérő egységek vizsgálata zajlik ilyenkor. Például egy ellenőrzés alkalmával feltárt hibát a következő alkalommal vagy azt követőn újra elemezhetik, ezzel figyelemmel kísérve a javítást vagy a mulasztást az ellenőrzött részéről.

Bejelentés módja

Az ellenőrzés alá eső objektum előre bejelentett, illetve előre nem bejelentett módon is tesztelhető, ellenőrizhető. Ebben az esetben a közlés módja a csoportosítás alapja. Bejelentett ellenőrzésről akkor beszélünk, amikor a vizsgálandó veszélyes objektummal előre egyeztett időpontban és módon történik a helyszíni ellenőrzés. Ilyenkor az ellenőrzött fél felkészülhet minden szükséges és lehetséges módon a vizsgálatra. Például előkészíthet dokumentumokat, berendelheti az állományt, vagy egyszerűen felkészítheti alkalmazottjait. Ezzel szemben a nem bejelentett ellenőrzés alkalmával a meglepetés erejével élve kezdődik meg az objektum vagyonvédelmi rendszerének ellenőrzése. Az ilyen típusú szemle elsődleges célja a védettségi kultúra fejlesztése, annak fontosságára való felhívás. A védettségi kultúra, mint fogalom magába foglalja a biztonságtudatosságot, biztonságtechnikai, vagyonvédelmi szempontból. Egy gondolkodásmód, látásmód, amely központba helyezi a biztonságtechnikai rendszert, komplex módon. A *Nemzetközi Atomenergia Ügynökség Védettségi Sorozat* 7. számú kiadványában úgy nyilatkozik, hogy minden olyan szervezet, aki a biztonság, biztonságtechnika területén dolgozik, kiemelten kell, hogy kezelje a védettségi kultúra kérdését. Így annak a fejlesztése és karbantartása szükséges ahhoz, hogy a szervezet azt hatékonyan implementálni tudja működésébe [3]. A nem bejelentett ellenőrzés képes rávilágítani olyan hibákra is a meglepetés ereje miatt, amelyek tervezett módon ritkábban látnak napvilágot. Ebben az esetben az ellenőrzés idejét is úgy választják ki, hogy a megszokottól eltérő legyen. Így például éjszaka vagy ünnepnapokon.

Kivitelezés lehetőségei

Az ellenőrzések következő csoportosításának alapja, hogy a szükséges vizsgálathoz az ellenőrzést végzőknek a helyszínen kell-e tartózkodni, vagy távoli elérés segítségével is kivitelezhető a vizsgálat. A helyszíni ellenőrzés a leggyakoribb, leginkább bevált módszer, többek között a veszélyes objektumok ellenőrzésére. Azonban a programozható rendszerek védelmi rendszereinek, azaz az információvédelmi rendszerek tesztelése, vizsgálata távolról is történhet. Az információvédelem az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzését jelenti. A fentieken kívül az információ más tulajdonságai is beleérthetők, mint a hitelesség, az elszámoltathatóság, a letagadhatatlanság és a megbízhatóság [4]. Ebben az esetben is beszélhetünk bejelentett és nem bejelentett formáról. Többek között ilyenkor is látszik, hogy a kategóriák között sok átfedés lehet. A helyszíni és távoli eléréssel megvalósított ellenőrzés is kiemelten fontos. Utóbbi esetében napjainkban felértékelődött szerepe miatt egyre inkább teret kap a távoli eléréssel történő ellenőrzési módszer.

Elérés módja

Egy veszélyes objektumban az ellenőrzés módja lehet elkészített menetrendszerű, valamint véletlenszerű, provokatív jellegű. Menetrend alapokon nyugvó ellenőrzésről akkor beszélünk, amikor az ellenőrzést végző egy metódust követve elkészít egy előzetes tervet, azt engedélyezteti, így a helyszínen annak pontjáról pontjára halad az ellenőrzött fél kíséretében. Véletlenszerű, provokatív ellenőrzések azok a típusú vizsgálatok, amikor az ellenőrzési terv nem egy pontokba szedett tervet követ, hanem például egy szabálytalanság elkövetésével provokálja ki az ellenőrzés tárgyát képező viselkedést, eszközhasználatot vagy eljárásrend alkalmazását. Ebben az esetben nem szemrevételezi például az őrszemélyzet ruházat-átvizsgálás módszerét, hanem rejtett tárgy akár csempészési szándékával kiprovokálja annak alkalmazását. Ugyanilyen kontextusban ellenőrizhetők különböző biztonságtechnikai berendezések is. Például csomagvizsgáló berendezések vagy kerítésvédelmi elemek is. Az ellenőrzések ilyen típusa abban az esetben alkalmazható, amikor az ellenőrzés alá eső személyek közvetlen felettese erre a létesítmény teljes egészének működése ismeretében engedélyt ad.

Következtetések

A veszélyes objektumok normál, üzemszerű működése számos vagyonvédelmi összetevő együttes, összhangban történő munkájának eredménye. Vagyonvédelmi szempontból kiemelt jelentőségűek ezek a létesítmények, hiszen azok tervezése, üzemeltetése valamint karbantartása nem átlagos feladat, így nem átlagos tudást igényel. Rendszerszintű tervezésük, komplex vagyonvédelem kiépítése valamint üzemeltetése ezekben a speciális létesítményekben olyan szakmai tapasztalatokon, nemzetközi jó gyakorlatokon valamint számos teszten alapul, amelyek előremutatók szakmai körökben. Ezekben a létesítményekben az üzemszerű működés alappillérei a karbantartás, valamint a rendszerellenőrzés. A karbantartás, mint feladat az adott létesítmény saját felelőssége. Ezt a feladatot a létesítmény úgymond házon belül, saját alkalmazásban álló szakemberek által, valamint szerződéssel, külső munkavállalók segítségével is megvalósíthatja. A karbantartás lehet megelőző, javító, valamint helyreállítást követő. Ezek a karbantartások mind dokumentáltan folynak, ezzel segítve a folyamatos munkát és fejlesztést. Ezek dokumentálása legtöbb esetben papíralapon történik, azonban digitális alapú verziói is fejlesztés alatt vannak számos helyen. Ez utóbbi esetében érdemes megemlíteni, hogy amennyiben a dokumentáció szenzitív vagy minősített információkat tartalmaz, úgy annak jogszabályban meghatározott kereteiről a létesítménynek kötelessége gondoskodni.

A karbantartás mellett az ellenőrzés, mint feladat már nem kizárólagosan a létesítmény feladata, hanem az illetékes ellenőrző szervé is. Ez az ellenőrzés lehet helyszíni, távoli, bejelentett, nem bejelentett, menetrendszerű, provokatív, részegységes, komplex. Az ellenőrzés fajtái között lehet természetesen átfedés is. Az ezekből az ellenőrzésekből levont következtetések, javaslatok, ajánlások teljesülése azok súlyától függhet. Így például egy akár jogszabályba ütköző eltérés javítása nagyobb hangsúlyt kaphat, mint egy belső szabályzóval szembeni kisebb eltérés.

Összességében tehát elmondható, hogy a veszélyes objektumok esetében is a karbantartási valamint ellenőrzési stratégia meghatározza a teljes működés minőségét.

Hivatkozások

[1] L. Berek, T. Berek és L. Berek, *Személy- és vagyonbiztonság,* Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 3071, 2016.
[2] 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről, 34. §.
[3] International Atomic Energy Agency, *Nuclear security culture: Implementing Guide NSS7,* Vienna, 2008.
[4] Országos Atomenergia Hivatal, *FV-18. sz. útmutató, Nukleáris létesítmények programozható rendszereinek védelmi követelményei,* Országos Atomenergia Hivatal, 2016.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG, ABV- ÉS KATASZTRÓFAVÉDELEM

14. évfolyam (2019) 3. szám 13–20.
DOI: 10.32567/hm.2019.3.2

Beke Dóra,[1] Földi Alexandra,[2] Kuti Rajmund[3]

Közúti balesetek során bekövetkező talajszennyezések és kárelhárítási eljárások vizsgálata

Investigation of Soil Contamination and Remediation Processes Following Road Accidents

A közúti közlekedésben részt vevő járművek száma az elmúlt évtizedekben folyamatosan növekedett Magyarországon is, amit a közlekedési infrastruktúra fejlesztése nem tudott követni. A forgalom növekedése nagyon gyakran közúti balesetek bekövetkezéséhez vezet. A balesetek során a járművek olyan súlyos sérüléseket is szenvedhetnek, hogy a motorból és az erőátvitel elemeiből kenő- és hűtőfolyadékok, üzemanyagok juthatnak a közútra, onnan lefolyva pedig a talajba szivároghatnak. A környezetvédelem fokozott előtérbe kerülésével párhuzamosan a közúti balesetek környezetterhelésének vizsgálata nem kapott megfelelő hangsúlyt, ezért írásunkban, a legtöbb esetben a talajba jutó olajszármazékok káros hatásait vizsgáljuk. A kárfelszámolást végző szervezetek tevékenységének környezeti szempontú fejlesztése, a jövőbeli fejlesztési irányok kijelölése fontos, aktuális feladat. Jelen cikk szerzőinek célja, hogy kutatási eredményeik bemutatásával hozzájáruljanak a közúti balesetek során bekövetkező környezetszennyezések csökkentésének kezeléséhez, továbbá a hatékony kárfelszámolási tevékenységhez.

Kulcsszavak: közúti baleset, környezeti hatások, talaj, talajszennyezés, kárfelszámolás

The number of vehicles involved in road traffic has continuously increased in Hungary in the recent decades, which could not be followed by the development of transport infrastructure. Heavy traffic can frequently lead to road accidents. Due to accidents,

[1] Széchenyi István Egyetem, egyetemi docens, e-mail: beke.dora@sze.hu, ORCID: https://orcid.org/0000-0002-5440-6394
[2] Telenor Magyarország Kft, junior készülékelemző, e-mail: foldia.lexy@gmail.com, ORCID: https://orcid.org/0000-0001-5858-7551
[3] Széchenyi István Egyetem, egyetemi docens, e-mail: kuti.rajmund@sze.hu, ORCID: https://orcid.org/0000-0001-7715-0814

vehicles can be so seriously damaged that fuel, lubricants or coolants from the engine, gearbox and other components can spill onto the road surface and infiltrate into the soil. Although environmental protection is one of the main points of interest, the research of the environmental impact of road accidents has not get adequate attention so far, so in this paper we examine the harmful effects of hydrocarbons as the most frequent pollutants to the soil. The most relevant task is the improvement of the remediation organisations in an environmental-conscious way and determine the direction of development. With the introduction of our research results the purpose of the authors is to contribute to proper remediation of contaminated areas due to road accidents and help these activities to be more effective.

Keywords: **road accident, environmental impacts, soil, soil contamination, remediation**

Bevezetés

Az elmúlt évtizedekben rendkívüli mértékben emelkedett a gépjárművek száma Magyarországon, aminek következtében a közutak is folyamatosan leterheltebbekké váltak. A forgalom növekedésével a közlekedési morál is megváltozott, ami a közutakon bekövetkezett balesetek számának a növekedéséhez vezetett. Egy-egy bekövetkezett baleset során a járművekben keletkezett fizikai sérülések következményeként a gépkocsik belsőégésű motorjainak vagy a hajtáslánc egységeinek kenőanyagai, továbbá a hűtőfolyadékok, valamint az üzemanyagok a közútra, onnan pedig, ha nem érkezik rövid időn belül a kárfelszámoló egység, az út melletti árokba jutnak, ahol bekövetkezik a talajszennyezés. Jelen cikkben a közúti balesetek során a talajba kerülő szennyezések hatásait vizsgáljuk, a környezetbiztonsági szempontokat előtérbe helyezve. Jelen írás tartalmi követelményei nem teszik lehetővé az összes szennyező vizsgálatát, ezért az olajszennyezéseket helyezzük fókuszba. Tapasztalatainkkal a környezeti károk csökkentéséhez kívánunk hozzájárulni.

A talaj fázisai

Mielőtt a szennyezések talajba jutásának folyamatát, továbbá azok hatásait vizsgáljuk, fontosnak tartjuk a talaj fázisait bemutatni. A talaj különböző ásványi és kémiai összetételű, méretű, alakú és térbeli elrendeződésű részecskék halmaza, és ez teszi lehetővé a víz, a levegő, valamint felvehető formában lévő (oxidált, oldott) tápanyagok egyidejű jelenlétét, többé vagy kevésbé biztosítva ezzel a talaj élővilágának, valamint a természetes növényzetnek és termesztett növényeknek a talajökológiai feltételeit [7].

A talaj, mint három (négy) fázisú, négydimenziós, polidiszperz rendszer (különböző méretű, alakú és térbeli elrendeződésű részecskék horizontálisan és vertikálisan egyaránt heterogén, struktúrába rendeződött, és időben is dinamikusan változó halmaza) képes a talajjal közvetlen vagy közvetett kapcsolatban álló élő szervezetek, így a természetes növényzet és a termesztett kultúrák talajökológiai igényeit (leegyszerűsítve levegő-, víz- és tápanyag-igényét) többé vagy kevésbé kielégíteni. Mégpedig úgy, hogy e tevékenysége közben a talaj nem fogy, állagában nem változik alapvetően, minősége nem

romlik szükségszerűen. A talaj feltételesen megújuló (megújítható) természeti erőforrás. Nemcsak termékenységgel rendelkezik, hanem egy csodálatos megújuló-képességgel is. Megújulása azonban nem megy végbe automatikusan, hanem feltételekhez kötött, amelyek közül a legfontosabbak az észszerű földhasználat, a megfelelő agrotechnika, és bizonyos esetekben a melioráció. Ezek tudatos teljesítésével a talaj zavartalan – a társadalom részéről egyre sokoldalúbban használt – multifunkcionalitása hosszú távon is biztosítható. A talaj termékenysége fenntartható, sőt fokozható, a nem megfelelő talajhasználat káros talajtani és környezeti hatásai (talajtermékenységet gátló tényezők, talajdegradációs folyamatok) eredményesen megelőzhetők, kivédhetők, de legalább bizonyos tűrési határig mérsékelhetők [1].

A szennyezőanyagok talajbeli terjedésének, valamint károsító hatásaik vizsgálatának érdekében fontos ismerni a szennyezett talaj mechanikai összetételét, fizikai féleségét és a porozitását. A szemcseösszetétel (mechanikai összetétel) azt fejezi ki, hogy a talajban milyen arányban találhatók a különböző méretű szemcsék. A jelen lévő különböző méretű szemcsék arányából a klasszikus háromszögdiagram alapján megadható a fizikai féleség. A talaj porozitása vagy pórustérfogata a szilárd részek által elfoglalt tér és a hézagtér viszonyából következik. A talajban különböző átmérőjű pórusok találhatók, amelyek feladata – méretüktől függően – biztosítani a vízáteresztést, vízvisszatartást, a levegőztetést, életteret nyújtani a talaj mikroflórájának és teret biztosítani a növények gyökérfejlődéséhez. A különböző méretű pórusokban más-más erők hatnak a víz (és egyéb beszivárgó folyadékok például motorhajtóanyagok, kenőanyagok) mozgására. Általánosítva elmondható, hogy a nagyméretű pórusokban (gravitációs pórusok) könnyen felvehető vizet találunk [2].

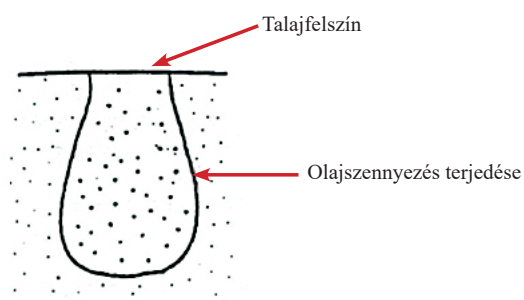
Közúti balesetek során előforduló talajszennyezések

Közúti balesetek során a szennyezőanyagok többféle módon juthatnak ki a sérült járművekből. Egyrészt hajtóanyagok, másrészt a motor és az erőátviteli rendszer hűtő- és kenőanyagai, harmadrészt pedig a sérült járműveken különféle formában szállított különféle halmazállapotú anyagok [3]. Kutatásunk szempontjából a különféle szénhidrogén-származékok, alkoholok, szerves oldószerek kerülnek előtérbe. Az olajszármazékok mellett fontosnak tartjuk ismertetni az illékony vagy illékony komponenseket is tartalmazó anyagok (például motorbenzinek) talajra gyakorolt hatásait, ugyanis ezek a folyadékok az olajszármazékokhoz képest eltérően viselkednek a talajba kerülve. Amennyiben a közúti baleset során szennyezés formájában az előbb említett illékony vagy illékony komponenseket is tartalmazó anyagok kerülnek a talajba, a szennyezés további terjedése a talajgázok közvetítésével lehetséges a talaj pórusaiban. A szennyezőanyag illékony tulajdonságának függvényében a részleges vagy teljes kármentesítés levegőztetéssel (sztrippelés) valósítható meg.

A kenőolaj-származékok nagy molekulaméretű szerves vegyületek, magas szénhidrogén tartalmuk mellett heteroatomokat és aromás csoportokat is tartalmaznak, ennek következményeként toxikus tulajdonságokkal is rendelkeznek. A motorolajokat, típustól és felhasználási területtől függően több összetevő megfelelően kiegyensúlyozott keveréke alkotja. Nagyobb részben – 65–85%-ban – alapolajokból és kisebb

részben – 15–35%-ban – különféle adalékanyagokból állnak. Az alapolajok fizikai és kémiai tulajdonságait a kenőképesség növelése érdekében adalékokkal javítják. A kiindulási olajok és a felhasznált adalékanyagok aránya a kenőanyag viszkozitási osztályától, valamint az elvárt teljesítményszinttől függ. Az olajok vízben oldódásra nem képesek, ezért a talajban lassan bomlanak le. Viszkózus anyagok lévén a talajvizet nem veszélyeztetik, de a talajból öntisztulással csak nagyon hosszú idő elteltével távoznak [4].

Az olaj kétfázisú heterogén rendszert alkot a talajjal. Az olajszennyezés terjedési tulajdonságait befolyásolják a talaj paraméterei, a talajba jutott olaj mennyisége és minősége, továbbá az adott térfogatú szennyezőanyagnak a talaj felszínére kerüléséhez szükséges idő. Kiszáradt, repedezett, vagy laza szerkezetű talajban a szennyezés függőleges mozgást végez, míg tömött (nehéz mechanikai összetételű) talajban az oldalirányú szennyezőanyag-terjedés a jellemző folyamat. Az olajszennyezés a talajvíznél lassabban mozog, akadályozza a talaj öntisztuló képességét és nagymértékben rontja a talajvíz minőségét. A nyersolajtermékek csoportjából a középpárlatok, kenőolajok és a benzinek veszélyesek a talajszennyezés tekintetében. A mélyhűtve vagy nyomás alatt cseppfolyósított gázok még beszivárgás előtt elpárolognak, míg a sűrű kenő-, vagy a nehézolajok nem jutnak be a talajba. A szennyezésterjedésre történő képességének szempontjából a szennyezőanyag vízben oldhatósága fontos tényező, mivel ezáltal a környezetbe került olajszármazék mozgékony vegyületté válik, és könnyebben kerül bele a talajvízbe, azután pedig továbbjut a vízbázishoz. Egynemű, homogén talajba kerülve az olajszennyezés profilja közel szabályos, viszont rétegzett talajban, az egyes rétegek eltérő áteresztőképessége miatt ez a profil erősen módosulhat. A szennyezőanyag vertikális irányú mozgása abban az esetben tud csökkenni vagy megszűnni, ha a leszivárgás intenzitása nagyobb, mint az adott talajréteg olajáteresztő képessége. Ekkor a kérdéses réteg felett a folyadéknak oldalirányú mozgása következik be. A szivárgás egészen a talajvízig terjedhet, ha a szennyezés mennyisége nagyobb, mint amennyit a talajvíz feletti rétegek esetlegesen még vissza tudnának tartani. A szennyezés terjedésének sebessége a víztükör feletti kapilláris zónában csökken a kapillárisok víztelítettsége miatt. Ennek következtében a zónában a bejutott olaj mennyisége jelentősen feldúsul és önálló fázist képez. Amennyiben a szivárgás nem szűnik meg, a talajvíz felszínén is kialakul az olajlencse. A következő ábrák az olaj különféle szerkezetű talajokban történő terjedését szemléltetik [5].

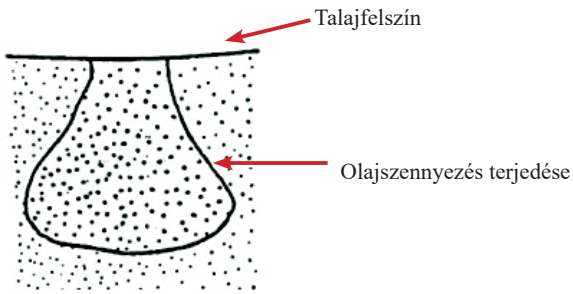


1. ábra

Olajszennyezés terjedése nagy áteresztőképességű homogén talajban

(a szerzők összeállítása [5] adatainak felhasználásával)

Az 1. ábrát áttekintve könnyen megállapítható, hogy a nagy áteresztő-képességű homogén talajban gyorsan terjed az olajszennyezés, viszonylag rövid idő alatt kiterjedt szennyezés alakulhat ki.

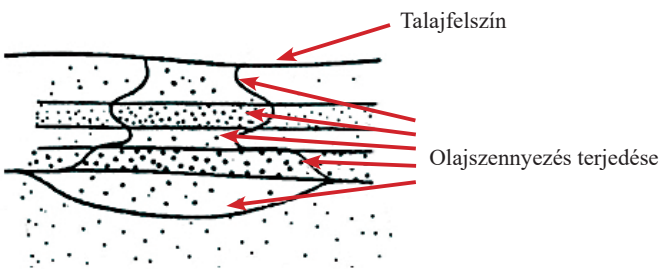


2. ábra

Olajszennyezés terjedése kisebb áteresztő-képességű homogén talajban

(a szerzők összeállítása [5] adatainak felhasználásával)

A 2. ábra elemzése alapján megállapítható, hogy a kevésbé áteresztő homogén talajban is viszonylag gyorsan terjed az olajszennyezés, viszont az ilyen mechanikai összetételű talajnál nagyobb horizontális terjedés következik be, mint a nagy áteresztőképesség esetén. Ebben az esetben is elmondható, hogy viszonylag rövid idő alatt jelentős szennyezés alakulhat ki.



3. ábra

Olajszennyezés terjedése rétegzett, különböző áteresztő-képességű rétegekből álló talajban

(a szerzők összeállítása [5] adatainak felhasználásával)

A 3. ábra megmutatja, hogy a különböző áteresztő-képességű talajrétegekben egymástól eltérő mértékben terjed az olajszennyezés, horizontális és vertikális irányok tekintetében.

Talajszennyezések kármentesítése

A talajok kármentesítése során az alkalmazható kárelhárítási technológiák tekintetében a folyamatnak három fontos célt kell szolgálnia:

- a szennyezés továbbterjedésének megakadályozása (lokalizáció),
- a talaj részleges mentesítése (a szennyezett fázis(ok) kitermelése),
- a teljes ártalmatlanítás.

A kármentesítési eljárásokat a következő módokon csoportosíthatjuk.

Tisztítási elv szerint beszélhetünk:

- fizikai,
- kémiai,
- biológiai,
- és termikus tisztításról.

Előbbieken kívül a különböző technológiákat kategorizálhatjuk a mentesítendő szennyezőanyagok szerint is [5].

A kárhelyszín adottságait figyelembe véve a talajtisztítás történhet in situ (eredeti helyzetben) és ex situ (nem eredeti helyzetben), különféle technológiák alkalmazásával. In situ technológia alkalmazásakor a szennyezett földtani közeget vagy felszín alatti vizet olyan módon tisztítják meg, amelynek során a tisztítandó földtani közeg kitermelésére nem kerül sor, a felszín alatti vizet a munkaterületen belül visszatáplálják a tisztítási folyamat során. Ezzel ellentétben az ex situ technológia alkalmazása során első lépésben a mentesítendő közeg kitermelése történik, ezután a szennyezett talajt elszállítják, végül pedig a megtisztított közeget visszajuttatják a helyszínre. Ezt a technológiai csoportot még további két kategóriára bonthatjuk aszerint, hogy a mentesítendő közeget a munkaterületen (ex situ on site) vagy egy távolabbi, erre alkalmas helyen (ex situ off site) tisztítják meg. Mint a két technológia alkalmazása után megtisztított talajt juttatnak vissza a szennyezés helyszínére [5].

A talaj kitermelése nem minden eljárás alkalmazása során történik meg, például az átlevegőztetési, talajmosási, biológiai lebontási (mikroorganizmusok mentesítik a közeget a szennyezéstől) eljárások során, továbbá a sztrippelés és stabilizálás során sem történik meg a szennyezett talaj kiemelése. A termikus technológia a talaj kitermelésével jár, valamint a talajmosási eljárások és a biológiai lebontással történő tisztítási eljárások (mikrobiológiai kezelés) alkalmazásához szintén ki kell emelni a szennyezett talajt [5].

Az elmúlt években bekövetkezett közúti balesetek során a kárfelszámolást végző szervezetek tevékenysége során is előtérbe kerültek a környezetbiztonsági szempontok [6], fő tevékenységük mellett egyre nagyobb hangsúlyt helyeznek a kijutott szennyezőanyagok közvetlen felitatására, eltávolítására, ennek ellenére súlyosabb esetekben így is kerülnek olajszármazékok a talajba.

Következtetések

A környezet- és biztonságtudatos szemlélet kialakítása környezeti elemeink védelme szempontjából kiemelten fontos. Az emberi tevékenység folyamatos környezetterheléssel jár, ugyanakkor a közúti balesetek során a sérült járművekből vagy a rakományukból a környezetbe kerülő veszélyes anyagok, különösen az olajszármazékok talajra gyakorolt hatásainak tudományos vizsgálata elengedhetetlen a szennyezések terjedésének, károsító hatásainak pontosabb megismeréséhez. Arra a következtetésre jutottunk, hogy a tudományos eredmények a szennyezések következtében kialakuló veszélyek értékeléséhez/értelmezéséhez elengedhetetlenül szükségesek, ami a kockázatokra történő magasabb szintű reagálást eredményezhet a kárfelszámolások során. A talajszennyezések kezeléséhez kollektív munkára van szükség a kárfelszámolásban és a helyreállításban részt vevő szervezetek és az állampolgárok részéről is. Fontos feladat a környezetünkben végbemenő változások folyamatos tudományos alapú összehasonlító vizsgálata, továbbá a kutatási eredmények gyakorlatba ültetése, ami környezeti elemeink védelméhez elengedhetetlen.

Összegzés

A világunkban végbemenő technikai fejlődés a mobilitásra is hatást gyakorolt, aminek következtében a különféle közúti közlekedési eszközök is egyre nagyobb számban és szélesebb körben terjedtek el. Ez a folyamat az utak fokozódó leterheltségéhez vezetett, ami a közlekedési balesetek számának növekedését okozta. Írásunkban a balesetet szenvedett járművekből a talajba kerülő olajszármazékok szennyezőhatásait vizsgáltuk, ugyanis a talaj az egyik legfontosabb környezeti elemünk, amelynek védelme komoly feladatként jelentkezik. Áttekintettük az egyes olajszármazékok által okozott szennyezések terjedési lehetőségeit, figyelembe véve a különböző talajtípusokat. Megállapítottuk, hogy az általunk bemutatott kármentesítési eljárások alkalmasak a talaj remediációjára. Rávilágítottunk, hogy a kárfelszámolási tevékenység nagyban hozzájárul a közúti balesetek során bekövetkező környezetszennyezések csökkentéséhez. Felhívtuk a figyelmet arra is, hogy fontos az egyes talajszennyezések, továbbá a kárfelszámolási feladatok tudományos alapú vizsgálata, annak érdekében, hogy az új kihívások kezelése komplex módon történhessen. Kutatási eredményeinkkel a környezetbiztonság fenntartásában közreműködő szervezetek hatékony és eredményes működését kívánjuk segíteni.

Hivatkozások

[1] Gy. Várallyay, *Növényi tápanyagellátás és a talaj vízgazdálkodása,* Gödöllő: Szent István Egyetem, 2003.
[2] P. Stefanovits, *Talajtan,* Budapest: Mezőgazda Kiadó, 1992.
[3] R. Kuti, *Műszaki mentések I-II.*, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2007.

[4] L. Rácz, G. Tölgyessy, L. Papp és G. Lesny, *Környezeti Kémia,* Eger: EKF Líceum Kiadó, 2002.
[5] I. Barótfi, *Környezettechnika,* Budapest: Mezőgazda Lap- és Könyvkiadó Kft., 2003.
[6] L. Földi és L. Halász, *Környezetbiztonság,* Budapest: Complex Kiadó Kft., 2009.
[7] Gy. Várallyay, „A talajfizika gyakorlati alkalmazásai a fenntartható talajhasználatban," *Gyakorlati Agrofórum,* 1. kötet 10. évf. 7. sz. pp. 4–7, 1999.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG, ABV- ÉS KATASZTRÓFAVÉDELEM

14. évfolyam (2019) 3. szám 21–34.
DOI: 10.32567/hm.2019.3.3

Frigy Éva Gyöngyi[1]

Éltető levegő – a levegő minőségével kapcsolatos problémák összefoglalása

Sustaining Air – Summary of Problems Regarding Air Quality

A születés első pillanatától kezdve a szervezet működéséhez nélkülözhetetlen a folyamatos légzés. Ebből következik, hogy a földi élet lételeme és alapvető feltételrendszere a levegő, amely az életminőségünket közvetlenül meghatározza. Jelen cikk rendeltetése, hogy ismertesse a levegő természetes összetételét és az azt szennyező anyagokat, azok előfordulásának okait, a magyarországi légszennyezettség helyzetét, valamint egészségügyi és pszichés hatásait. Ezenkívül kitekintést ad más, külföldi nagyvárosok helyzetéről.

Kulcsszavak: **levegőszennyezés, kén-dioxid, szén-monoxid, nitrogén-oxidok, por, PM_{10}**

From the moment of birth, continuous breathing is crucial to keep the body functioning. From this it comes that air is the essence and the basic condition which directly effects our lives. The purpose of this article is to describe the natural components of air and its pollutants and their causes of occurrence, the state of the air pollution in Hungary, and its effect on health and psyche. Apart from this, it gives an outlook on the air pollution situation of other foreign metropolises.

Keywords: **air pollution, sulphur dioxide, coal monoxide, nitrogen oxide, dust, PM_{10}**

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: freevick@gmail.com, ORCID: https://orcid.org/0000-0002-0432-5385

Bevezetés

A születés első pillanatától kezdve a szervezet működéséhez nélkülözhetetlen a folyamatos légzés, épp ezért ezt a nem tudatos, automatikus reflexet – egy visszacsatolásos rendszer segítségével – az agytörzs irányítja. Hogy ez mennyire így van, az is bizonyítja, hogy még az ember is csak egy rövid ideig tudja akaratlagosan visszatartani a lélegzetét, mert a reflex egy meghatározott idő múlva visszaveszi az irányítást. Ebből következik, hogy a földi élet lételeme és alapvető feltételrendszere a levegő, amely az életminőségünket közvetlenül meghatározza. A levegő tisztaságának fontosságát jól prezentálja az is, hogy az elmúlt időszakban többször volt tájékoztatási fokozatú szmogriadó elrendelve. A környezeti levegőbe kijutó, a levegőminőséget rontó komponensek a környezet károsodásán túl, sajnálatos módon a tüdő ártalmát, a vérbe bejutó, veszélyes tulajdonságú anyagok az egész emberi test meghibásodását okozhatják. Naponta majdnem tízszer annyian halnak meg a rossz levegőminőség miatt, mint közlekedési balesetben. A légszennyezettséggel összefüggő évi közel 400 ezer korai haláleset hátterében a lakossági közlekedés, a helytelen fűtés, az ipar és mezőgazdaság által az értékes levegőnkbe került kisméretű szálló por (PM), a nitrogén-dioxid (NO_2), a kén-dioxid (SO_2), illetve a talajközeli ózon (O_3, nyári szmog) áll, miközben a természetes megújulási, tisztulási folyamat forrása, vagyis a növényzet folyamatos irtásnak, pusztulásnak van kitéve. Az elmúlt évtizedekben Magyarország légszennyezettségi szintje kritikus mértéket ütött meg, amely miatt az Európai Unió – nem túl sok sikerrel – többször szólította fel hazánkat a legveszélyesebb légszennyező-anyagok kibocsátásának a légszennyezettségi határértékek alá történő mérséklésére.

A légkör összetétele

„A levegő nagyon érdekes gázkeverék. Kb. 78%-ban nitrogénből, 21%-ban oxigénből és 1%-ban egyéb anyagból, főleg gázokból áll. A 78% nitrogén teljesen semleges, a 21% oxigén az ember (és a Földön élő minden más ismert többsejtű élőlény) számára nélkülözhetetlen, de igazán a legkisebb összetevő, az 1% egyéb anyag határozza meg, hogy mennyire tiszta és egészséges a levegő" [1].

Ideális esetben alig mérhető mennyiségben vannak jelen a levegőben a szennyezőanyagok, mint amilyen a szén-monoxid, kén-dioxid, nitrogén-oxidok, metán, aromás szénhidrogének, halogénezett szénhidrogének, és különböző méretű szilárd részecskék (ülepedő por és szálló por). Ezek a szennyezőanyagok ugyan kis mennyiségben vannak a légkörben, de az emberre, más élőlényekre, és bizonyos esetekben a használati tárgyainkra, de akár még az épületekre is még ebben a kis mennyiségben is veszélyesek lehetnek.

Az emberre irányuló hatásuk alapján minden szennyezőanyagra egészségügyi határértékeket állapítanak meg a hatóságok, és akkor mondják tisztának a levegőt, ha a szennyezések mennyisége a határérték alatt van. A levegő tisztaságát tehát nem a fő összetevők, hanem a kis mennyiségben jelen lévő, de még ekkora mennyiségben is káros szennyezőanyagok határozzák meg (lásd az 1. táblázatot). Az iparilag fejlett országokban már az 1970-es évektől kezdték felismerni ennek jelentőségét,

és lépéseket tettek annak érdekében, hogy a lehetőségekhez mérten minimálisra szorítsák a levegőszennyezettség mértékét és az ebből eredő fizikális és mentális egészségügyi problémák kialakulásának lehetőségét. „A környezeti hatásvizsgálatok lebonyolításának szabályozott módszere az USA-ban alakult ki először, az angol nyelvű szakirodalomban EIS (Environmental Impact Statement), illetve EIA (Environmental Impact Assesment) rövidítésekkel jelölik. Ezt követően számos ország vezette be ezt kötelező, vagy ajánlott eljárásként. Nagy-Britanniában kötelező előírás helyett segédletet dolgoztak ki a helyi hatóságok számára, amelynek alkalmazásával a döntéseiket megalapozhatják. Az Európai Gazdasági Közösség országai 1980-ban véglegesítették irányelveiket a környezeti hatások értékelésére" [2].

1. táblázat

Főbb légszennyező anyagok egészségügyi határértékei a 4/2011. (I. 14.) VM rendelet 1. számú melléklete alapján (a szerző szerkesztése [3] felhasználásával)

Légszennyező anyag	Órás határérték ($\mu g/m^3$)	24 órás határérték ($\mu g/m^3$)	Éves határérték ($\mu g/m^3$)
Kén-dioxid (SO_2)	250 (a naptári év alatt 24-nél többször nem léphető túl)	125 (a naptári év alatt 3-nál többször nem léphető túl)	50
Nitrogén-dioxid (NO_2)	100 (a naptári év alatt 10-nél többször nem léphető túl)	85	40
Szén-monoxid (CO)	10 000	5 000 (napi 8 órás mozgó-átlag-koncentrációk maximuma)	3 000
Szálló por (PM_{10})		50 (a naptári év alatt 35-nél többször nem lépheti túl)	40
Szálló por ($PM_{2,5}$)			25
Ólom (Pb)			0,3
Higany (Hg)			1
Benzol		10	5
Ózon (O_3)		120 (napi 8 órás mozgó átlagkoncentrációk maximuma)	
Arzén (As)			0,01
Kadmium (Cd)			0,005
Nikkel (N)			0,025
3,4-Benz(a)pirén		0,001	0,0012

Az ember mellett a természet is igyekszik a maga módszereivel megszabadulni a szennyeződésektől. Az eső sok szennyezést felold és kitisztít a levegőből, ezért tisztább esős időben és közvetlenül eső után a levegő. A szél, a napsütés szintúgy levegőtisztító hatással bírnak. Azonban fontos észben tartani, hogy a szennyezések az esővel leérkezve talaj- és vízszennyezéssé alakulnak, eső után pedig a légszennyezés is újratermelődik, amennyiben a légmozgás nem tisztítja a továbbiakban a levegőt.

„Az éghajlatot többek között a következő tényezők befolyásolják leginkább: napból érkező sugárzás mennyisége, a felszín anyagi összetétele, a domborzati viszonyok (tengerszintfeletti magasság), általános földi légkörzés és a tengeráramlások hő és vízgőzszállítása. A felsorolt tényezők mellett egy terület levegőminőségére még hatással van a kibocsátott szennyezőanyagok mennyisége, a beépítettség és a nagy távolságokról érkező szennyezés. A szennyezőanyagok többféleképp hatnak az élő szervezetekre közvetett vagy közvetlen módon, többek között kiválthatnak irritációt, bűzhatást, okozhatnak mérgezést, és a rákkeltő tulajdonsággal rendelkezők halálhoz is vezethetnek. Megkülönböztetünk rövid-, illetve hosszú távú szennyezőket, melyeket a légkörbe, talajba kerülve az állatok és a növények felvesznek és a táplálékláncon keresztül az emberi szervezetbe is bejutnak. A külső és a belső terekben különböző szennyező anyagok fordulnak elő. A külső terekben a főbb szennyező források a lakosság, a közlekedés, az ipar, az erőművek és a mezőgazdaság; a belső terekben pedig a dohányzás, a fűtés, a tisztítószerek használata és az építőanyagokból a légkörbe kerülő komponensek jelentenek veszélyt" [4].

Közismert tény, hogy a fűtési szezonban magasabb a károsanyag-kibocsátás, mint általában. Ez annak tudható be, hogy az emberek jelentős – ha nem túlnyomó – része a mai napig fával, rosszabb esetben műanyag vagy papíralapú hulladékkal tudja csak megoldani a fűtést, és ezek elégetésével a hőtermelés mellett korom, hamu és más szennyezőanyagok jutnak a légkörbe. Városi környezetben bár a központi fűtés az elterjedt, azonban az ennek alapjául szolgáló víz felmelegítéséhez energiára van szükség; energiára, amit modernebb környezetben földgáz, egyéb esetben szén, fa, olaj elégetésével tudnak előállítani, amivel jelentős mennyiségű szén-dioxidot juttatnak a levegőbe. Különösen veszélyes ez akkor, ha a fűtőrendszerben valamilyen meghibásodás keletkezik, ez ugyanis tökéletlen égést eredményezhet, amely során szén-dioxid helyett szén-monoxid és/vagy korom keletkezik, amely közvetlenül okozta a múltban és okozza napjainkban is évente átlagosan tucatnyi ember halálát és hozzávetőlegesen több száznak sérülését Magyarországon. Egy 2017-es kimutatás szerint az Amerikai Egyesült Államokban 2010 és 2015 között több áldozatot szedett a szén-monoxid-mérgezés, mint a terrorizmus, ezzel a negyedik helyre került a vezető halálokok listáján [5].

Hazánk légszennyezettsége

Magyarország levegőminőségét a földrajzi paraméterei is nagyban befolyásolják, hiszen a magas hegységekkel körülölelt Kárpát-medencében elhelyezkedve a szennyezőanyagok nehezen tudnak kiáramolni, illetve feloszlani és megrekednek hazánk területén. Ezek télen nagyobb koncentrációban vannak jelen a légkörben, amikor anticiklon esetén

napokon át tartós hideg alakul ki, vagy a ciklon esetén a párás és ködös időszak állandósul. Az elmúlt évtizedekben hazánk levegőterhelése egyes szennyezők tekintetében számottevően enyhült, ugyanakkor bizonyos szennyezőanyagok koncentrációja még mindig túlzottan magas, amely folyamatos egészség- és környezetromboló hatást gyakorol az élő- és élettelen világunkra [4].

A Hermann Ottó Intézet 2018-ban kiadott jelentése szerint: „Az ember, a növények, az állatok és az épített környezet védelme érdekében ezeken az értékeken javítanunk kell. Ehhez szükségesek a folyamatos mérések és ellenőrzések és ahol problémát észlelünk, azokon a területeken szigorúbb előírásokat hozni, valamint ahol lehetséges technológiai fejlesztések segítségével tisztább levegőminőséget elérni" [4].

Magyarország levegőszennyezettségi állapotát mai napig jelentősen meghatározza az 1979-ben a Nagy Távolságra Jutó, Országhatáron Átterjedő Légszennyezésről szóló (Long-range Transboundary Air Pollution, LRTAP) genfi egyezményhez, illetve később 2004-ben az Európai Unióhoz (a továbbiakban: EU) való csatlakozása, hiszen mindkét fórum szigorú előírások bevezetésével komoly erőfeszítéseket tesz a levegőminőség-védelemmel kapcsolatosan. Bár elmondható, hogy a szilárd tüzelésről – jellemzően – földgáztüzelésre, a megjelenő megújuló energiákra való átállással, illetve az atomenergia-felhasználással az energetikai szektor és általában az ipari tevékenységek okozta levegőterhelés számottevően visszaszorult. Ugyanakkor a közlekedés, illetve a téli időszakban a száraz tűzifa, fapellet vagy fabrikett helyett – az energiahordozók (földgáz) árának emelkedése miatt – a nem megfelelő lakossági szilárd tüzelés (nedves fa, szén – főként lignit – és egyéb háztartási hulladék) során továbbra is jelentős mennyiségű egészséget és környezetet súlyosan károsító légszennyező anyag, kisméretű szálló por (PM), szén-monoxid (CO), nitrogén-oxidok (NOx), kén-dioxid (SO_2), valamint ammónia (NH_3) keletkezik [6].

Jelenleg hazánk számos településén, ahol az ipar, az energiatermelés és a közlekedés koncentrálódik, a levegőterhelési faktorok összeadódása miatt a levegőszennyezettség szintje jóval meghaladja az EU által meghatározott értéket. Az olyan településeken élő emberek, mint Budapest, Dorog, Miskolc, Nyíregyháza és Szeged, fokozottan ki vannak téve a rossz levegő által okozott fizikai és szellemi egészségügyi kockázatoknak.

A főváros levegőszennyezettségére már Széchenyi István felhívta a figyelmet *A pesti por és sár* című írásában: „Sőt, kérdem, nem vált-e már soknak tűrhetetlenné a némelykor valóban »késsel metszhető por« vagy azon sár, mellyel néha téli időben küszködünk […] egészségünket oly sokszor kockára bocsátanunk kell? Nem kételkedem, sőt bizonyos vagyok, sok magában ilyféle okoskodást már tett, és piszkainkon, mocskainkon velem együtt nemcsak bosszankodott, de – kivált idegen előtt – pirult is" [7]. A 20. század első felében a főváros levegőszennyezettsége elsősorban az energiatermelésre és a fűtésre vezethető vissza. Az éves szénfogyasztás emelkedő tendenciája és az átlagemberek számára túlságosan magas korszerűsítési díjak, valamint a kevés alternatív lehetőség vezetett ahhoz a helyzethez, hogy az elektromos áram vagy földgáz használata a háztartások túlnyomó többségében luxusnak számított. Egyetlen megoldásnak az állami támogatással történő távfűtő-berendezések felállítása és a pályaudvarok villamosítása tűnt.

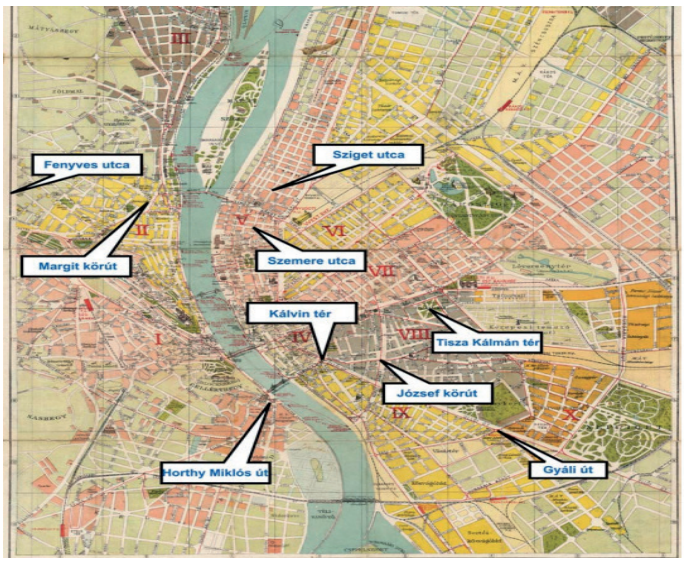
Az 1980-as évektől kezdve a széntüzelés fokozatosan kiszorult az olaj-, majd gáztüzelés, illetve távfűtési megoldások megjelenésével. 1990 és 2003 között a megváltozott

új ipari technológiáknak köszönhetően az ipari eredetű légszennyező anyagok kibocsátása is számottevően csökkent, ugyanakkor ez idő alatt a motorikus közlekedés a közutakon egyre frekventáltabbá vált, a gépjárműforgalom jelentősen megnövekedett, így a közlekedés, illetve azon belül is főként a dízeljárművek levegő-egészségkárosító, szennyező hatása jelentősebbé vált. „Becslések szerint az utóbbi évtizedben a fővárosban a nitrogén-oxidok, a porterhelés, a szén-monoxid, a PAH-ok és az illékony szénhidrogének (VOC) kb. 80%-a a közlekedés révén kerül a levegőbe" [8].

„Egyre több kémiai anyag káros környezeti és egészségügyi hatását ismerték fel, így igény merült fel új határértékek megállapítására. […] Megkülönböztettek 24 órás és 30 napos, illetve éves határértékeket." [7] Budapest területét felosztották és tisztaságvédelem szempontból különböző kategóriákba sorolták, amelyekre a 21/1986. (VI. 2.) MT rendelet alapján eltérő határértékeket állapítottak meg. A „kiemelten védett" kategóriában „védett I." „védett II." csoportokba osztották a főváros részeit, az előbbibe a főváros legnagyobb hányadát, az utóbbiba az iparterületeket osztották be [7].

Napjainkban a magyar jogszabály az EU-irányelvekkel összhangban álló szabályokat rögzít a levegőtisztaság védelméről. A légszennyezettségi határértékekről, a helyhez kötött légszennyező pontforrások kibocsátási határértékeiről a 14/2001. (V. 9.) KöM-EüM-FVM együttes rendelet, míg a kibocsátás ellenőrzésével és értékelésével kapcsolatos feladatokat a 17/2001. (VIII. 3.) KöM rendelet szabályozza. A korábban érvényben lévő védettségi osztályok megszűntek, a légszennyezettség egészségügyi határértékei az egész ország területére érvényesek. Ezek alól kivételt képeznek az ökológiailag érzékeny területek, amelyekre külön határértékeket állapítottak meg [7].

„Levegőminőséggel kapcsolatos (szén-dioxid, ammónia és por) méréseket Budapesten Fodor József (1843–1901) végzett elsőként a Budapesti Orvostudományi Egyetemen a 19. század végén. Az első kifejezetten ilyen tárgyú tanulmány *A füst elleni küzdelem kérdésének állása hazánkban és külföldön* címmel 1928-ban jelent meg Frischfeld Ede, Hubert Ernő és Johan Béla szerkesztésében a *Népegészségügy* folyóirat IX. évfolyamának 10. számában. Ennek hatására a Székesfővárosi Közegészségügyi és Bakteriológiai Intézet nagyobb anyagi támogatásban részesült, és megkezdődhettek a légszennyezettség vizsgálatát célzó teljesebb körű mérések. Az 1930-as évektől kezdve beszámoltak kutatási eredményeikről, többek között felismerték a légszennyezettség és az időjárási tényezők, valamint az energiahordozók minősége közti összefüggést (Városi Szemle 16. évf., 1930; Népegészségügy XX, 1935)" [7]. Mérőhelyek a Gyáli úton és a József körúton voltak a fővárosban 1935-ben, de a rá következő két évben több állomással is növekedett a számuk (lásd az 1. ábrát). Ez lehetővé tette egyidejűleg több mérés elvégzését, amely átfogóbb kép kialakulásához vezetett a város levegőjének akkori koromtartalmát és térbeli eloszlását illetően. Mérőpontokat helyeztek el a forgalmas belvárosi kerületekben és a külvárosi körzetekben egyaránt.



1. ábra

Az 1930-as évek végén létesített levegőminőségi mérőhelyek Budapesten [7]

Az Egészségügyi Világszervezet (WHO) által kiadott ajánlásához igazodva 1979 januárjában átszervezték a mérőhálózatot, és az állomások számát csökkentették. Az így felszabaduló készülékeket a közlekedési csomópontok, gyárak vagy nagyobb üzemek közelébe helyezték át, amelyek a lakosság egészségét potenciálisan veszélyeztető szennyezőforrásoknak bizonyultak. Az átszervezés célja az volt, hogy olyan adatsorokat kapjanak, amelyek lehetővé teszik a külföldi nagyvárosok eredményeivel való összehasonlítást [7].

Külföldi légszennyezettségi állapotok rövid összefoglalása

A légszennyezettség nem tiszteli az országhatárokat. A légmozgás szállítja a nehézfémeket és az ellenálló szerves gyököket, szennyezve a vizeket és a talajt távol az eredési helyüktől is. A kései 1990-es években az erdőtüzek, főleg Indonéziában, óriási füstfelhőket képeztek, amelyek hónapokig lebegtek a szomszédos délkelet-ázsiai országok felett. Iskolákat és óvodákat kellett bezárni, míg a helyi kórházak nagyszámú, ködd el kapcsolatos megbetegedéses gyermeket jelentettek. Az 1952-es *Nagy Londoni Köd* rászorította a világ figyelmét a légszennyezettség problémájára, és azóta jelentős javulás történt a fejlett országokban. Akárhogy is, minden évben a kinti levegőszennyezettség Európán belül több száz, világviszonylatban nézve több mint 24 ezer gyermek haláláért felelős. Az ipari növekedés és a gyors urbanizáció szítja a problémát, olyan terhet róva ki ezzel, amelyet leginkább a világ fejlődő nagyvárosaiban lehet érzékelni. A tisztább üzemanyagok és technológiák, továbbfejlesztett motorok, és a tömegközlekedés használata alapvető fontosságú, hogy biztosítsa a gyermekek számára a tiszta levegőt.

Az 1996-os olimpiai játékok idején a tömegközlekedést ösztönözték, valamint Atlanta egyes részeit lezárták a magángépjárművek előtt, és ösztönözték a távmunkát. Az ózonszennyeződés által előfordult akut asztmaesetek száma 42%-kal csökkent. A kibocsátáscsökkentő stratégia a játékok ideje alatt a következő lépéseket foglalta magában: 24 órába integrált tömegközlekedési rendszer, ezer további busz, a helyi üzletek alternatív munkaideje és az otthoni munkavégzés, a városközpont lezárása a magángépjárművek előtt, nyilvános figyelmeztetések a potenciális közlekedési és levegőminőségi problémákra. A következő eredményeket jelentették: az olimpiai játékok idején az ózon koncentrációja 28%-ot zuhant, 217%-kal többen használták a tömegközlekedést, 11–44%-kal csökkent az akut asztmaesetek száma [9].

London levegőszennyezettsége

A London típusú füstköd (smoke és fog) szóból ered a szmog szó, amelyet reduktív szmognak is szoktak említeni a füstködben lévő korom korrodáló hatása miatt. Az Egyesült Királyságban a 19. században észlelték először, hogy változott a náluk viszonylag sűrűn előforduló köd szaga, színe, vastagsága és gyakorisága. Az 1980-as évekig rendszeres jelenség volt, amelynek kialakulásához a sajátos időjáráson túl a légszennyezés nagyban hozzájárult. Bár felfigyeltek a fűtés és a téli köd összefüggésére, de a rossz tüzelési módot okolták a rossz minőségű tüzelőanyagok helyett. Akkoriban széntüzelés volt jellemző a lakossági és az ipari méretű energia-előállításban, amelynek minősége romlott az első világháború utáni gazdasági visszaesés miatt.

A 20. század elején már Londonban, sőt egész Nagy-Britanniában a korábbiakhoz képest jelentősen kevesebb ködös napot figyeltek meg, azonban a légszennyezés intenzitása nem csökkent, mivel a 20. század elejére a korábban épített épületek, berendezések felújítására nem került sor. A málladozó, erősen korrodálódott épületek és bomló berendezések a légszennyező anyagokkal vegyülve kémiai reakcióba léptek (például a vasúti tartóoszlopok a kénes füst miatt csaknem 10%-ban tartalmaztak vas(II)-szulfátot [$FeSO_4$]).

A 20. század közepére tovább romlott a helyzet és – jellemzően a téli évszakokban – újra rendszeressé vált a büdös és már feketévé váló füstköd, amelyből a kiáramló korom miatt korrodálódtak a fémek, megfeketedtek házfalak, illetve textíliák [10].

A (London-típusú) füstköd főként télen, fagypont körüli (–3 és +5 °C közötti) hőmérsékleten, szélcsend, magas légnyomás és jellemzően magas páratartalom és az úgynevezett inverzió légjelenség mellett, kén-dioxid, szén-monoxid, por és korom jelenlétében alakul ki. Magyarországon 1990. januárban Budapesten és Miskolcon volt tapasztalható ilyen típusú szmog.

Los Angeles levegőszennyezettsége

A világ más nagyvárosaiban sem jobb a helyzet, sok helyen kifejezetten rosszabbul állják meg helyüket a légszennyezés elleni harcban. Az amerikai Kalifornia állam egészében – az AirNow szerint – a levegőminőségi indexet használva, a levegő minősége

többnyire átlagos (51-től 100-ig terjed, ami sárga zónás) és középtávon elfogadható minőségűnek tekintett. Azonban Los Angelesben a levegő minősége ózonos (101-től 150-ig terjed, ami már narancssárga zónás) és az érzékenyebb szervezetekre (mint például, akik enyhébb asztmában szenvednek) káros. Az Amerikai Tüdő Egyesület (American Lung Association) szerint az ózon általi egészségügyi kockázatokba beletartozik a fejlődési és immunrendszer károsodása, asztmarohamok, tüdőrák, légszomj és akár a korai halál. Az Amerikai Egyesült Államok által jelenleg legrosszabbul kontrollált és egyik legveszélyesebbnek tekintett szennyező az ózon [11].

A közlekedés által kibocsátott (nitrogén-oxidok, szénhidrogének, szénmonoxid) légszennyező-anyagok alacsony páratartalom és 2 m/s alatti gyenge légmozgás mellett, 25–35 °C hőmérsékletű erős napsugárzás (UV-sugárzás) hatására fotokémiai folyamatot indítanak el, amely során nitrogén-dioxid és ózon, majd szabadgyökök, hidrogén-peroxid és peroxi-acetil-nitrát (PAN) keletkezik. Ezekből jön létre az oxidáló (Los Angeles-típusú, fotokémiai) szmog, amely a nagy forgalmú, száraz, napfényes nyarú területeken jellemző, különösen, ahol a levegő megreked (például Los Angeles, Athén, illetve 1985 óta Magyarország is ide sorolható) [10].

Spanyolország légszennyezettségének állapota (nitrogén-oxid és ózon)

Míg Toledóban egy járókelő a madridi Gran Vía sugárúton kialakult közlekedési dugó által szennyezett levegőt szívja be, Sierra Norte-ban, Madridon kívül emberek százai a fővárosból azzal a tudattal töltik a hétvégéjüket, hogy tiszta, friss levegőt szívnak, anélkül, hogy tudnák, tavaly az volt az egyik legszennyezettebb levegőjű terület Spanyolországban.

Mindeközben egyéb vidéki területeken, mint amilyen a Vic-i puszta Katalóniában és a falvakban, mint Villaneuva del Arzobispo Jaén-ban, Andalúziában olyan szinten van a szennyezettség szintje, hogy megszegi az EU levegőminőségi szabályzóit.

Ez csak néhány példa a pollenparadoxonokból, amelyek – az *El País* népszerű spanyol napilap becslése szerint – ártóan hatnak Spanyolországban legalább 15 millió ember egészségére. A legsúlyosabban fertőzött területek Madrid és Barcelona, de az andalúziai, extremadurai, Kasztília-La Mancha-i és valenciai régiók szintúgy magas kockázati szintekkel küzdenek.

Spanyolország fő szennyezői a nagyvárosokban uralkodó, közlekedésből eredő nitrogén-oxidtól a közlekedés, a központi fűtőrendszerek, a gyárak és az építkezések által termelt porból, hamuból, koromból és hasonló anyagokból álló PM_{10} részecskeanyagoktól és végül a többihez kapcsolódó ózontól, amelynek nem árt a meleg időjárás és nagy távolságokra képes szétszóródni – amiért a tisztának feltételezett területek, mint Madrid Sierra Norte-ja magasan szennyeződhetett.

Az úti forgalom, különösen a dízelautók felelősek a nitrogén-dioxid (NO_2) kibocsátás több mint 50%-áért.

A spanyol Ökonómiai Átmenet Minisztériuma 2017-ből származó legfrissebb adatai felhasználásával az *El País* kiszámította azoknak a számát, akikre hatással voltak a fentiekben leírtak, számításba véve azon területek lélekszámát, ahol a három szennyező túllépi az EU-s limitet.

Mindegyik zónában van egy vagy több levegőminőség-mérő állomás. Elég, ha csak az egyik állomás nagyobb értéket mutat a megengedettnél, és máris nem felel meg a törvényi követelményeknek. Ez a legnagyobb vagy legnépesebb régiókban, mint például Andalúzia, elég gyakori jelenség.

Az Ecologists in Action környezetvédelmi szervezet tavaly 17,5 millió spanyol emberre tette azok számát, akik rossz minőségű levegő hatása alatt állnak. Az Ökológiai Átmenet Minisztériuma szerint lehetetlen úgy pontosan felmérni az egészségügyi hatást, hogy minden egyes állomás által lefedett terület népességi számadatához csak az egyes régiók férnek hozzá.

Amennyire a kormány érintett, a 2018-ból származó előzetes pollenszint adatok „mutatnak bizonyos javulást" különös tekintettel a nitrogén-dioxidra (NO_2). Az időjárás is segített, mivel több szél és eső volt. „Azt gondolhatnánk, hogy a hatóságok által bevezetett intézkedések működnek" – mondja a kormányszóvivő [12].

De Miguel Ángel Ceballos az Ecologists in Action-től szkeptikus. Bár elismeri, hogy a helyzet rosszabb volt a gazdasági válság előtt, továbbra is állítja: „a gazdasági helyreállás 2015-től beindította a problémát újra, azzal hogy megnőtt a fosszilis (szénalapú) üzemanyagok égetése és az ebből következő emissziók mértéke" [12]. Hozzáteszi, hogy a hatóságok nem alkalmaznak megfelelő intézkedéseket, hogy ezt visszafordítsák.

Az Ökonómiai Átmenet Minisztériuma azonban elismeri, hogy Spanyolországban 2017-ben az egyensúly negatív volt, ami azt jelenti, hogy az azt megelőző évben a levegő minősége rosszabb volt [12].

A légszennyezők egészségügyi kockázatai, keletkezésének okai

Elsősorban a rossz levegőnek a keringési és légzőszervekre való káros hatásait kell megemlíteni. A belélegzett levegővel az általa hordozott különböző apró részecskék, mint például a szálló por, bekerülnek a szervezetünkbe, illetve a véráramba is, izgatva a nyálkahártyákat, gyulladásokat, véralvadékonyságot, és ez utóbbiból kifolyólag vérrögösödést okozva. Kutatások kimutatták, hogy a légszennyezettség növeli a stroke, a koraszülés, a szív- és érrendszeri zavarok kialakulásának valószínűségét, valamint jelentősen kártékony hatással lehet a magzat agyi funkcióinak alakulására és egészségére nézve. Továbbá a kültéri levegő szállópor-tartalmának hosszú távú hatásaként a várható élettartam jelentősen csökkenhet a légzőszervi betegségek, valamint a tüdőrák miatti halálozás növekedése következtében.

Pszichés hatásait tekintve sem veszélytelen tényező a levegőszennyezettség. A *The Guardian* angol országos napilap szerint – a fiatalok sokkalta inkább hajlamosabbak depresszióra 18 évesen, ha 12 évesen rossz levegőnek vannak kitéve.

Az első arra irányuló elemzésben, hogy hogyan hatnak az általános levegőszennyező anyagok a tinédzserek szellemi egészségére, tudósok olyan fiatalokat találtak, akik 3-4-szer hajlamosabbak voltak depresszióra 18 évesen, amennyiben 12 évesen szennyezettebb levegőnek voltak kitéve. Korábbi munkájukkal összehasonlítva kimutatták, hogy a levegőszennyezettség nagyobb kockázati faktor a kamaszkori depresszió kialakulásában, mint a fizikai erőszak.

A szakértők szerint az eredmény különösen jelentős, mivel a mentális egészségügyi problémák 75%-a gyermekkorban vagy kamaszkorban kezdődik, amikor az agy viharos gyorsasággal fejlődik. A tanulmány összefüggést sejtet a szennyezett levegő és az antiszociális viselkedés között, azonban ennek megerősítéséhez további munkára van szükség. Egy nagyobb tanulmány várható még ebben az évben.

„A magas szintű légszennyezettség nem tesz sem neked, sem a gyermekednek jót, legyen szó a fizikai vagy mentális egészségről" – mondta Helen Fisher a londoni Kings College kutatásvezetője. „Észszerű dolog megpróbálni elkerülni a legszennyezettebb levegőjű területeket. Arra kellene szorítani a helyi és nemzeti kormányokat, hogy csökkentsék ezeket a szinteket" [13].

A *Psychiatry Research*ben publikált tanulmány londoni gyermekek vonatkozásában gyűjtött össze részletes adatokat a légszennyezettség hatásairól. A 284 tanulmányozott gyermekből, akik 12 évesen a legszennyezettebb levegőjű területek felső 25%-ában éltek kiderült, hogy 18 éves korukra 3-4-szer lesznek hajlamosabbak depresszióra, azokhoz képest, akik a legkevésbé szennyezett területek 25%-ában élnek. Összehasonlításképpen a korábbi kutatás kimutatta, hogy azoknál a gyermekeknél, akik fizikai erőszaktól szenvednek másfélszer esélyesebb a depresszív zavarok kialakulása. A kutatók számításba vették azokat a dolgokat, amik hatással lehetnek a mentális egészségre, mint a családon belül örökletes mentális betegségek, a jövedelem mértéke, erőszak és dohányzási szokások. Nézték az idegesség és az ADHD mértékét, azonban nem találtak kapcsolatot a levegőszennyezettséggel.

Az antiszociális viselkedés kockázatának növekedése 3-5-ször magasabb volt, de a depresszióhoz való kapcsolattól eltérően az eredmény nem volt statisztikailag jelentős, minden bizonnyal azért, mert a kutatásban szereplő rossz magaviseletű kamaszok száma alacsony volt.

A fizikai egészséggel összevetítve a légszennyezés szellemi egészségre való hatása sokkal kevésbé volt tanulmányozva eddig. A felnőtteken való kísérletezés eddig egymásnak ellentmondó eredményeket produkált, bár bizonyíték van rá, hogy a légszennyezés hosszabb távon akár jelentős mértékű intelligenciacsökkenést is eredményezhet. Bár a tanulmány célja nem a kamaszkori depresszió okának felfedése, Fisher szerint a mérgező anyagok okozta belső láz a legvalószínűbb: „Tudjuk, hogy a szennyezőrészecskék elég kicsik ahhoz, hogy átjussanak a vér-agy gáton, és tudjuk, hogy hatalmas összefonódások vannak az agyban lévő belső láz és a depresszív tünetek kialakulása között" [13].

Állítása szerint a gyermekek és a kamaszok különösen sérülékenyek, hiszen ebben az életszakaszban intenzív az agyi fejlődésük és jelentős hormonális változásokon mennek keresztül, valamint sok stresszhatás éri őket a világ megismerése közben, mint például a tanulmányaik során a számonkérések, illetve maga a munkakeresés folyamata.

A légszennyezés során egészségügyi szempontból is a gyermekek a legsebezhetőbbek. A gyerekek tüdőfejlődése születéskor még nem fejeződik be, hanem keresztülmegy különféle érproliferációkon egészen 2 éves korig, és még tovább fejlődik 5-8 éves korig. A tüdő a teljes méretét csak a kamaszkorban, a végleges testmagasság kialakulásakor éri el.

Valamint a felnőttekhez képest az újszülötteknek és kisgyermekeknek gyorsabb az anyagcseréjük és oxigén-felhasználásuk, mivel nagyon gyorsan növekednek, valamint a méretükhöz képest megnövekedett oxigénszükséglethez a felnőttekétől keskenyebb légútjuk van. Ezért a felnőtteknél egy kis légúti irritáció enyhébb reakciót vált ki, mint egy kisgyereknél, akiknek légútját el is dugíthatja ugyanakkora mértékű szennyeződés. Ennélfogva bármilyen légszennyezőnek sokkal inkább ki vannak téve [9].

Fisher szerint fontos a további kutatás, mert a levegőpollenek elleni harc kevésbé küzdelmes, mint a többi olyan faktor, amely pszichikai sérülést okozhat. „Ha meg tudjuk érteni, hogy miről van szó, akkor lehetőségünk nyílik a korai beavatkozásra, és hogy tegyünk ellene valamit" – mondta [13].

„Ez a tanulmány felhívja a figyelmet a levegőpollenek veszélyeire az Egyesült Királyságbeli tinédzserpopuláció körében, különös tekintettel azokra, akik városi környezetben élnek, ahol a mentális problémák gyakoribbak." – mondta Robin Russel-Jones közegészségügyi orvos [13].

Az Egyesült Királyság nagy részében a levegő nitrogén-oxid koncentrációja határérték feletti szinten van, és az apró részecskeszennyeződés mértéke sok helyen meghaladja az Egészségügyi Világszervezet (WHO) irányértékét. A kormány elfogadja, hogy a szennyezett levegő megrövidíti a gyermekek életét és károsítja őket, azonban a legújabb akcióterve az útmenti polleneket illetően „szánalmasnak" lett leírva a környezetvédelmi ügyvédek által.

A Doctors Aganist Diesel kampány egyik alapítója, Chris Griffiths professzor szerint további kutatások szükségesek, azonban a fiatalok mérgező levegőnek való kitettségének drámai szintű csökkentésének sürgőssége megmaradt.

„A fejlemények igazán sokkolóak és elszomorítóak, jól mutatván azt, hogy mennyire kritikus dolog az, hogy a népegészségügyi krízis megfelelően legyen kezelve" – mondta Jenny Bates a „Föld Barátaitól" [13].

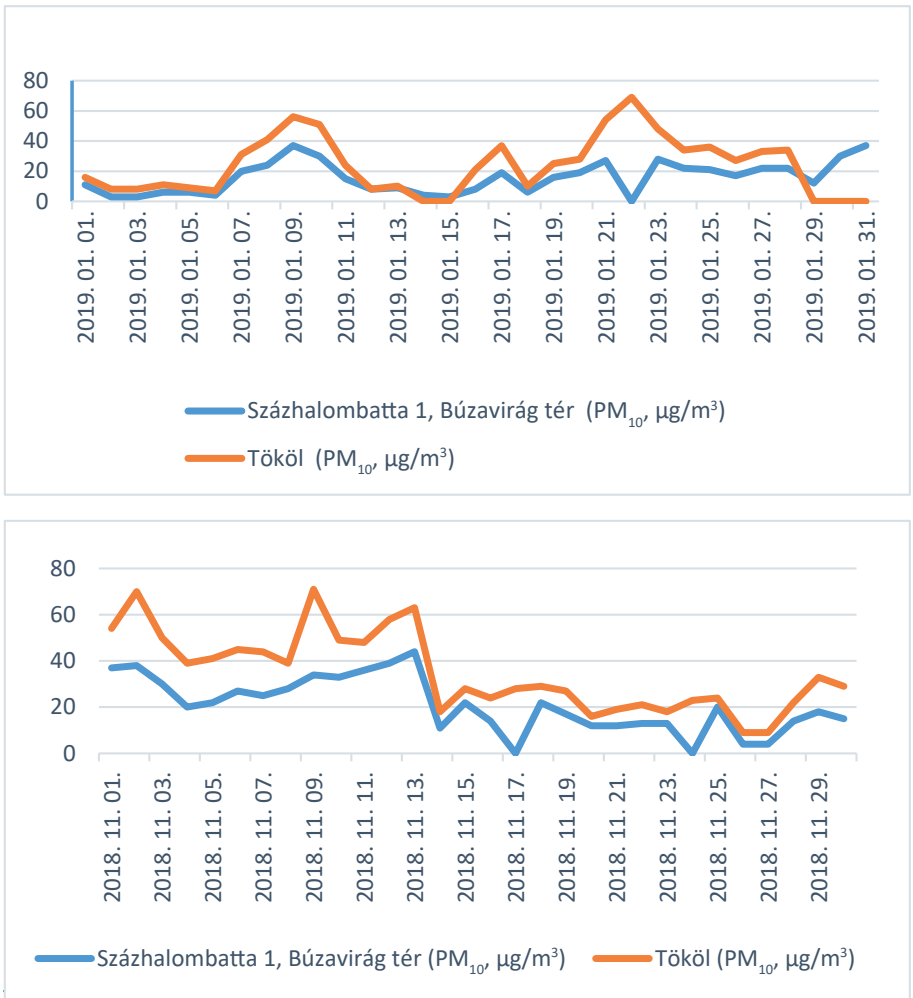
A Medact egészségügyi jótékonysági szervezetnél Rebecca Daniels azt mondta, hogy „a kormány válasza erre nagyon hiányzik – robusztus és átfogó jogszabályokra van szükség a tiszta levegőt illetően, beleértve a szennyező járművek számának drasztikus csökkentését az utakon" [13].

Következtetés

Az Európai Unió eddigi évtizedes törekvései a tagországok károsanyag-kibocsátásának mérséklésére eddig – a levegőszennyezést tekintve – nem hoztak túl nagy eredményt, így feltételezhetően az ebből adódóan bekövetkező megbetegedések és halálozások száma továbbra is növekvő tendenciát fog mutatni. Úgy vélem, a légszennyezés visszaszorítására jól átgondolt és szervezettebb nemzeti és nemzetközi összefogásra lenne szükség. Az állami és nemzetközi szabályozásokon túl, nagyobb ráfordítás és komolyabb vezetés mellett országos szinten energiatakarékos és környezettudatos technológiákra való maradéktalan átállás lenne a megoldás, valamint a dízel üzemanyaggal működő járművek városi közlekedésből való kivonására.

Hazánk vegyipara nagyon összetett, a levegőminőség megóvása érdekében tett törekvések több irányból is szolgálják a környezetvédelmi elveket [14], [15]. Azonban

fontos tény, hogy jelentős mértékben fosszilis energiahordozókra épül hazánk vegyipara, szezonálisan az évben többször előfordulhat, hogy a határértékek feletti egyes szennyezőkomponensek jelenléte. Példaként a 2. ábrán bemutatom Tököl, és Százhalombatta 2018. novemberi, és 2019. januári időszakban mért PM_{10}-koncentrációját. A határérték 50 µg/m³, tehát egyértelműen látható, hogy esetenként a mért értékek túllépik a megengedett tartományt, amelyet adott légköri jelenségek elősegíthetnek.



2. ábra

A PM_{10} koncentrációja µg/m³ értékben Százhalombatta és Tököl városok levegőszennyezettségének bemutatására [16]

(Megjegyzés: határérték 50 µg/m³)

Hivatkozások

[1] A. Mészáros, „A magyar környezetvédelem – Légszennyezés és levegőtisztítás," 2014. 09. 15. [Online]. Elérhető: http://kornyezetblog.weebly.com/andras/a-magyar-kornyezetvedelem-legszennyezes-es-levegotisztitas (Letöltve: 2019. 02.13.)

[2] Á. Rédey, A. Fejes Lászlóné Utasi, T. Yuzhakova és L. Dióssy, *Környezetállapot értékelés,* Veszprém: Pannon Egyetem – Környezetmérnöki Intézet, 2014. [Online]. Elérhető: www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0089_06_kornyezetallapotertekeles/adatok.html (Letöltve: 2019. 02. 13.)

[3] Országos légszennyezettségi mérőhálózat, „Főbb légszennyező anyagok egészségügyi határértékei, a 4/2011 (I. 14.) VM rendelet 1. melléklet alapján," országos légszennyezettségi mérőhálózat. [Online]. Elérhető: http://levegominoseg.hu/hatarertek?AspxAutoDetectCookieSupport=1 (Letöltve: 2019. 02. 13.)

[4] A. Holes szerk., *Magyarország környezeti állapota 2017,* Budapest: OOK Press Kft., 2018.

[5] A. Berezow, "Carbon Monoxide Kills More Americans Than Mass Shootings, Terrorism Combined," American Council on Science and Health, March 6. 2017. [Online]. Elérhető: www.acsh.org/news/2017/03/06/carbon-monoxide-kills-more-americans-mass-shootings-terrorism-combined-10954 (Letöltve: 2019. 02. 23.)

[6] L. Riesz szerk., *Magyarország környezeti állapota 2015.,* Budapest: Adu Press Kft., 2016.

[7] S. Zichler, R. Ocskay és I. Salma, *Budapest levegőszennyezettségének története,* Budapest: ELTE – Kémiai Intézet, Levegő Munkacsoport, 2007.

[8] L. Bozó, J. Szlávik, B. Vaskövi és I. Váraljai, „Az 1990–2003 közötti időszak levegőminőségének értékelése" („A levegőminőség alakulása Magyarországon az 1990–2003 közötti időszakban" című tanulmány alapján), Környezetvédelmi és Vízügyi Minisztérium, 2004.

[9] World Health Organization (WHO), "Outdoor air pollution – Children's Health and the Environment", World Health Organization (WHO), July 2008. [Online]. Elérhető: www.who.int/ceh/capacity/Outdoor_air_pollution.pdf (Letöltve: 2019. 02. 23.)

[10] A. Anda, *Levegőtisztaság védelem,* Kempelen Farkas Hallgatói Információs Központ, 2011. [Online]. Elérhető: www.tankonyvtar.hu/hu/tartalom/tamop425/0032_Levegotisztasagvedelem/adatok.html. (Letöltve: 2019. 02. 13.)

[11] M. Espiritu, "California/Los Angeles Air Pollution," *Gryphon Gazette,* 03 February, 2019.

[12] E. Sánchez és E. G. Sevillano, "15 million Spaniards are breathing air the EU considers polluted," *El País,* 7 December, 2018. [Online]. Elérhető: https://elpais.com/elpais/2018/12/05/inenglish/1544008632_514634.html (Letöltve: 2019. 02. 14.)

[13] D. Carrington, "Growing up in dirty air quadruples chances of developing depression," *The Guardian,* 30 January, 2019.

[14] J. Dobor, "Major Chemical Accidents in the 21st Century Europe and its Lessons Learned in Higher Education," *AARMS,* vol. 16. no. 3, pp. 93–108, 2017.

[15] J. Dobor, „Veszélyes gázok felhasználási lehetőségei az iparban és a mezőgazdaságban, illetve e tevékenységek kockázatai," *Hadmérnök,* 13. évf. 1. sz. pp. 28–42, 2018.

[16] Földművelésügyi Minisztérium, „Országos Légszennyezettségi Mérőhálózat," *Földművelésügyi Minisztérium,* [Online]. Elérhető: www.levegominoseg.hu/automata-merohalozat (Letöltve: 2019. 02. 14.)

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG, ABV- ÉS KATASZTRÓFAVÉDELEM

14. évfolyam (2019) 3. szám 35–51.
DOI: 10.32567/hm.2019.3.4

Hábermayer Tamás,[1] Túriné Barta Ágnes,[2]
Sárossy Gábor,[3] Kiefaber Gábor[4]

A katasztrófavédelmi műveletek támogatása önkéntesek bevonásával

The Use of Volunteers to Support Disaster Management Operations

A katasztrófavédelem sikeresen szavatolja az ország lakosságának és anyagi javainak védelmét. Viszont annak ellenére, hogy a védelmi szervezetek alapvetően rendelkeznek a különböző veszélyek elhárításához, a károk felszámolásához szükséges erőkkel és eszközökkel, a mindennapi életben előfordulhatnak olyan veszélyhelyzetek, katasztrófák, amelyek során szükségessé válhat a mentő erők önkéntes mentőszervezetekkel történő megerősítése vagy a nemzetgazdaságból anyagi és technikai erőforrások bevonása. A katasztrófavédelmi műveletek sikere öt fő tényező folyamatos koordinációja révén valósul meg (információ, legitimáció, időbeliség, technikai eszközök, humán erőforrás), amelyek működését a szerzők a cikkben vizsgálják.

Kulcsszavak: **katasztrófavédelem, önkéntes, ár- és belvíz**

Disaster management successfully guarantees the defence of country citizens and their goods. Despite the fact that defence organisations have the necessary tools and numbers to prevent the different dangers and to settle the damages, during the normal daily routine there can be hazardous situations or disasters, when the rescuing forces must be strengthened with volunteer organisations or material and technical resources from the national economy. The success of the

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: dr.habermayer.tamas@katved.gov.hu, ORCID: https://orcid.org/0000-0002-6677-9163
[2] BM Országos Katasztrófavédelmi Főigazgatóság, kiemelt előadó, e-mail: agnes.turinebarta@katved.gov.hu, ORCID: https://orcid.org/0000-0001-5782-3997
[3] Tolna Megyei Katasztrófavédelmi Igazgatóság, megyei polgári védelmi főfelügyelő, e-mail: gabor.sarossy@katved.gov.hu, ORCID: https://orcid.org/0000-0002-0004-560X
[4] Szekszárdi Katasztrófavédelmi Kirendeltség, kirendeltség-vezető, e-mail: gabor.kiefaber@katved.gov.hu, ORCID: http://orcid.org/0000-0003-1803-9563

disaster management operations depends on the coordination of five main factors (information, legitimacy, temporality, technical capabilities, human resources).

Keywords: **disaster management, volunteer, support, flood and inland water**

Bevezetés

A katasztrófavédelem nemzeti ügy. A 2012-ben megújított katasztrófavédelmi törvény alapján megalakult rendszer immáron hat éve működik, szavatolja a lakosság és az anyagi javak biztonságát. Az eltelt időszakban a katasztrófavédelem folyamatos fejlődése mellett a szervezet hatás- és jogköre is bővült. A feladatok egyre növekvő száma újabb és újabb kihívásokat eredményez, a sikeres és eredményes teljesítéshez viszont egyre több erőforrásra van szükség. A hazai katasztrófavédelem rendszere természetesen nemcsak katasztrófák vagy más veszélyek esetén lép működésbe, hanem naponta több száz tűzoltói beavatkozást, hatósági ellenőrzést hajt végre, a folyamatos szakmai képzés és gyakorlatok mellett. A területi és helyi szervezetek kialakítása során alapvető követelmény volt, hogy azok legyenek képesek a napi szintű feladatok végrehajtására, valamint egy kiterjedt káresemény bekövetkezése esetén, a kialakult helyzetnek megfelelően, a szükséges erők és eszközök átcsoportosítására, erőcsoportok kialakítására. Az érintett helyi és területi szervek kezelik az eseményt, szükség esetén megváltozott munkarendben, vagy túlmunka elrendelésével, esetenként más katasztrófavédelmi szervektől átvezényelt állomány megerősítésével. Bármennyire is kiterjedt az esemény, a napi feladatokat is el kell végezni. Adott esetben egy kiemelt beruházás hatósági véleményezése nem csúszhat időben azért, mert a hatósági osztály állománya árvíz elleni védekezési feladatokat lát el vezénylés alapján. Ezért fontosabbá válik ilyen esetekben a személyi állomány és a korlátozottan rendelkezésre álló erőforrások elosztása, a lehetséges megerősítő erők igénybevétele. A műveletek során akkor hatékony a működés, ha a koordinációs tényezők egyensúlya megvalósul. A megerősítő – támogató erők közül speciális helyzetben vannak az önkéntesek, akiket tudatosan egyre inkább bevon a katasztrófavédelem a védekezési feladatok ellátásába.

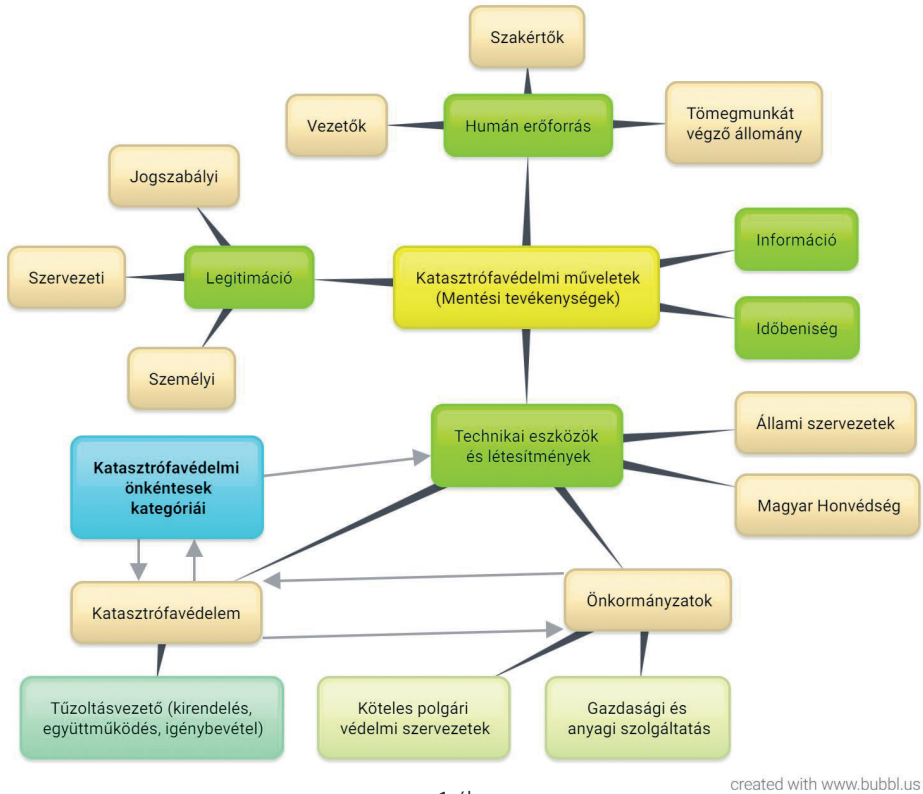
Az önkéntes tűzoltóságok és mentőszervezetek mentési képességének javítása érdekében az Országos Katasztrófavédelmi Főigazgatóság évente több százmilliós pályázatot ír ki. A Főigazgatóság a kiírás részleteit, a pályázathoz szükséges valamennyi dokumentumot, illetve később a nyertes pályázatok információit minden évben közzéteszi a hivatalos honlapján. A szervezetek a pályázaton elnyert összeg jelentős részét eszközbeszerzésekre fordítják. Ezen eszközök palettája széles, a quadoktól kezdve a drónokig, a csapatszállító eszközöktől kezdve a mentőcsónakokig sok minden megtalálható benne. A pályázatokon elnyert eszközök sok esetben speciális szakértelmet is igényelnek (például kishajóvezetői jogosítvány, búvár képzettség), amellyel az érintett önkéntes szervezetek tagjai rendelkeznek, és így kiegészíthetik a katasztrófavédelmi állomány szakértőit, beavatkozóit.

Felmerül ugyanakkor a kérdés, hogy a katasztrófavédelmi rendszer képes-e hatékonyan kezelni az önkéntesek állományát, eszközeit. A téma aktualitását a műveletek támogatásába bevont önkéntesek egyre növekvő száma adja, akik minden alkalommal jelentős mértékben hozzájárulnak a védekezések sikeréhez. 2010-ben mind az árvízi

védekezéseknél, mint a vörösiszap-katasztrófa elhárításánál napi szinten több ezer fő önkéntes jelentkezett és segítette a mentési feladatokat. A 2013-as rendkívüli árvíz esetében még nagyobb önkéntesi részvételről beszélhetünk, és a sikeres védekezés tovább alapozta az önkéntesség erejét. Esetünkben a cikk és a kutatás célkitűzése az, hogy vajon a katasztrófavédelmi önkéntesek tényleg képesek-e hatékonyan támogatni a katasztrófavédelmi műveleteket, valamint kellőképpen hatékonyan történik-e az önkéntesek eszközeinek nyilvántartásba vétele. A célkitűzéseket a szerzők a rendelkezésre álló szakirodalom feldolgozásával és elemzésével, valamint az eddigi szakértői és nemzetközi szintű tapasztalataik felhasználásával végzik.

A katasztrófavédelmi műveletek koordinációjának tényezői, azok tartalma és egymáshoz való viszonya

A katasztrófavédelmi művelet fogalmát a BM OKF Főigazgató 61/2016. számú intézkedése határozza meg: az adott káreseménnyel kapcsolatos iparbiztonsági, polgári védelmi, tűzmegelőzési, tűzoltási, műszaki mentési, valamint tűzvizsgálati tervezési, szervezési, beavatkozási, lakosságvédelmi és hatósági tevékenység. A katasztrófavédelmi műveletek célja az adott káresemény kezelése, a veszély elhárítása, a tapasztalatok összegyűjtése és elemzése, a megelőzés során történő felhasználása, a helyreállítás/újjáépítés megvalósítása. A katasztrófavédelmi műveletek alaprendeltetésükből adódóan lehetnek mentési, megelőzési, tervezési, szervezési, lakosságvédelmi és hatósági tevékenységek. Az önkéntesek bevonhatósága kapcsán a következőkben kiemeljük a mentési tevékenységek (iparbiztonsági, polgári védelmi, tűzoltási és műszaki mentési) végrehajtását, és a továbbiakban elemzésünk csak erre korlátozódik. A katasztrófavédelmi műveletek (mentési tevékenységek) koordinációjának megértéséhez a szerzők készítettek egy fogalomtérképet, amelyen keresztül egyszerűsített formában, könnyen átláthatóvá válnak a tényezők (világoszöld színnel jelölve) és azok tartalma. A cikk e részében az információ, humán erőforrás, legitimáció és időbeliség magyarázata történik, az utolsó, a technikai eszközök részletezése annak terjedelme miatt a következő önálló fejezetben jelenik meg.



1. ábra

A katasztrófavédelmi műveletek (mentési tevékenységek) koordinációja

[a szerzők szerkesztése]

A katasztrófavédelmi műveletek talán legfontosabb tényezőjeként van jelen az információ. Az 1. ábrán is látható, hogy közvetlenül kapcsolódik a mentési tevékenységekhez. Minden további tényező alapját képezi, hiszen, ha nem áll megfelelő módon és időben rendelkezésre, akkor az a műveletek minden további tényezőjére hatást gyakorol. Hiánya esetén a humán erőforrások, valamint a technikai eszközök és létesítmények bevetése nem tervezhető megfelelően, hiszen nem tudható, hogy mekkora létszám vagy mennyiség, milyen kapacitás szükséges. Amennyiben túl sok, a feldolgozás (ellenőrzés) a műveletek lelassulását eredményezheti. Téves információ pedig félrevezet, erőket mozgat meg feleslegesen, vagy annak ellenkezőjeként nem a megfelelő módon történik a beavatkozás, ami viszont kudarcot okoz.

A műveletek következő fontos tényezője a humán erőforrások meglétének kérdése. Ahogy az ábra is mutatja, három fontos alkategóriára (vezető, szakértő, tömegmunkát végző állomány) bontható elemzésünk szempontjából. Amennyiben nincsen meg a szükséges létszám a védekezések végrehajtásához, valamint nem valósul meg a hármas felbontás egészséges arányban történő eloszlása, akkor az egész tevékenység sikertelenné válik. A három önálló humán alkategóriát mindenképpen

el kell különíteni (vezetők, szakértők, tömegmunkát végző állomány) egymástól. A siker szempontjából mindegyik ugyanolyan fontossággal bír, és egyik a másik nélkül nem képes a feladatok elvégzésére. A vezetői állománynak kell átfognia a védekezés egészét, átlátni a folyamatokat, és szükség esetén korrigálni a működést. A koordináció szempontjából a vezetők döntései határozzák meg az erők, eszközök elosztását az egyes feladatok végrehajtásához. Ha kell, akkor többleterőforrás-igényeket kell leadniuk, amely ugyanakkor nem lehet túlzó, hiszen előfordulhat, hogy a korlátozott rendelkezésre állás miatt másokkal is osztozni kell. A vezetőknek rendszerben kell gondolkodniuk, hiszen hiába oldanak meg egy feladatot, ha az nem csak rajtuk múlik. Vegyünk példának egy árvízi védekezést, amelyben több vezető egymást követő szakaszokon védekezik. Hiába teljesít jól egyikük, és nyeri meg saját területén a védekezést, hiszen, ha a többiek közül egy is elbukik, akkor a víz betör, és minden vezető munkája értelmetlenné válik, a védekezés sikertelenül zárul.

A következő szerep a szakértőké. Hogy ki válik azzá, azt mindig az egyes katasztrófatípusok határozzák meg. Amíg ár- és belvízi védekezés szempontjából egy vízügyi szakember a szakértő, egy járvány esetén orvos válhat azzá. Ők a különleges ismeret vagy képzettség birtokában speciális feladatok ellátására alkalmas személyek. Jellemző, hogy más, képzetlen személyt az adott feladatra nem is lehet igénybe venni (például búvárt nem helyettesítheti pilóta az árvízi védekezésnél), ezért szerepük felértékelődik. Ők a védekezésben részt vevők önálló csoportját fogják alkotni, akiket a vezetők egyedi, speciális feladatra terveznek.

A tömegmunkát végző állomány a harmadik kategória. Esetükben a feladatuk végzése külön felkészítést és megfelelő vezetői irányítást igényel, amelynek megléte és a megfelelő létszám esetén válnak biztosítottá a műveletek. A harmadik koordinációs tényező a legitimáció. Magyarországon jogrendszer működik, a mentési tevékenység végzése hatáskörön és illetékességen alapul. Az egyes védekezések kapcsán a felelősségi körök személyhez (például polgármester), illetve szervezethez kötöttek. A katasztrófavédelmi műveletek kapcsán a legitimáció megléte ugyanakkor azért válik kiemelt koordinációs feladattá, mert a katasztrófavédelmi szakemberek számára teljesen egyértelműek a szabályok, de a védekezés további résztvevőinél sajnos sok félreértés előfordul. Egy katasztrófahelyzetben ez pedig nem engedhető meg. Sajnos volt már arra példa, hogy civil egyesület (magát félkatonai szervezetként feltüntetve) próbálta meg a lakosságot irányítani árvízi védekezés idején. Az egyenruhájuk rendkívüli módon hasonlított a Magyar Honvédség, illetve a rendvédelmi szervek egyenruhájához, ez pedig megtévesztőleg hatott a helyi civilekre. Az irányításhoz azonban se szakképzettséggel, se szakmai tapasztalattal nem rendelkeztek, valamint súlyosbította a helyzetet, hogy nem kapcsolódtak be a védekezés rendszerébe, hanem önállók akartak lenni. A felelőtlenségükkel veszélyeztették a lakosságot, és rendőri beavatkozás vált szükségessé az ügy rendezése kapcsán. A negyedik tényező az időbeliség. Az irányítást végzőknek a megfelelő információ birtokában a kellő erő és a szükséges technikai és létesítményi ellátottság, valamint legitimáció egyidőben kell, hogy rendelkezésre álljon. Ha ez nem valósul meg, az a mentési tevékenység végrehajtását veszélyezteti. Az ár- és belvízi védekezés esetében például könnyen belátható, hogy hiába van a védekezés helyszínén homok és homokzsák, ha nincsen meg hozzá a legitim irányító és beavatkozó-állomány, aki a védművet építi és a további logisztikát szervezi.

A katasztrófavédelmi műveletek koordinációjának technikai eszköztényezője, -tartalma

Amennyiben a humán feltételek biztosítottak, akkor a technikai eszközök és létesítmények kérdésköre következik. Egy katasztrófa esetében a védekezés eszköz- és létesítményrendszerének alapját a katasztrófavédelmi szerveknél lévők adják. Ezek elsősorban a katasztrófavédelem napi szinten meglévő és működő technikai állományát, létesítményeit és raktározott készleteit jelentik, amelyek jogszabály által biztosított módon kiegészülhetnek további eszközök azonnali kijelölésével és műveletekbe vonásával. (Példa erre a tűz elleni védekezésről szóló törvény felhatalmazása a tűzoltásvezető részére, aki a törvény alapján a fegyveres erők, a rendőrség, a polgári védelem, a vám- és pénzügyőrség, a büntetés-végrehajtási és a környezetvédelmi szervek, a mentőszolgálatok és a közüzemi vállalatok kirendelését igényelheti.) Ezek a szervek, ha az alapfeladataik ellátását nem veszélyezteti, kötelesek eleget tenni a kirendelésnek [1], illetve a kiegészítés történhet például gazdasági és anyagi szolgáltatásra kötelezéssel [2], esetenként köteles polgári védelmi szervezetek alkalmazásával. Bár alapesetben nem ez a fő feladatkörük, de szükség esetén kormányzati (akár különleges jogrendi) intézkedésre, vagy az adott szervezet felsővezetői utasítására, esetenként együttműködési megállapodás vagy szerződés alapján az állami, karitatív és társadalmi szervezetek, önkormányzatok és a Magyar Honvédség erőforrásokat biztosíthatnak. Sok esetben az érintetteknek már kiépült rendszereik vannak (például MH – Honvédelmi Katasztrófavédelmi Rendszer) az igénybevétel megvalósítására.

Létesítmények kapcsán ez akár az alaprendeltetésüktől történő teljes eltérést is jelenthet átmeneti időszakra, hiszen befogadóhelyként, óvóhelyként vagy védett vezetési pontként is funkcionálhatnak, bár erősen kétséges, hogy ilyenkor teljesítik a szükséges építészeti és gépészeti jellemzőket [3]. A technikai eszközök esetében egyre inkább számolhatunk, számolnunk kell a katasztrófavédelmi önkéntesek eszközeivel is. Öt önkéntesi kategória létezik, mindegyik esetében az eszközellátottság és a támogatás lehetősége más és más. A mentési tevékenységek hatékonysága érdekében ugyanakkor ismerni célszerű őket. A katasztrófavédelmi önkéntesek esetében az alábbi kategóriákat kell megkülönböztetnünk [4].

1. állampolgárok (önkéntesen segítséget nyújtó személyek),
2. polgári védelmi szervezetek,
3. önkéntes civil szervezet
   a) önkéntesen közreműködő karitatív szervezet,
   b) önkéntesen közreműködő társadalmi szervezet,
4. gazdálkodó szervezetek önkéntesei,
5. nemzetközi önkéntesek:
   a) megfigyelők (például EU Koordinációs Csapat, ENSZ Katasztrófa Kárfelmérő és Koordinációs Csapat),
   b) beavatkozók (például EU Önkéntes Egységbe regisztrált modul, ENSZ Minősített Városi Kutató-Mentő Csapat).

A különböző kategóriák hatékonyan képesek támogatni a katasztrófavédelmi műveleteket, azonban az eszközeik nyilvántartásba vétele, a támogatásba történő bevonásuk

tervezése meglehetősen nehézkes. Az állampolgárok felajánlásai mozognak a legszélesebb spektrumon. Eszközeik bevonása nem tervezhető, hiszen azok folyamatosan változhatnak. Jellemzően egy adott katasztrófa miatt (például lakóhelyét, közeli hozzátartozóját érintő helyzet) válik önkéntessé, és az eszközeinek bevethetősége földrajzilag kötött. Ugyanakkor egy kiterjedt káresemény kapcsán számos alkalommal tapasztalhatjuk, hogy közülük sokan eszközöket biztosítanak a feladatok végrehajtásához (például saját busszal vagy traktorral végrehajtott kimenekítés, lakosságtájékoztatási feladatok végrehajtása hangszórós járművel), vagy önállóan végzik azokat, ezáltal segítve a védekezési feladatokat. A 2013-as dunai árvíz idején számos önkéntes jelentkezett a katasztrófavédelemnél. Az állampolgárok árvízi védekezési munkára jelentkeztek, illetve eszközeiket ajánlották fel a történelmi ár elleni védekezéshez. Ezeket a felajánlásokat a honlapon speciálisan erre a célra létrehozott felületen, továbbá telefonon keresztül egységesen szervezte a szervezet. A következő az önkéntesen polgári védelmi szervezetbe osztottak kategóriája.

A katasztrófavédelmi törvény lehetővé teszi, hogy állampolgár önként polgári védelmi szervezetbe jelentkezzen. Ilyen esetekben az önkéntes nyilatkozatot tesz, majd a polgármester, egyetértése esetén határozattal beosztja. Jogai és kötelezettségei megegyeznek a köteles szervezetbe osztott személyekével. Mint polgári védelmi szervezet az eszközöket esetükben a katasztrófavédelmi törvény alapján kell biztosítani, amely leginkább a települések indulókészletei esetében kézzelfoghatók. Ezek a katasztrófavédelmi és a települési nyilvántartásokban rögzítettek, szükség esetén jól tervezhetők.

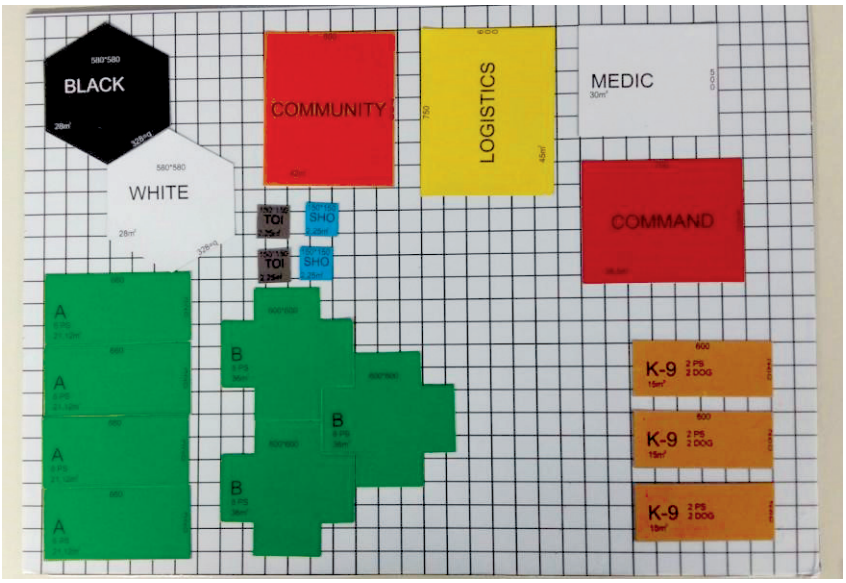
A következő kategória az önkéntes civil szervezeteké. Az ő eszközeiket jelenleg a katasztrófavédelem nem tartja nyilván, és nem tervez rájuk. A gyakorlati tapasztalat ugyanakkor azt mutatta, hogy az egyes szervezetek akár helyben rendelkeznek a katasztrófavédelmi műveletekben is jól hasznosítható eszközökkel (például sátrak, terepjáró gépjárművek), amelyeket indokolt volna felmérni, és szükség esetén akár együttműködési megállapodás alapján tervezni. Ez jelentős mértékben javíthatná a helyi védekezések hatékonyságát. Az önkéntes szervezetek rendkívül innovatívak lehetnek, számos hasznos újítást hozhatnak az állami szervek, szervezetek részére. A következő három ábra három civil szervezet esetében mutat be a védekezések során is jól hasznosítható technikai eszközöket.

1. kép
„Quadronca" – A kaposvári KÖTÉL Egyesület járműve
[a szerzők felvétele]

A „Quadronca" a Kaposvári KÖTÉL Egyesület által kifejlesztett technikai eszköz (lásd 1. kép). Számos hasznos képessége mellett kiemelkedően hatékony nagy tömegű ládák tehergépjárműre történő pakolása esetén – egy targoncához hasonló módon. A HUSZÁR ENSZ minősítéssel rendelkező közepes Városi Kutató-Mentő Szervezet részeként a KÖTÉL „Quadroncája" nagymértékben megkönnyíti a Mentőcsapat felszereléseinek málházását, rövidíti a mentőcsapat készenlétbe helyezésének idejét, valamint segíthet a kárhelyszínek felderítésében.

2. kép
„Tábori vízrendszer" – A Pest Megyei Kutató-Mentő Szolgálat tervezése
[a szerzők felvétele]

A tábori vízrendszert a Pest Megyei Kutató-Mentő Szolgálat tervezte a 2017. évi HUSZÁR Mentőszervezet ENSZ újraminősítésére. A 2. képen látható felszerelések és a napelem segítségével 54 fő részére több napon keresztül volt teljes mértékben megoldott a melegvizes fürdetés. A nemzetközi minősítők részéről is kiemelt elismerést kapott a tábori eszköz.



3. kép

„Méretarányos mágneses táborhelytervező tábla" – Készítette a Zala Különleges Mentők Egyesülete

[a szerzők felvétele]

A méretarányos mágneses tábla kivételesen egyszerűen és gyorsan képes segíteni bármely mentőcsapatot a megfelelő táborhely kialakításában és kiválasztásában. A 3. képen látható A, B, WHITE, BLACK, K–9, COMMUNITY, LOGISTICS, MEDIC, COMMAND elnevezésű mágnesek egy-egy sátrat jelölnek, méretarányosan. Mielőtt a valóságban egy sátorcölöpöt is leütnének, a táborhely kialakításával megbízott logisztikus a táblán előre megtervezheti a tábor teljes elhelyezkedését, esetenként jelentős munkától kímélve meg társait.

A gazdálkodószervezetek önkénteseinek és eszközeinek bevonása jelenleg az egyik legbonyolultabb kérdés. Mivel profitorientált gazdálkodószervezetről beszélünk, a felajánlott egyes eszközök vagy saját dolgozók katasztrófavédelmi műveletekben történő részvétele mindenképpen veszteséget fog részükre termelni (minimum az eszközök amortizációs költsége, illetve a dolgozók munkabére). Ennek elkerülésére a szervezet vagy a létszámot fogja valószínűleg minimalizálni, vagy az önkéntesek rendelkezésre állási idejét. Helyi és területi szinten ugyanakkor muszáj ismerni a lehetőségeket, mert az egyes feladatok elvégzésénél hatékonyan segítséget jelenthet egy-egy ilyen lehetőség (például vállalati buszok kimenekítési feladatokra, mobilszolgáltató kis létszámú csapata a helyszíni kommunikáció megszervezésére és biztosítására, céges

kishajó biztosítása vízről mentési feladatokhoz). A technikai eszközeik bevonása esetükben tervezhető, a katasztrófavédelmi szervek megfelelő előkészítő munkájával (például együttműködési megállapodás kötése), a település/térség veszélyeztetettségnek figyelembevételével.

Az utolsó kategória a nemzetközi önkénteseké. Bár nagyon kicsi a valószínűsége annak, hogy olyan katasztrófa következik be az országban, amelynek megoldása a nemzetközi közösségen múlik, de a lehetőség nem zárható ki. Az egyes országok nemzetközi katasztrófavédelmi műveletek végzésére felajánlott szervezetei kivételesen jól képzettek, kimagasló minőségű és technológiai fejlettségű eszközökkel rendelkeznek, amelyek hathatósan alkalmazhatók egyes szituációkban. Magyarország az Európai Unió és az ENSZ tagállamaként is jogosult ilyen képességek igénybevételére, de akár két- vagy többoldalú nemzetközi szerződések révén is lebiztosíthat erőforrásokat. Ez kifejezetten előnyös helyzetet teremthet például a határ menti együttműködések és események kapcsán, ha a káresemények az országhatáron átterjednek és a műveletek több országot is érintenek.

A nemzetközi beavatkozó-önkéntesek bevetésének tervezése kapcsán külön ki kell emelnünk a földrengések elleni védekezés tervezési kategóriáját. Szakmailag eldöntött tény, hogy egy metropoliszban bekövetkezett rengés esetén a szakszerű kutatás-mentési feladatok végrehajtása az időtényező és a nagyszámú kárhelyszínek okán kivitelezhetetlen más országok csapatainak igénybevétele nélkül, így itt az esemény megköveteli a tudatos nemzetközi igénybevétel tervezését és fogadását. A nemzetközi megfigyelők kapcsán pedig szakértői segítségére ad példát az egyes speciális járványok esete, ahol az oltásra megfelelő ellenanyag csak nemzetközi forrásból áll rendelkezésre, és a vakcina használatához biztosítják a szakembert.

Példa a katasztrófavédelmi műveletek önkéntesek által történő támogatására Tolna megyében

A katasztrófavédelem fő célkitűzései között szerepelt az önkéntesek széles körű bevonása a katasztrófavédelmi műveletekbe, hogy növelni lehessen a települések önmentőképességét. A BM Országos Katasztrófavédelmi Főigazgatóság által kiírt pályázaton Tolna megyében nyert a Bonyhádi Önkéntes Tűzoltó Egyesület (Gemenc Megyei Önkéntes Mentőszervezet részeként) egy DJI Phantom 3 Professional Mikro UAV (kisméretű drón) eszközt (lásd a 4. képet). Megyei és helyi szinten a katasztrófavédelem jelenleg nem rendelkezik ilyen típusú eszközzel. Az Önkéntes Tűzoltó Egyesület (a továbbiakban: ÖTE) együttműködési megállapodással rendelkezik a Tolna Megyei Katasztrófavédelmi Igazgatósággal, és önként vállalta a részvételt katasztrófavédelmi műveletekben. Tűzoltósági, iparbiztonsági és polgári védelmi szempontból is felmerült a kérdés, hogy milyen típusú feladatok végrehajtását tudja a kisméretű eszköz segíteni.

4. kép
DJI Phantom 3 Professional
(a szerzők szerkesztése [5] alapján)

A DJI–3 drónt alapvetően nem katasztrófavédelmi feladatok végrehajtására tervezték, ugyanakkor már a jelenlegi képességeivel is hatékonyan bevonható egyes műveletek végrehajtásába, további célzott kisebb átalakításokkal pedig még több katasztrófavédelmi feladat végrehajtására lehet képes. (Például radiológiai felderítés – szonda alkalmazásával, vegyi felderítés – gázérzékelő műszerrel, tűzoltási feladatok – hőkamera funkció; közvetlen képkapcsolat biztosítása a katasztrófavédelmi munkaszervek részére.) Tolna megyét érintően nukleáris baleset bekövetkezése miatt kiemelt szerepet kaphat minden olyan eszköz, amely a beavatkozások támogatására, a biztonság fokozására alkalmas. A drónok bevethetőségének elemzését ilyen esetekre Manga László már megtette, cikke végén egyértelmű megállapítást tett, miszerint a drónok a jövő eszközeivé válnak [6]. Vizsgáljuk meg a DJI–3 képességeit és technikai adatait, lehetőségeit. A kisméretű drón minden felszerelésével, akkumulátoraival közel egymillió forintba került, legfontosabb képességeit tekintve technikai adatai a következők:

- Maximum távirányíthatóság: 5 km
- Súlya (akkumulátorral együtt): 1280 g
- Max. sebessége: 16 m/s
- Max. emelkedési sebessége: 5 m/s
- Max. süllyedési sebessége: 3 m/s
- Repülési idő: egy akkumulátorral megközelítőleg 30 perc
- Beépített kamera: Sony 4K felbontással
- Valós idejű HD képtovábbítási lehetőség
- Beépített GPS

- Útvonal-kijelölési lehetőség
- Követő üzemmód

A fenti képességek és az érintett katasztrófavédelmi (tűzoltósági, iparbiztonsági, polgári védelmi, ügyeleti, hatósági) szakterületek állásfoglalása alapján alapképességeivel az alábbi katasztrófavédelmi műveletek támogatására tervezhető (önkéntes kezelővel):

1. Keresési és mentési műveletekhez légi támogatás biztosítása.
2. A drónnal magas épületek felderítése beavatkozások döntés-előkészítéséhez.
3. Lefeketítés után az épületszerkezetek, tetőmaradványok, nehezen megközelíthető helyek kamerás átvizsgálásával az utómunkálatok, későbbi tűzvizsgálat támogatása céljából.
4. Pixelanalízis használatával adott pont vagy beavatkozói csoport tevékenységének követése végezhető (biztonsági szempontok miatt).
5. A lezárt kárterületen nagy magasságból a ki- és beléptetés ellenőrzése.
6. Kitelepítés vagy kimenekítés esetén a kitelepített zóna gyors átvizsgálása.
7. Nehezen megközelíthető helyekre gyógyszer, kommunikációs eszköz, minimális mennyiségű alapvető étel és ital eljuttatása.
10. Azonosított, kiemelt kockázati helyszínek normál állapotban történő rögzítése (például autópálya-csomópontok), adatbevitele és dokumentálása meglévő katasztrófavédelmi rendszerbe.
11. Azonosított kockázati helyszínek rendkívüli helyzetben történő állapotfelmérése, rögzítése.
12. Biztonsági felderítés (nehezen megközelíthető, vagy a védekezések során kockázatossá vált védművek víz feletti állapotfelmérése).
13. Bel- és külterületi vízelvezető-rendszerek gyors, rendkívüliállapot-felmérése.
14. Belvízi, árvízi és helyi vízkáros jelenségek felmérése, adatgyűjtés.
17. Erdő- és vegetációtüzek, szabadtéri tüzek felderítése, felmérése, adatok gyűjtése.
18. Károk felmérése, kárterület méretének meghatározása.
19. Gyakorlatok rögzítése, dokumentálás és kiértékelés céljából.
20. GPS-pontok alapján repülés, pontos térinformatikai adatok szolgáltatása (például a teljes repült útvonal GPS-adatai; geokódolt fénykép készítése a levegőből).
21. A műszaki mentési munkálatok precíz irányítása valós idejű légi nézőképek segítségével. A közúti balesetek ortogonális dokumentálását (feltérképezését és archiválását) is lehetővé teszi. (például két tűzoltódaru egyidejű működtetése).
22. Saját szervezet vagy sajtó részére promóciós videó készítése, rendezvények rögzítése.
23. Tűzmegelőzési bizottság szakmai munkájának támogatása oktatási segédanyagok készítésével.

A felsorolt feladatok mellett a drón fejlesztésével, felszerelésével további feladatok valósulhatnak meg:

1. Különböző, akár a már katasztrófavédelmi rendszerben lévő mérőműszerek felszerelésével egyes veszélyes anyag jelenlétében történő beavatkozásoknál meg lehet határozni az egyes gázok arányát, jelenlétét anélkül, hogy a személyi állománynak közel kellene mennie a veszélyes zónához.
2. Lefeketítés után az épületszerkezetek, tetőmaradványok, nehezen megközelíthető helyek átvizsgálása megvalósítható hőtérképezéssel az utómunkálatok támogatása céljából.
3. Tolna megye esetében kiemelkedően fontos kérdés a nukleáris balesetek elleni védekezési feladatok minél magasabb szinten történő megvalósítása. Jelentős fejlesztés lehet, ha a pilóta nélküli eszközök segítségével a drón irányítója a távolból is képes a szennyezett terület határainak felderítésére, térinformatikai dokumentálására, ezáltal saját magát nem teszi ki kockázatnak. A drón beküldhető szennyezett, veszélyes területekre, kritikus esetben akár lezárt épületek belsejében is végezhetünk méréseket. A DJI–3 akár kis magasságban (1 m) is képes stabilan és megbízhatóan repülni, képeket készíteni.

A drón mozgásáról, az elvégezhető tevékenységekről videófelvétel készült [7]. A megyében az eszközt a Tolna Megyei Katasztrófavédelmi Igazgatóság kérésére önkéntesek segítségével számos alkalommal bevetették, ár- és belvizes területek kiterjedésének vizsgálata, a károk felmérése, valamint a rendőrség felkérése alapján eltűnt személyek kutatása céljából. A fenti táblázatok alapján azonban egyértelműen megállapítható, hogy az önkéntes eszköz számos további feladat esetén tudja támogatni a katasztrófavédelmi műveleteket, és nem csak a mentési tevékenységek végrehajtása során. Ez egyértelműsíti azt is, hogy a humán erőforrásokkal történő gazdálkodás során az irányítást végző önkéntest a szakértők csoportjába kell sorolni, a drón használatához szükséges képzettsége okán. A megyei katasztrófavédelmi igazgatóság felismerte a lehetőségeket, az öt tényezőnek megfelelően kialakította a rendszerét az önkéntesek és a DJI–3 bevonásához. Az önkéntes mentőszervezet részére drón felkészítést szervezett, hogy rendelkezésre állhasson a megfelelő létszámú kezelő (ezzel biztosítva lett a humánerőforrás-tényező). Az eszköz riasztása a megyei igazgató elrendelése alapján a katasztrófavédelem megyei főügyeletéről, a Gemenc Mentőcsoport részeként történik (ezzel megvalósul a megfelelő információ, legitimáció és időbeliség). A DJI–3 eszköz felhasználhatósága és nyilvántartásba vétele a HELIOS polgári védelmi adatnyilvántartó programban [8] megtörtént, így szükség esetén akár országos szinten is bevethetővé válik.

A katasztrófavédelmi műveletekbe bevonható humán erőforrás és technikai eszközök nyilvántartása

A katasztrófavédelem részéről a műveletek végzéséhez rendelkezésre álló nyilvántartások naprakészek és pontosan vezetettek, hiszen a személyi állomány és technika napi szinten végzi a beavatkozásokat. A bevezetőben kiemeltük, hogy előfordulhatnak olyan katasztrófavédelmi műveletek, amely során többleterőforrásokra lehet szükség. Az 1. ábrán jól látható, hogy ilyenkor sor kerülhet állami szervezetek,

a Magyar Honvédség, önkormányzatok, önkéntesek eszközeinek igénybevételére. Ennek a feladatnak a kivitelezése azonban sok esetben nem megy zökkenőmentesen. Példaként említhető, hogy a katasztrófavédelemi feladatok ellátása érdekében a települési önkormányzatok végzik az eszközök lebiztosítását (elsősorban a polgári védelmi szervezetek részére), amely a védelmi tervezésbe és az adatnyilvántartó rendszerbe bekerül. Ennek ellenére azonban számos alkalommal előfordul, hogy az eszközök nyilvántartása nem helytálló, mivel azokat leselejtezik, eladják, meghibásodnak, elavulttá válnak és a szükséges időszakban nem lesznek elérhetők. Az eddigi tapasztalatok azt mutatták, hogy amennyiben egy adott feladatra történt előzetes egyeztetés az eszközök lebiztosításáról és igénybevételének lehetőségéről, ott sokkal kisebb arányban fordult elő bármely hibalehetőség. Az állami szervezetek és a Magyar Honvédség esetében a lehetőségek egyértelműek, a megfelelő rendszerek használatával, a szükséges idő figyelembevételével és a vezetői döntések meghozatalával elérhetővé válnak. Figyelembe kell azonban venni, hogy az önkéntesek kategóriáinak eszközei is folyamatosan fejlődő, jelentős potenciált képviselnek, amelyet nagyon kis arányban használ ki a katasztrófavédelmi rendszer. A legfontosabb jellemzője az elérhetőségüknek és a használatnak az előre egyeztetett módon történő igénybevétel. Példaként hozhatjuk bármely veszélyeztetett település esetét. Egyre fontosabbá válik, hogy adekvát szinten és a valódi veszélyforrások felmérésével történjen a katasztrófavédelmi feladatok kockázatalapú megközelítése, a veszélyek azonosítása [9], hiszen ez egyértelműen kihatással bír mindegyik koordinációs tényezőre, az igénybevételre tervezett szervezetekre, erőforrásokra, eszközökre.

Jelenleg Magyarországon jogszabályban előírt módon felmérik minden egyes település esetében az előírt veszélyeztető hatásokat, megvalósul a település katasztrófavédelmi osztályba sorolása. A veszélyeztető hatások ellenében a polgármester köteles polgári védelmi szervezetet kell, hogy létrehozzon, állampolgárokat kell határozattal a szervezetbe osztania. Amennyiben van állampolgár, aki önként vállalja a feladatot, akkor ő is beosztható, jogai és kötelezettségei a köteles személyével megegyeznek. A polgári védelmi szervezet mellett, ha a településen jelen vannak a veszély elhárításához segítséget nyújtani képes gazdálkodó szervezetek, civil szervezetek, karitatív szervezetek, akkor indokolt őket megkeresni, és előre egyeztetni velük, hogy eszközeikkel és állományukkal milyen jellegű feladatokba lennének bevonva. (például árvízi védekezés esetén a helyi polgárőrség nem tömegmunkát végez, hanem önálló feladatként végzi a figyelőszolgálat megszervezését és fenntartását. Másik példa, hogy a helyi karitatív szerv bekapcsolódik a logisztikai vagy adomány nyilvántartásba vételi és elosztási feladatokba.) Ez azt is eredményezheti, hogy az érintett szervezet tudatosan készülni fog ezekre a feladataira, és akár további hasznosítható eszközöket szerez be. A katasztrófavédelmi műveletek elsősorban a saját és a településeken tervezett eszközökre alapozódnak, de mint a fenti példa is mutatja, számos további eszköz is bevonható.

A HELIOS polgári védelmi adatnyilvántartó rendszer rendkívül modern, hasznos segítség a katasztrófavédelmi műveletek végrehajtása során. A hozzáférési jogosultsággal rendelkező katasztrófavédelmi szakemberek központi, területi és helyi szinten is láthatják a bevitt adatokat. Amennyiben egy szakembert káresemény-kezelés miatt ismeretlen területre, településre vezényelnek, a HELIOS segítségével képes azonnal

tájékozódni az ottani viszonyokról, és látja a rendszerbe vonható előre leszervezett erőket és eszközöket. Az önkéntesek kategóriáinak eszközei közül az adatnyilvántartó-rendszerben számos megtalálható, de ugyanakkor nagyon sok speciális vagy helyi szinten használható eszköz hiányzik, még nem rögzítették azokat. Ez nem hiányosság, hanem annak a megszokottságnak a kérdése, hogy a biztonsághoz szükséges eszközök állami szinten vannak szavatolva. Ettől a gondolatmenettől mindenképpen indokolt továbblépni, hiszen a katasztrófavédelmi önkéntesek bevonása, az általuk felajánlott képességek és eszközök nagymértékben támogathatják a katasztrófavédelmi műveleteket. Alátámasztja ezt az a gondolatmenet is, amely szerint az elkövetkezendő időkben mindent meg kell tenni a lakosság helyi ellenálló-képességének (rezilienciájának) fokozásához, hiszen egy-egy káresemény kapcsán valószínű, hogy a helyi erő lesz képes a leggyorsabban a mentési feladatok végzésére, a katasztrófavédelmi erők és egységek támogatására [10]. A katasztrófavédelmi rendszerben jelenleg is találhatunk erre példát (beavatkozó önkéntes tűzoltó egyesületek). Az önkéntesek igénybevételének tudatos tervezése a katasztrófavédelmi szervek feladata. Az érintett szakembereknek rendszerben kell látniuk a lehetőségeket, és törekedniük kell arra, hogy lehetőséget teremtsenek az önkéntes szervezetek (például települési, járási mentőcsoportok, mentési képességgel rendelkező egyesületek) fejlesztésére. Ez megvalósulhat a pályáztatások útján, de akár szponzorszervezetek, önkormányzatok támogatásának útján is. Amennyiben sikerül a megvalósítás, akkor a bevonásra tervezett szervezetek állományát legitimálni, majd a nyilvántartásokban szerepeltetni szükséges.

Következtetések

A cikkben a szerzők áttekintették a katasztrófavédelmi műveletek kapcsán az önkéntesek bevonásának lehetőségét. A korábban feltett kérdésre, miszerint hatékonyan vonja-e be a katasztrófavédelem a műveletekbe az önkéntesek állományát és eszközeit, a szerzők véleménye szerint nem teljesen a válasz.

1. Részeiben már kialakult a bevonás feltételeinek megteremtése, ugyanakkor számos helyen jelenleg rugalmatlan a rendszer. Mivel a védekezések megvalósítása elsősorban állami feladat, ezért a tervezés az állami eszközökre alapozódik, és sok esetben a helyi szinten meglévő önkéntes eszközök, felajánlások szóba sem kerülnek. A káresemény bekövetkezésénél viszont sok esetben előfordul, hogy az önkéntesek saját eszközeikkel megjelennek a helyszínen, hogy segítsék a feladatokat. Ilyenkor tenni szeretnének a településük és a lakosság, családtagjaik megvédése érdekében, amelyből nem célszerű kizárni őket. Könnyen elképzelhető olyan szituáció, hogy az önkéntes képzettsége vagy saját fejlett technikai eszköze okán hatékonyabban tud megoldani egy feladatot, mint az állami szervek. (Például ipari búvár, alpintechnikával foglalkozó önkéntes, esetleg nehézgép- vagy targoncakezelő, aki napi szinten ebből a tevékenységből képes megélni).
2. Az eszközök nyilvántartására feltett kérdésre is hasonló a válasz: a rugalmatlanság okán nem teljesen hatékony a működés. A nyilvántartás vezetésére

a modern és korszerű digitális program és feltételrendszer adott, viszont az önkéntesek megszólítása és rendszerbe vonásuk elmaradása miatt nem kerül bele minden lehetőség. Ezzel egyidőben az önkéntesekkel történő kommunikáció fejlesztése időszerű feladattá vált. Magyarországon számos veszélyeztető hatás létezik, egy-egy kiterjedt katasztrófaesemény során szükséges az erők, eszközök lehető leggyorsabban és leghatékonyabban történő felhasználása. Az önkéntesek erői és eszközei jelentős potenciált képviselnek, így a jelenkorban egyre inkább indokolttá válik az önkéntesek katasztrófavédelmi műveletekbe vonásának tudatos tervezése, a vonatkozó jogszabályok és feltételrendszer kialakítása a végrehajtáshoz. Ennek egyik legfontosabb elemévé kell, hogy váljon a motiváció megteremtése, annak elérése, hogy minél több önkéntes akarjon részt vállalni a feladatokból. Ennek nagyon jó példája a beavatkozó önkéntes tűzoltó egyesületek működése, amelyhez hasonlóan a térség veszélyeztetettsége és a települési katasztrófavédelmi osztályba sorolás figyelembevételével, állandó normatív állami támogatással elsőként a megyei és járási mentőszervezetek folyamatos képzése, rendszerben tartása és alkalmazása megvalósulhatna. A támogatásnak el kellene érnie azt a szintet, hogy egy kezdeti beavatkozás feltételei meglegyenek, a további költségek elszámolása pedig az adott település vis maior pályázatából lenne rendezhető.

3. Fontos kérdés az önkéntesek részére szabadidő szempontjából a jogvédelem rendezése. Önkéntest ne érhessen amiatt hátrány, mert katasztrófavédelmi műveletekben vesz részt. Jelenleg az önkéntesek döntő hányada vállalja a feladatokat, és saját szabadidejét, sok esetben éves szabadságát áldozza arra, hogy képzéseken, gyakorlatokon és még az éles beavatkozásokon is részt tudjon venni. Ezt indokolt lenne megváltoztatni, és az önkéntesek számára a kötelező képzéseken, gyakorlatokon és éles beavatkozásokon történő részvételét törvényi szinten kellene rendezni. A munkáltatókat érdekeltté kell tenni abban, hogy egy bizonyos mértékig engedélyezzék az önkéntesek részvételét a műveletekben, amiért kompenzálást kapnának (például állami adókedvezmény biztosítása a szervezetnek). Amennyiben a szükséges önkéntes erőforrások előteremtése és koordinációja helyi vagy települési szinten megtörténik, akkor az a katasztrófavédelmi erők igénybevételét csökkenti, és a kor követelményeinek megfelelően hozzájárul a lakosság rezilienciájának kialakításához.

Hivatkozások

[1] Nemzeti Jogszabálytár, „1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról," [Online]. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=26565.366929 (Letöltve: 2019. 08. 28.)

[2] Nemzeti jogszabálytár, „2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról," [Online]. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=139408.367079 (Letöltve: 2019. 08. 28.)

[3] L. Györök és R. Tóth „A lakossági óvóhelyek és a vezetési pontok alaprendeltetése, építészeti, gépészeti kialakításuk közötti különbségek," *Műszaki Katonai Közlöny,* 26. évf. 3. sz. pp. 74–92, 2016.
[4] T. Hábermayer, „A magyar önkéntesek kategóriái és lehetséges fejlesztésük iránya az ár- és belvizek elleni védekezések tükrében," *Védelem Tudomány,* 2. évf. 2. sz. pp. 88–124, 2017.
[5] DJI, [Online]. Elérhető: www.dji.com (Letöltve: 2019. 08. 28)
[6] L. Manga, „A drónok és alkalmazási területeik, avagy szóba jöhetnek-e egy esetleges nukleáris baleset esetén," *Műszaki Katonai Közlöny,* 26. évf. 2. sz. pp. 183–196, 2016.
[7] T. Hábermayer, „Youtube Csatorna – DJI repülése videó," [Online]. Elérhető: www.youtube.com/watch?v=voQG6zJu1VI (Letöltve: 2019. 08. 28.)
[8] T. Hábermayer és K. Csekő, „A katasztrófavédelmi műveletek támogatása a HELIOS polgári védelmi adatnyilvántartó programban," *Hadmérnök,* 12. évf. 2. sz. pp. 137–150, 2017.
[9] Á. Muhoray, *Katasztrófamegelőzés I.*, Budapest: NKE Szolgáltató Nonprofit Kft., 2016.
[10] J. Hornyacsek, „A mentési időszak feladatai és szerepe egy közösség katasztrófákkal szembeni rezílienciájának növelésében," *Hadmérnök,* 12. évf. 2. ksz. (KÖFOP), pp. 25–48, 2017.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG, ABV- ÉS KATASZTRÓFAVÉDELEM

14. évfolyam (2019) 3. szám 53–64.
DOI: 10.32567/hm.2019.3.5

Muhammad Khaliq,[1] Axel Hagemann,[2]
Kristóf Horváth,[3] József Solymosi[4]

Nuclear Security Related Attributes and Characteristics of Different Types of Nuclear Facilities

Nukleáris létesítmények nukleáris védettségi szempontból lényeges tulajdonságai

The existing International Atomic Energy Agency (IAEA) Nuclear Security Series (NSS) publications do not provide specific guidance for the different types of nuclear facilities; these are typically meant as a general guidance for nuclear facilities rather than having specific application to any specific facility type. Accordingly, the question may rise whether operators of different nuclear facilities would need to take account of the specific characteristics of their facilities during the implementation of the recommendations and guidance provided in IAEA NSS publications. The comprehensive answer to the question (regarding each type of nuclear facility) requires the identification of the above mentioned specific characteristics of all nuclear facility types and the systematic assessment of the exiting IAEA NSS publications, including IAEA Nuclear Security Series No. 13 and other implementing and technical guides. The identification of specific characteristics of different nuclear facilities that may influence the design and implementation of their physical protection systems and measures is the starting point of this comprehensive review process.

[1] International Atomic Energy Agency, Head of the Nuclear Security of Materials and Facilities Section of the IAEA's Division of Nuclear Security, e-mail: mkhaliq56@gmail.com ORCID: https://orcid.org/0000-0001-6391-2531
[2] retiree, GRS mbH 2013, e-mail: axel_hag@yahoo.com ORCID: https://orcid.org/0000-0002-6828-3057
[3] International Atomic Energy Agency, Senior Nuclear Security Officer, e-mail: k.horvath@iaea.org ORCID: https://orcid.org/0000-0001-8979-9995
[4] National University of Public Service, Faculty of Military Science and Officer Training, Professor Emeritus, e-mail: jozsef.solymosi@uni-nke.hu ORCID: https://orcid.org/0000-0003-3737-1932

Keywords: **nuclear security, nuclear facilities, security relevant characteristics, IAEA, physical protection**

A Nemzetközi Atomenergia Ügynökség Nukleáris Védettségi Sorozatban eddig megjelent útmutatók nem adnak specifikus útmutatást a különböző típusú nukleáris létesítményekre vonatkozóan. A meghatározott követelmények és ajánlások általános érvényűek az összes nukleáris létesítményre. Felmerül a kérdés, hogy a különböző típusú nukleáris létesítmények üzemeltetőinek figyelembe kell-e venni a saját létesítmények specifikus tulajdonságait a NAÜ-követelmények és -ajánlások alkalmazásakor. A kérdés átfogó megválaszolásához meg kell határozni a különböző típusú nukleáris létesítmények nukleáris védettségi szempontból releváns tulajdonságait és értékelni kell, hogy ezek befolyásolják-e a követelmények és ajánlások alkalmazhatóságát. A különböző nukleáris létesítményeknek a fizikai védelmi rendszer tervezése és megvalósítása szempontjából releváns tulajdonságainak meghatározása és vizsgálata az első lépése ennek az átfogó feladatnak.

Kulcsszavak: **nukleáris védettség, nukleáris létesítmények védettségi szempontból releváns tulajdonságai, NAÜ, fizikai védelem**

IAEA Nuclear Security Series

Nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorised access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities are addressed in the publications of IAEA Nuclear Security Series. These publications are consistent with, and complement, international nuclear security instruments, such as the amended Convention on the Physical Protection of Nuclear Material [1], the Code of Conduct on the Safety and Security of Radioactive Sources, United Nations Security Council Resolutions 1373 and 1540, and the International Convention for the Suppression of Acts of Nuclear Terrorism.

Publications in the IAEA Nuclear Security Series are issued in the following categories:

- Nuclear Security Fundamentals contain objectives, concepts and principles of nuclear security and provide the basis for security recommendations.
- Recommendations present best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals.
- Implementing Guides provide further elaboration of the Recommendations in broad areas and suggest measures for their implementation.
- Technical Guidance publications include: Reference Manuals, with detailed measures and/or guidance on how to apply the Implementing Guides in specific fields or activities; Training Guides, covering the syllabus and/or manuals for IAEA training courses in the area of nuclear security; and Service Guides, which provide guidance on the conduct and scope of IAEA nuclear security advisory missions [2].

Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities

In the hierarchy of the Nuclear Security Series, IAEA Nuclear Security Series No. 13 [3] together with IAEA Nuclear Security Series No. 14 [4] comprehensively cover the area of nuclear security of nuclear material and other radioactive material, associated facilities and associated activities, including the use, storage and transport of such material. As a recommendation level document, IAEA Nuclear Security Series No. 13 contains recommendations and recommended requirements which apply to the physical protection of nuclear material against unauthorised removal with the intent to construct a nuclear explosive device, and to the physical protection of nuclear facilities and nuclear material against sabotage. Protection requirements against unauthorised removal of nuclear material (as radioactive material) for potential subsequent off-site dispersal are provided in IAEA Nuclear Security Series No. 14.

By definition contained in IAEA Nuclear Security Series No. 13, nuclear material is that material which is listed and categorised in its Table 1 (i.e. unirradiated and irradiated plutonium and uranium). A nuclear facility is defined as a facility (including associated buildings and equipment) in which nuclear material is produced, processed, used, handled, stored or disposed of and for which a specific licence is required.

The recommended requirements for the physical protection against unauthorised removal in IAEA Nuclear Security Series No. 13 follow a graded approach, applying a categorisation system which is based on the attractiveness of the nuclear material for the construction of a nuclear explosive device. The recommended requirements on physical protection against sabotage apply to nuclear material and nuclear facilities. They are based on the inventory, not considering the characteristics of different types of nuclear facilities. The basis for the graded approach of protection against sabotage is not the category of the nuclear material, but the concern on potential radiological consequences resulting from the radioactive inventory present in the facility as a result of a successful sabotage. The recommended requirements apply to all nuclear facilities, including nuclear reactors (nuclear power plants and research reactors) and nuclear fuel cycle facilities (including conversion, enrichment, fabrication, reprocessing, and storage facilities). There is one set of requirements for material in use and storage, which implies that this material is located in a facility and another set of requirements is defined for nuclear material during transport.

Existing IAEA Nuclear Security Series publications do not provide specific guidance for different types of nuclear facilities; these are typically meant as a general guidance for nuclear facilities rather than having specific application to any specific facility type. While in the area of nuclear safety, the safety standards series provide safety fundamentals, safety requirements, and facility type specific requirements and guidance for all relevant types of nuclear facilities.

Different Types of Nuclear Facilities

Conversion and enrichment facilities

In conversion and enrichment facilities, most of the uranium is in the chemical form UF_6. The physical form of UF_6 could be either gaseous, liquid or solid. Depending on the enrichment of the final product, the nuclear material would be of Category III (uranium enriched above natural, but less than 10% U_{235} or Category II (Uranium enriched to 10% U_{235} but less than 20%) nuclear material.

A significant potential hazard associated with these facilities is a loss of the means of confinement resulting in a release of uranium hexafluoride (UF_6) and hazardous chemicals such as hydrofluoric acid and fluorine. In addition, for enrichment facilities and conversion facilities that process uranium, criticality can also be a significant hazard. The radiotoxicity of the uranium is low, and any potential off-site radiological consequence following a sabotage would be expected to be limited; however, the radiological consequences of an accidental release of reprocessed uranium would be likely to be greater.

The enrichment process relies to a large extent on operator intervention and administrative controls to ensure safety, in addition to active and passive engineered safety measures. Since for enrichment of nuclear material to the required level, the nuclear material will be imported from conversion facilities, moved on-site, heated and processed, filled into containers, stored and exported to customers, e.g. fuel fabrication facilities, the administrative control must manage all these activities in a way that safety and security is well coordinated and robust against insider threat activities. In addition to protection against unauthorised removal and sabotage, protection of enrichment technology plays an important role.

Fuel fabrication facilities

In uranium fuel fabrication facilities, large amounts of radioactive material are present in a dispersible form. This is particularly so in the early stages of the fuel fabrication process. In addition, the radioactive material encountered exists in diverse chemical and physical forms and is used in conjunction with flammable or chemically reactive substances as part of the process. Depending on the requested fuel enrichment degree, these facilities used and stored Category III and Category II nuclear material.

The main hazards in these facilities are the potential criticality and the release of UF6 and uranium dioxide (UO_2), from which workers, the public and the environment must be protected by means of adequate design and construction and by safe operation.

The fuel fabrication processes rely to a large extent on operator intervention and administrative controls to ensure safety, in addition to active and passive engineered safety measures. The potential for a release of energy in the event of an accident at a uranium fuel fabrication facility is associated with nuclear criticality or chemical reactions. The potential for release of energy is small in comparison with that of a nuclear power plant, with generally limited environmental consequences.

Nuclear power plants

Several decades have passed since the appearance of the first nuclear power plants. The different types and generations of these energy producing facilities can be well characterised from a safety point of view [5], but these aspects are not always relevant from the perspective of nuclear security.

The nuclear fuel in most commercial nuclear power plants is made of low enriched uranium and belongs to Category III when fresh. Some plants operate with fresh mixed uranium-plutonium fuel belonging to Category I because of its unirradiated plutonium content. During burnup, the fuel becomes irradiated and as spent fuel, it belongs to Category II. During operation, the fission process produces a significant inventory of radioactive substances of very high activity. Physical protection against sabotage dominates the concern on unauthorised removal in most NPPs. The physical protection of nuclear material would be an integral part of the PPS at NPPs.

IAEA Nuclear Security Series No. 13 associates the nuclear power plants as facilities having high radiological consequence regarding sabotage and formulates requirements similar to a facility where Category I nuclear material is in use or storage. Similarly, general safety requirements assign facilities, such as nuclear power plants, for which on-site events (including those not considered in the design) are postulated that could give rise to severe deterministic effects off the site that would warrant precautionary urgent protective actions to the highest emergency preparedness category.

Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states. These safety functions are the control of reactivity; removal of heat from the reactor and from the fuel store; and confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases. In order to prevent an attempt of sabotage from becoming successful, these functions must also be maintained during and after malicious acts performed by insider or external threats.

Main overhauls for maintenance and refuelling, or major repairs require extensive human interactions, a huge number of contractors' staff needs to be authorised for access to conduct technical inspections, maintenance, or repair. In addition, different equipment and material needs to be cleared when entering the facility.

Moreover, when the reactor pressure vessel is open, the vulnerability to malicious acts rises. Security measures should be adjusted to the situation in order to maintain security on an appropriate level and to enable the work.

Small modular reactors

A variety of types of large reactors that have been developed in the past are considered small modular reactors. Such facilities represent not a newly defined reactor technology, but are differentiated by the power level and the modular concept from nuclear power plants. The electricity production of a typical small modular reactor is less than 300 MW, which requires a smaller fuel inventory, and a lower frequency of fuel

loading and unloading. In addition, the amount of radioactive waste stored on the site will be less than in existing nuclear power plants.

Some small modular reactors use fuel enriched at the top end of what is defined as low-enriched uranium (i.e. a bit below 20% enrichment), other designs use fuel made of uranium enriched around 5%. Accordingly, their inventories belong to Category II.

Depending on the type of facility, such as floating, underground, capsuled unmanned and remote controlled, the specific facility has features representing robustness against unauthorised removal as security is part of its specific design.

In harmony with the smaller inventory and power level, a successful act of sabotage may result in less severe radiological consequences.

Research reactors

Research reactor fuel today typically is enriched to less than 20% and belongs to Category II. The fuel assemblies are typically plates or cylinders of uranium-aluminium alloy clad with pure aluminium. In an open pool reactor, the fuel is in principle accessible under water. The sizes and weights of research reactor fuel bundles are much smaller than of those used in nuclear power plants; therefore, they are relatively easily portable, if radiation is not considered.

Some research reactors are used to produce isotopes which would represent an additional inventory of other radioactive material.

The potential for radiological consequences of a sabotage at a research reactor depends on its power, design, inventory, lay-out and location.

Spent fuel storage

The inventory of a spent fuel storage facility is composed of spent fuel generated by operating nuclear reactors. After a typically 1–5 year storage period in the spent fuel pool next to the reactor, the spent fuel is stored prior to reprocessing or disposal in a wet or dry spent fuel storage facility. A spent fuel storage facility is by definition not a disposal facility, thus its operating lifetime is limited but could last several decades.

Applying the categorisation table, spent fuel is assigned to Category II. The required retrievability would enable removal of the fuel assemblies including their unauthorised removal.

The potential radiological consequences of a spent fuel storage facility are typically a magnitude lower than those of a nuclear power plant. The driving force represented by the high thermal and nuclear power of a nuclear power reactor is missing so that indirect sabotage is less attractive. The success of a sabotage depends on the robustness of casks and building structures.

Reprocessing facilities

Large quantities of fissile material, radioactive material, radiotoxic and other hazardous materials are present (stored, processed and generated) in a fuel reprocessing facility, often in easily dispersible forms (e.g. solutions, powders and gases) and sometimes subjected to vigorous chemical and physical reactions.

Separation and purification processes will lead to significant amounts of uranium and plutonium belonging to Category I.

The fuel reprocessing processes are a mixture of high and low hazard, chemical and mechanical processes, including high hazard fine particulate processes and processing involving hazardous solid, liquid, gaseous and particulate (dry, air and water-borne) wastes and effluents. Reprocessing facilities have the potential for serious nuclear and radiological emergencies. The main risks of a sabotage are criticality, loss of confinement, radiation exposure and associated chemical hazards.

Disposal facilities

The nuclear material in a disposal facility is generally processed to produce stable and solid forms, and reduced in volume and immobilised, as far as practicable, to facilitate their transport and disposal.

The content of nuclear material would belong to Category II. The term "disposal" implies that retrieval is not intended, but it does not mean that retrieval is not possible. Unauthorised removal of radioactive waste, also for off-site dispersal needs to be considered when securing the facility.

The inventory of radioactive waste represents a potential hazard to the biosphere.

Attributes and Characteristics of Security Relevance

As recommended in IAEA Nuclear Security Series No. 13: "Three types of risk should be taken into consideration for the protection of nuclear material and nuclear facilities [3]:

- Risk of unauthorized removal with the intent to construct a nuclear explosive device;
- Risk of unauthorized removal which could lead to subsequent dispersal;
- Risk of sabotage."

Different types of nuclear facilities represent different levels of these risks. The risk is a function of severity of consequences of an event and the probability that the event would occur. The categorisation table in IAEA Nuclear Security Series No. 13 and the thresholds for radiological consequences are related to the severity. The probability of an event leading to these consequences would be strongly determined by the type and design of a facility.

IAEA Nuclear Security Series No. 13 requires the consideration of specific facility characteristics when implementing physical protection.

The different types of nuclear facilities, including research reactors [6] with regard to the implementation of nuclear security measures, can be characterised according to the following attributes and their characteristics.

Security vulnerabilities inherent in design and operational practice

The older facilities were not designed with security as a priority, which can complicate the task of providing physical protection. The designs of these facilities were typically optimised around their specific objectives. The focus on these objectives often led to the inclusion of features that are not conducive to nuclear security and could be exploited by an adversary intent on committing unauthorised removal or sabotage, such as easy access to nuclear material, frequent reconfiguration of the core, glass walled control rooms, access to computer systems through open network, open fuel storage, accessible tools and equipment like cranes, forklifts, casks.

Specific safety design

The safety design including provisions against natural or human made external events generate robustness against malicious acts. More robust safety systems require more complicated attack scenario to be developed for a successful malicious act. Safety requirements to be met and the robustness of the required safety features, including the required level of redundancy and diversity depend on the radiological hazard meant by the facility that correlates with the type of the facility. As safety standards are developed continuously and lessons learned during the years are taken into account, a new facility is built according to more stringent safety requirements.

Attractiveness of material

The categorisation system of nuclear material basically takes into account the applicability of the material to build a nuclear device, but higher enrichment level and lower fuel burnup make the nuclear material more attractive as a target of unauthorised removal. In addition, lower dose rates from spent or irradiated material may be less likely to be incapacitating to an adversary.

Colocation with other facilities

A nuclear facility can be a part of a larger organisation operating other nuclear related and also non-related facilities and activities. These other facilities and activities may mean security concerns for the nuclear facility. Such security concerns can be raised by armed security forces employed in another facility, the adverse consequences

of an accident or a security event occurring at the other facility that may result in difficulties of the implementation of the nuclear security measures.

Openness of access, exchange of information

Some facilities or certain areas of some facilities are easily accessible to contractors, staff, guests, students and other visitors. A large number of temporary personnel with unescorted access may require special considerations during the design and implementation of the nuclear security system and measures. In addition, the environment of information sharing and data transparency may create vulnerability for the security of computer based systems.

Variety of uses

Some facility types are designed to fulfil different specific purposes, such as training, research, irradiation, experiments, radioisotope production, medical therapy or neutron activation. Such diversity complicates the standard approach of meeting security requirements.

Funding

The extent and predictability of funding, including that for security can be adversely influenced by the budget basis and provision of the facility, especially for those which do not have income from the operation. Funding limitations may influence the maintenance of security system elements.

Regulatory and operator issues

An operating organisation(s) may lack an appropriate nuclear security culture, at times believing that the purpose or mission is more important than compliance with regulatory nuclear security requirements [7]. This can be exacerbated by a lack of nuclear security expertise and/or organisational independence in the regulatory body in States where operation/promotion and regulatory oversight responsibilities are within the same government organisation. Such conditions may result in the lack of effective regulatory oversight. This, combined with the lack of a nuclear security, can significantly complicate effective implementation of security measures.

The staff responsible for security often lack specialised experience and knowledge of the security system or of security measures. This can be exacerbated by a lack of security expertise in senior management within the organisation and/or at the regulatory authority, which limits the ability to perform effective checks and balances. Lack of expertise can result in the following:

- The responsibility for overseeing and implementing security is effectively ignored.
- The security responsibility is undertaken, but the resulting security is ineffective due to the limited depth of knowledge and experience in security.
- The security responsibility is transferred to a commercial contractor, whose primary motivation is profit rather than effective security.

Site location

Certain geographic locations might be undesirable from nuclear security perspective, such as close proximity to densely populated areas, dense traffic in the surrounding area, harsh weather conditions, seismic activity, site topography, remote location. Depending on the location, such facilities may provide increased robustness against sabotage, i.e. off-site or airborne attacks, when located underground or underwater. The latter will change the paths for radiological releases. At the same time, sea contamination and vulnerability to marine/sub-marine threats or underground threats may need to be considered in the nuclear security design.

Facility ageing

The effectiveness of those security and safety features that were present originally may have degraded with age. The maintenance of older security system elements may require special parts, non-standardised methods and expertise. Protection against emerging threats may be difficult with the ageing security system.

Number of employees

The implementation of security measures, especially those related to trustworthiness verification, access and regress control, including package checks, recording and verification of access rights, operation of turnstiles, verification of identities become more complex with the growing number of employees.

Public acceptance, rejection

The public awareness regarding local security threats would be higher, if the public accept and support the operation of the facility.

Potential radiological consequences

Depending on the radioactive material inventory of the facility, the radiological consequences of a successful sabotage may be different with magnitude.

Complexity of the site

The development of attack scenarios based on the current threat statement should consider the complexity of the site. A more complex site allows more complex attack scenarios and require more complex security system, including a larger number of response personnel.

Specific nuclear material accounting and control requirements

Protracted theft is easier in bulk facilities. More stringent accounting and control requirements, including more frequent inventory taking and verification support the effectiveness of the detection of unauthorised removal.

Conclusion

The existing IAEA NSS publications do not provide specific guidance for different types of nuclear facilities; Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (IAEA NSS No. 13) and implementing guides address technical areas such as nuclear security culture, measures against insider threat, design basis threat and computer security; but these are typically meant as a general guidance for nuclear facilities rather than having specific application to any specific facility type (i.e. enrichment facilities, fuel fabrication facilities, nuclear power plants, research reactors, small modular reactors, storage facilities and disposal facilities). Accordingly, the question whether operators of different nuclear facilities would need to take account of the specific characteristics of their facilities when implementing recommendations and guidance provided in IAEA NSS publications and thus additional guidance or technical documentation would be beneficial for them to be developed, or the recommendations and guidance are applicable to each type of nuclear facility.

The comprehensive answer to the question (regarding each nuclear facility type) requires the identification of the above mentioned specific characteristics of all nuclear facility types, and the systematic assessment whether exiting IAEA NSS publications, including IAEA NSS No. 13 and other implementing and technical guides can be unambiguously implemented or require further guidance.

The identification of specific characteristics of different nuclear facilities that may affect their physical protection systems and measures was the starting point of this comprehensive review process.

References

[1] Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980); Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10–GC(49)INF/6, IAEA, Vienna, 2005.
[2] International Atomic Energy Agency, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna, 2013.
[3] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna, 2011.
[4] International Atomic Energy Agency, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna, 2011.
[5] Z. Antal, L. Kátai-Urbán, and Gy. Vass, "Atomerőmű generációk fejlődésének vonzatai" [Developmental Consequences of Atomic Power Plant Generations," *Hadmérnök,* vol. 13, no. 3, pp. 150–163, 2018. Available: www.hadmernok.hu/183_11_antal.pdf (Downloaded: 02.09.2019.)
[6] International Atomic Energy Agency, Nuclear Security Management for Research Reactors and Related Facilities, IAEA Non-Serial Publications, IAEA-TDL-004, IAEA, Vienna, 2016.
[7] M. Solymosi, "Assessing and Enhancing Nuclear Safety and Security Culture for Small Facilities that Handle Radioactive Material," *International Journal of Nuclear Security,* vol. 3, no. 1, pp. 1–11, 2017. DOI: https://doi.org/10.7290/ijns030112

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG, ABV- ÉS KATASZTRÓFAVÉDELEM

14. évfolyam (2019) 3. szám 65–74.
DOI: 10.32567/hm.2019.3.6

Márton Attila[1]

A hazai vízkészlet-gazdálkodási gyakorlat változásainak bemutatása a 20. századtól

Changes in Hungarian Water Management Planning in the 20th Century

A hazai vízkészlet-gazdálkodási szakág gazdag múlttal rendelkezik, a 20. században nagy fejlődésen ment át. Vízmérlegek készítésével a század közepétől kezdtek el foglalkozni a szakemberek, azóta pedig számos kiadvány született a témában. A számítási módszerek több eleme változott ebben az időben, viszont maradt néhány alap, ami a kezdetek óta állandó. Jelen cikkben áttekintem a szakág magyarországi fejlődését, röviden értékelem a módszereket, valamint felvázolom a jövőben várható fejlődés irányát

Kulcsszavak: **vízkészlet, keretterv, évkönyv, vízmérleg, modellezés**

The Hungarian water resources management has a long history. In the 20th century it has improved greatly. The water engineers have been making water balances since the middle of the century and they have also been publishing a lot on this topic. The methods have been changed, but the main elements remained the same, just like in 1965. In this article, the author reviews the history of Hungarian water resources management, analyses the methods and delineates the possible future changes.

Keywords: **water resources, framework, almanac, water balance, modelling**

[1] Közép-Duna-völgyi Vízügyi Igazgatóság, kiemelt műszaki referens, e-mail: marton.attila@kdvvizig.hu, ORCID: https://orcid.org/0000-0001-5070-2359

Bevezetés

A vízkészlet-gazdálkodás a legfiatalabb klasszikus vízügyi szakág, amelynek jelentőségét a 20. század második felében, a vízügyi igazgatás államosítása után ismerte fel az ágazat, korábban főként a vizek kártételeivel szemben való védekezésre helyezték a hangsúlyt [1]. Fogalmára számos definíció született Magyarországon, ezek nagy része jól kifejezi annak lényegét is. A vízkészletekkel való gazdálkodás során először meg kell határozni egy vízgyűjtő vízkészleteit valamilyen módszerrel, majd ezeket össze kell vetni a társadalmi igényekkel.

A fenti egyszerűsített meghatározásból látszik, hogy a feladat elvégzésére, azon belül főként a vízkészletek meghatározására több módszer is alkalmas, és annak elvégzése a technológia fejlődésével más-más irányba haladhat. A vízkészlet-gazdálkodás az 1970-es évek elejére ért el fejlődésének arra a fokára, amikor szükségessé vált a tervszerű, komplex gondolkodás a témában [2], ebben az időszakban több tankönyv is készült az akkori vízügyi mérnökök képzésének elősegítésére.

Jelen cikk célja a hazai vízkészlet-gazdálkodás történetének áttekintése, fejlődési irányainak és módszereinek vázlatos bemutatása és a jövőben várható változások felderítése.

A magyar vízkészlet-gazdálkodás rövid történeti áttekintése

Az 1900-as évek elején a vízkészleteket szinte korlátlanul rendelkezésre álló természeti kincsnek tekintették, ezért ebben az időszakban Magyarországon az ár- és belvízelöntések elhárítása jelentette a prioritást a vízgazdálkodásban. Az évszázad első felében már távlati terveket és beruházási programokat készítettek a szakemberek (1908, 1929), azonban ezek a dokumentumok nem a vízkészletekkel való gazdálkodás elvégzését helyezték előtérbe [3].

Érdemes ebből az időszakból Sajó Elemér munkásságát kiemelni, aki a két világháború közötti időszak vízügyi szolgálatának kiemelkedő vezetője volt. Fő műve, az *Emlékirat vizeink fokozottabb kihasználása és újabb vízügyi politikánk megállapítása tárgyában* 1931-ben jelent meg, a Magyar Tudományos Akadémia Chorin Ferenc-díjjal jutalmazta. Ebben a munkájában évtizedekre kijelölte az országban szükséges vízügyi fejlesztéseket. Életének utolsó éveiben foglalkozott az Alföld öntözési gondjainak megoldásával, a szikes területek problémáival és a Duna-Tisza-csatorna kérdéskörével, amelyeknek már egyértelmű a vízkészlet-gazdálkodással való kapcsolata [4].

A második világháború után 1948-ban megtörtént a vízügyek államosítása, így az állam feladatává vált minden vízgazdálkodási tevékenység. Ekkor megalakult az Országos Vízgazdálkodási Hivatal és területi szervei, a vízgazdálkodási körzetek és kirendeltségek. 11 minisztérium képviselőjéből létrejött az Országos Vízgazdálkodási Tanács is. 1953. október 1-jén alakult meg az önálló vízügyi államigazgatás, amellyel megkezdte működését az Országos Vízügyi Főigazgatóság és 11 vízügyi igazgatóság [1].

A vizek hasznosításának hatékonyságát tűzte ki célul az 1954-ben kiadott első Országos Vízgazdálkodási Keretterv, azonban ez nem volt széleskörűen elterjedt az ágazatban és a tervezett megvalósítás ütemezése sem volt végrehajtható. A vízmérlegre

támaszkodó vízkészlet-gazdálkodás szükségessége 1949-ben merült fel először az iparvidékeken kialakuló vízellátási nehézségek megoldása érdekében, így ez a terv már tartalmazott átfogó jellegű vízmérleget. A jelentősebb helyi problémákra választ adó vízmérlegek szerkesztésére 1959-ben került sor [3].

A hazai vízkészlet-gazdálkodás éves eredményeit és módszereit a Vízgazdálkodási Intézet által 1960-tól kiadott *Vízkészletgazdálkodási Évkönyv* sorozat kötetei tartalmazták. Ezek a kiadványok sem csak vízkészlet-gazdálkodással foglalkoztak, azonban a hangsúly erre a szakágra tevődött.

1965-ben adták ki a második Vízgazdálkodási Kerettervet, amely országos és 13 területi egység terveit is tartalmazta külön kiadványként. A keretterv általános tájékoztatója a következő gondolatokkal indul: „Korábban a víz a korlátlanul rendelkezésre álló természeti javak egyikének tűnt. A népszaporodás, a nagyobb városok kialakulása, az ipari és mezőgazdasági termelés fejlődése, a kultúra előrehaladása a vízigények olymértékű növekedésével járt, amelyet a természetes vízkészlet a Föld egyes területein már nem elégít ki. A száraz években vagy évszakokban Magyarországon is mindinkább jelentkezik a vízhiány, ugyanakkor nedves években, vagy csapadékos évszakokban az ország területének jelentős részét árvíz- és belvízelöntések veszélyeztetik" [3: 7.].

Látható tehát, hogy felismerték ebben az időszakban a vízkészletekkel való hatékony gazdálkodás fontosságát. Az 1965-ös keretterv 19 fejezete közül a második a vízkészletek számbavételéről szól, a tizenhetedik pedig a területi vízmérlegről.

Az 1970-es évekre jutottak el az országban a vízkészlet-gazdálkodás fejlődésének arra a fokára, amikor szükségessé vált a tervszerű, komplex gondolkodás [2]. Ebben az időszakban számos egyetemi tankönyv, műszaki tájékoztató született a témáról, olyan szerzőktől, mint Dégen Imre, Domokos Miklós vagy Börzsöny Dénes.

1984-ben adták ki a harmadik *Országos Vízgazdálkodási Keretter*vet, amelynek felépítése hasonló volt a korábbihoz és itt is hangsúlyos szerepet kapott a vízkészlet-gazdálkodás témaköre. Meghatározták a hasznosítható vízkészleteket a nagyobb vízgyűjtőkre, valamint az igényekkel összevetve vízmérleg is készült [8].

A *Vízkészletgazdálkodási Évkönyv*eket 1988-ig adták ki, 1993–2010-ig pedig megjelent Magyarország vízkészleteinek állapotértékelése a Környezetvédelmi és Vízgazdálkodási Kutató Intézet (VITUKI) kiadásában.

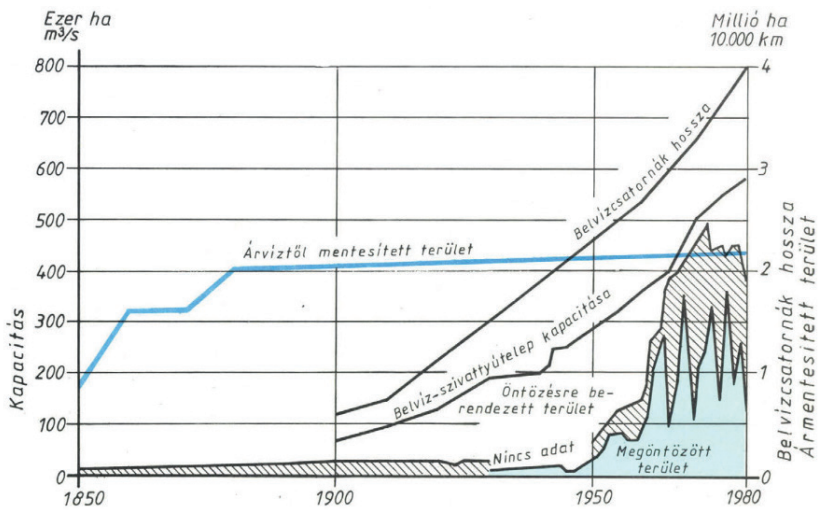
Szemléletbeli változást hozott az Európai Unió 2000-ben kiadott Vízkeret Irányelve (a továbbiakban: VKI), ennek 25. pontja szerint: „A vizek állapotának leírására minőségi, és, ahol az környezetvédelmi szempontból lényeges, mennyiségi szempontból közös fogalmakat kell meghatározni. Környezeti célkitűzéseket kell meghatározni annak biztosítására, hogy a Közösségben mindenütt elérhető legyen a felszíni és a felszín alatti vizek jó állapota, és hogy a vizek állapotának romlása közösségi szinten megelőzhető legyen" [6]. Előtérbe helyeződött tehát a vizek minőségének kérdése azok mennyiségi leírásával szemben. A VKI előírásait alapul véve Magyarország 2009-re elkészítette első Vízgyűjtő-gazdálkodási Tervét (VGT), majd 2015-re felülvizsgálta azt. Jelenleg a harmadik VGT-terv előkészítése zajlik, ahol a tervek szerint hangsúlyosabb szerepet kap a vizek mennyiségi értékelése is.

A számítástechnika fejlődésével egyre nagyobb szerepet kaptak a vízügyi ágazatban a különböző számítógépes modellek, ennek megfelelően a vízkészlet-gazdálkodásban is elindult 2016-ban egy átfogó modellezési célkitűzés vízmérlegek készítésére [5].

A magyar vízkészlet-gazdálkodási módszerek fejlődésének ismertetése felszíni vizek vonatkozásában

A 20. század első felében a meglévő hidrológiai módszerekre alapuló számítások voltak jellemzők a hazai vízkészlet-gazdálkodásban, nem készítettek nagy volumenű vízmérlegeket, néhány zsúfolt mezőgazdasági területnél azonban ebben az időben is szükség lehetett a vízelosztás tervezésére.

1949-től kezdve fokozatosan nőtt a vízhasználatok száma és a fajlagos vízfogyasztás is, valamint ezzel egy időben a szennyvízkibocsátás is növekedett. Ezek következményeként mennyiségi és minőségi problémák is adódtak a vizeinkben, ami indokolta a szakágazatok közötti koordinációt, valamint a vízkészlet-gazdálkodás fejlesztését [8]. Jól látható az 1. ábrán az öntözött területek nagyságának növekedése, ami magával hozta a növekvő vízigényeket is.



1. ábra

A vízügyi infrastruktúra alakulása Magyarországon 1980-ig [8: 231.]

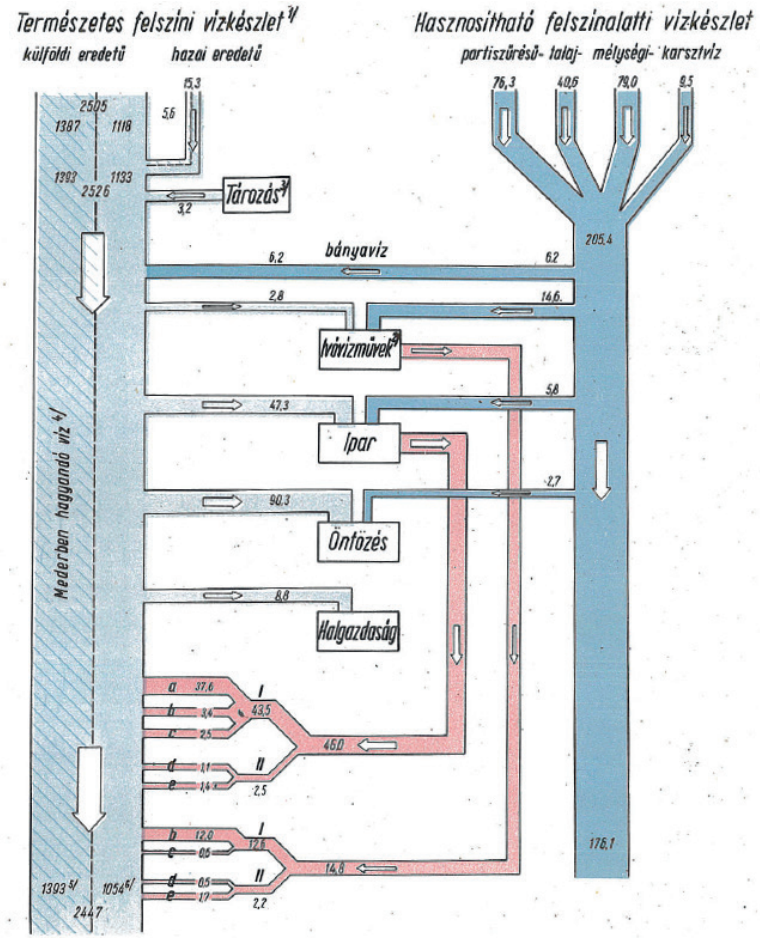
Vízkészlet-gazdálkodás esetén össze kell vetni a vízigényeket az ismert készletekkel, amit szemléletesen vízmérlegek készítésével lehet elvégezni.

Ilyen vízmérleget először az 1954-es kerettervhez készítettek és ebben az időben alakult ki az a gyakorlat is, hogy a sokévi augusztusi napi 85%-os és 80%-os tartósságú vízhozamokat vették mértékadónak a rendelkezésre álló vízkészletek számításánál. A vízmérlegkészítés kezdeti szakaszaiban alkalmazták a szeptemberi 99%-os tartóságot is, azonban erről kiderült, hogy nem elég finom módszer és nem mutat sehol hiányokat [8]. 1950-ben volt olyan elképzelés is, hogy az öntözési idény mértékadó készleteit számolják, azonban ez torz eredményt, több rendelkezésre álló vízkészletet adott volna a május-júniusi csapadékosabb időszak miatt [8].

Az 1960-tól kiadott *Vízkészletgazdálkodási Évkönyv*ben vízgazdálkodási egységeknek (területileg összefüggő vízgyűjtők, például Balaton, Közép-Duna stb.) határozták

meg a hasznosítható készletét az oda be- és kilépő vízhozamok különbségéből, figyelembe véve a tározásból származó pótlást, a mederben hagyandó készletet, a szennyvízhozamokat és az esetlegesen más vízgyűjtőkről átkönyvelendő mennyiségeket.

A vízigényeket korábbi kerettervek alapján számolták, néhol pedig mért adatok vagy becslés alapján. Az öntözési és halgazdálkodási igényeket növénycsoportonkénti és területi víznormákkal vették figyelembe [7].



2. ábra

Az 1962-es országos vízhozammérleg (m^3/s) [7: 63.]

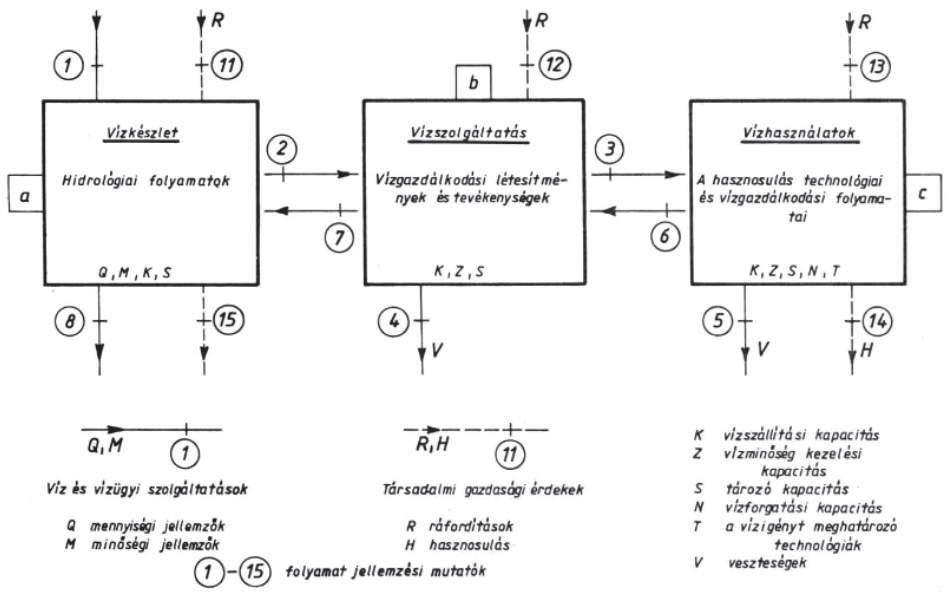
A 2. ábrán az évkönyv országos vízhozammérlege látható, amely szemléletesen kifejezi a készletek és a vízhasználatok közti kapcsolatokat is.

Az ezután kiadott vízkészletgazdálkodási évkönyvek is hasonló metodikát követtek, azonban az évek során több újítás is megjelent, például a csatornákra lebontott vízmérlegek, részletes rajzok a területi vízmérlegekről vagy szerkesztett vízgazdálkodási hossz-szelvények.

Az 1965-ös kerettervnél az 1954-eshez hasonlóan készítették el a vízmérleget, tehát szintén a sokévi augusztusi napi 85%-os és 80%-os tartósságú vízhozamokat vették mértékadónak a rendelkezésre álló vízkészletek számításánál.

A vízkészlet-gazdálkodás fejlesztésére és az üzemirányítás támogatására több műszaki segédlet is megjelent az 1970-es években. Ebben az időszakban ismerték fel, hogy a szakterület fejlődése olyan mértékű, hogy egyre komplexebb problémák jelentkeznek, így az automatizálás bevezetésére is szükség lehet [9]. Olyan módszereket ismertettek a szerzők ezekben a kiadványokban, mint a különböző modellek és mátrixok alkalmazása vagy vízgazdálkodási hossz-szelvények készítése.

Az 1984-es kerettervben a korábbiakhoz hasonlóan számított vízmérleg készült, azonban új fejlesztési irányt is tartalmazott. Ennek a lényege, hogy az igényeket és készleteket három alrendszerben kellene vizsgálni, a vízkészlet, vízszolgáltató és vízhasználati alrendszerekben. Az ezek között lejátszódó folyamatok (3. ábra) figyelembevétele adhat értékelést a vízmérlegre vonatkozóan [8].



3. ábra

A vízkészlet-gazdálkodás három alrendszere [8: 260.]

A Vízkeret Irányelv, illetve az ahhoz kapcsolódó segédletek iránymutatásait követték a magyar vízgyűjtő-gazdálkodási tervek (a továbbiakban: VGT) vízmérlegei. Az 1. VGT-ben alapvetően az augusztusi 80%-os tartósságú kisvízhozamok alapján értékelték a víztesteket hidrológiai szempontból. A kisvizes készlet számítása azért fontos, mert „a vízfolyásokban az idő túlnyomó részében a sokéves középvízhozamnál (a továbbiakban: KÖQ) kisebb lefolyást találunk: kisvízfolyásokban az év kétharmadában nem többet, mint a KÖQ 10-50%-át. A Víz Keretirányelv szerinti jó vízállapotnak tehát elsősorban kisvízi lefolyási körülmények között kell teljesülnie. A jó ökológiai

állapothoz mindig meg kell lennie annak a vízmennyiségnek, amely a vízi élővilág fennmaradásához szükséges, a jó kémiai állapot eléréséhez pedig a vízszállításnak elegendőnek kell lennie ahhoz, hogy a vízfolyás szennyezőanyag terhelése ne lépje túl a megengedett koncentrációkat, továbbá, hogy a vizek mennyiségi terhelése (vízkivételek, vízátvezetések) kisvízi körülmények között se haladja meg a megengedett mértéket." [10: 7.] Az ökológiai kisvizet a felszíni víztestek típusától függő arányosító szorzó adta meg (az augusztusi 80%-os vízmennyiségeket beszorozva), míg a korábbi magyar gyakorlatban többször a 0,75-ös szorzó merült fel. A 2. VGT-ben is hasonló elvekre épülő vízmérlegszámítás készült el.

Változás a jelenleg készülő 3. VGT-nél várható a gyakorlatban. Itt a vízgyűjtőkre az Európai Bizottság *Technical Report 2015-090*-ja alapján, azaz a hidrológiai körfolyamat elemeit részletesen figyelembe véve [12] készülne vízmérleg, valamint gyakorlati megfontolás alapján külön vízfolyásokra is. A klasszikus statisztikai módszerek mellett valós idejű modellezés lesz a mérlegkészítés eszköze. A modellezés célja, hogy az üzemirányításban támogassa a vízügyi igazgatóságokat a pillanatnyi szabad vízkészlet meghatározásával, amivel az adott vízfolyás terhelhetőségét lehet számolni, ami pedig közvetve a távlati tervezést hivatott támogatni. Továbbá azokon a vízfolyásszakaszokon, ahol már 70% fölött van a szabad vízkészlet kiadása, a részletesebb engedély segítségével feltárható a még fel nem használt vízkészlet. Készülni fognak továbbá hidrológiai és vízkészlet-gazdálkodási hossz-szelvények az 1984-es keretterv mintájára [11].

A jelenleg érvényes 2008-as magyar jogszabály szerint a szabad vízkészleteket továbbra is a statisztikai feldolgozás alapján az augusztusi 80%-os tartósságú középvízhozamokra kell meghatározni, de megenged némi eltérést is ettől.

A 30/2008. (XII. 31.) KVVM rendelet 8. paragrafusa szerint:

„(1) Felszíni vizek igénybevételének tervezésekor a vízháztartási mérleg készítésére mértékadó időszak az augusztus hónap. A mértékadó vízhozam statisztikai jellemzője a 80%-os tartósságú középvízhozam, vagy, ha rendelkezésre állnak adatok, a napi középvízhozam. Rendkívüli esetben, amikor a vízigény egyéb hónapban is meghaladja ezen értéknek a 25%-át, ettől el lehet térni azzal, hogy ebben az esetben a szűkebb mérleget mutató időszak a mértékadó.

(2) Felszíni vízkivételek, átvezetések tervezésekor a mederben hagyandó vízhozam értéke legalább a mértékadó kisvízi vízhozam kétharmada, amitől részletes ökológiai és hidrológiai vizsgálat alapján el lehet térni. A mértékadó vízhozam számításánál figyelembe kell venni az aktuális hidrológiai alapadatokat, a tározási lehetőségeket és a vízjogi állapotot"[13].

Következtetések

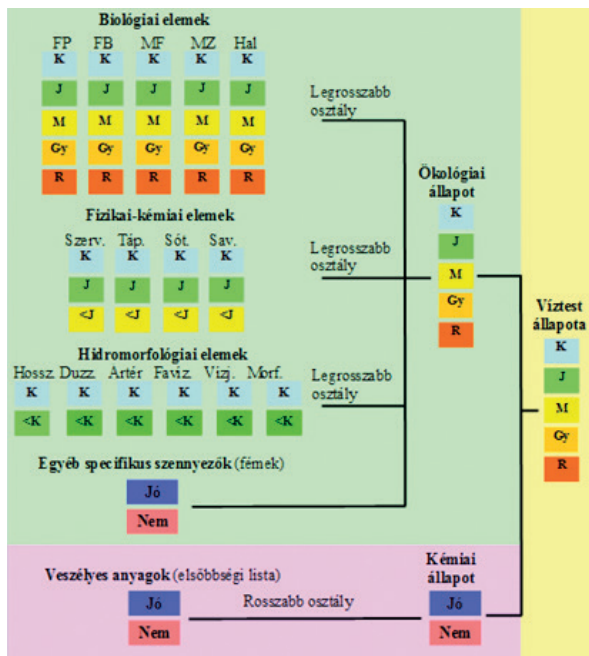
A hazai vízkészlet-gazdálkodás a 20. század második felében komoly változásokon ment keresztül, azonban néhány alapvető eljárás a kezdetektől ugyanaz maradt. A módszerek fejlődését az 1. táblázatban bemutatott korszakokra tudtam beosztani:

1. táblázat

A vízkészlet-gazdálkodás korszakai Magyarországon [a szerző szerkesztése]

időszak	leírás
1949 előtt	nem jellemző vízmérlegek készítése, helyi vízkészlet-gazdálkodás
1949–1960	az igények növekedésével egyre több helyi és átfogó vízmérleg, távlati tervek
1960–1984	vízkészlet-gazdálkodási évkönyvek, műszaki segédletek, távlati koncepciók kidolgozása
1984–2000	az 1984-es keretterv utáni időszak jelentősebb újdonság nélkül
2000–napjainkig	a VKI ajánlásai alapján elvégzett feladatok
napjainktól–	a vízkészlet-gazdálkodás modellezéssel történő fejlesztése

Általánosságban elmondható, hogy a vízkészlet-gazdálkodási szakág legnagyobb ütemű fejlődése az 1950–1970-es évekre tehető, amikor a legtöbb újdonság született meg a témában. Az 1980-as évektől a Víz Keretirányelv megjelenéséig stagnáló időszak volt jellemző, nem jelentek meg jelentős módszertani változások. A VKI azonban szemléletében különbözött a korábbi hozzáállástól a víztestek minőségének, ökológiai állapotának előtérbe helyezése miatt. Korábban is értékelték a vízkészletek minőségét Magyarországon (például az évkönyvekben vagy a kerettervekben), azonban ez egyenrangú volt a mennyiségi értékeléssel. A vízgyűjtő-gazdálkodási tervekben jól szemlélteti az alábbi ábra a mennyiségi értékelés szerepét.



4. ábra

A felszíni vizekre vonatkozó minősítési rendszer sémája [14]

A mennyiségi értékelés a hidromorfológiai értékelés egyik eleme és legrosszabb esetben is csak jó besorolási kategóriába ronthatja az állapotot az ötös skálán, tehát főként következtetéseket lehet levonni ebből, nem befolyásolja érdemben az állapotértékelést.

Napjainkban felismerték a szakemberek, hogy az éghajlatváltozás és a tervezett öntözési fejlesztések miatt újra fontosabb szerepet kell szánni a vízkészletek mennyiségi értékelésének és új metodikák kidolgozásának. Ezt a számítógépes hidrodinamikai és hidrológiai modellek (HecRAS, HecHMS) használatával, valamint módszertani fejlesztésekkel érnék el.

Véleményem szerint ez mindenképpen szükséges, ugyanis a korábbi gyakorlatok más rendszerben és környezetben alakultak ki, a technológia fejlődésével pedig új utakat lehet igénybe venni.

A hazai szakemberek szerint Európában vízhiányok miatti korlátozások és a szokatlan szélsőséges állapotok is egyre gyakrabban előfordulhatnak a következő évtizedekben [15], ezért feltehetően nőni fog az igény a hatékony vízkészlet-gazdálkodásra. Lényeges lehet ezzel kapcsolatban az országhatárral osztott vízgyűjtők határvízi egyeztetésein kialakított közös vízkészletszámítási metodikák kidolgozása, megkönnyítve az érintett országok közti vízkészlet-gazdálkodással kapcsolatos megállapodások megkötését.

Az embereknek egyre fontosabb lesz a környezetükben lévő vízkészletek pontos ismerete, és az információs technológiák fejlődése is megkívánja az adatok egyszerű elérésének lehetőségét, így a jövő mindenképpen egy olyan digitális platform lehet, ahol az emberek megtehetik ezt. Példaként említhető az úgynevezett Danube GIS honlap [16], ahol a Duna-vízgyűjtő vizekkel és élőhelyekkel kapcsolatos mérési eredményei és az ezek állapotát befolyásoló különböző hatások jeleníthetők meg, bárki által elérhető, átlátható, térképes formátumban.

Egy ilyen platform mögé természetesen szakszerű módszertan és hatalmas adatbázis szükséges, de a vízügyi ágazatnak célja az ilyen irányú fejlődés elérése a közeljövőben. A fejlődés kényszere miatt várható továbbá, hogy az 1970-es évekhez hasonlóan egyre több szakirodalom szülessen a felszíni és felszín alatti vízkészlet-gazdálkodás témájában, továbbá a jogszabályi környezetet is felülvizsgálhatják.

Hivatkozások

[1] Közép-Duna-völgyi Vízügyi Igazgatóság, „Történelmi áttekintés," *Közép-Duna-völgyi Vízügyi Igazgatóság,* [Online]. Elérhető: www.kdvvizig.hu/index.php/rolunk/vizugy-tortenete (Letöltve: 2019. 02. 14.)

[2] D. Bőzsöny és M. Domokos, *A vízkészletgazdálkodás alapjai és a vízgazdálkodási mérleg.* Budapest: Tankönyvkiadó, 1975.

[3] OVF Vízügyi Tervező Vállalat, *Közép-Tisza és Mátravidék Vízgazdálkodási Keretterve.* Budapest: OVF Vízügyi Tervező Vállalat, 1965.

[4] Magyar Hidrológiai Társaság, „Sajó Elemér életrajza," *Magyar Hidrológiai Társaság,* [Online]. Elérhető: www.hidrologia.hu/mht/index.php?option=com_content&task=view&id=226&Itemid=143 (Letöltve: 2019. 02. 14.)

[5] I. Láng, „A vízkészlet-gazdálkodás megújítása," XXXIV. Országos Vándorgyűlés, július 6–8, 2016, Debrecen, Hungary [Online]. Elérhető: www.hidrologia.hu/vandorgyules/34/dolgozatok/word/0108_lang_istvan.pdf (Letöltve: 2019. 03. 06.)
[6] Directive 2000/60/EC of the European Parliament and of the Council establishing a framework for the Community action in the field of water policy, [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000L0060 (Letöltve: 2019. 03. 06.)
[7] Vízgazdálkodási Tudományos Kutató Intézet, *Vízkészletgazdálkodási Évkönyv 1962.* Budapest: Vízgazdálkodási Tudományos Kutató Intézet, 1963.
[8] Vízgazdálkodási Intézet, *Országos Vízgazdálkodási Keretterv.* Budapest: Országos Vízügyi Hivatal, 1984.
[9] M. Domokos, *Vízkészletgazdálkodási rendszerek modellezése.* Budapest: Vízügyi Dokumentációs és Tájékoztató Iroda, 1975.
[10] M. Szalay, *A felszíni vizek mennyiségi jellemzése: kisvízi készlet.* Budapest: ÖKO Zrt. vezette konzorcium, 2009.
[11] VITUKI Hungary Kft., *A felszíni tervezési egységekre a vízkészlet-gazdálkodás számításainak, jellemzőinek, táblázatainak, térképeinek és modelljeinek elkészítése az ország területére Zagyva modellterület.* Budapest: VITUKI Hungary Kft., 2018.
[12] European Commission, „Guidance document on the application of water balances for supporting the implementation of the WFD," Luxembourg, Office for Official Publications of the European Communities, Technical Report – 2015-090, 2015. DOI: https://doi.org/10.2779/352735
[13] 30/2008. (XII. 31.) KvVM rendelet a vizek hasznosítását, védelmét és kártételeinek elhárítását szolgáló tevékenységekre és létesítményekre vonatkozó műszaki szabályokról [Online]. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=117437.362753 (Letöltve: 2019. 08. 06.)
[14] Országos Vízügyi Főigazgatóság, *A Duna-vízgyűjtő magyarországi része Vízgyűjtőgazdálkodási Terv.* Budapest: Országos Vízügyi Főigazgatóság, 2015.
[15] I. Ijjas, L. Somlyódy és J. Józsa, „Vízbiztonság Európában, a Duna vízgyűjtőjén és Magyarországon" in *Biztonsági kihívások a 21. században*, G. Finszter és I. Sabjanics, szerk. Budapest: Dialóg Campus, 2017, pp. 423–462.
[16] ICPDR, „About the DanubeGIS," *danubegis.org,* [Online]. Elérhető: www.danubegis.org/about (Letöltve: 2019. 08. 14.)

HADMÉRNÖK
VÉDELMI ELEKTRONIKA, INFORMATIKA, KOMMUNIKÁCIÓ

14. évfolyam (2019) 3. szám 75–89.
DOI: 10.32567/hm.2019.3.7

Gerevich János,[1] Négyesi Imre[2]

A fenntartható és zavartalan elektronikus ügyintézés szoftvertechnológiai háttere – 2. rész

The Technical Background of Sustainable and Continuous Electronic Administration – Part 2

Az informatikai rendszerek térnyerése olyan új kihívások elé állítja a szoftverfejlesztőket, amelyekre csak új technológiákkal és tervezési mintákkal lehet hatékonyan válaszolni. A közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményeknek való megfelelés összetett kérdéseket vet fel a hierarchikus szervezetek életében. Ebben a tanulmányban a több szálon futó iratkezelési folyamatok és a változó szervezeti struktúra kapcsolatát vizsgálják meg a szerzők. Végül a feltárt problémák megoldására tervezési mintákat találhatunk a dolgozatban.

Kulcsszavak: **Általános Adatvédelmi Rendelet, elektronikus ügyintézés, szoftvertechnológia, tervezési minta, holder**

The wide expansion of IT systems brings new challenges to software developers that can be effectively answered with new technologies and design patterns. Compliance with the requirements for records management software for public services raises complex issues in the life of hierarchical organisations. The authors are discussing the multi-threaded record management processes in changing organisational structures through the pages of this paper. At the end, we can find some design patterns to solve the identified problems.

Keywords: **GDPR, electronic administration, software technology, design pattern, holder**

[1] Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, doktorandusz, e-mail: gerevich.janos@agilex-pert.hu, ORCID: https://orcid.org/0000-0001-7236-4514

[2] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, egyetemi docens, e-mail: negyesi.imre@uni-nke.hu, ORCID: https://orcid.org/0000-0003-1144-1912

Bevezetés

Magyarországon az előző évtizedben jelent meg az első elektronikus iratkezelésre vonatkozó kormányrendelet a 24/2006. (IV. 29.) BM-IHM-NKÖM [1] együttes rendelet a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről, az eltelt időszakban több jogszabály is foglalkozott a kérdéskörrel, a területet szabályozó dokumentumok közül még mindig hatályos a 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről [2]. A dokumentum a hagyományos papíralapú iratkezelés és az elektronikus iratkezelés mozzanatait, folyamatait írja le – terjedelmét tekintve nem kirívóan nagyméretű, ugyanakkor fontosságát külön érdemes hangsúlyozni, mert a tárgyalt fogalmak az e-közigazgatás alapját képezik. Az internet szerepével foglalkozó, az előző évtized végén megjelent angol nyelvű cikkében [3: 152.] Négyesi Imre már rávilágított az internet elterjedésével járó kihívásokra, miszerint az üzleti szférán túl az egyes nemzeti kormányoknak is lépéseket kell tenniük az új internet alapú technológiák megfelelő alkalmazásához, a továbbfejlesztés elősegítéséhez. A cikkben bemutatott folyamat elindult és még mindig tart Magyarországon az iratkezelési szoftverek vonatkozásában is. Időközben több rendelet is szabályozta a területet, ezek azonban folyamatos változtatásra szorultak az információtechnológia és a kapcsolódó európai uniós szabályozások gyors fejlődésének következtében. Mindazonáltal, az informatikai rendszerekkel kapcsolatosan megjelent követelmények nem tértek ki különösen a személyes adatok védelmére és megvalósulni látszott *Az információgyűjtés jövőképe* című tanulmányban [4] felvázolt orwelli jövőkép. 2016-ban az Európai Parlament és Tanács rendeletben szabályozta a személyes adatok védelmét, elfogadták az (EU) 2016/679. számú Általános Adatvédelmi Rendeletét [5] (a továbbiakban angol rövidítéssel: GDPR), amely a kézi és a gépi adatfeldolgozás vonatkozásában is előírja a személyes adatok védelmét. A magyar szabályozást még az iratkezelési szoftverek tekintetében nem harmonizálták az EU eme direktívájával – tagállami szinten, erre lehetőség is van, azonban az elkövetkező években várható, hogy a személyes adatok védelmével kapcsolatos szabályozás meg fog jelenni a kormányzati rendszerek vonatkozásában is. A továbbiakban a jelenlegi magyar szabályozás bemutatása következik, a párhuzamosan végzett adatkezelési tevékenységek és a személyes adatok védelmének szem előtt tartásával.

A 335/2005. (XII. 29.) Korm. rendelet meghatározza az iratkezelés folyamatát, ahol a következő tevékenységekkel találkozhatunk: *küldemények átvétele, küldemények felbontása és érkeztetése, iktatás, szignálás, kiadmányozás, expediálás, irattározás, selejtezés és levéltárba adás* [2: 4. fejezet]. A felsorolt fogalmak iratkezelési szoftverbe szervezését a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről szóló 3/2018. (II. 21.) BM rendelet [6] szabályozza, amelynek értelmében 2018. március 1-jét követően már csak a szabályozásnak megfelelő iratkezelési szoftverek alkalmazása engedélyezett [6: 2.41.2] a közszférában.[3]

[3] A fővárosi és megyei kormányhivatalok esetében 2021. január 1-jét követően kell az iratkezelési szoftverekre vonatkozó rendeletet alkalmazni [6: 2.41.3].

Az iratkezelési szoftverek folyamattámogatási képességét az iratok[4] és az ügyiratok[5] esetében a következőképp határozza meg a rendelet. „Az ISZ az ügyirathoz és az iktatott irathoz kapcsolódóan képes támogatni

a) a feladat kiosztását;
b) a kiadott feladathoz határidő rendelését;
c) több feladat hozzárendelését;
d) egy feladat több szereplőhöz történő hozzárendelését;
e) a feladat címzett általi megtekintésének naplózását;
f) egy feladathoz több kapcsolódó feladat létrehozását;
g) azt, hogy a feladat kiosztója bármikor lezárja vagy törölje a feladatot;
h) azt, hogy a feladat címzettje rögzíthesse a feladat elintézését;
i) a kiadott feladat továbbdelegálásának lehetőségét;
j) azt, hogy az egy ügyirathoz vagy irathoz tartozó feladatok legyenek listázhatóak és személyenként csoportosíthatóak" [6: 2.7.14].

A felsorolásban szereplő követelmények a hagyományos iratkezelési tevékenységeken túl [6: 4. fejezet] egyfajta iratkezelési szoftverbe ágyazott feladatkezelő rendszer meglétét határozzák meg. A felsorolt pontok konkrét iratkezelési szoftverekkel szemben támasztott követelményekre lefordítva azt jelentik, hogy egy ügyirathoz, irathoz kapcsolódóan több párhuzamos feladat végrehajtását is lehetővé kell tenni. Az Általános Adatvédelmi Rendelet terminológiájával: egy informatikai nyilvántartáson belül több adatkezelési tevékenység párhuzamosan történő végzését is lehetővé kell tenni. A követelményekből az is kiderül, hogy az informatikai nyilvántartás olvasása, személyekhez kötése a párhuzamosan végzett feladatok kapcsán is megvalósítandó funkció. Cikksorozatunk előző részében [9] bemutattuk a GDPR és az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény [8] adatkezelési tevékenységek szemszögéből érdekes fejezeteit. A korábbi tanulmányban arra a problémára kerestük a választ, hogy milyen szoftvertechnológiai eszközök segítségével lehet támogatni a személyes adatokhoz fűződő adatkezelési tevékenységeket. Ebben a dolgozatban a beérkező és kimenő küldemények problémakörét, majd a több szálon futó ügyintézés és a feladatkezelés témáját járjuk körül a hierarchikus felépítésű szervezetek életében. Természetesen a bemutatott tervezési minták figyelembe veszik a GDPR-alapelveket.[6]

[4] Irat: „valamely szerv működése vagy személy tevékenysége során keletkezett vagy hozzá érkezett, egy egységként kezelendő rögzített információ, adategyüttes, amely megjelenhet papíron, mikrofilmen, mágneses, elektronikus vagy bármilyen más adathordozón; tartalma lehet szöveg, adat, grafikon, hang, kép, mozgókép vagy bármely más formában lévő információ vagy ezek kombinációja;" [7: 3.(c)].

[5] Ügyirat: „egy ügyben keletkezett valamennyi irat;" [6: 2.36].

[6] GDPR-alapelvek: *célhoz kötöttség, az adattakarékosság, a pontosság, a korlátozott tárolhatóság, az integritás és a bizalmas jelleg.*

Kommunikáció modellezése

Az információt hordozó küldemények sok ezer éves múltra tekintenek vissza, a küldemény fogalma a hozzá tartozó küldővel és címzettel az első írott üzenetek kézbesítésekor jelent meg a kőtáblák és a papirusztekercsek korában. Napjainkban a papíralapú küldemények felépítése nem sokat változott, sőt, az informatikai hálózatok protokolljain is tetten lehet érni a küldemény fogalmát és a megfelelő formátumban – leggyakrabban IP-címek segítségével – megadott küldőt és címzettet.

A bevezetésben áttekintett jogszabályok a kormányzati szervek szabályozott iratkezelési folyamatait írják le. Ezen iratkezelési folyamatokat két élesen elkülönülő halmazra lehet bontani. A kormányzati szervhez beérkező, illetve az onnan elküldött küldemények folyamatai együttesen alkotják az első halmazt. A második halmazt az ügyintézéshez kapcsolódó iratkezelési folyamatok teszik ki. Az utóbbi halmazhoz tartozó folyamatokat a későbbiekben tárgyaljuk.

Egy papíralapú iratkezelést folytató kormányzati szerv a küldeményekkel kapcsolatos nyilvántartások vezetésére a hagyományos értelemben vett érkeztetőkönyvet, iktatókönyvet, postázási naplót és hasonló társaikat használta és használhatja. Egy informatikai nyilvántartást megvalósító iratkezelési szoftvernek egyaránt képesnek kell lennie a papíralapú és az elektronikus iratok érkeztetésére, postázására és a megfelelő nyilvántartások vezetésére. A felsorolt feladatok ellátásához egy átfogó, jól átgondolt adatmodell szükséges.

Az adatmodell kialakítása előtt a 335/2005. (XII. 29.) Korm. rendelet iratkezelési folyamatokat leíró 4. fejezetének bejövő küldeményekkel, érkeztetéssel, iktatással és expediálással foglalkozó paragrafusainak elemzése következik a bejövő és a kimenő küldemények szemszögéből [2: 18–39., 55–58.].

A fizikai küldemények átvételére a címzett, a szervezet vezetője, az iratkezelést felügyelő vezető, a postai meghatalmazással rendelkező személy, az ügyfélszolgálat és az ügyeleti szolgálat jogosult, illetve elektronikus küldemények esetén az erre a célra szolgáló informatikai rendszer [2: 19]. A továbbiakban feltételezzük, hogy egy iratkezelési szoftverben kell megvalósítani a felsorolt követelményeket, azaz a küldemény átvételekor a címzés alapján a legbővebb – akár múltbéli – adatokat is felajánlva kell lehetőséget biztosítani az átvevőnek a címzett megkereséséhez. Erre azért van szükség, mert egy átszervezés esetén elképzelhető, hogy az adott személy vagy szervezeti elem már más adatokkal rendelkezik, mint amelyekről a feladó a küldemény elküldésének pillanatában tudott.

Ha tovább vizsgáljuk a jogszabályban foglaltakat, akkor azt is megtudhatjuk, hogy a küldemény felbontása jogosultsághoz kötött tevékenység, amelyet a minősített iratok kivételével a címzett, az arra írásban felhatalmazott személy vagy egy meghatározott szervezeti elem dolgozója végezhet el. A digitális küldemények bontását egy erre a célra alkalmazott informatikai rendszer hajthatja végre, amely része lehet az iratkezelési szoftvernek, vagy akár tőle elkülönülten is működhet [2: 27]. Fizikai iratok esetében a saját kezűleg felbontandó küldeményeket a címzettnek magának kell felbontania, míg egy iratkezelési szoftver esetén elektronikus állomány megismerését a címzett számára kell először lehetővé tenni [2: 28]. Utóbbi esetben egy átszervezés érdekes kérdéseket vethet fel, elképzelhető, hogy a címzett már nem képezi részét

az informatikai rendszernek, ekkor a megfelelő jogutódnak kell elvégeznie a postabontást, az elektronikus állomány megismerését.

Az iktatással kapcsolatos követelmények között szerepel, hogy az iktatókönyvnek kötelezően tartalmaznia kell a küldő megnevezését és azonosító adatait [2: 39.(f)], valamint a címzett megnevezését és azonosító adatait [2: 39.(g)]. Fizikai iratkezelés esetén ezek az adatok nehezen tarthatók karban, egy emelt szintű informatikai szolgáltatás keretében akár a múltbeli eredeti adatok feltüntetése mellett az időközben megváltozott, aktuális adatok megjelenítése, esetlegesen kereshetővé tétele nagyban segítheti az ügyintézési, ügyviteli folyamatokat. Az expediálással – a küldemény feladásával – kapcsolatos követelmények nem térnek ki külön a küldőre és a címzettre [2: 55–58.], ugyanakkor a címzés kitöltésekor a küldőnek nagy segítséget nyújthat egy iratkezelési szoftver, ha egy válaszirat esetén az eredeti küldőt fel tudja ajánlani alapértelmezett címzettként, a címzett legfrissebb adataival. Az 1. ábrán a küldemény és a hozzá kapcsolódó küldő és címzett primitív adatmodellje szerepel.

1. ábra

A küldővel és címzettel rendelkező küldemény primitív adatmodellje

[a szerző szerkesztése]

A fenti modell nem tesz különbséget a kormányzati szervhez érkező kimenő és bejövő küldemények között, a küldő és a címzett általánosan van megjelenítve. Vizsgáljuk meg ezt a modellt a GDPR-alapelvek és a küldemény küldőjén és címzettjén végzett CRUD[7]-műveletek szemszögéből. Az egyszerűbb tárgyalás kedvéért a küldő legyen minden esetben egy természetes személy, míg a címzett egy felelős, ami lehet egy szervezeti elem vagy egy ügyintéző – közfeladatot ellátó szervnél munkaviszonnyal rendelkező természetes személy.

1. CREATE – a beérkező küldemény létrehozása során létrejön a küldő és a hozzá kapcsolódó küldemény, valamint a címzett, ami egy szervezeti elem vagy egy ügyintéző lehet. Abban az esetben, ha a küldő több küldeményt is küld a kormányzati szerv számára, már azonnal problémákba ütközhetünk, mert ha a küldő, illetve a címzett adatai módosulnak, akkor minden esetben új küldőt kell létrehozni és a címzettet is duplikálva kell felvenni, így sérül az adattakarékosság elve.
2. READ – ha több küldeményt is küldött már a küldő, akkor ebben a modellben egy adatváltozás problémát jelenthet, mert a küldőhöz tartozó személyes adatok megváltoztatása a korábbi küldemények küldővel kapcsolatos adatait inkonzisztenssé tehetik. A címzettek esetében hasonló problémákba ütközhetünk. Mindig csak az utolsó állapot nyerhető ki az informatikai nyilvántartásból.

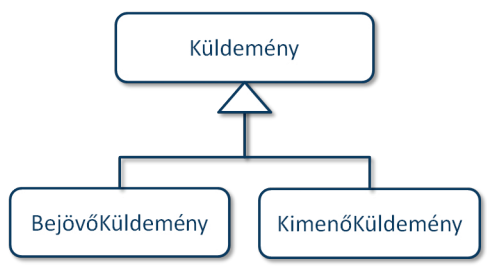
[7] CRUD-műveletek – mozaikszó a **C**REATE **R**EAD **U**PDATE **D**ELETE angol szavak kezdőbetűiből, magyarul: létrehozás, olvasás, módosítás, törlés.

3. UPDATE – egy név, postai cím, elérhetőség-változás bejelentése vagy egy ügyintézés közben végrehajtott átszervezés inkonzisztens állapotot okozhat a küldemény vonatkozásában. Teljes egészében vagy részben sérülhetnek a korábbi küldemények esetében a küldő és a címzettek adatai.
4. DELETE – a küldőre vagy a címzettre vonatkozó törlés művelete ebben a modellben adatvesztéssel jár, inkonzisztens állapotot okoz, nem támogatott művelet. Elképzelhető, hogy a későbbiekben a GDPR térnyerése kapcsán még a közfeladatot ellátó szervek iratkezelésében is előírássá válhat a törlés művelete bizonyos esetekben.

Az iménti elemzés alapján látható, hogy a küldemény primitív modellje önmagában kevés a probléma megfelelő kezeléséhez, a jogszabályi követelményekből fakadó aktív és történeti értékek tárolását a vázolt modell nem támogatja megfelelően. A vizsgálat során ki sem tértünk a kimenő küldemények kérdésére, amikor a küldő és a címzett szerepet cserél. Ebben az esetben a küldő egy szervezeti elemhez tartozó ügyintéző, míg a címzett egy természetes személy vagy egyéb tetszőleges elérhetőséggel rendelkező külső entitás (gazdasági társaság, kormányzati szerv stb.).

Bejövő és kimenő küldemény fogalma

A küldemények vonatkozásában a jogszabályi követelmények kielégítéséhez egy részletesebb modellre van szükség, ahol a bejövő és kimenő küldemények külön kezelhetők. A probléma kezelésére a küldemény fogalmának további bontására van szükség. A 2. ábrán a korábban tárgyalt *Küldemény* szétbontását láthatjuk egy *BejövőKüldemény*-re és egy *KimenőKüldemény*-re, az absztrakció lehetővé teszi a *Küldemény* hozzákapcsolását tetszőleges adatkezelési tevékenységhez – ügyintézési folyamathoz –, míg a belőle származó két küldeménytípus speciális viselkedése a továbbiakban külön-külön modellezhető, kényelmesen kezelhető.

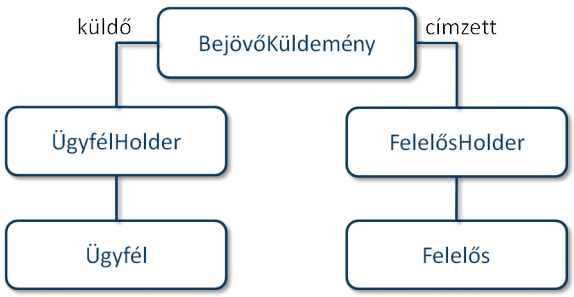


2. ábra
„Küldemény" tervezési minta

[a szerző szerkesztése]

A továbbiakban a bejövő küldemények problémakörének további vizsgálata következik. Célunk egy olyan modell kialakítása, ahol az aktív és a történeti adatok megfelelően és rugalmasan tárolhatók az ügyfelekhez és a címzettekhez kapcsolódó személyes

adatok és egyéb információk vonatkozásában. A cikksorozatunk előző részében bemutatott *ÜgyfélHolder* és *FelelősHolder* [9] tervezési minták alkalmazása célszerű lehet a bejövő küldeményekhez kapcsolódó szereplők kapcsán. Ebben az esetben a bejövő küldemény küldőjét egy *ÜgyfélHolder* segítségével, míg a címzettet egy *FelelősHolderrel* kapcsolhatjuk a *BejövőKüldeményhez.* A kialakított modell a 3. ábrán látható, a továbbiakban el fogjuk végezni a bejövő küldeménytervezési minta és a kapcsolódó CRUD-műveletek elemzését a korábbi vizsgálatokhoz hasonlóan.



3. ábra

„BejövőKüldemény" tervezési minta

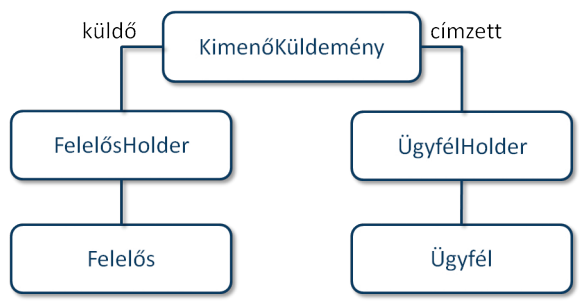
[a szerző szerkesztése]

1. CREATE – egy kormányzati szervhez beérkező küldemény átvételekor létrejön a bejövő küldemény, valamint ha az ügyfél már ismert, akkor az ügyfelet és a bejövő küldeményt összekapcsoló *ÜgyfélHolder*. Ha egy új ügyfél a küldő, akkor létre kell hozni a megfelelő *Ügyfél* entitást is. Az *ÜgyfélHolderek* a bejövő küldemények altípusai szerint tovább specializálhatók. A küldemény megjelenési formája (fizikai, elektronikus) és a feladóval kapcsolatos adatok figyelembe vehetők az *ÜgyfélHolder* kialakításakor. A tárolt adatok az ügyintézési folyamatok számára testre szabhatók. A kormányzati szervhez tartozó felelős szervezeti elemről, illetve ügyintézőről feltételezhető, hogy a bejövő küldemény átvételének pillanatában az adott informatikai rendszerben léteznek – egyébként téves címzésről beszélnénk, így a *FelelősHolder* tervezési minta segítségével a címzett a bejövő küldeményhez kapcsolható. Ekkor a címzett és bejövő küldemény közötti kapcsolat a használati esetek tükrében az ügyfelek esetével analóg módon megfelelően specializálható.
2. READ – ha a fentiek szerint hozzuk létre a bejövő küldeményekhez kapcsolódó adatmodellt, akkor lehetőség nyílik a történeti adatok kinyerésére a küldő és a címzett vonatkozásában a *Holderekből,* ha küldő vagy a címzett már nem képezi a részét az informatikai rendszernek. Ha még aktív ügyintézési folyamatok kapcsolódnak a bejövő küldeményhez, akkor a *Holdereken* keresztül elérhető az aktív küldő *(Ügyfél)* és címzett *(Felelős),* így a folyamatok helyessége garantálható.
3. UPDATE – a küldők és a címzettek adataiban bekövetkező változásokat a bemutatott tervezési minta segítségével rugalmasan lehet kezelni. A beérkezés pillanatában eltárolt adatokat a *Holderek* a szükséges időtartamig képesek

eredeti formájukban tárolni, ugyanakkor az aktív *Ügyfél* és *Felelős* entitásokon végzett műveletek ezeket az információkat nem veszélyeztetik.

4. DELETE – a küldők és a címzettek végleges törlését a vázolt modell támogatja, mert a *Holderek* a szükséges időtartamig tárolhatják mindkét fél adatait. A kialakított modell képes kezelni egy átszervezési folyamat következményeit – szervezeti elemek jogutóddal történő felszámolása, személyek törlése – a felelősök esetében a *FelelősHolder* mutatójának átállításával a jogutód felelősre. Ezzel a beérkező saját kezűleg felbontandó fizikai küldemények és az elektronikus küldemények kézbesítése is garantálható, amely a zavartalan ügyintézés egyik alappillére. A küldők fizikai törlése kezelhető a modell segítségével, akár egy aktív ügyintézési folyamattal párhuzamosan is. Az ügyintéző a válaszküldemény elküldése előtt értesülhet a küldő törléséről az *ÜgyfélHolder* segítségével, és intézkedhet a megfelelő válaszcím lekérdezéséről, az ügyintézési folyamat megfelelő lezárásáról.

A küldemény primitív modelljében tapasztalható rugalmatlanságokra a *BejövőKüldemény* tervezési minta megfelelő válaszokat ad. Az Általános Adatvédelmi Rendelettel kapcsolatos várható jogharmonizációból fakadó követelmények kezelésére megoldás lehet a bemutatott tervezési minta alkalmazása az iratkezelési szoftverekben. A kimenő küldemények esetében hasonló problémákkal találkozhatunk, mint amelyeket a bejövő küldeményeknél tapasztaltunk, azonban a tervezési minta részletes elemzése meghaladja e tanulmány kereteit. A *KimenőKüldemény* tervezési minta a 4. ábrán látható, ez esetben a küldő egy felelős – általában egy ügyintéző –, míg a címzett az ügyfél.

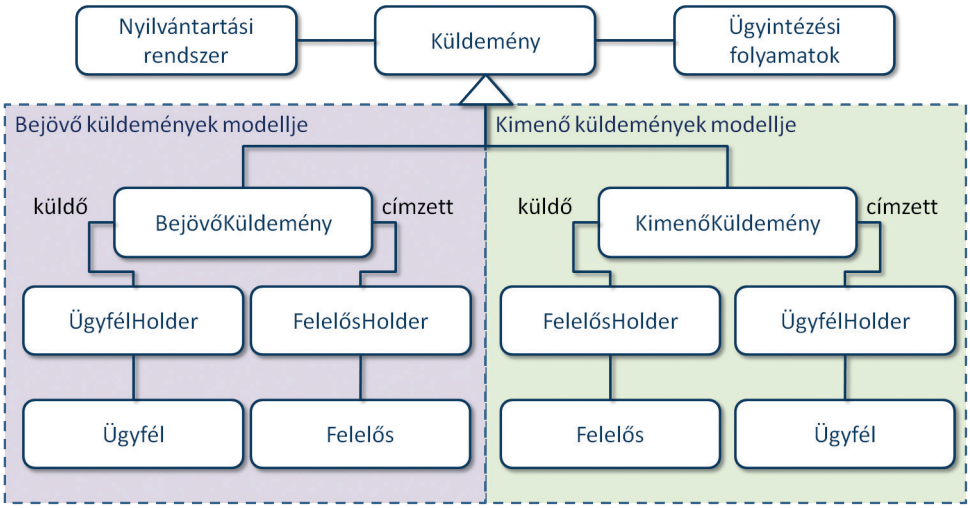


4. ábra

„KimenőKüldemény" tervezési minta

[a szerző szerkesztése]

A *Küldemény* absztrakció bevezetésével, a *BejövőKüldemény* és a *KimenőKüldemény* tervezési minták kialakításával megfelelően kezelhetők a küldőkön és a címzetteken végzett CRUD-műveletek. A *Küldemény* entitás tetszőlegesen hozzákapcsolható az iratkezelési szoftverek nyilvántartási rendszeréhez, az ügyintézési folyamatokhoz, segítségével kezelhetővé válik a visszavárólag elküldött küldemények, a többszöri érkeztetés és postázás problémaköre is. Az előbb bemutatott probléma kezelésére alkalmas modellt az 5. ábrán láthatjuk.



5. ábra

„Küldemény" tervezési minta és iratkezelési fogalmak kapcsolata

[a szerző szerkesztése]

Hierarchikus szervezetek modellezése

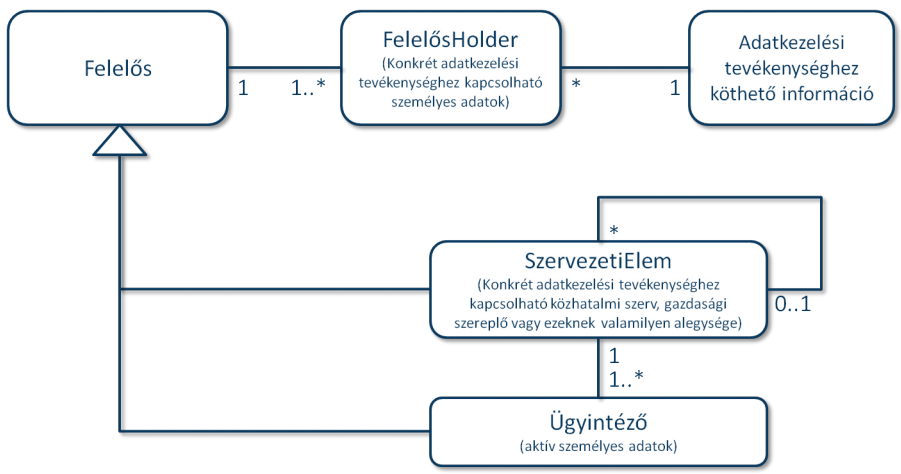
Már az ókorban is komoly jelentőséggel bírt, hogy egy hadsereg mennyire volt képes pontosan, összehangoltan végrehajtani a hadvezér utasításait egy csata során, a fegyveres konfliktus végkimenetele nagy részben a parancsvégrehajtás minőségétől függött. Egy kisebb létszámú, de szervezett hadsereggel szemben az ellenségnek minden esetben nehéz dolga volt. Ebből a megfontolásból a rendelkezésre álló haderőt, haderőnemekre és ezen belül jól vezényelhető egységekre és alegységekre formálták, amelyek a mindennapokban a fegyverforgatást és a parancsvégrehajtást gyakorolták, így a parancsnokok, ezáltal a vezetési szintek szerepe kulcsfontosságúvá vált. A technikát legsikeresebben a Római Birodalom alkalmazta, amely így egy több évszázadon át regnáló szuperhatalommá válhatott a saját korában.

Ez a fajta hierarchikus szervezeti felépítés napjainkban is megfigyelhető a különböző fegyveres erőknél, rendvédelmi és államigazgatási szerveknél. A katonai és félkatonai szervezetek esetében a parancselvű működés a szervezetek feladatrendszeréből fakad, alapvetően abból, hogy a fegyveres testületek számára parancs alapján akár erőszak alkalmazása is végrehajtandó feladat lehet. A közigazgatási és ezen belül az államigazgatási szervek számára a „parancs" az adott ország törvényeiben, jogszabályaiban keresendő, amelyek végrehajtása hasonlítható egy katonai szervezet parancsvégrehajtó mechanizmusához – jó esetben kizárólag demokratikus keretek között.

Egy hierarchikus szervezet számára fejlesztett informatikai rendszer esetében a helyesen működő folyamatok garantálásához szükséges a megfelelő informatikai

modell alkalmazása. Az e-kormányzás és a hatékony közigazgatás megvalósításában alapvető szerepe lehet a kiválasztott modellnek. Bizonyos szervezeti létszám fölött minden területen megfigyelhető a vezetési szintek megjelenése, ilyenkor az informatikai rendszerekben olyan modell kialakítása szükséges, amely tetszőleges mélységben képes kezelni a különböző szervezetek felépítését.

A *FelelősHolder* tervezési minta kiterjesztését a 6. ábrán láthatjuk. Az ábra tartalmazza a számosságra utaló 0, 1, * (tetszőleges számú) jelöléseket. A modellre igazak a következő állítások: egy adatkezelési tevékenységhez több *FelelősHolder* tartozhat, ahol a kapcsolódó felelős lehet egy szervezeti elem vagy egy ügyintéző. Egy felelőshöz akár több *FelelősHolder* is tartozhat, akár más és más adattartalommal, az adott adatkezelési tevékenységből fakadó használati eset függvényében. Minden szervezeti elemhez legalább egy ügyintézőnek kell tartoznia, ez a kitüntetett ügyintéző reprezentálja a szervezeti elem vezetőjét, hadtudományi megközelítésben a parancsnokot. Magától értetődően további ügyintézők szervezeti elemhez kapcsolása is megengedett. A hierarchikus szervezeti modell a szervezeti elemek egymáshoz kapcsolásával valósul meg, minden szervezeti elemnél lehetőség van egy felettes szervezeti elem hozzákapcsolásához. Egy elektronikus iratkezelési szoftver számára a bemutatott tervezési minta alapot képezhet a hierarchikus szervezeti felépítés modellezésére.



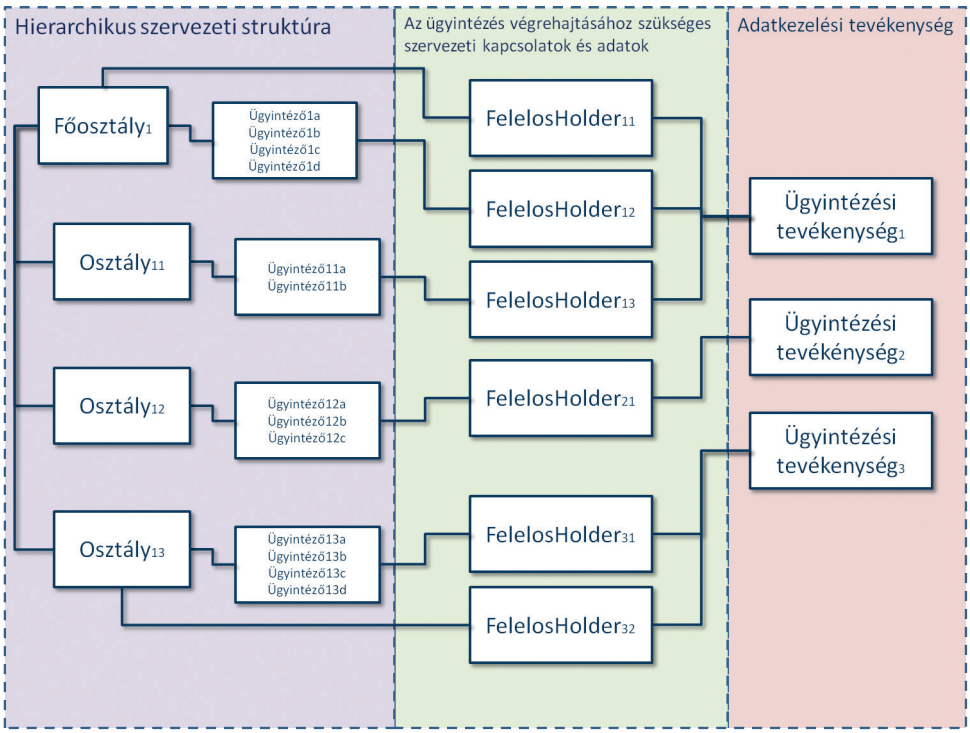
6. ábra

A „FelelősHolder" tervezési minta kiterjesztése hierarchikus szervezetekre

[a szerző szerkesztése]

Az alábbi ábrán a kiterjesztett *FelelősHolder* tervezési minta egy lehetséges használati esetét láthatjuk. A 7. ábra egy kétszintű szervezetet mutat be, ahol a legmagasabb vezetési szintet egy főosztály és a hozzá tartozó alsó szinteket három osztály alkotják. Három ügyintézési folyamatot láthatunk, ahol az első ügyintézési folyamat a főosztályhoz kapcsolódik és két természetes személy vesz részt az ügyintézési tevékenységben. A második ügyintézési folyamat egyetlen ügyintézőhöz kapcsolódik, míg a harmadik

ügyintézési folyamat egy osztályhoz és egy az osztályon dolgozó ügyintézőhöz kapcsolódik. Utóbbi a hagyományos ügyintézés menetét mutatja be, ezzel az esettel lehet a legegyszerűbben szemléltetni a CRUD-műveletek és a hierarchikus szervezetekben végmenő folyamatok kapcsolatait. A vizsgálat szempontjából érdekes lehet az ügyintéző változása, szervezeti elem felszámolása és módosítása.



7. ábra

*A hierarchikus szervezetekre kiterjesztett „**FelelősHolder**" tervezési minta használati esetei több ügyintézési folyamat esetén*

[a szerző szerkesztése]

1. CREATE – egy ügy keletkezésekor egy-egy kapcsolat jön létre az ügy és az ügyintéző, valamint az ügy és az adott ügyintéző szervezete között. A kapcsolatok az adott ügytípushoz igazított *FelelősHolderekkel* specializálhatók a GDPR-alapelveknek megfelelően.
2. READ – Ameddig az ügyintézés folyamatban van, addig a *FelelősHolderen* keresztül az aktív szervezeti és belső személyekre vonatkozó adatok érhetők el. Így pontos információhoz juthat az ügyintéző, illetve a folyamatban részt vevő többi természetes személy is a részt vevő szervezeti elemekről, személyekről. Szervezeti elem esetén példa lehet a szervezeti elem neve, nevének rövidítése, vagy azonosítója. Több természetes személy esetén példa lehet az adott felhasználó neve és beosztása, azonosítója.

3. UPDATE – Egy folyamatban lévő ügyintézés során elképzelhető, hogy az ügyintézésért felelős szervezeti elemek, személyek adatai megváltoznak. Ebben az esetben nagyon fontos, hogy milyen típusú adatról van szó: egy történetiség igazolásához szükséges egyszer letárolandó személyes-, illetve szervezeti adatról vagy az ügyintézést támogató folyamatosan frissítendő adathalmazról. A probléma kezelhető különböző viselkedésű *FelelősHolderek* segítségével. Egyik esetben inicializáláskor a szervezetek és a személyes adatok lenyomata egyszer töltődik ki és már soha többé nem frissül a *FelelősHolder*-ben. Ezzel szemben a második esetben csak a folyamat végén válik véglegessé az adattartalom – mindig a konkrét használati esetnek megfelelően.
4. DELETE – a GDPR-alapelvekből kiindulva a szervezeti elemeket és az ügyintézésért felelős személyeket is fizikailag törölhetővé kell tenni a rendszerben. Egy folyamatban lévő ügy kapcsán a másodlagos ügyintézési feladatokat ellátó személyek (segítők, bedolgozók stb.) törlése akár azonnal elvégezhető művelet lehet, míg az elsődleges ügyintéző törlése már nem az. A probléma kezelhető az ügyintézőkre mutató *FelelősHolderek* segítségével, ha valamelyik ügyintézőt eltávolítják a rendszerből, akkor az informatikai rendszeren belül továbbra is nyoma marad annak, hogy milyen ügyintézési tevékenységben vett részt az illető, az adat nem tűnik el. Egy szervezeti elem felszámolása is érdekes kérdéseket vethet fel, mert elképzelhető, hogy valahol tárolni kell a jogelődd el kapcsolatos adatokat, erre ugyancsak megoldás lehet egy speciális *FelelősHolder,* amelyik a régi szervezet adatait tárolja, de már a jogutódra mutat a fizikai törlést követően.

A hierarchikus szervezetekre kiterjesztett *FelelősHolder* tervezési minta segítségével egyenként kezelni lehet a szervezetben végbemenő strukturális és személyi változásokat a használati esetek tükrében. A megoldás kellő rugalmasságot kölcsönöz a tervezési feladatokat végző szakembereknek – a *Scrum* agilis szoftverfejlesztési módszertan esetén a terméktulajdonosnak és a fejlesztőcsapat tagjainak. A megoldás támogatja az egyszálú hagyományos ügyintézési folyamatokat (beérkező irat, válasz irat). Ezen túlmenően a modell lehetőséget biztosít a több párhuzamos szálon végrehajtott, digitális alapokon megvalósuló ügyintézési folyamatok támogatásához is. A vázolt modell jó választás lehet a 3/2018. BM rendeletben [6] foglalt folyamattámogatással kapcsolatos követelmények kielégítésére.

Ügyfolytonosság fenntartása változó szervezeti környezetben

A hagyományos papíralapú iratkezelés során az ügyek kezeléséért, a jogfolytonosság fenntartásáért az ügyviteli irodák voltak a felelősek. Az iktatólapok, előadói ívek kiadása és ellenőrzése manuális lépésként történt meg. Az átszervezések során az ügyviteli irodák segítségével voltak kezelhetők az ügymenetben kialakult problémák – az új felelősök megkeresése ezen a szinten indult újra, ha az átszervezés során a jogutódokról nem rendelkeztek egyértelműen. Az iratkezelési szoftverek világában az elektronikus iratok és elektronikus állományokhoz kapcsolódó folyamatok kezelése már manuálisan

nehézkesen vagy egyáltalán nem kezelhető, az iratkezelési szoftvernek kell képesnek lennie a szervezeti változásokból kialakuló folyamatok támogatására.

A 335/2005. (XII. 29.) Korm. rendelet 4. fejezetében az eddig tárgyalt iratkezelési tevékenységeken túl az iktatással [2: 39–50.], a szignálással [2: 51.], a kiadmányozással [2: 52–54.] és az expediálással [2: 55–58.] találkozhatunk.

Szignálás során az illetékes szervezeti egység vezetője vagy megbízottja jelöli ki az érkezett irat ügyintézőjét [2: 51.(a)]. Hierarchikus szervezetek esetében elképzelhető, hogy szignáláskor egy szervezeti elemet jelölnek ki felelősnek, ahol egy újabb szignálás következik. A létrejövő szignálások sorozata úgynevezett szignálási láncot képez, amely érzékeny lehet az átszervezési folyamatokra. A szignálási lánc egy közbülső elemének változása kihathat a szabott határidőkre, felelősökre. Ez a folyamat egy nagy létszámú, többszintű hierarchikus szervezet életében szinte mindennapos lehet. A *FelelősHolder* tervezési minta segítségével a *Szignáláshoz* kapcsolhatók azok a szereplők, akiket valamilyen formában érinthet a szervezeti struktúra változása, ilyenek lehetnek a szignáló, a szignálást rögzítő, a felelős szervezeti elem és az ügyintéző is.

A kiadmányozási folyamat során a külső szervhez vagy külső természetes személyhez – érintetthez – küldött iratot egy kiadmányozónak kell aláírnia [2: 52.(1)]. A hierarchikus szervezetek esetében a fizikai iratok esetében nagyon gyakori a többes aláírás intézménye, amikor a kiadmányozás – végső aláírás – előtt, az egyes szakterületi vezetők is aláírják az adott iratot. Az iratkezelési szoftverek esetében megfelelő folyamattámogatás mellett az aláírások száma csökkenthető, ha a többes aláírások helyét az iratkezelési szoftverben végrehajtott jóváhagyásokkal helyettesítik. Ebben az esetben a szervezeti változásoknak nem kell egyértelműen a tervezet visszautasítását okozniuk. Amennyiben lehetséges a megfelelő jogutódok azonosítása az átszervezés után, akkor ők is elvégezhetik a jóváhagyási feladatokat és az irat kiadmányozható. A folyamat támogatásához a *FelelősHolder* tervezési minta alkalmazható a jóváhagyók és az aláírók esetében.

Expediáláskor a szervezeti egység iratkezelőjének dokumentálnia kell a nyilvántartással, továbbítással kapcsolatos információkat [2: 55.]. A postázás előtti pillanatban az aktuális ügyintéző és felelős szervezeti egység küldeményekhez kapcsolása lényeges mozzanat lehet, mert elképzelhető, hogy a küldeményt visszavárólag küldik el, illetve válaszirat is érkezhet a kimenő küldemény alapján a szervezethez. Egy átszervezés ezeket a folyamatokat is felboríthatja, a *FelelősHolder* segítségével az eredeti ügyintéző, illetve a felelős szervezeti elem jogutódja a kimenő küldeményhez kapcsolható, tehát a zavartalan iratkezelési folyamat fenntartható a küldemények vissza- és beérkezésekor.

Az iktatókönyvek tartalmával kapcsolatosan egy nagyon lényeges követelmény jelenik meg az ügyintézést illetően, fel kell tüntetni az ügyintéző szervezeti egységet és az ügyintéző személyét is [2: 39.(j)]. Egy iratkezelési szoftver vonatkozásában a történeti bejegyzéseken túl, a megfelelően kialakított *FelelősHolderek* segítségével az aktuális, illetve a szervezeti átszervezések után a jogutód felelősök is hozzákapcsolhatók a különböző típusú nyilvántartásokhoz, ezen belül az iktatókönyvekhez. A kialakított megoldás segítségével az iktatókönyvek a papíralapú iratkezelés történeti lenyomatai helyett az iratkezelési szoftver nyilvántartási rendszerének nagyon hasznos valós idejű nézeteivé válhatnak.

Következtetés

Az iratkezelési szoftverek fejlesztése napjainkra komoly kihívás elé állítja a területen tevékenykedő szoftverfejlesztőket. Az iratkezelés rendjére vonatkozó korábbi jogszabályok a fizikai iratkezelés folyamatait alaposan lefedték, azonban az elektronikus iratok esetére a folyamatleírások különösebben nem tértek ki, eltekintve a beérkezés és a kézbesítés mozzanataitól. Napjainkra megjelentek a többszálú, párhuzamos feladatvégzésre vonatkozó követelmények is [6: 2.7.14]. A követelményeknek való megfelelés önmagában sem egyszerű szoftvertechnológiai probléma, ugyanakkor a kormányzati szervek életében is tapasztalható folyamatos strukturális és személyi változások együttes kezelése összetett problémát okoz.

Tanulmányunk előző részében a GDPR tanulmányozása során a zavartalan külső kapcsolattartáshoz és a folyamatos ügyintézés támogatásához kialakítottuk a *Holder* tervezési minta két speciális alesetét az *ÜgyfélHoldert* és a *FelelősHoldert*. A küldemények esetében a *BejövőKüldemény* és *KimenőKüldemény* tervezési minta alkalmazása jó választásnak bizonyul, ahol a *Holderek* az ügyfelek és ügyintézésért felelős elemek összekapcsolására szolgálnak.

Ezt követően láthattuk, hogy a *FelelősHolder* tervezési minta lehetővé teszi a több szálon futó ügyintézést a hierarchikus szervezetek életében, a tervezési minta segítségével megfelelően lehet támogatni a zavartalan ügyintézést a szignálási folyamattól a kiadmányozási folyamatig. Az iratkezelési szoftverekben kötelezően vezetendő nyilvántartások bővítése a megfelelő *Ügyfél-* és *FelelősHolderek* bevezetésével lehetővé teszi az aktuális és a múltbéli adatokban való keresést is. A hagyományos és a többszálú iratkezelési tevékenységek modellezéséhez a kialakított tervezési minták jól alkalmazhatók.

A cikksorozatban bemutatott tervezési minták segítségével szoftvertechnológiai oldalról emelt szinten támogatható az iratkezelési szoftverek tervezése, a jogszabályi követelmények könnyedén leképezhetők a *Holder* tervezési minta kiterjesztésével, ezáltal az e-kormányzáshoz szükséges informatikai rendszerek kialakítása egyszerűbben és rugalmasabban valósítható meg.

Hivatkozások

[1] A belügyminiszter, az informatikai és hírközlési miniszter, valamint a nemzeti kulturális örökség minisztere 24/2006. (IV. 29.) BM–IHM–NKÖM együttes rendelete a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről, Magyar Közlöny, 51. sz. 2006, pp. 4058–4064. [Online]. Elérhető: https://magyarkozlony.hu/dokumentumok/a3be226fc3dd4253e04ed8e9f301ca1b80956e00/megtekintes (Letöltve: 2018. 12. 20)

[2] 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről, Magyar Közlöny, 172. sz. I. kötet, 2005. pp. 12408–12419. [Online]. Elérhető: https://magyarkozlony.hu/dokumentumok/d49128c85520fcac3628edf1a23fa62db36f4fe9/megtekintes (Letöltve: 2019. 01. 03.)

[3] I. Négyesi: "Changing role of the internet in the light of an international conference" (Az internet szerepének változása egy nemzetközi értekezlet tükrében), *Hadmérnök,* 3. évf. 3. sz. pp. 147–153, 2008.
[4] I. Négyesi: „Az információgyűjtés jövőképe," *Hadtudományi Szemle,* 1. évf. 3. sz. pp. 95–100, 2008.
[5] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=HUA (Letöltve: 2018. 12. 03.)
[6] A belügyminiszter 3/2018. (II. 21.) BM rendelete a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről, Magyar Közlöny, 23. sz. pp. 984–1019. 2018. [Online]. Elérhető: https://magyarkozlony.hu/dokumentumok/a2d76c6e46db22a7b33f18c6aa67b0597d7c5001/megtekintes (Letöltve: 2019. 01. 08.)
[7] 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről, [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=99500066.TV (Letöltve: 2019. 01. 08.)
[8] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól, [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A1500222.TV (Letöltve: 2018.12.03.)
[9] J. Gerevich és I. Négyesi, „A fenntartható és zavartalan elektronikus ügyintézés szoftvertechnológiai háttere – 1. rész," *Hadmérnök,* 14. évf. 2. sz. pp. 281–292, 2019.

HADMÉRNÖK
VÉDELMI ELEKTRONIKA, INFORMATIKA, KOMMUNIKÁCIÓ

14. évfolyam (2019) 3. szám 91–100.
DOI: 10.32567/hm.2019.3.8

Attila Horváth[1]

Countering the Counterspace – Doctrinal and Operational Aspects of Preserving Space Capabilities

Ellenállás a világűrben – az űrképességek megőrzésének doktrinális és műveleti aspektusai

This paper presents the outer space as a military operational domain, describes the various means an adversary could affect our space capabilities, and also our ways to protect them.

Keywords: **space operations, counterspace**

Ez a cikk bemutatja a világűrt, mint a katonai műveletek egyik színterét, leírja, milyen módszerekkel tudja a szembenálló fél befolyásolni az űrképességeinket, és egyúttal azt is, hogyan tudjuk megvédeni azokat.

Kulcsszavak: **űrműveletek, űrtámadás**

Introduction

Space is a military operational domain. That is not new, it has been since the 1960s, whether it was declared in doctrines or not. Since time immemorial, there were military and national security services which operated by wartime regimes even in peacetime. Counterespionage, strategic missile forces, national air defence and cyber are like that. And space also. Our space operators are safeguarding our own space assets, are searching for weaknesses in those of the enemy, and are, of course, developing solutions to exploit those weaknesses. The enemy does the very same.

[1] National University of Public Service Doctoral School of Military Sciences, PhD student, e-mail: horvatt@gmail.com, ORCID: https://orcid.org/0000-0001-9768-5357

Of course, with the advance of technology, the weapons and tactics change. The main focus of this article therefore is not those, but the analysis of the relevant US [1] and NATO [2] doctrines to clarify the strategic viewpoint regarding counterspace, anti-counterspace and counter-counterspace military activities.

In the context of this article, counterspace means actions taken to hinder one actor's space activities by another; anti-counterspace means actions taken to increase the resiliency of the one actor's space assets against counterspace operations, and counter-counterspace means active actions taken to prevent the use of enemy counterspace weapons or to minimise their effects when they strike.

It is important to remember that, just as space systems do not necessarily reside on orbit in outer space, the counterspace and counter-counterspace activities can be executed in all operational domains, be it space, land, air, sea or cyber. Likewise, offensive and defensive actions are defined by their outcome, not by their execution. It is entirely possible to mount an operation with an offensive execution to prevent the deployment of a counterspace asset, and this way the operation can be classified as defensive.

Components of Space Systems

Traditionally, space systems are subdivided into ground segment, link segment and space segment [1: I-2, I-3].

The ground segment resides on the surface of the Earth (including the lower atmosphere where aircraft operate), and typically contains the user terminals and the system operation facilities (tracking, telemetry and control stations, communication teleports and mass data downlink receivers). The terrestrial communication network connecting the space system to the end users can also be included in the ground segment, but just as well it can be considered a separated system which provides service for the users by enabling the data flow between the space system and the end user systems.

The space segment resides in outer space, and consists of the orbiting spacecraft (unmanned artificial satellites in the majority of cases today). The characteristics of these spacecraft define the services and capabilities offered by the space system.

The link segment connects the two other segments, and it is typically a radio (microwave) connection, or nowadays laser links are also used, especially in the uplink (ground to space) path. In space systems where more than one spacecraft is operated for the purpose of providing a service, intersatellite links can be used to connect the individual satellites to each other, without the use of ground stations. One of the most representative examples of intersatellite link usage is the architecture of the Iridium satellite telephone constellation, which uses microwave links to interconnect the spacecraft, but laser links can also be used this way. These intersatellite links, while residing in outer space, should be considered parts of the link segment, because of their vulnerability profile.

In a complex architecture of "system of systems" space capabilities, I recommend adding a fourth element to the mix, namely the service segment. The service segment

(in contrast to the first three) is intangible, as it consists of the actual services provided by the end users, regardless of their physical or system-specific base. Emphasising the service segment is important because that is what the end users ultimately care for, and services also have a different and very specific vulnerability profile. Moreover, in many practical space systems, services of one space system are used as enablers of the operation of another one. Two easy to understand examples are the use of communication satellites as data relays between remote sensing satellites and ground control/downlink stations, and the use of positioning, navigation and timing services (such as the NAVSTAR GPS) in the tracking and time synchronisation of various space, link and ground segment elements. Therefore, the protection of such embedded services ultimately results in the protection of end-user services.

The service segment is different from the first three segments because it cannot be attacked directly, as all service degradation originates from attacks on any one of the first three. However, it can be protected directly, when the diversity of the space system portfolio allows for a successful attack on one space system or asset, because the service can be provided from a different source.

Attack Options and Vulnerability Profiles

The unique physical characteristics of outer space, the complex architecture of space systems and the various level of ambition of the adversary create a very diverse portfolio of attack options on space assets.

The military space operation which concerns itself with inflicting damage to the enemy's space assets is the Offensive Space Control, as defined by the relevant US doctrine [1: II-2]. The actions of the Offensive Space Control are:

- Deceive: deception injects information into the decision-making cycle of the enemy which is not true, out of context or gives rise to false interpretation. In itself it has no permanent damaging effects (however, the decisions made based on the deception, for example, orbital manoeuvres using valuable fuel, can have lasting negative effects).
- Disrupt: disruption lowers the level of operational quality of a system or a service, for a period of time, again without causing permanent damage.
- Deny: denial is disruption elevated to the next level, that is, the denied system becomes completely unavailable, its usefulness for the operator becomes zero. This action is also non-physical.
- Degrade: degradation lowers the level of operational quality of a system or a service, but this time the effects are long-lasting, even permanent. To cause such effects, physical damage might be required.
- Destroy: destruction removes permanently and completely the space system or service from the usable portfolio of the enemy. It is usually a physical action.

The means of attacks can be subdivided into kinetic, electronic warfare and cyber categories. Sometimes electronic warfare is considered a part of cyber operations,

but for the context of this article, I treat them separately. The reason behind this is the inherent differences of the execution and outcome of the two approaches.

Kinetic attack against the ground segment is not different from any traditional military strike. The identified and selected ground segment components are subjected to land, aerial and seaborne fires, or overrun and captured by conventional or special operations forces. Because the ground segment components of space systems can be located very far from the area of actual military operations, the employment of special operations forces using infantry weapons (long-range, large calibre anti-material rifles, shoulder-launched antitank or bunker-buster missiles, small-calibre mortars) against the outdoor equipment, or providing target designation for aerial or long-range missile artillery bombardment can be surprising, very effective and limits collateral damage.

Kinetic attacks against the space segment can be achieved by co-orbital or direct-ascent anti-satellite effectors [3: xv].

Co-orbital assets are launched into orbit like any space vehicle, where they perform rendezvous and proximity operations to establish themselves near their target. From this position, effectively formation-flying with the target, they can observe it (providing valuable reconnaissance information and/or positive target identification), and then execute their attack by colliding onto the target, firing projectiles toward it or physically grabbing and reorienting it. This makes co-orbital weapons very dangerous: the operators of the target, even if they detect the forming-up of the attacker with their satellite (we should keep in mind that the attacker can reduce the optical, infrared and radar signature), cannot know the intentions of the weapon. Close inspection of a satellite, while it can be considered an unfriendly act, does not necessitate counteractions in itself, as long as the co-orbital weapon is not interfering directly with the operation of the satellite. The formation flying can be continued for hours, days, even weeks, and the weapon can visit several satellites, if it carries enough fuel to supply the necessary delta-v (the description of such an operation can be found in [3: 1–5, 1–6]). Therefore, while the operators of the target satellites can be aware of the threat in general, they cannot know when the actual strike will come, if ever. So co-orbital operations can be used to coerce the operator of the satellite to change orbit, therefore using up its own delta-v budget prematurely, which in itself can be counted as a mission kill in the long term.

Direct-ascent weapons are launched into a suborbital collision course towards their targets. They can carry conventional or nuclear explosive warheads, but the relative velocities of the interceptor and the target makes this unnecessary, as long as the interceptor, most often called kill vehicle, can actually strike the satellite. The kinetic energy released during the collision will do the job. The main difference between co-orbital and direct-ascent is the timeline of the attacks. As we have seen, co-orbital weapons take longer to reach their targets, but the actual destructive strike can be executed very fast; direct-ascent weapons finish the whole attack sequence faster, but the intention is known from the very beginning of the attack. Therefore, the satellite operator knows immediately what to expect, and can execute defensive manoeuvring, and the kill vehicle can only attack once. In addition to this, direct-ascent assets are destructive weapons with no other purpose. There is no time to collect intelligence, and positive target identification must occur before the actual interception.

Kinetic attacks executed with surgical precision against the antennas, amplifiers (or laser upbeam equipment) of the ground stations can be considered link segment kinetic attacks, but this is only playing with words. Such attacks have already been considered above.

On the other hand, the link segment is the very area for electronic warfare (and directed energy weapon) attacks. In this article I will not elaborate on interception, traffic analysis and exploitation of the electromagnetic radiation originating from the space systems, just the offensive jamming of them.

Both ends of the link segment can be subjected to jamming [1: II-15]. When operating against the receivers onboard the satellite, the action is called uplink jamming. This attack can be very effective against the traffic carried by communication satellites, but every satellite is vulnerable to control channel jamming. Uplink jamming is received by the satellite from anywhere within the receiver antenna beamwidth (the projection of which onto the surface of the Earth is called footprint). This way, if the antenna has a wide beamwidth, the satellite is very vulnerable, and the adversary is in a very advantageous position.

Such jammers can be installed onboard ships or (theoretically) aircraft, which can operate from international waters or airspace, therefore attribution of the attack is even more difficult. Moreover, jamming does not have a lasting effect, it does not cause any permanent harm, can be applied and turned off instantly, so it can be applied when it is necessary within the operational timeline, and leaves no recoverable evidence.

Uplink jammers can theoretically be installed onboard co-orbital anti-satellite space vehicles. Such application would be very surprising to the victim, and as the jamming signal would arrive from much closer that the user signals, even a very limited power jammer would be effective.

A special case of uplink jamming is executed against the sensors of remote sensing satellites. This will be detailed below, together with directed energy weapons.

Downlink jamming is executed against the terrestrial end of the link. It is especially effective against satellite navigation receivers, and communication ground terminals with omnidirectional antennas. In these scenarios, small power (therefore, small size) jammers can be effective, because of the limited power of the user signal and the receiver antenna cannot discriminate between the user signal and the jamming signal. Such jammers can even be deployed from aircraft or artillery rockets.

The drawback of downlink jamming is the necessity of line-of-sight between the jammer and the jammed equipment, therefore, the limited operational range. However, this also makes it possible to tailor the jamming to the operational area. Such limited range can be overcome via numbers, with the deployment of a large number of jammers. An example of this is the prepared area defence against satellite navigation based precision-guided munitions or drones [4].

Electromagnetic energy can be used against the sensors of remote sensing satellites. Such energy, depending on the power level, can be used to temporarily disable the sensor or distort the recorded data, in which case it is usually called dazzling (this expression is usually used in relation to optical sensors, but the mechanics of a microwave beam directed against a radar or ELINT/MASINT satellite are no different)

[3: 1–18]; or can cause permanent damage, in which case we are talking about directed energy attack. It is important to repeat that the only difference between dazzling and directed energy attack is the power level. Therefore, a dazzling can readily be a strategic warning or a means of coercing, by the implication of a much more serious, damaging attack. Moreover, directed energy weapons with a level of power in the destructive range can also be utilised against other types (like communications) satellites, not just against recon ones.

Theoretically, nuclear electromagnetic pulse effects (also known as high-altitude electromagnetic pulse, or HEMP) can be used against space systems. Such attacks are, however, by their very nature, indiscriminate and it is practically impossible to target a specific adversary. Moreover, most military space vehicles are hardened against electromagnetic pulse effects. On the other hand, such attacks would be very destructive to the civilian space (and terrestrial) infrastructure, therefore they can be considered as counter value operations initiated to damage the enemy society as a whole.

Just as with kinetic attacks, cyberattacks against space systems are not fundamentally different from similar attacks against any other type of computer systems [3: 7–1]. As the onboard networks and computers of satellites are pretty much isolated from any other computer system, the only link being the tracking, telemetry and control system, they can be very well protected against cyber operations. But if this separation can be overcome by some means, the attacker can access the onboard systems and, lacking protection in depth, can freely wreak havoc. Therefore, the separation must not be the only protection, the other best practices of the cyber industry must be applied to satellite onboard systems, as well. Cyberattacks can have any level of effect listed above, and just in the case of dazzling, a carefully limited strike can be a precursor or warning of another one with much sever consequences.

Cyberattacks are well suited to disable services without inflicting any harm to the actual components of the space system. For example, disabling the terrestrial network used to disseminate the raw sensor data to the analyst has the same tactical consequence as blowing the satellite up. Therefore, it is better to have a holistic approach regarding cyber security which covers all levels and subsystems of one's information infrastructure, instead of focusing on single assets and treating them as islands. Just as with real-life island groups, even if the single land masses are left unharmed, blockading the sea and air lines of communications between them will hurt the group as a whole.

Protection of Space Assets and Service Assurance

Naturally, the doctrines which define counterspace actions also define the means to preserve and protect space systems and services [2: 5–7]. We can classify these means as [1: II-3]:

- active defensive actions taken to reduce the effectivity of enemy offensive systems by taking actions against them,

- reactive actions taken upon the realisation of an imminent or ongoing enemy attack,
- and passive protective actions which are included in the design and operation of space systems, and are aiming to reduce the effectiveness of any future attacks,
- finally, deterrent actions [1: I-9] which discourage the potential enemy from even considering any attack.

The active defensive actions are similar to their offensive counterparts, but as their targets are the attack capabilities of the adversary, their outcome is defensive from our point of view.

The last category can build upon the first three, because the adversary can be persuaded that a successful attack is simply not possible within their technological means and/or political will. Therefore, they are better to leave the space systems alone, as their attack simply cannot be successful. However, deterrence can be achieved via proof-positive attack attribution and the demonstration of military means and political will to act against any adversary following an attack on our space systems. This assured post-attack strike makes the enemy realise that the advantage of an attack on our space capabilities will be nullified by the consequences of our counterstrike.

More attention needs to be focused, however, on the second and third categories. The reactive actions are initiated when Space Situational Awareness, Satellite Operations or service system operations activities signal that an attack is under way (or, preferably, is being initiated). After the characterisation of the strike, Satellite Operations or the service system operation must react without delay, and execute some kind of manoeuvre to counter the attack. Depending on the attack, the manoeuvre can be, for example:

- orbital, to counter a direct-ascent or co-orbital kill vehicle,
- frequency or transmit power adjustment, to counter a downlink jamming,
- antenna radiation pattern modification, to counter an uplink jamming (or downlink jamming, if the technology permits it).

All the possibilities of manoeuvre should be identified based on the architecture of the actual systems, and operational procedures should be developed for them.

Regardless of the potential of the aforementioned three categories, the most important, in my opinion, are the passive protective measures, built into the systems during their design and maintained during operations. They enable the manoeuvres and support the deterrence, therefore they are essential for the preservation of the space capabilities. Moreover, these measures readily offer protection against natural and unintentional man-made threats.

The US doctrine, on which this part is largely based, classifies reconstitution as an active, follow-up action to the actual attack [1: I-8]. In my opinion, however, reconstitution must be planned in advance, preferably during system design, and the means of reconstitution must be readied well before the attack. Reconstitution means the activities taken after the loss or degradation of a space system or service, to restore the services themselves, not necessarily the actual systems. For example,

the loss of a SATCOM asset can be followed up by the activation of a service contract with a different service provider, utilising a different satellite. This way, from the user perspective, the loss is mitigated or even eliminated, if the newly activated service can replace the lost one entirely.

The US doctrine considers resilience [1: I-8] the designed and built-in approach to ensure the continuation of space systems and services in the face of an attack. According to the doctrine, resilience can be achieved via:

- Disaggregation, that is, the careful assignment of different services to different assets. As the name implies, it is the opposite of aggregation, and this way the systemic approach can easily be understood. Focus the assets to a limited set of services, and deploy a combination of them to enable the required level and spectrum of space support to the forces. For example, the combined weather-and-SATCOM satellites of the early stages of the INSAT program of India were designed with aggregation in mind (to save on satellite buses and launches), and when later they decided to deploy specialised, separated communication and weather satellites, they executed disaggregation.
- Distribution, that is, the elimination of single points of failure (from the service point of view), by deploying independent, but interrelated groups of assets to realise any given task. So, the disaggregated space systems become even more fragmented, as more than one satellite is used to support a mission. Distribution is not the same as proliferation (see later), because in a distributed system the components work together, not simply next to each other. A distributed system is capable of "graceful degradation", when the loss of one or more system elements, while undoubtedly has some negative effects on the service quality, does not make the system completely unusable. There exists, however, a critical point, when enough of the elements is taken out of service, and consequently the system as a whole ceases to operate. It takes a lot more effort to achieve this (from the adversary's point of view), than it would take against a system which is concentrated.
- Diversification, that is, the use of different systems to provide a similar service to the users. This way, the user is (ideally) not concerned with, or (realistically) is prepared to switch between, the systems that operate to support their mission. When one system is completely taken out of operation, another one takes over with minimal outage, and the mission can go on.
- Protection, that is, to build and deploy components and systems which are capable of continuing their operation even in a hostile or adverse environment. The threats protection required against are identified during the design phase and appropriate countermeasures are added to the system. This means that a protected, hardened satellite is generally heavier than a non-protected satellite with similar capabilities. Electromagnetic shielding, ballistic armour and extra delta-v budget are expensive in weight.
- Proliferation, as mentioned earlier, means the deployment of a large(er) number of system elements than required for normal operation. A commercial SATCOM satellite operator can successfully operate with a single satellite anchored to a single teleport. For a military operator, this approach is risky.

By proliferating the teleports, the job of the attacker becomes harder, as any one of the teleports can support the missions, therefore, all of them must be taken out. This is the main difference between proliferation and distribution. In a distributed system, the workload is shared among the system elements, but there is no individual element which can carry all the load. In a proliferated system, any element can carry the minimum required workload, and by adding extra elements, we achieve resiliency and at the same time, extra capacity within the system. During an attack, this extra capacity will be lost, but as long as a single element is operational, the minimum requirement is met.

- Deception, that is, the hiding of the full capability spectrum of a space system from the adversary, is the final element of resilience. During peacetime operations, the full capabilities are not utilised. A part of them are kept in reserve, and no indication is given about their existence. In an ISR system, this can be the resolution, when the peacetime data is not as well-detailed as the full physical resolution of the sensor. In SATCOM, this can be output power or bandwidth, or even waveforms.

Conclusions

In this article I summarised the doctrinal basis of counterspace operations, and at the same time, the basis for the protection, preservation, and if all else fails, the restoration of space capabilities. This topic is getting all the more important. If we look at the dynamics, India tests an anti-satellite weapon system, while at the same time NATO is working on their space policy, and the US is planning to create a new branch of their armed forces, the space force. This also shows that outer space is not losing its traditional importance in military operations.

Added to this are the proliferation of space technology, space systems and services, and also the proliferation of counterspace (including counter service) and dual-use solutions. The outcome is that we need to concentrate on the hardening and protection of our own space assets. This is only possible if at the same time we ourselves also study those counterspace activities, not necessarily to use them, but at least to get to know our enemies.

The basics of a successful and credible space capability are space situational awareness and satellite operations. Connected to those are the credible deterrence (to warn off any adversaries) and restoration capabilities, to assure the adversary that their efforts would be in vain. Nations with smaller economies and space programs can acquire these via alliances, and this way even they could be meaningful contributors to collective defence efforts.

References

[1] *Space Operations.* US Department of Defense Joint Publication, pp. 3–14, 2018.
[2] *Allied Joint Doctrine for Air and Space Operations Edition B Version 1.* NATO Allied Joint Publication 3.3, 2016.
[3] B. Weeden, V. Samson, Eds., *Global Counterspace Capabilities: An Open Source Assessment.* Washington, D.C.: Secure World Foundation, 2019. [online] Available: https://swfound.org/media/206408/swf_global_counterspace_april2019_web.pdf [Accessed May 5, 2019].
[4] R. Beckhusen, *Russia Plans to Turn Cell Phone Towers Into Cruise Missile Jammers,* 2016. [online] Available: https://nationalinterest.org/blog/the-buzz/russia-plans-turn-cell-phone-towers-cruise-missile-jammers-18067 [Accessed May 5, 2019].

HADMÉRNÖK
VÉDELMI ELEKTRONIKA, INFORMATIKA, KOMMUNIKÁCIÓ

14. évfolyam (2019) 3. szám 101–111.
DOI: 10.32567/hm.2019.3.9

Károly Krisztián[1]

LoRaWAN-technológia felhasználási lehetőségei a katonai alkalmazások tükrében

Application Opportunities of LoRaWAN in the Point of Military Deploying

Napjaink automatizálási trendjeinek köszönhetően előtérbe kerültek az emberi beavatkozást nem igénylő, úgynevezett gép-gép kommunikációt (M2M) lebonyolító távközlési megoldások. Ilyen kommunikációs eljárás a LoRaWAN-technológia is, amely Chirp moduláció segítségével képes csillag topológiájú hálózatokba szervezni szenzorainkat, akár viszonylag nagyobb területek lefedése mellett is.
Kutatásomban a LoRaWAN-technológia katonai felhasználási lehetőségeit vizsgálom. Feltárom a technológia katonai szempontból előnyös tulajdonságait, valamint az alkalmazhatóság korlátait.

Kulcsszavak: LoRaWAN, LPWAN, szenzor, Chirp

Gratitude to today's automation trends the machine to machine (M2M) technologies came into the scene. Based on their specified characteristics they do not require any human intervention. The LoRaWAN technology is one of them and it is based on Chirp modulation. It is able to organise and re-organise the applied sensors into star topology network covering wide operational areas.
My intention is to present the most likely courses of actions of LoRaWAN's military applications pointing out the advantages and disadvantages with focus on the military deployability.

Keywords: LoRaWAN, LPWAN, sensor, Chirp

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: krisztian.karoly@mil.hu, ORCID: https://orcid.org/0000-0002-5835-7980

Bevezetés

Napjainkban robbanásszerű növekedést figyelhetünk meg az IoT[2]-alapú megoldások területén. Az ezeket kiszolgáló eszközök képesek emberi beavatkozás nélkül, akár nagyméretű hálózatokba integráltan kommunikálni egymással, ezáltal megvalósítva a gép – gép (M2M[3]) interakciót. Az Ericsson vállalat elemzése alapján [1: 16.] 2017-ben 7,5 milliárd db mobiltelefon és 1,6 milliárd db PC/laptop/tablet volt használatban, míg 2022-re várhatóan az előbbiek száma 8,6 milliárd db-ra, az utóbbiaké pedig 1,7 milliárd db-ra növekszik majd. Eközben 2017-ben a nagy területet lefedő hálózatokba (WAN[4]) szervezett IoT-eszközök száma 0,8 milliárd db (ebből 0,7 milliárd mobilhálózati), míg a rövid hatótávolságú hálózatokba szervezett IoT-eszközök száma 6,2 milliárd db volt. Ezeken a területeken 2023-ra 17–30%-os éves növekedést prognosztizálnak, azaz addigra várhatóan a WAN-hálózatokba szervezett IoT-eszközök száma eléri majd a 4,1 milliárd db-ot (ebből 3,5 milliárd mobilhálózati), a rövid hatótávolságú hálózatokba szervezett IoT-eszközök száma pedig 15,7 milliárd db-ra növekszik. Az előrejelzések alapján megállapítható tehát, hogy 2023-ra várhatóan közel kétszer annyi IoT-eszköz lesz használatban, mint telefon vagy számítógép.

Természetesen a hálózatba integrált infokommunikációs eszközök piacának ilyen irányú átrendeződése a katonai szektorra is hatással lehet. Az autonóm szenzorhálózatok alkalmazása révén rövid idő alatt, nagy mennyiségű adatot csatornázhatunk be különböző rendszereinkbe, amelyekből célszoftverek segítségével olyan információkat nyerhetünk ki, amelyek nagyban képesek támogatni a parancsnokokat és törzseiket a minél reálisabb helyzetismeret (SA[5]) kialakításában. Mindez a vezetési fölény jelenleginél lényegesen rövidebb idő alatt történő kivívásának lehetőségét hordozhatja magában.

A rövid hatótávolságú IoT-hálózatok kommunikációs protokolljai közé tartozik az IEEE 802.15.1 Bluetooth [2], az IEEE 802.15.4 ZigBee [3], és ezen IoT-hálózatokat támogatja az IEEE 802.11 Wifi [4] szabvány is. A Bluetooth és Wifi technológiák köztudottan széles körű szakirodalommal rendelkeznek, a Zigbee technológia katonai alkalmazhatóságával kapcsolatban egy korábbi publikációmban foglalkoztam [5]. A nagy területeket lefedő IoT-hálózatok terén kiemelkedők az LPWAN[6]-megoldások [6], amelyeket kritikus energiaigényű szenzorhálózatoknál érdemes alkalmazni, és alacsony adatrátát biztosítanak. Mint azt az előbb említett Ericsson-felmérésből is láthattuk, a legnagyobb darabszámú fejlődést a mobilhálózati megoldásoktól várhatjuk, ilyen az NB-IoT[7] is [6: 10–14.]. E technológia alkalmazásának kritérium-feltétele a 3G/4G/5G mobilhálózati lefedettség, amely a katonai műveletek során számos esetben nem biztosítható. További LPWAN-technológiák a LoRaWAN[8], a Sigfox, Wi-SUN Alliance FAN[9] technológiák [6], amelyek közül a LoRaWAN kommunikációs eljárást vizsgálom

[2] Internet of Things – dolgok internete.
[3] Machine to machnine – gép és gép közötti kommunikáció.
[4] Wide Area Network – nagy kiterjedésű hálózat.
[5] Situational Awareness – helyzetismeret.
[6] Low-Power Wide Area Network – alacsony energiaigényű nagykiterjedésű hálózat.
[7] Narrow-Band IoT – keskeny sávú IoT kommunikációs protokoll.
[8] Long Range Wide Area Network – nagy hatótávolságú és nagy területet lefedő hálózat.
[9] Field Area Network – földfelszíni hálózat.

a katonai alkalmazhatóság szempontjából számos előnyös tulajdonsága miatt, többek között az önálló infrastruktúra lehetősége, és Chirp modulációs eljárás miatt.

Fontos megemlíteni, hogy a LoRaWAN-technológiát többek között már sikerrel alkalmazták környezetbiztonsági, klímaváltozási kutatások során [7], ahol nagy kiterjedésű telekommunikációs infrastruktúra nélküli területeket fedtek le. E példa mentén érdekes lehet a LoRaWAN alkalmazásának megvizsgálása a Nemzeti Közszolgálati Egyetem egyéb kutatási területein is, mint például a klímaváltozás hazai hatásainak nyomon követése során, például a csapadékmennyiségek és intenzitások tekintetében [8], [9], [10], [11].

Kutatási célkitűzésem a LoRaWAN-technológia katonai alkalmazhatóságának behatárolása, az esetleges korlátok feltárása, és ezekre megoldási javaslatok megfogalmazása.

A LoRaWAN-technológia

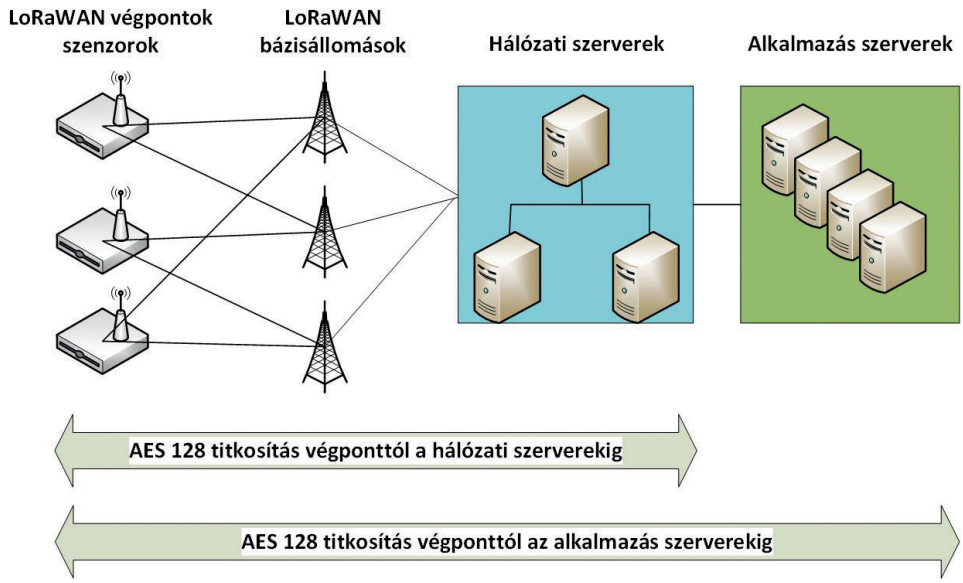
A Semtech cég fejlesztette ki [12] eredetileg a LoRa[10]-technológia alapjait, amely az OSI[11]-modell szerinti fizikai- (L1[12]) és adatkapcsolati rétegbeli (L2[13]) ajánlásokat fogalmaz meg. A technológia fizikai rétegbeli specifikációit szokás még LoRaPHY-ként is emlegetni. A LoRaWAN-protokollkészlet már a LoRa-végpontok (node-ok) hálózatszervezési kérdéseivel foglalkozik, adatkapcsolati- (L2) és hálózati rétegbeli (L3[14]) definíciókat rögzít, ugyanakkor szűkíti a fizikai réteg egyes paramétereit. Jó példa erre, hogy LoRaWAN alkalmazása esetén 125 kHz, 250 kHz és 500 kHz-es sávszélességű csatornákkal tervezhetünk, míg az eredeti LoRa esetén lehetőség van akár 25 kHz-es csatornák kialakítására is. A LoRaWAN szigorúbb szabályozási keretei annak a gyakorlati felismerésnek köszönhetők, hogy a kisebb sávszélesség sokkal pontosabb oszcillátorokat követel meg a végpontoknál, amelyek aránytalanul megdrágítanák ezen node-ok előállítási költségeit [13], [14], [15]. További különbség, hogy LoRa-kapcsolat alatt többségében pont-pont összeköttetéseket értünk, míg LoRaWAN esetében csillagtopológiájú hálózatokról beszélhetünk.

A LoRa Európában a 868 Mhz-es rádióengedély nélkül használható ISM[15]-sávban működik, 25 mW maximális adóteljesítmény mellett 0,1–1% adáskitöltési tényezővel. A LoRa-technológia fizikai rétegét tekintve, úgynevezett „LoRa modulációt" alkalmaz, amely egy speciálisan kialakított Chirp szórt spektrumú (CSS[16]) modulációs technika. A szinuszos hullámformájú jelet lineáris frekvenciamodulációval (LFM[17]) modulálják, amely a Chirp-jelet eredményezi. Ennek a modulációnak köszönhetően rövid idő alatt, keskeny sávszélességen, minimális energiafelhasználás mellett vihetők át a továbbításra szánt adatok. Ez az eljárás olyan szenzorhálózati megoldásoknak kedvez, ahol a szenzor

[10] Long Range – nagy hatótávolságú.
[11] Open Systems Interconnection Reference Model – nyílt rendszerek összekapcsolása referenciamodellje.
[12] Layer 1 – 1. réteg.
[13] Layer 2 – 2. réteg.
[14] Layer 3 – 3. réteg.
[15] Industrial, Scientific and Medical – ipari, tudományos és orvosi.
[16] Chirp Spread Spectrum – Chirp szórt spektrumú moduláció.
[17] Linear Frequency Modulation – lineáris frekvenciamoduláció.

teljes élettartama alatt csak minimális szintű kommunikációra van szükség, például éveken keresztül történő napi néhány alkalommal történő adatközlés esetén [13].

A Chirp-modulációnak köszönhetően –137 dBm vevőérzékenység, és –19 dB jel-zaj viszony (SNR[18]) mellett képes a kapcsolat fenntartására, amely rendkívül jó zavarállóságot biztosít a rendszernek [13]. A LoRaWAN alapvetően csillagtopológiájú hálózatok kialakítását teszi lehetővé, amelyet az 1. ábrán láthatunk.



1. ábra

LoRaWAN hálózat részei, multicsomópontú csillagtopológiába szervezve

(a szerző szerkesztése [15: 168.] alapján)

A szenzoroktól begyűjtött adatokat a LoRaWAN-végpontok a bázisállomások (átjárók) felé továbbítják, amelyek TCP/IP[19] hálózatokra csatolják ki az adatokat. A bázisállomásoktól a hálózati szervereken keresztül jutnak el az adatok az alkalmazásszerverekig. A LoRaWAN-technológia kétszintű titkosítást biztosít a rendszernek, egyrészt a végponttól AES[20] 128-cal titkosított adatfolyamon jut el az információ a hálózati szerverekig, azonban, hogy a hálózati szolgáltatásokat biztosítók ne lássanak bele a kommunikációba, a végpont-alkalmazás szerverkapcsolat is kaphat egy AES-128-as titkosítást [13], [14] (lásd 1. ábra).

A LoRaWAN-technológia kétirányú kommunikációt biztosít végpont és átjáró között. Az „A" osztályú eszközök vételi időablakai csak rövid időre vannak nyitva. Ehhez képest a „B" osztályú eszközök extra vételi időablakokat nyitnak meg a vételi periódusokban. A „C" osztályú eszközök az adásidejüket leszámítva szinte folyamatosan

[18] Signal-Noise Ratio – jel-zaj viszony.
[19] Transmission Control Protocol/Internet Protocol – átviteli vezérlő protokoll/internetprotokoll.
[20] Advanced Encryption Standard – továbbfejlesztett titkosítási szabvány.

vételen vannak, így minimálisra csökkentve a rendszer késleltetését, azonban ezzel energiafelhasználásuk lényegesen magasabb az „A" osztályú eszközökénél.

A katonai alkalmazás korlátai

A katonai felhasználás szempontjából a LoRaWAN számos kedvező tulajdonsága ellenére csak bizonyos korlátozásokkal alkalmazható.

Az első kihívás a bázisállomás-végpont klasszikus csillagtopológiájú elrendezéséből adódhat, ahol egy bázisállomáshoz kapcsolódhat több száz vagy akár ezer végpont is. Ez esetben a kritikus csomópontok működésének akadályozásával (akár pusztításával) darabjaira eshet szét a hálózat. Ez a kockázat részben kompenzálható, amennyiben a bázisállomások lefedettségi területét úgy alakítjuk ki, hogy egy végpont akár több bázisállomáshoz is képes legyen kapcsolódni. Ezt a multicsomópontú csillagtopológiás kialakítást is szemlélteti az 1. ábra.

Megítélésem szerint a másik fő kihívást az ISM-sávú frekvenciahasználat jelenti. Amint azt az afganisztáni példák is mutatták [16], a 868–869 MHz-es sávban működő például egyszerű kapu-távirányítón alapuló rádióvezérelt improvizált robbanóeszközök (RC-IED[21]), komoly biztonsági problémát jelentettek a szövetséges erőknek. Az erők megóvása érdekében a szövetséges csapatok aktív zavaró-berendezéseket (jammereket) helyeztek el többek között a járművekben, vagy háti hordozható verzióban a gyalogos kisalegységeknél. A rádiófrekvenciás erőforrások tervezése során figyelembe kell tehát venni, hogy a jelzett frekvenciasávot akár az ellenséges akár a szövetséges csapatok is alkalmazhatják, illetve zavarhatják. Az adott frekvencia ellenség általi felhasználása adott esetben nagyobb fenyegetettséget jelenthet, mint amennyi előnnyel járnak a szenzorhálózatokból nyert adatok, így egy felelős parancsnok e sáv elektronikai úton történő korlátozását rendeli el [17: 233.]. Bár korábban említettem a LoRaWAN-technológia kimagasló zavartűrő-képességét, adott alkalmazási körülmények között (például távolság- és terepviszonyok) mindenképpen mérési eredményekkel kell róla meggyőződnünk, hogy például az üzemi sávban működő aktív zavaró-berendezés, milyen mértékben korlátozza a LoRaWAN-eszközök kommunikációját, illetve a közeli térben való üzemeltetés milyen EMC[22]-problémákat okozhat. Ugyanakkor annak érdekében, hogy mégis igénybe lehessen venni egy ilyen rendszer által biztosított, előnyös tulajdonságokkal rendelkező szolgáltatásokat, egy praktikus megoldás lehet, ha a LoRaWAN működési frekvenciatartományt, olyan sávra is kiterjesztjük (vagy áthelyezzük), amelyet a későbbiekben nem szükséges korlátoznunk. (Természetesen különböző adaptív rádiófrekvenciás megoldásokkal lehetőség lenne olyan rendszerek kialakítására is, amelyek rugalmasan, autonóm módon képesek alkalmazkodni akár egy folyamatosan változó elektromágneses környezetben is, ugyanakkor ezek a megoldások lényegesen bonyolultabb hardver- és szoftvertechnikákat igényelnek, amelyek integrációja nagyságrendekkel növelné meg a fajlagos költségeket.)

[21] Radio Controlled Improvised Explosive Device.
[22] Electromagnetic Compatibility – Elektromágneses Kompatibilitás.

Kitekintésként megjegyezném, hogy a bevezetőben említett NB-IoT-technológiánál is fennáll a fenti sávhasználati korlát, mert az a mobilhálózati frekvenciákon működik, amelyet az afganisztáni példából láthatóan [16] is szintén előszeretettel alkalmazott a szembenálló fél. Így az említett kihívás várhatóan az LPWAN-technológiák döntő többségét érintheti. Azonban mivel az NB-IoT-technológia frekvenciaallokációjának megváltoztatása lényegesen nagyobb problémát jelentene (hiszen itt pont a mobilhálózatok által biztosított infrastruktúrán van a fókusz), ez egy újabb érvet jelenthet egy módosított LoRaWAN-technológia katonai alkalmazása mellett az alacsony energiaigényű szenzorhálózatok kommunikációs vonalainak biztosítása területén.

Bár elsőre merésznek tűnhet a frekvenciaallokáció megváltoztatásának gondolata, szeretnék kiemelni egy honi innovációt, amelyet a Bonn Hungary Elektronikai Kft. – Óbudai Egyetem – Budapesti Műszaki Egyetem közösen valósított meg [18]. A kutatás során Chirp-modulációs csatornákat alakítottak ki drónok vezérlésére sávszélesség-takarékossági szempontok figyelembevétele mellett. A megvalósult fejlesztés végeredményének kedvező tulajdonságai alapján kijelenthető, hogy a hazai ipar is képes akár a LoRaWAN-technológián alapuló, továbbfejlesztett katonai szenzorhálózati célú kommunikációs megoldások fejlesztésére, előállítására.

Felmerülhet a kérdés, hogy a kétszintű AES-128-as titkosítással védett szenzoradatok kielégítik-e a katonai alkalmazás követelményeit? Megítélésem szerint a szenzorhálózatok egyes nodejai által továbbított adatokhoz való hozzáférés – azok jellege miatt – önmagában nem sok információt hordoz, míg a teljes forgalom (százas–ezres nagyságrendű alacsony sugárzási intenzitású forgalmi csatorna) felderítése és ellenőrzése a rádióspektrumban aránytalanul nagy erőfeszítést, illetve erőforrásokat igényelne, ilyen szempontból ez a titkosítási eljárás megfelelő szintű védelmet jelenthet. Lényegesen magasabb kockázatot jelent az alkalmazásszerveren tárolt, feldolgozott információkhoz való hozzáférés lehetősége, így annak támadása elleni védelemre nagyobb hangsúlyt kell fektetni. A nagyobb problémát megítélésem szerint nem a lehallgatás, hanem a LoRa-csatornák zavarása/elnyomása jelentheti, amely esetén visszatérünk a frekvenciaallokáció problémaköréhez, amivel korábban már foglalkoztam.

A katonai felhasználás lehetőségei

A LoRaWAN-technológia valós műveleti körülmények között történő alkalmazása előtt szükséges megvizsgálni az esetleges ellenséges elektronikai hadviselési tevékenységek által jelentett kockázatokat, és ennek függvényében dönteni, hogy milyen struktúrában, műszaki specifikációban alkalmazzuk a technológiát (például az előzőkben említett allokáció). A LoRaWAN általánosságban felhasználható WAN – MAN[23] kiterjedésű szenzorhálózatok rádiófrekvenciás átviteli útjaként. Ilyenek lehetnek például a határzárak vagy demilitarizált övezetek elektronikai védelmi rendszerei, de különböző objektum- vagy táborfelügyeleti, illetve védelmi megoldások esetén is lehet létjogosultsága a technológia alkalmazásának. Adott területen egy rendszeren belül

[23] Metropolitan Area Network – Nagyvárosi Kiterjedésű Hálózat.

akár többféle szenzort (például nyitásérzékelőket, szakadásjelzőket, infrakapukat) is köthetünk egy LoRaWAN-végpontra ezzel optimalizálva a hálózati erőforrásokat, de a feladat függvényében a technológia lehetőséget biztosít lényegesen komplexebb, többszintű, és/vagy redundáns megoldások kialakítására is.

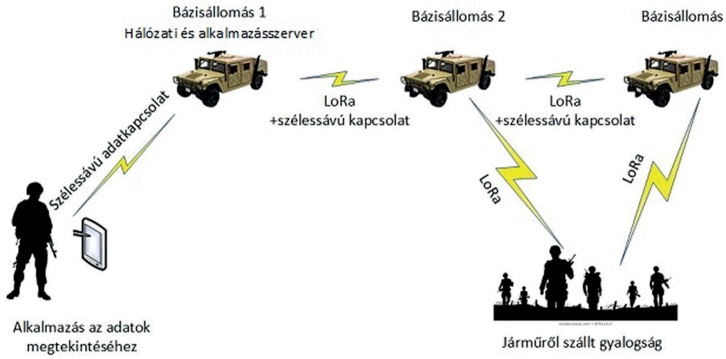
További lehetőségként jelentkezik a katonai objektumok, laktanyák, repülőterek, adótornyok stb. IoT-eszközei kommunikációs igényeinek kiszolgálása, akár fő-, akár tartalék adatátviteli útvonalként. Ilyen szenzorhálózati megoldások lehetnek például különböző infrastrukturális (épületgépészeti, villamos, hulladékkezelési) rendszerek visszajelzései, vezérlése, illetve elektronikai vagyonvédelmi jelzőeszközök, riasztási rendszerek átviteli vonalai. A robosztus hálózatszervezés támogatása érdekében lehetőség nyílik a korábbi elterjedten használt vezetékes és GSM-átviteli eljárásokat (amennyiben szükséges) kiegészíteni, kritikus erőforrások esetén NB-IoT, ZigBee, LoRaWAN stb. megoldásokkal tartalékútvonalakat kiépíteni.

A LoRaWAN felhasználási trendjeit napjainkban vizsgálva [19] azt tapasztalhatjuk, hogy megjelentek a geolokális pozíció megosztását célzó felhasználások, amelyekben a GNSS[24]-vevők által előállított pozícióadatokat LoRaWAN-hálózatokon keresztül osztják meg az alkalmazásszerverekkel. A vonatkozó NATO-ajánlások [20] értelmében a helyzetismeret információk továbbításának földi eszközre telepített terminál esetén 5 percenként, vagy 800 méterenként kell megtörténnie, míg légi járművek esetén – alapvetően a lényegesen nagyobb sebesség miatt – percenként, vagy 2300 méterenként kell frissülniük az információknak. Ezeknek a követelményeknek a LoRaWAN műszaki specifikációja és tulajdonságai alapján képes megfelelni. Ugyanakkor azt is szükséges megjegyezni, hogy a rendszer által kicsatolt adatok nem felelnek meg a vonatkozó NATO-szabályzók adatformátumának [21], [22], [23], [24], [25], amit az alkalmazásszerverek szintjén mindenképpen orvosolni szükséges, amennyiben egyéb hálózatok felé [26], [27] kívánjuk publikálni adatainkat.

E vezérfonal mentén egy újabb területen is megnyílik a felhasználás lehetősége, mégpedig a kisebb méretű és hatótávolságú drónok forgalmának egységes légtérbe történő biztonságos integrációja során. Egy LoRaWAN alapú megoldás képes lehet megfelelni akár egy nagyforgalmú városi légtér egységes forgalomirányítási rendszerében való alkalmazással szemben támasztott követelményeknek azáltal, hogy biztosítja a robosztus, megbízható kétirányú kommunikáció lehetőségét a pilóta nélküli légi járművek, és a légi irányítás rendszere között (például nyomkövetés, illetve biztonsági protokollok végrehajtása során a járművek vezérlésébe történő beavatkozás lehetősége) [28], [29], [30].

Az alábbi példában egy menetoszlop LoRaWAN-szenzorhálózattal történő támogatásának lehetőségét mutatjuk be, amelyet a 2. ábra szemléltet.

[24] Global Navigational Satellite System – Globális Műholdas Navigációs Rendszer.



2. ábra

Menetoszlop szenzorhálózati kommunikációjának támogatása LoRaWAN-technológiával

[a szerző szerkesztése]

Az ábrán a gép- és harcjárművek feltöltöttségi adatait, hadrafoghatóságát (például üzemanyagfogyás, lőszerfogyás, toronyfegyver csőhőmérséklet, keréknyomás stb.) szenzorhálózati úton monitorozzuk. Ennek egyik leghatékonyabb módja, ha a szükséges adatokat a járművek CAN[25]-buszrendszeréből nyerjük ki és csatoljuk a LoRa-végpontra. Az egyéb szenzorokat a szükség szerint csoportosíthatjuk, és így rendelhetjük őket egyéb LoRa-végpontokhoz. Modulrendszerben a deszantállomány is kaphat LoRaWAN-nodeokat annak érdekében, hogy geolokális adataikat a jármű elhagyását követően is nyomon lehessen követni. Ezeket az adatokat a LoRaWAN-átjárók gyűjtik össze. A bázisállomásokat a menetoszlopon belül célszerű járművekre telepíteni, és közöttük szélessávú vezeték nélküli rádiókapcsolatot [31] létesíteni, hogy képesek legyenek megosztani a hálózati szerver irányába a begyűjtött adatokat. Több átjáró telepítésével képesek vagyunk a korábban említett multicsomópontú csillagtopológiájú hálózat kialakítására is. Ezáltal, ha egyes átjárók kiesnek a hálózatból (például műszaki meghibásodás vagy lemarad a jármű) a hatókörön belül lévő szenzorok adatai továbbra is monitorozhatók. A hálózati és alkalmazásszervereket célszerű az oszlopparancsnok járművébe telepíteni. Innen a szerverről kliensalkalmazáson keresztül (például tableten) adatok kérhetők le (vezetékes vagy vezeték nélküli úton) a menetoszlopról.

Következtetések

Kutatásom során a LoRaWAN-technológia lehetséges katonai alkalmazásának lehetőségeit vizsgáltam. A publikációm bevezetésében felvázolt elemzés alapján néhány éven belül jelentős átalakulások várhatók a hálózatba kapcsolt információtechnológiai eszközeink területén. Az IoT-eszközök robbanásszerű terjedésével párhuzamosan, várhatóan megjelenik katonai felhasználásuk is. A LoRaWAN-technológia Layer 1–3 szintű

[25] Car Area Network – Jármű Kiterjedésű Hálózat.

működésének elemzését követően analizáltam a katonai alkalmazás szempontjából előnyös tulajdonságokat, úgymint a LoRa-moduláció, a kiemelkedő energetikai mérleg, a kedvező vételi jel-zaj viszony, valamint az önálló infrastruktúra lehetősége. Mindemellett feltártam a katonai felhasználás szempontjából lehetséges korlátokat is, úgymint a csillagpontos topológia sebezhetősége, vagy az ISM-sávú működés. A csillagtopológiából eredő kihívások az átjárók számának növelésével és a lefedettségi területek átlapolásával kompenzálhatók. Az ISM-sáv használatából eredő esetleges fenyegetettségek feltárása további kutatásokat indukál. Megítélésem szerint katonai szempontból a későbbiekben mindenképpen szükséges előzetes mérésekkel bizonyítani, hogy a LoRaWAN-technológia képes lehet-e vagy képessé tehető-e a szándékos zavarás káros hatása kockázatának csökkentésére a különböző ellenséges elektronikai hadviselési tevékenységek mellett történő megbízható üzemelésre, illetve megfelel-e a katonai alkalmazásból eredő kiberbiztonsági [32], [33] követelményeknek.

Mindezen elemzésen túlmenően beazonosítottam a LoRaWAN-technológia lehetséges katonai felhasználási területeit. A kutatás következő lépéseként javasolt a felállított modellek életképességének gyakorlati úton történő bizonyítása, mérések, kísérletek útján.

A kutatás az Emberi Erőforrások Minisztériuma ÚNKP-18-3-IV-NKE-27 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

The research is supported by the ÚNKP-18-3-IV-NKE-27 New National Excellence Program of the Ministry of Human Capacities.

Hivatkozások

[1] F. Jejdling, *Ericsson Mobility Report.* Svédország, Stockholm: Ericsson, június, 2018. [Online]. Elérhető: www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf (Letöltve: 2019. 05. 05.)

[2] IEEE, „802.15.1-2002 – *IEEE Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN – Specific Requirements – Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)*," June 14, 2002. [Online]. Elérhető: https://ieeexplore.ieee.org/document/1016473 (Letöltve: 2019. 05. 05.)

[3] Zigbee szövetség hivatalos honlapja, Zigbee Alliance, Elérhető: www.zigbee.org/ (Letöltve: 2019. 05. 05.)

[4] AZ IEEE WLAN munkacsoportjának hivatalos honlapja, Elérhető: www.ieee802.org/11/# (Letöltve: 2019. 05. 05.)

[5] K. Károly, „Szenzorhálózatok adatainak integrálási lehetőségei a perspektivikus erőkövetési rendszerekbe, különös tekintettel az egyéni egészségügyi adatokra," *Hadmérnök,* 14. évf. 1. sz. pp. 260–270, 2019.

[6] RFC 8376, S. Farell, „*Low-Power Wide Area Network (LPWAN) Overview*," IETF, Trinity College Dublin, p. 43, 2018. május, [Online]. Elérhető: https://tools.ietf.org/html/rfc8376 (Letöltve: 2019. 05. 05.)

[7] N. Hisham, N. Ibrahim, A. R. Ibrahim, I. Mat, A. N. Harun, és G. Witjaksono, „LoRaWAN in Climate Monitoring in Advance Precision Agriculture System," In: Proc. 2018 International Conference on Intelligent and Advanced System (ICIAS), Kuala Lumpur, Malajzia, 2018. DOI: https://doi.org/10.1109/ICIAS.2018.8540598
[8] R. Kirovné Rácz, „Magyarország hidrológiai eredetű katasztrófaveszélyeztettsége 2017. szeptembertől 2018. januárig az extrém mennyiségű és intenzitású csapadékhullás tükrében," *Hadtudományi Szemle,* 11. évf. 2. sz. pp. 252–267, 2018.
[9] R. Rácz, „The economical aspects of the climate change," *AARMS,* vol. 9, no. 1, pp. 153–157, 2010.
[10] B. Lóderer és R. Rácz, „A klímaváltozás és annak következményeire való felkészülés lehetséges jövőbeni aspektusai," *Hadtudományi Szemle,* 4. évf. 3. sz. pp. 91–98, 2011.
[11] R. Rácz, „The function of the system of national defence and disaster management in the disaster management structure," *AARMS,* vol. 10, no. 1, pp. 173–181, 2011.
[12] A Semtech cég hivatalos weboldala, Elérhető: www.semtech.com/lora (Letöltve: 2019. 05. 09.)
[13] T. Holman, B. Márkus, oktatóanyag, „LoRaWAN workshop," ChipCAD Kft. Budapest, február 21. 2019.
[14] T. Holman, „A LoRaWAN technológia hazai bevezetésének tapasztalatai," *Magyar Elektronika,* 35. évf. 9. sz. pp. 42–44, 2018.
[15] T. Holman, B. Márkus, és A. Gnandt, „LoRaWAN technológia 2019", in *Rádiótechnika Évkönyve 2019,* F. Békei szerk. Budapest: Rádióvilág Kft., pp. 168–171.
[16] A. Gulyás, „The Radio Controlled Improvised Explosive Device (RCIED) threat in Afghanistan," *AARMS,* vol. 12, no. 1, pp. 9–23, 2013.
[17] Zs. Haig, L. Kovács, L. Ványa, és S. Vass, *Elektronikai hadviselés.* Budapest: NKE-HHK, 2014, p. 271.
[18] Z. Belső, K. Elek, I. Koller, és Gy. Mikó, „Magyar fejlesztésű korszerű kommunikációs rendszer mobil alkalmazásokra," Elektronet.hu, 2012. 04.18, [Online]. Elérhető: www.elektro-net.hu/konstruktor/3594-magyar-fejlesztesu-korszeru-kommunikacios-rendszer-mobil-alkalmazasokra (Letöltve: 2019. 05. 08.)
[19] B. Márkus és T. Holman, „Építsünk együtt nyílt LoRaWAN hálózatot!", in: *Rádiótechnika Évkönyve 2017,* Budapest: Rádióvilág Kft., pp. 191–196.
[20] NATO STANAG 5500, "Concept of NATO Message Text Formatting System," (CONFORMETS) -ADATP-3 (A), 2. Nov. 2010.
[21] A. Gulyás, „Gondolatok az adatátviteli rendszerek fejlődéséről," *Seregszemle,* 15. évf. 2. sz. pp. 162–188, 2017.
[22] A. Gulyás, „Kognitív üzemmódok katonai alkalmazása," *Seregszemle,* 14. évf. 1. sz. pp. 59–75, 2016.
[23] A. Gulyás, „Szabványosított hullámforma azonosításra (1. rész)," *Seregszemle,* 16. évf. 1. sz. pp. 160–172, 2018.
[24] A. Gulyás, „Szabványosított hullámforma azonosításra (2. rész)," *Seregszemle,* 16. évf. 2. sz. pp. 146–154, 2018.
[25] A. Gulyás, „Szoftvervezérelt rádiók azonosító jelsorozatai," *Seregszemle,* 11. évf. 4. sz. pp. 56–81, 2013.

[26] Sz. Jobbágy, „A Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata," *Hadmérnök,* 12. évf. 3. sz. pp. 223–236, 2017.
[27] A. Gulyás, "Force Tracking System in SOF applications," *AARMS,* vol. 8, no. 4, pp. 601–617, 2009.
[28] A. Németh, „UAV-k alkalmazása a közfeladatok ellátása során I," *Hadmérnök,* 13. évf. 2. sz. pp. 37–60, 2018.
[29] A. Németh, „UAV-k alkalmazása a közfeladatok ellátása során II," *Hadmérnök,* 13. évf. 3. sz. pp. 68–86, 2018.
[30] B. Márkus, S. Jeszenszky, „Repülős LoRaWAN teszt Magyarországon," micromite.chipcad.org [Online]. Elérhető: http://micromite.chipcad.org/home/repuelos-lorawan-teszt-magyarorszagon (Letöltve: 2019. 05. 12.)
[31] A. Németh, A. Horváth, és A. Gulyás, „Ultra wideband data channels for special operations forces," *Hadmérnök,* vol. 8, no. 1. pp. 154–165, 2013.
[32] D. Dévai, "The U.S. Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace (Part 1)," *AARMS,* vol. 18, no. 1. pp. 39–57. 2019. DOI: https://doi.org/10.32565/aarms.2019.3 [Online]. Elérhető: https://folyoiratok.uni-nke.hu/document/nkeszolgaltato-uni-nke-hu/AARMS_2019_01_03_Dora-DeVAI1.pdf (Letöltve: 2019. 06. 23.)
[33] D. Dévai, "The U.S. Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace (Part 2)," *AARMS,* vol. 18, no. 1. pp. 59–77. 2019. DOI: https://doi.org/10.32565/aarms.2019.4 Elérhető: https://folyoiratok.uni-nke.hu/document/nkeszolgaltato-uni-nke-hu/AARMS_2019_01_03_Dora-DeVAI1.pdf (Letöltve: 2019. 06. 23.)

HADMÉRNÖK
VÉDELMI ELEKTRONIKA, INFORMATIKA, KOMMUNIKÁCIÓ

14. évfolyam (2019) 3. szám 113–128.
DOI: 10.32567/hm.2019.3.10

Nagyné Takács Veronika[1]

Hogyan írjunk informatikai biztonsági szabályzatot?

How to Write an IT Security Regulation?

A tanulmány a jogszabályi környezet áttekintésével, az előírások számbavételével és rendszerezésével, továbbá személyes tapasztalatok megosztásával kívánja segíteni azokat, akik munkájuk során informatikai biztonsági szabályzat előkészítését, megírását kapták feladatul, vagy személyes kíváncsiságból érdeklődnek a téma iránt.

Kulcsszavak: **információbiztonság, szabályozás, informatikai biztonsági szabályzat**

The study aims to help those who have been involved in the preparation and writing of the IT Security Regulation, or personally interested in it in their work, by reviewing the legal environment, listing and organising the regulations, and sharing personal experiences of the author.

Keywords: **information security, regulation, information security regulation**

Bevezetés

Bizonyára sokan emlékeznek Umberto Eco[2] *Hogyan írjunk szakdolgozatot?* című, Magyarországon 1992-ben megjelent könyvére [1], amelyben főiskolások, egyetemisták számára adott módszertani útmutatót életük első nagyobb lélegzetű tudományos munkájának megírásához.

Jelen tanulmány címe így nem titkoltan Ecótól ered, egyben utólagos köszönet az akkoriban jókor érkezett segítségért, és nagyon szerény tisztelgés a nagy tudású író emléke előtt, aki regényei, tanulmányai, publicisztikája mellett egy hasznos, ugyanakkor szórakoztató segédlet megírására is energiát fordított.

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: takacs.veronika2016@gmail.com, ORCID: https://orcid.org/0000-0002-4868-5622

[2] Umberto Eco (1932–2016) olasz író, irodalomkritikus és filozófus. *Hogyan írjunk szakdolgozatot?* című esszéjét magyarul a Gondolat Könyvkiadó adta ki 1992-ben, Budapesten, Klukon Beatrix fordításában.

Az *Informatikai biztonsági szabályzat* (a továbbiakban: IBSZ) megírásához készítendő módszertani útmutató szükségessége már saját tapasztalatokon alapuló felismerés. A cikk előzménye közel tízévnyi IBSZ-írási tapasztalat (eredmény és kudarc) és többéves tudományos kutatás, célja pedig az előzőkből származó felismerések megosztása annak érdekében, hogy mások számára az IBSZ megírásához szükséges előkészületi időszak, illetve maga a kidolgozás folyamata lerövidülhessen. A cikk – természetesen – elfogult nézőpontból közelít a kérdéshez: a szerző hisz abban, hogy a szabályozás nem felesleges adminisztrációs teher, hanem egy adott szervezet működését és az ott dolgozók munkavégzését támogató tevékenység, amit – mint minden mást – érdemes jól végezni, így eredményeit is lehet hasznosítani.

A cikk az alábbi kérdésekre adható/adandó válaszok áttekintésével és néhány gyakorlati tanáccsal – nem kizárólagosságra törekedve és nem konkrét, *egy az egyben* használható mintadokumentum átnyújtásával – kívánja segíteni az IBSZ-írás iránt önszorgalomból vagy kötelezettség alapján érdeklődőket:

- Miért van szükség az IBSZ-re?
- Milyen szabályozási környezetben szükséges elhelyezni az IBSZ-t?
- Mit tartalmazzon és hogyan az IBSZ?

Az IBSZ és szükségessége

Az IBSZ az infokommunikációs eszközöket tevékenysége során alkalmazó (azaz ma már szinte minden) szervezet egyik szabályozási alapdokumentuma. Tartalmazza – tartalmaznia kell – mindazon előírásokat, amelyek az adott szervezetnél az infokommunikációs eszközök rendeltetésszerű és biztonságos használatához szükségesek, ezért kötelezően alkalmazandók.

Az IBSZ megírásának szükségességét a szakmai konszenzust tükröző szabványok, ajánlások évtizedek óta rögzítik és hangsúlyozzák. A nemzetközi példákat követve a hazai Informatikai Tárcaközi Bizottság (ITB)[3] 8. és 12. számú ajánlásai 1994-ben és 1996-ban, majd a Közigazgatási Informatikai Bizottság (KIB)[4] 25. számú ajánlása 2008-ban alapvető dokumentumnak tekintették az IBSZ-t [2: 115.], [3: 29.], [4: 49.]. Az információbiztonsági szabványok fejlődéstörténetének bemutatása meghaladná

[3] A 3296/1991. (VII. 5.) Korm. határozat alapján a Miniszterelnöki Hivatal (MeH) közigazgatási államtitkárának irányításával létrehozott, a MeH-en belül működő Informatikai Koordinációs Iroda tevékenységére támaszkodó ITB a kormányzati informatikai (elsősorban fejlesztési) feladatok összehangolásáért volt felelős. Feladatai közé tartozott – az 1066/1999. (VI. 11.) Korm. határozat szerint – a kormányzati informatikai fejlesztések stratégiai tervezésében való közreműködés, a kiemelkedő jelentőségű kormányzati informatikai részterületek szakmai koncepcióinak kidolgozása és megvalósulásuk figyelemmel kísérése, kormányzati informatikai ajánlások kidolgozása, több tárcát érintő informatikai rendszerek létrehozásával, korszerűsítésével kapcsolatos koordináció végrehajtása.

[4] Az 1026/2007. (IV. 11.) Korm. határozattal – három korábbi tárcaközi bizottságból – létrehozott KIB koordinációs fórumként támogatta a stratégiai szintű közigazgatási informatikai programok tervezését, végrehajtását, az infokommunikációs technológiák, eszközök közigazgatáson belüli terjesztését, szabályozásokat kezdeményezett és ajánlásokat készített az informatika közigazgatáson belüli alkalmazásának támogatásához. A KIB elnöke a közigazgatási informatikáért felelős kormánybiztos volt, tagjai a központi államigazgatási és az önkormányzati igazgatási szervek delegáltjai, valamint a közigazgatási informatikai fejlesztésekben érintett szervezetek képviselői. A KIB munkáját albizottságok segítették.

jelen munka kereteit, a témában lásd például Muha Lajos és Krasznay Csaba Nemzeti Közszolgálati Egyetemen készült tananyagát [5: 26–36.].

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) megjelenését követően a törvény hatálya alá tartozó szervezetek vezetői számára „a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályok" rögzítése és az informatikai biztonsági szabályzat kiadása jogszabály alapján előírt kötelezettséggé vált [6]. A jogalkotó maga gondoskodott arról, hogy az IBSZ kiadása a vezető megbízásából eljáró, neki felelős személy feladatkörébe kerüljön; a szabályzat kiadásának előkészítését az elektronikus információs rendszer védelméért felelős személy feladatává tette [6].

Az Ibtv. hatálya alá tartozó szervezetek IBSZ-eit az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét ellátó, a kormány által kijelölt hatóság, a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) nyilvántartja és kezeli [6].

Az IBSZ helye a szabályozási rendszerben

A szabályozási tevékenység céljáról, tartalmáról, módszeréről (egyes szkeptikusok szerint: értelméről) való gondolkodás meghaladná jelen munka kereteit, így a szabályozás – általában vett és tudomásul vett – szükségességét a szerző alapvetésként kezeli. Kitekintésként mindössze annyi megjegyzést érdemes tenni, hogy nem az információvédelem az egyetlen terület, ahol a szabályozás jogszabályban foglalt kötelezettség. *A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről* szóló 1995. évi LXVI. törvény (Ltv.) a hatályba lépésének napjától (1995. 06. 30.) előírta a közfeladatot ellátó szervek számára iratkezelési szabályzat kiadását [7], *a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról* szóló 1992. évi LXIII. törvény (Avtv.) 2004. január 1-jétől a belső adatvédelmi felelős feladataként határozta meg belső adatvédelmi és adatbiztonsági szabályzat készítését [8] – az előírás az Avtv.-t hatályon kívül helyező *az információs önrendelkezési jogról és az információszabadságról* szóló 2011. évi CXII. törvényben (Info tv.) is szerepel [9], *a számvitelről* szóló 2000. évi C. törvény (Számv. tv.) szintén hatályba lépésétől (2000. 09. 21.) rögzíti kötelezettségként a gazdálkodók esetében, hogy a számviteli politika keretében el kell készíteni az eszközök és a források leltárkészítési és leltározási szabályzatát, az eszközök és a források értékelési szabályzatát, az önköltségszámítás rendjére vonatkozó belső szabályzatot, a pénzkezelési szabályzatot [10]. A felsorolás nem teljes, ez nem is cél, inkább bevezető a további megállapításokhoz.

Az IBSZ tehát jogszabály által előírt szabályzat. *A szabályzat*, amennyiben az információvédelem általános tárgyköréről van szó. Az IBSZ további – információvédelmi tárgyú – szabályozóeszközök kiindulópontja is lehet (tehát *alapszabályzat*). De az IBSZ csak *egy szabályzat*, amennyiben egy szervezet jogszerű működésének szabályozásáról van szó.

Fentiekből következik, hogy fogalomhasználatában, tartalmában, szerkezetében illeszkednie kell a szervezet egyéb belső szabályozóeszközeihez, és lehetővé kell tennie, elő kell segítenie további szabályozóeszközök kidolgozását.

Ezért amikor az IBSZ megírásáról vagy újraírásáról születik döntés, alapul lehet venni a szervezet korábbi, akár az éppen hatályos IBSZ-ét vagy más szervezetek IBSZ-eit (az internet e tekintetben számos forrással szolgálhat); a lényeg az aktuális szabályozási rendszer figyelembevétele és a kidolgozandó dokumentum ehhez illesztése.

Egy szervezet szabályozási rendszerét részben a jogszabályok, de – a részletek tekintetében – leginkább saját felépítése és tevékenysége, valamint hagyományai határozzák meg. *A jogalkotásról* szóló 2010. évi CXXX. törvény (Jat.) szerint az arra jogosultak *közjogi szervezetszabályozó eszközök*ben *(normatív határozat* és a *normatív utasítás)* rögzíthetik a szervezetre és a működésre, valamint a tevékenységre vonatkozó előírásokat [11]. Az egyes – már idézett – jogszabályok a szervezet vezetője által kiadott *szabályzatok*ra hivatkoznak. A belső szabályozóeszközök körébe az egyes szervezeteknél leggyakrabban a *szabályzatok*, az *utasítások*, az *eljárásrendek*, a *munkautasítások* tartoznak, ezek pontos fogalma, hatálya, tartalma azonban szervezetenként eltérő. Ugyancsak jelentős eltérést mutat a szabályozóeszközök hierarchiája, egymáshoz való viszonya. Egyes szervezeteknél kizárólag a szervezet első számú vezetőjének van szabályozási joga, azaz ő adhat ki szabályozóeszközt. Más szervezeteknél a szabályozási jog különböző vezetői szintekre lett telepítve.

Az Ibtv. végrehajtási rendelete, *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* szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban: 41/2015. BM rendelet) 4. melléklete – a *szabályzatok* mellett – *eljárásrendek* kialakítását és rögzítését írja elő, és elvárásként rögzíti azt is, hogy az eljárásrendeket megsértő személyekkel szemben szankciót kell alkalmazni [12]. A 41/2015. BM rendelet 2. melléklete *munkautasítást*, *belső rendelkezést*, *szabályozást, vagy más erre a célra szolgáló* dokumentumot (*együtt: szabályzat*ot) említ [12].

A szervezeti szabályozási rendszerbe illesztés követelménye a fentieken túl azt is jelenti, hogy ha egy szervezet a szabályozás kidolgozására külső erőforrást vesz igénybe – számos vállalkozás van a piacon, amely IBSZ és egyéb szabályozóeszközök jogszabály- vagy szabványkonform elkészítését vállalja –, ügyelni kell arra, hogy a külső szakértők által elkészített (kellően absztrahált, így több szervezet felé is kiajánlható) dokumentumminta szervezetre adaptálása, testreszabása kellő mértékben megtörténjen. Ha erre a testreszabásra nem kerül sor, az IBSZ külső dokumentum marad, ennek minden következményével. Ha elmarad, későbbre halasztódik a szervezeti szabályozási rendszerbe illesztés, a szervezettől idegen fogalomhasználat, tartalom és szerkezet esetén nehezebbé válik az IBSZ értelmezése és alkalmazása, és természetesen nehezebbé válik az IBSZ alapján elkészítendő további szabályozóeszközök kidolgozása is.

Az IBSZ kiadásával az információvédelmi szabályozás jogszabályban elvárt feladata még korántsem teljesül. A 41/2015. BM rendelet 4. mellékletének 3. alcíme szerinti *Védelmi intézkedés katalógus*ban meghatározott szabályozási kötelezettségeket az 1. táblázat 1. és 2. oszlopa foglalja össze.

1. táblázat

Szabályozási kötelezettségek [a szerző saját szerkesztése]

41/2015. Korm. rendeletben nevesített vagy hivatkozott szabályozóeszköz		Az IBSZ tartalmára vonatkozó előírás
szabályzat	***eljárásrend***	
Informatikai biztonsági szabályzat (IBSZ) *3.1.1.1.*[5]		
Kockázatelemzési és kockázatkezelési szabályzat *3.1.2.1.1.1.*	Kockázatelemzési és kockázatkezelési eljárásrend *3.1.2.1.*	kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz) *3.1.1.1.3.1.*
általános beszerzési szabályzat[6] *3.1.3.1.1.1.*	Beszerzési eljárásrend *3.1.3.1.*	az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás beszerzés (ha az érintett szervezet ilyet végez vagy végezhet) *3.1.1.1.3.3.*
Üzletmenet-folytonosságra vonatkozó szabályzat *3.1.4.1.1.1.*	Üzletmenet-folytonosságra vonatkozó eljárásrend *3.1.4.1.*	üzlet-, ügy- vagy üzemmenet-folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása stb.) *3.1.1.1.3.9.*
	Biztonsági eseménykezelési eljárásrend *3.1.5.1.*	biztonsági helyzet- és eseményértékelés eljárási rendje *3.1.1.1.3.2.*, a biztonsági események – ideértve az adatok sérülését is – bekövetkeztekor követendő eljárás, ideértve a helyreállítást *3.1.1.1.3.15.*
	Személybiztonsági eljárásrend *3.1.6.1.* *belső szabályozás*ban rögzített eljárás a jogviszony megszűnésekor *3.1.6.4.* *belső eljárási rend* szerint fegyelmi eljárás kezdeményezése *3.1.6.7.1.1.*	az emberi erőforrásokban rejlő veszélyek megakadályozása (például személyzeti felvételi és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése stb.) *3.1.1.1.3.6.*

[5] A könnyebb azonosíthatóság érdekében minden esetben feltüntetésre kerül az előírás *Védelmi intézkedési katalógus* szerinti sorszáma.

[6] Dőlt betűvel vannak jelezve a nem konkrét (néven nem nevezett) szabályozóeszközökre történő utalások (amelyek jellemzően egy-egy tevékenység szabályozásának előírásakor jelennek meg).

41/2015. Korm. rendeletben nevesített vagy hivatkozott szabályozóeszköz		Az IBSZ tartalmára vonatkozó előírás
szabályzat	***eljárásrend***	
*belső szabályzat*ban meghatározott, interneten megvalósuló tevékenység tiltása (például chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták stb.) *3.1.6.9.1.2*		
Képzési szabályzat *3.1.7.2.1.1.*	Képzési eljárásrend *3.1.7.2.*	az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében *3.1.1.1.3.7.*
(*elektronikus információbiztonsági vagy egyéb szabályzat* részét képező) Fizikai védelmi szabályzat *3.2.1.2.1.1*	Fizikai védelmi eljárásrend *3.2.1.2.*	fizikai és környezeti védelem szabályai, jellemzői *3.1.1.1.3.5.*
Biztonságtervezési szabályzat *3.2.2.1.*		biztonsággal kapcsolatos tervezés (például beszerzés, fejlesztés, eljárásrendek kialakítása) *3.1.1.1.3.4.*
	az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési folyamatok kialakítása, dokumentálása és kihirdetése *3.3.1.1.1.*	
	az elektronikus információs rendszer más elektronikus információs rendszerhez kapcsolódásának *szabályozás*a és belső engedélyhez kötése *3.3.1.3.1.1.*	szabályrendszer felállítása és alkalmazása a külső elektronikus információs rendszerekhez való kapcsolódáshoz *3.3.1.3.3.*
Biztonságértékelési szabályzat *3.3.4.1.1.1.*	Biztonságelemzési eljárásrend / Biztonságértékelési eljárásrend *3.3.4.1.*	
	elektronikus információs rendszer tesztelésével, képzésével és felügyeletével kapcsolatos eljárások megfogalmazása, dokumentálása és kihirdetése *3.3.5.1.1.*	

41/2015. Korm. rendeletben nevesített vagy hivatkozott szabályozóeszköz		Az IBSZ tartalmára vonatkozó előírás
szabályzat	*eljárásrend*	
Konfigurációkezelési szabályzat *3.3.6.1.1.1.*	Konfigurációkezelési eljárásrend *3.3.6.1.*	
a szoftver használatra meghatározott *szabályzatok* *3.3.6.7.2.2.*		
szoftvertelepítésre vonatkozó *szabályok* érvényesítése 3.3.6.11.1.2.		
Rendszer karbantartási kezelési szabályzat *3.3.7.1.1.1.*	Rendszer karbantartási eljárásrend *3.3.7.1.* *folyamat* kialakítása a karbantartók munkavégzési engedélyének kezelésére *3.2.1.19.1.1.*	az elektronikus információs rendszerek karbantartásának rendje *3.1.1.1.3.10.*
Adathordozókra vonatkozó védelmi szabályzat *3.3.8.1.1.1.*	Adathordozók védelmére vonatkozó eljárásrend *3.3.8.1.*	az adathordozók fizikai és logikai védelmének szabályozása *3.1.1.1.3.11.*
Azonosítási és hitelesítési szabályzat *3.3.9.1.1.1.*	Azonosítási és hitelesítési eljárásrend *3.3.9.1.*	az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése *3.1.1.1.3.12.*
Hozzáférés ellenőrzési szabályzat *3.3.10.1.1.1.*	Hozzáférés ellenőrzési eljárásrend *3.3.10.1.*	
minden engedélyezett távoli hozzáféréstípusra a felhasználásra vonatkozó korlátozások, a konfigurálási vagy a kapcsolódási követelmények és a megvalósítási útmutatók kidolgozása ás dokumentálása *3.3.10.13.1.1.*		
*belső szabályozás*ban felhasználási korlátozások, konfigurálásra és kapcsolódásra vonatkozó követelmények, valamint technikai útmutató kiadása a vezeték nélküli technológiák kapcsán *3.3.10.14.1.1.*		
*belső szabályozás*ban felhasználási korlátozások, konfigurálásra és kapcsolódásra vonatkozó követelmények, valamint technikai útmutató kiadása az ellenőrzött mobil eszközökre *3.3.10.15.1.1.*		

41/2015. Korm. rendeletben nevesített vagy hivatkozott szabályozóeszköz		Az IBSZ tartalmára vonatkozó előírás
szabályzat	***eljárásrend***	
(az IBSZ részét képező) Rendszer- és információsértetlenségre vonatkozó szabályzat *3.3.11.2.1.1.*	Rendszer- és információsértetlenségre vonatkozó eljárásrend *3.3.11.2.*	
	az elektronikus információs rendszer hibáinak azonosítása, *belső eljárásrend* alapján jelentése és kijavítása vagy kijavíttatása *3.3.11.3.1.1.*	
Naplózásra és elszámoltathatóságra vonatkozó szabályzat *3.3.12.1.1.1.*	Naplózási eljárásrend *3.3.12.1.*	ha az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása *3.1.1.1.3.13.*
Rendszer- és kommunikációvédelmi szabályzat *3.3.13.1.1.1.*	Rendszer- és kommunikációvédelmi eljárásrend *3.3.13.1.*	
		az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (ha az érintett szervezetnél ez értelmezhető) *3.1.1.1.3.8.*
		az adatok mentésének, archiválásának rendje *3.1.1.1.3.14.*
		az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét szabályozó (karbantartók, magán- vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az elektronikus információbiztonságot érintő, szerződéskötés során érvényesítendő követelmények *3.1.1.1.3.16.*

Az IBSZ-en túl konkrét megnevezéssel 14 szabályzat szerepel, ugyanezen címekkel – egy kivétellel – eljárásrend készítését is előírja a jogszabály, további 3 esetben konkrét

megnevezéssel szerepel elkészítendő eljárásrend. Az előzőkön kívül 7(8) esetben[7] szabályzat/szabályozás kialakítását, 5 esetben eljárás, folyamat kialakítását és dokumentálását írja elő a *Védelmi intézkedési katalógus*.[8] Ebből következően az IBSZ mellett a szabályozási rendszer részeit kell, hogy képezzék az említett „tematikus" szabályzatok, eljárásrendek is.[9]

Az *1. táblázat* rögzíti az IBSZ előírt tartalmával (lásd következő fejezet) történt összevetés eredményét is (3. oszlop). Eszerint az IBSZ-ben 17 elektronikus információs rendszerbiztonsággal kapcsolatos területet, tevékenységet kell szabályozni, ezekből 14 esetében szabályzat vagy eljárásrend kiadása is kötelező.

Az IBSZ tartalma

Az Ibtv. és a 41/2015. BM rendelet az IBSZ tartalmára vonatkozó (konkrét és kevésbé konkrét) előírásokat is tartalmaz.

Az Ibtv. alapján az IBSZ-ben a szervezet, valamint – a szervezeten belüli eltérések esetén – a szervezeti egységek biztonsági szintbe sorolásának eredményét és az elektronikus információs rendszerek biztonsági osztályba sorolását rögzíteni kell [6]. A *Védelmi intézkedés katalógus* e tekintetben némileg eltérően fogalmaz: az IBSZ-nek tartalmaznia kell a szervezet elvárt biztonsági szintjét és egyes elektronikus információs rendszereinek elvárt biztonsági osztályát [12]. A két rendelkezés összeolvasásának eredménye: a tényleges és az elvárt biztonsági szintet és osztályokat is rögzíteni kell az IBSZ-ben.

A *Védelmi intézkedési katalógus*ban az adminisztratív intézkedések között első helyen az IBSZ tartalmára vonatkozó előírások szerepelnek. Eszerint az IBSZ-ben rögzíteni kell:

1. a célokat, a szabályzat tárgyi és személyi (a szervezet jellegétől függően területi) hatályát,
2. az elektronikus információbiztonsággal kapcsolatos szerepköröket, a szerepkörhöz rendelt tevékenységet és a tevékenységhez kapcsolódó felelősséget, valamint az információbiztonság szervezetrendszerének belső együttműködését,
3. az elektronikus információs rendszerbiztonsággal kapcsolatos alábbi területekre, tevékenységekre vonatkozó előírásokat:
   a) kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz),
   b) biztonsági helyzet- és eseményértékelés eljárási rendje,

[7] A 3.3.10.13.1.1., 3.3.10.14.1.1., 3.3.10.15.1.1. pontban előírtak tartalmukat tekintve eltérők, logikailag és szerkezetileg szinte teljesen azonosak, azonban az első esetben nem szerepel a *belső szabályozásban* történő kiadásra utalás.

[8] A tanulmánynak nem célja a jogszabályokban foglalt szabályozási követelményrendszer értékelése; az előírások tényszerű ismertetésére szorítkozik. Annyit azonban szükséges megjegyezni, hogy a szabályozási koncepció, a fogalomhasználat és szerkesztésmód egyszerűsítése, pontosítása, következetesebbé tétele, illetve a szabályzat – eljárásrend fogalmi tisztázása megkönnyítené az alkalmazást.

[9] A nevesített szabályozóeszközökön kívül a *Védelmi intézkedési katalógus* számos további dokumentum előállítását, kezelését és nyilvántartások felállítását is előírja (például üzletmenet-folytonossági terv – 3.1.4.2.1.1. pont, információbiztonsági architektúraleírás – 3.3.2.5. pont, rendszerbiztonsági terv – 3.3.2.2. pont, adminisztrátori dokumentáció – 3.1.3.4.1.1. pont, karbantartási nyilvántartás – 3.3.7.2.1.6. pont stb.). Tételes felsorolásukat a szerző mellőzi, tekintettel arra, hogy bár a kidolgozásukra, felállításukra vonatkozó kötelezettségeket célszerű a szabályozóeszközökben rögzíteni, ezek nem szabályozóeszközök.

c) az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás-beszerzés (ha az érintett szervezet ilyet végez vagy végezhet),
d) biztonsággal kapcsolatos tervezés (például beszerzés, fejlesztés, eljárásrendek kialakítása),
e) fizikai és környezeti védelem szabályai, jellemzői,
f) az emberi erőforrásokban rejlő veszélyek megakadályozása (például személyzeti felvételi és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése stb.),
g) az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében,
h) az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (ha az érintett szervezetnél ez értelmezhető),
i) üzlet-, ügy- vagy üzemmenet-folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása stb.),
j) az elektronikus információs rendszerek karbantartásának rendje,
k) az adathordozók fizikai és logikai védelmének szabályozása,
l) az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése,
m) ha az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása,
n) az adatok mentésének, archiválásának rendje,
o) a biztonsági események – ideértve az adatok sérülését is – bekövetkeztekor követendő eljárás, ideértve a helyreállítást,
p) az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét szabályozó (karbantartók, magán- vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az elektronikus információbiztonságot érintő, szerződéskötés során érvényesítendő követelmények [12],
q) szabályrendszer felállítása és alkalmazása a külső elektronikus információs rendszerekhez való kapcsolódáshoz [12].[10]

A fenti felsorolás 1. pontjában foglaltak rögzítése szabályozási evidencia. A 3. pont az információbiztonsági szabályozás tárgyát rögzíti, ami szervezetenként értelemszerűen eltérő mélységű szabályozást igényel; a lényeg, hogy a felsoroltakból minden

[10] Ez a követelmény nem az IBSZ tartalmi elemeinek felsorolásánál, hanem a logikai védelmi intézkedések között szerepel.

elemre ki kell térni, hiszen az elvárás az információvédelmi tevékenységek teljes körének szabályozása. A *Védelmi intézkedési katalógus* komplexitását, a teljes szervezetre kiterjedő hatókörét – divatos szóval a holisztikus megközelítést – leginkább a fenti felsorolás 2. pontjában előírt kötelező tartalom kapcsán érdemes bemutatni. Az elektronikus információbiztonsággal kapcsolatos szerepkörök, feladatok és felelősségek meghatározása és telepítése a szervezet egészét érinti vertikális és horizontális szempontból is, ezek összefoglalását tartalmazza a 2. táblázat.

2. táblázat

Információbiztonságot érintő szerepkörök, feladatok, felelősségek [a szerző saját szerkesztése]

<table>
<tr><th>Általános</th><th>Informatikai szakmai</th><th>Információbiztonsági, szakmai</th><th>Funkcionális szakterületi</th></tr>
<tr><td>szervezet vezetője
Ibtv.-ben meghatározott feladatok, felelősségek</td><td>informatikai fejlesztési szakterület/szervezeti egység vezetői
speciális, tevékenységhez kötődő vezetői feladatok és felelősség</td><td>információbiztonsági szervezeti egység vezetője/elektronikus információs rendszer biztonságáért felelős személy (IBF)
Ibtv.-ben meghatározott feladatok, felelősségek</td><td>humánpolitikai és képzési szakterület vezetői és munkatársai
jogviszony létesítésével, megszűnésével kapcsolatos, illetve képzési feladatok</td></tr>
<tr><td>minden szervezeti egység vezetője
általános vezetői feladatok és felelősség, idézett jogszabályokban nincs részletezve (például utasítás adása, munka ellenőrzése stb.)</td><td>informatikai üzemeltetési szakterület/szervezeti egység vezetői
speciális, tevékenységhez kötődő vezetői feladatok és felelősség</td><td>információbiztonsági szervezeti egység munkatársai (esetenként privilegizált felhasználók)
IBF támogatása, közreműködés a feladatai ellátásában</td><td>személybiztonsági szakterület vezetői és munkatársai
speciális követelmények érvényesítése, például nemzetbiztonsági ellenőrzéssel, vagyonnyilatkozat-tétellel kapcsolatos ügyintézés stb.</td></tr>
<tr><td rowspan="3">adatgazda (szakmai területek vezetői; az Ibtv. alapján annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik)
az elektronikus információs rendszerek osztályba sorolásánál a szakmai értékelésért felelős (milyen adatokat kezel a rendszer, ezek értéke, meddig szükséges megőrzésük stb.)</td><td rowspan="2">munkatársak (jellemzően privilegizált felhasználók)
az infokommunikációs eszközök üzemeltetésével, fejlesztésével, használatával kapcsolatos jogok és kötelességek, felelősségek, tekintettel arra is, hogy jogosítványaik és így felelősségük is jellemzően meghaladják az átlagos felhasználóét</td><td rowspan="3"></td><td>objektumvédelmi szakterület vezetői és munkatársai
fizikai biztonsági feladatok és felelősségek</td></tr>
<tr><td>jogi szakterület vezetői és munkatársai
szerződésekben érvényesítendő információbiztonsági követelmények rögzítéséről gondoskodás</td></tr>
<tr><td>gazdasági szakterület vezetői és munkatársai
beszerzések, illetve eszköznyilvántartás során érvényesítendő információbiztonsági követelmények teljesítése</td></tr>
</table>

Általános	*Informatikai szakmai*	*Információbiztonsági, szakmai*	*Funkcionális szakterületi*
munkatársak (jellemzően felhasználók) *az infokommunikációs eszközök használatával kapcsolatos jogok és kötelességek, felelősségek*			**ügyvitelszervezési /iratkezelési szakterület vezetői és munkatársai** *iratkezelési, dokumentálási követelmények teljesítése*

Gyakorlati javaslatok

A szabályozási kötelezettségek elméleti áttekintése után következzék néhány megszívlelendő gyakorlati – már az IBSZ konkrét felépítésére, megszövegezésére vonatkozó – javaslat. Az alább megfogalmazottak a szerző IBSZ-írással és már elkészült IBSZ-ek olvasásával, értelmezésével és végrehajtásával, valamint az idézett jogszabályok szabályozásra vonatkozó előírásainak teljesítésével kapcsolatos, közigazgatási, közfeladatot ellátó szerveknél szerzett személyes tapasztalatain alapulnak.

1. Az IBSZ-ben legyen egy nagyon jó fogalomtár, aminek kiindulópontjai legyenek az Ibtv. értelmező rendelkezései, de az egyes fogalmak meghatározása, elkülönítése más fogalmaktól a szervezet egyéb szabályozóeszközeiben szereplő fogalmakra tekintettel történjen. Nem elég, ha a fogalmak meghatározását kimásoljuk jogszabályból, szabványból, internetes forrásból (e tekintetben a Wikipédia segítségül hívása – bár nagyon elterjedt – veszélyes: lehet, hogy a szerző – mindössze egy ember – elfogult vagy akaratlanul pontatlan álláspontját, nem ellenőrzött tudását, ismereteit tükrözi); a fogalmakat értelmezni is kell.

   Klasszikus példa az *esemény, biztonsági esemény* fogalomköre. Az *esemény* szó az ISO/IEC 27000:2018 szabvány szerint: „occurrence or change of a particular set of circumstances" [13], az *ITIL v3 Hungarian Glossary* bővebb magyarázata szerint szolgáltatásüzemeltetési fogalom: „olyan állapotváltozás, amelynek jelentősége van egy konfigurációelem vagy IT-szolgáltatás kezelésében. Az »esemény« kifejezést bármilyen IT-szolgáltatás konfigurációelem vagy megfigyelőeszköz által keltett riasztásra vagy értesítésre használják. Az események általában az IT-üzemeltető személyzet beavatkozását igénylik, és gyakran vezetnek naplózandó incidensekre" [14]. Az Ibtv. szerint a *biztonsági esemény*: „nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül" [6]. Az *esemény* informatikai szakmai (jellemzően üzemeltetői), illetve egyes esetekben a rendszer szakmai (nem informatikai) felügyeletét ellátó szervezeti egység részéről megteendő intézkedést igényel a szervezeten belül. Amennyiben egy esemény az Ibtv. szerinti *biztonsági eseménynek*

is minősül, arról a jogszabály alapján az elektronikus információs rendszer biztonságáért felelős személy köteles tájékoztatni a Nemzeti Elektronikus Információbiztonsági Hatóságot. Amennyiben *súlyos biztonsági esemény* („olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek" [6]) következik vagy következhet be, „amely a rendszert működtető szervezet működéséhez szükséges alapvető információk vagy személyes adatok sérülésével jár, az eseménykezelő központ a védelmi feladatainak ellátása érdekében kötelezheti a szervezetet, hogy a súlyos biztonsági esemény megszüntetése vagy a fenyegetettség elhárítása érdekében szükséges intézkedéseket tegye meg" [6]. Az előírások teljesítése érdekében pontosan tudni – szabályozásban rögzíteni – kell, hogy az *események* közül melyek minősülnek *biztonsági eseménynek* és *súlyos biztonsági eseménynek*.

2. Az IBSZ-ben a fogalomhasználat legyen következetes és puritán. A szabályzat ne legyen stilisztikai gyakorlat, ahol ugyanazon fogalomra szinonimákat használunk. Jobb megszokni egy szót és mindig azt alkalmazni; egy idő után már nemcsak a szabályzat írója, hanem olvasója/alkalmazója is ugyanarra a tartalomra fog gondolni a szó elolvasásakor.
3. Az IBSZ ne ismételje meg a jogszabályok rendelkezéseit (csak akkor, ha kifejezetten szükséges – erre a fogalomtár kivételével kevés esetben kerülhet sor). Az IBSZ-nek azt kell rögzítenie, hogy a jogszabályi előírásokat a szervezet az adott esetben hogyan teljesíti.

   Egy példa a *Védelmi intézkedés katalógus*ból: „Független értékelők. Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmaz a védelmi intézkedések értékelésére" [12]. Az IBSZ-ben nem azt kell rögzíteni, hogy a szervezet külső auditokon győződik meg az intézkedések megfelelőségéről, hanem azt, hogy ki/mely szervezeti egység tervezi meg és készíti elő, támogatja a külső auditokat, ki hagyja jóvá az auditok végrehajtását, azokra milyen gyakorisággal, milyen hatókörben kerül sor, hogyan hasznosulnak az auditok eredményei stb.
4. Az IBSZ ne legyen hosszú. Egy 20–25 A4-es oldal terjedelmet meghaladó dokumentumot már csak a legelszántabbak *kezdenek el* olvasni.
5. Az IBSZ tartalmazzon utalást mindazon szabályozóeszközökre, amelyeket az IBSZ mellett az információbiztonsági szempontból releváns tevékenység során alkalmazni kell. Amennyiben az IBSZ – kézikönyv jelleggel – utal a környező szabályozóeszközökre, megkönnyíti az alkalmazók dolgát, hiszen tudni fogják, milyen témában hol találhatják meg a további előírásokat. Ez a megoldás segíti a szabályozás előkészítőjét is: nem kell megismételnie (módosításkor frissítenie) a máshol már szereplő rendelkezéseket. A hivatkozások elhelyezhetők a szövegben (például „A mentésre, archiválásra vonatkozó részletes előírásokat a Mentési szabályzat tartalmazza."), de célszerű egy szabályozástérképet vagy

szabályozáskatalógust mellékletként csatolni; ez utóbbi a gyors áttekintést teszi lehetővé. A hivatkozások átlátható rendszerének mellékletben történő elhelyezése az IBSZ törzsszövegének terjedelmére is jótékony mérséklő hatással lehet. A korábban leírtak alapján magának a szabályozástérképnek vagy -katalógusnak a tartalma is meglehetősen összetett lesz.

6. Az IBSZ a valóságot rögzítse. A szabályzat létező és azonosítható személyekre, szerepkörökre, szervezeti egységekre telepítse a feladatokat és a felelősségeket. Gyakori megoldás, hogy „a vezető által kijelölt személy" lesz a felelőse egy-egy nehezebb, összetettebb, még nem teljesen pontosan körülhatárolt feladatnak – ez a nyelvi fordulat csak akkor támogatható, ha tudni lehet, ki, mikor, hogyan lett/lesz megbízva a feladattal és erről, illetve az esetleges módosulásról az érintettek hogyan szereznek tudomást. Amennyiben egy még nem létező eljárást, műszaki megoldást kívánunk rögzíteni, ami például egy projekt, fejlesztés eredményeként lép majd életbe, a szabályzat végén – az *Átmeneti és záró rendelkezések*ben – történjen utalás a későbbi bevezetésre és alkalmazásra. A várt/vágyott állapotok szabályzatban rögzítésével nehéz feladatra vállalkozna a szerző: folyamatosan figyelemmel kellene kísérnie és dokumentálnia, mi az, ami már igaz és mi az, ami csak *lesz* igaz.
7. Az IBSZ átlátható, teljességre törekvő, de nem túl részletes legyen. Adjon általános és teljes képet az információvédelem szervezeten belüli megvalósításáról, de ne vesszen el a részletekben. A törzsszöveg tartalmazza az információbiztonsági szempontból releváns beosztásokat, szerepköröket, tevékenységeket, az ezeket betöltő személyek együttműködési formáit, az ellenőrzés, a dokumentálás stb. rendjét. Hangsúlyozandó, hogy e tekintetben nemcsak a vezetői vagy az informatikusi, hanem a felhasználói szerepkör is releváns, azaz az IBSZ-nek az *egyszerű felhasználók* információbiztonsági szempontból jelentőséggel bíró jogait és kötelezettségeit is tartalmaznia kell. A módszertani leírásokat (például egy kockázatelemzési módszertant) nem a törzsszövegben, hanem a mellékletben célszerű elhelyezni. A részletező eljárásrendeket (például egy elektronikus információs rendszer jogosultságkezelését vagy mentési rendjét) önálló (esetleg alacsonyabb szintű vagy kisebb hatókörű, csak az adott tevékenységre vagy rendszerre vonatkozó) szabályozóeszközben lehet rögzíteni. Az IBSZ *szabályozzon*. Ne tartalmazza a nem normatív dokumentumok elemeit (politika, stratégia stb.).
8. Az IBSZ segítse, orientálja a gyakran ismétlődő tevékenységeket (akár elektronikus) nyomtatványok, űrlapok rendszeresítésével (nyilatkozat-minta, bejelentés-minta stb.).

Az *irodalmi felütés* után – zárásként – álljon itt két, történelmi példán alapuló módszertani javaslat:

„Egy nap, miután a szenátus bejelenti, hogy most már minden egyes orosz városnak megvan a maga katonai kormányzója, Katalin (Nagy Katalin cárnő, uralkodott: 1762–1796) hirtelen megkérdi: hány város van Oroszországban? Döbbent csend a válasz. Senki nem tudja. Ezen aztán ne múljék, majd megszámoljuk a térképen,

mondja Katalin. De a szenátus archívumában nincs térkép. Katalin mosolyogva ad öt rubelt egy fiatal tisztviselőnek azzal, hogy vásároljon térképet a Tudományos Akadémián. Kirilov Atlaszáról van szó. A szenátorok bűntudattal hétrét görnyednek az alázattól." [15: 186.]

Azaz: nem árt, ha mindenki tudja, miről beszél, miről beszélünk; a szabályozás rögzítése előtt nyugodtan nézzünk utána mindennek, ami nem ismert, nem világos.

Amikor Albert herceg, Viktória angol királynő férje (1819–1861) az 1840-es évek közepén megkezdte a királyi háztartás átszervezését, több ízben érthetetlen, indokolhatatlan hagyományokra bukkant. „Albert, miközben a számadásokat vizsgálta, megakadt egy 35 shillinges tételen, mely minden héten szerepelt: »Borköltség a vörös szoba részére.« Utánajárt a dolognak, és kisütötte, hogy III. György idejében (uralkodott: 1760–1820) a windsori kastély egyik vörös tapétás helyisége őrszoba volt, az őrségparancsnok napi öt shillinget kapott borra. Az őrszobát már régóta megszüntették, a vörös szobából lomtár lett, de a harmincöt shillinget a hagyomány szent nevében minden héten kiutalták. Egy félzsoldon levő tiszt vette fel, aki egyébként komornyik is volt a palotában. [16: 144.]"

Azaz: nem biztos, hogy az „így szoktuk" gyakorlata még az aktuális helyzetben is célszerű, hasznos, előremutató. Legyen a szabályozás rögzítésének szükséges velejárója a felülvizsgálat, újragondolás, korrekció.

Következtetések

Az IBSZ-írás – ahogyan arra a fentiek is utaltak – a jelenlegi jogszabályi környezetben összetett feladat. Meg kell felelni a jogalkotó által meghatározott számos – néha első ránézésre egyszerűnek nem tűnő – tartalmi és formai elvárásnak. Ismerni kell – átfogóan és részletekbe menően is – az érintett szervezet tevékenységét, nemcsak az információbiztonsági feladatokat, hanem az általános felépítést és működést is, hiszen az információbiztonsági szabályozás a szervezet egészére kiterjedő (speciális) funkcionális tevékenység. Együtt kell működni más szakterületekkel, egyrészt az informatikai, másrészt különösen a jogi-szabályozási, adatvédelmi stb. feladatokat ellátó szervezeti egységekkel, munkatársakkal.

Az IBSZ-írást fel lehet fogni kötelező adminisztratív feladatnak, ahol az elsődleges cél a készre jelentés. Ennél szerencsésebb megközelítés, ha az IBSZ-írást a szervezeti működést támogató, érdemi alkotótevékenységnek fogjuk fel, amelynek megvalósítása során nemcsak az előírások mechanikus rögzítése, hanem azok szervezetre adaptálása, a szervezeti működés és az előírások összhangba hozása is megtörténik.

Az IBSZ a szervezet munkatársai által akkor lesz hasznosítható, ha „felhasználóbarát" formában érdemi, konkrét ismereteket, szabályokat ad. Ez rendkívül fontos szempont, hiszen az információbiztonsági szabályozás célja a jogalkotó és az érintett szakemberek által szükségesnek ítélt előírások rögzítése annak érdekében, hogy azok megismerhetők és alkalmazhatók, sőt alkalmazandók (kikényszeríthetők, számonkérhetők) legyenek.

A jó IBSZ megírására nincsen kész recept, de az érintett szervezeteknél, a szervezetek munkatársainál az elmúlt évtizedekben felhalmozódott tapasztalatok alapján

azonosíthatók a jó gyakorlatok, ezek alapján segédletek készíthetők, amelyek megosztásából már többen profitálhatnak.

A tanulmányban közzétett áttekintéseket, összefoglalókat, illetve a szerző által megfogalmazott javaslatokat gyakorlati szempontok alapján és gyakorlati céllal rögzítettük – elősegítendő, hogy az IBSZ-írás hatékony és eredményes tevékenység lehessen. Ajánlás, amelynek követése, szükség szerinti felülvizsgálata vagy kiegészítése nem kötelező – de hasznos lehet.

Hivatkozások

[1] U. Eco, *Hogyan írjunk szakdolgozatot?* Budapest: Gondolat Könyvkiadó, 1992.
[2] Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, *Informatikai biztonsági módszertani kézikönyv*. Informatikai Tárcaközi Bizottság ajánlása, 8. sz. ajánlás, Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, 1994.
[3] Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, *Informatikai rendszerek biztonsági követelményei. Informatikai Tárcaközi Bizottság, 12. ajánlás,* Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, 1996.
[4] Közigazgatási Informatikai Bizottság, *A Közigazgatási Informatikai Bizottság 25. számú ajánlása: 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR) 1.0 verzió.,* Közigazgatási Informatikai Bizottság, 2008.
[5] Cs. Krasznai és L. Muha, *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem, 2014.
[6] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
[7] 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről
[8] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról
[9] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
[10] 2000. évi C. törvény a számvitelről
[11] 2010. évi CXXX. törvény a jogalkotásról
[12] 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
[13] ISO/IEC 27000:2018 (en) Information technology – Security techniques – Information security management systems – Overview and vocabulary
[14] ITIL® V3 Glossary of Terms, Definitions and Acronyms in Hungarian, Hungarian Glossary
[15] H. Troyat, *Nagy Katalin.* Budapest: Pesti Szalon Könyvkiadó, 1996.
[16] L. Strachey, *Viktória királynő. Történelmi életrajz.* Budapest: Szépirodalmi Könyvkiadó, 1984.

HADMÉRNÖK
VÉDELMI ELEKTRONIKA, INFORMATIKA, KOMMUNIKÁCIÓ

14. évfolyam (2019) 3. szám 129–146.
DOI: 10.32567/hm.2019.3.11

Török Péter[1]

Titkos üzenet száll a széllel! (IoT-ben használt vezeték nélküli adatátviteli technológiák összehasonlítása)

Secret Message Flies with the Wind! (Comparison of Wireless Data Transmission Technologies Used in IoT)

Ebben a publikációban bemutatom az IoT területén legelterjedtebb vezeték nélküli technológiákat. A vizsgálatom elsősorban a kis teljesítményű vezeték nélküli technológiákra összpontosít, mint például a ZigBee, WiFi, a LoRaWAN és a Bluetooth. A tanulmány a hatótáv, a teljesítmény és az elérhető adatátviteli sebesség szempontjából osztályozza a protokollokat és rövid összefoglalót ad azokról, illetve grafikusan összehasonlítja a tulajdonságaikat.

Kulcsszavak: **IoT, vezeték nélküli hálózatok, kis teljesítményű vezeték nélküli protokollok, alacsony fogyasztású technológiák**

In this publication I present the most widespread wireless technologies in IoT. My research focuses on low-power wireless technologies, such as ZigBee, WiFi, LoRaWAN, and Bluetooth. The study classifies the protocols in terms of range, throughput, and available data rates and provides a brief summary of the protocols under review, as well as graphically compares their properties.

Keywords: **IoT, wireless networks, low-power wireless protocols, low-power technologies**

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: torok.peter@uni-nke.hu, ORCID: https://orcid.org/0000-0002-7960-8945

Bevezetés

Napjainkban egyre nagyobb az igény a vezeték nélküli kommunikációra. Folyamatosan növekszik a hálózatra kötött eszközök száma. Ezek az eszközök kommunikálni szeretnének egymással. A jelenleg csatlakoztatott eszközök öt fő vezeték nélküli technológiát használnak: WiFi, Bluetooth Smart, ZigBee, Z-Wave és a Thread [1]. A felsoroltak kivétel nélkül az ISM[2]-sávot használják, leginkább a 2,4 GHz-es tartományban, ami ennek köszönhetően egyre jobban telített. Így az ezt a frekvenciasávot használó eszközök zavarhatják egymás adatátvitelét.

Az IoT[3]-technológia robbanásszerű terjedése csak tovább rontja a helyzetet. Kis léptékben az okosotthonok terjedése, nagy léptékben az okosvárosok kialakítása, a különböző közüzemi szolgáltatók szenzorhálózatai tovább terhelik a szabad sávokat. Igaz, ezek a rendszerek nem igényelnek nagy adatátviteli sebességet, de szükséges a kis késleltetési idő, ami romlik a túlterhelt sávokon.

A civil felhasználás mellett a katonai alkalmazás is egyre széleskörűbb. A hálózat alapú hadviselés, az optimális tájékozottság állapota megköveteli a szenzorhálózatok alkalmazását és a nagy sebességű adatkommunikációs hálózatot [2: 175.]. A digitális katonának is rendelkeznie kell nagy teljesítményű, viselhető számítógéppel és folyamatos, védett infokommunikációs kapcsolattal [3]. A katonai célú felhasználás is előnyben részesíti a vezeték nélküli technológiákat, mert egyszerűbben és gyorsabban telepíthetők, valamint gazdaságosabbak [4: 40.]. Általában a csatlakoztatott eszközök vezeték nélküli technológiájának kiválasztásakor a végső alkalmazás függvényében néhány szempontot figyelembe kell venni:

- maximális áteresztőképesség;
- energiafelhasználás;
- maximális távolságtartomány [5].

A szaporodó feladatok egyre újabb és sokrétűbb kihívásokat jelentenek a vezeték nélküli kommunikáció terén. Ezek leküzdésére újabb, speciálisabb protokollokra van szükség. Naponta születnek új megoldások, könnyen eltévedhetünk a számunkra megfelelő kiválasztása közben [6], [7].

Ezért ebben a munkámban összehasonlító elemzést végzek különböző, IoT-ben is használt vezeték nélküli protokollok vonatkozásában, ami segítheti a vezeték nélküli kommunikációs rendszer kiválasztását és kialakítását.

Protokollok csoportosítása

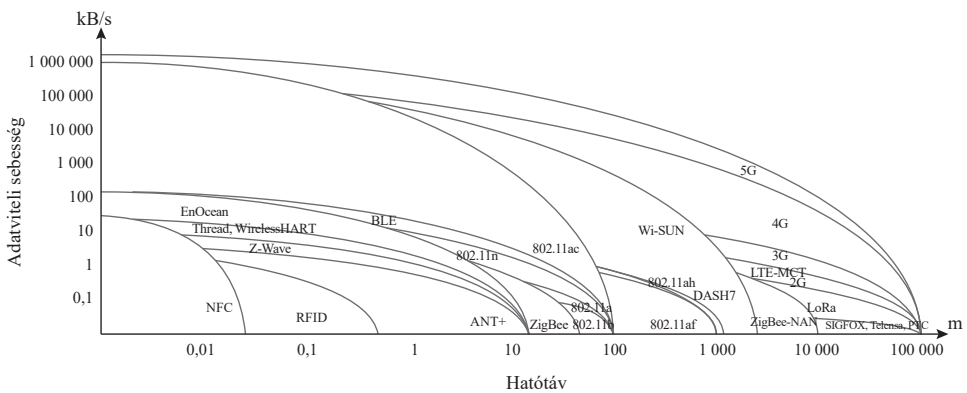
Több különböző vezeték nélküli technológiát használnak az IoT-hez. Ezek néhány centimétertől több kilométerig terjedő adatátvitelt tesznek lehetővé. A legrövidebb hatótáv az érintkezési távolság, ahol az eszközök akár egymáshoz is érhetnek a kommunikáció idejére, de nincs szükség vezetékes adatátviteli közegre. A rövid hatótávolságú

[2] Industrial, Scientific and Medical.
[3] Internet of Things.

kommunikációhoz a vezeték nélküli személyi hálózat (WPAN[4]) használata ajánlott. Itt figyelhető meg az IoT térnyerésének hatása. Sok ilyen új technológia jött létre az elmúlt években. Következő kategória a rövid/közepes hatótáv protokolljai, amelyek a vezeték nélküli helyi hálózati technológiákat (WLAN[5]) tartalmazzák. A hosszú távú kommunikációra a nagy kiterjedésű, vezeték nélküli hálózati technológiákat (WWAN[6]) használják. Ezek két további csoportra oszthatók fel: az engedélyköteles és az engedélymentes technológiára.

Vizsgálatomban a másik fő paraméter az elérhető adatátviteli sebesség. Fontos, hogy alkalmas legyen a szükséges vagy a keletkező adatmennyiség továbbítására.

Az 1. ábra összefoglalja a különböző technológiákat a távolság és az elérhető adatátviteli sebesség függvényében. Az értékek széles határok között változtak, így logaritmikus skálát használtam a tengelyeken.



1. ábra

IoT-ben használt vezeték nélküli adatátviteli protokollok összehasonítása
[a szerző szerkesztése]

Az áthidalható távolság és az elérhető adatátviteli sebesség mellett fontos szempont a protokoll által használt frekvencia. A megfelelő megoldás kiválasztásnál ez is szempont lehet. Könnyebbé teszi a váltást az azonos hullámhosszt használó protokollok között, mert az adó RF[7]-egysége azonos hardvert tartalmaz. Így csak szoftverben térnek el egymástól, ami egy frissítéssel cserélhető. Hátrány viszont, hogy az azonos frekvencián üzemelő eszközök zavarhatják egymás működését. A nagyobb teljesítményű adó zavarja a kisebb teljesítményű adó kommunikációját. Erre megoldás lehet a különböző feladatokra eltérő frekvenciát használó protokollok választása. A protokollok által használt frekvenciákat az 1. táblázat mutatja be.

4 Wireless Personal Area Network.
5 Wireless Local Area Network.
6 Wireless Wide Area Network.
7 rádiófrekvenciás.

1. táblázat

A vizsgált protokollok által használt frekvenciák [a szerző szerkesztése]

	13,56 MHz	220 MHz	54-698 MHz	315 MHz	779 MHz	868 MHz	900 MHz	915 MHz	920 MHz	1800 MHz	2400 MHz	5800 MHz
NFC	•											
RFID	•											
ANT+											•	
BLE											•	
EnOcean				•				•	•			
Thread											•	
Wireless-HART											•	
ZigBee					•	•		•	•		•	
Z-Wave						•		•	•			
DASH7								•	•			
802.11a												•
802.11b											•	
802.11g											•	
802.11n											•	•
802.11ac											•	•
802.11af			•									
802.11ah								•	•			
Wi-SUN									•			
ZigBee-NAN									•			
2G							•					
3G							•			•		
4G										•		
5G										•		
LTE-MTC							•			•		
LoRa						•		•				
PTC		•										
SIGFOX						•		•				
Neul								•				
Telensa						•		•				

Vizsgált protokollok

NFC (Near Field Communication)

A Nokia, Philips és a Sony alapításával 2004-ben létrehozott protokoll a Near Field Communication (NFC) Forum által 2006-ban definiált olyan kommunikációs protokoll, amely két elektronikus eszköz kontaktus nélküli kommunikációját teszi lehetővé. Az adatátvitel a mágneses téren keresztül, nem pedig a kísérő elektromos mezőn keresztül történik. Előnye, hogy biztosítja az elektronikus eszközök közötti egyszerű és biztonságos kétirányú kommunikációt. Ezt használják fel az okostelefonok esetében,

amelyek lehetővé teszik a fogyasztók számára a kapcsolat nélküli fizetési tranzakciókat, a digitális tartalmak elérését és az elektronikus eszközök csatlakoztatását [8].

Az összehasonlításhoz használt adatok:

Távolság:	4 cm
Adatátviteli sebesség:	412 kb/s
Frekvencia:	13,56 MHz

Honlap: https://nfc-forum.org/

RFID (Radio Frequency IDentification)

Az RFID automatikus azonosításhoz és adattovábbításhoz használt legrégebbi technológia. Már a második világháborúban használta a Brit Királyi Légierő a rádióhullámokat a saját repülőgépeinek felismeréséhez (IFF[8]). A modern RFID-technológiát az amerikai Los Alamos-i kutatóintézetében alkották meg 1973-ban. A kommunikáció RFID-címkék és -eszközök segítségével történik. Az RFID-címke lehet egy apró tárgy, amely rögzíthető vagy beépíthető az azonosítani kívánt objektumba, vagy egy azonosítókártya, esetleg egy kulcstartó is. Csak egyirányú kommunikációt tesz lehetővé. Külön eszközbe kerül az adó és a vevő rész [9].

Az összehasonlításhoz használt adatok:

Távolság:	75 cm
Adatátviteli sebesség:	80 kb/s
Frekvencia:	13,56 MHz

Honlap: www.ieee-rfid.org/

ANT+

Az ANT+ az *ANT Wireless* által 2004-ben kifejlesztett, meglehetősen sajátos és specializált fizikai és MAC réteg protokoll, amelyet a vezeték nélküli érzékelő hálózatok (WSN[9]) számára terveztek. Ezt a protokollcsomagot a PAN[10]-re épülő fitneszberendezések alkalmazzák kommunikációra. Az ANT+ úgy konfigurálható, hogy alacsony teljesítményű „alvó" üzemmódban várakozzon hosszú ideig, majd rövid időn belül felébredjen, és adattovábbítás után visszatérjen „alvó" üzemmódba. Az eszközök között a kommunikáció kétirányú [10].

Az összehasonlításhoz használt adatok:

Távolság:	100 m
Adatátviteli sebesség:	60 kb/s
Frekvencia:	2,4 GHz

Honlap: www.thisisant.com/

[8] Identify Friend or Foe.
[9] Wireless Sensor Network.
[10] Personal Area Networks.

BLE (Bluetooth Low Energy)

A Bluetooth SIG[11] által 1999-ben útjára indított protokoll. Alapvető feladata a vezeték nélküli rádiófrekvenciás kommunikáció biztosítása rövid hatótávolságon belül kis teljesítménnyel és olcsón. A 4.0 verziójával megérkezett a BLE, amelynek elsődleges célja, hogy biztosítsa az eszköz működését. Ezt alacsony fogyasztással teszi lehetővé. Ezzel párhuzamosan csökken az adott eszköz teljesítménye, ezért főként szenzorokban használják [11].

Az összehasonlításhoz használt adatok:
Távolság: 100 m
Adatátviteli sebesség: 1 Mb/s
Frekvencia: 2,4 GHz
Honlap: www.bluetooth.com/

EnOcean (Energy Harvesting Wireless Technology)

Egy fizikai és MAC réteg protokoll, amit az EnOcean Alliance hozott létre 2008 áprilisában. A felsőbb rétegek feladatait szabványos WPAN[12]-szenzorokat csatlakoztatva lehet megvalósítani. A moduljai a mikrohullámú adatátvitelt ötvözik az ultra alacsony fogyasztással. Elsősorban épületfelügyeleti és automatizálási, illetve ipari rendszerekben alkalmazzák önműködő vezeték nélküli érzékelő, vezérlési, felügyeleti és jelzőrendszerekhez [12].

Az összehasonlításhoz használt adatok:
Távolság: 30 m
Adatátviteli sebesség: 1 Mb/s
Frekvencia: 2,4 GHz
Honlap: www.enocean-alliance.org/

Thread

Fiatal protokollnak számít. 2014 közepén kezdte a fejlesztését a Thread Group azzal a céllal, hogy egy új, IP-alapú mesh-kommunikációs[13] megoldást fejlesszenek ki. IPv6 hálózati protokoll, amelynek célja az intelligens otthoni hálózat eszközeinek kommunikációja. Elsősorban a WiFi kiegészítéseként tervezték, kiküszöbölve annak korlátait az otthoni automatizálásban. Úgy tervezték, hogy a már meglévő IEEE802.15.4 vezeték nélküli vezérlőket használják [13].

[11] Bluetooth Special Interest Group.
[12] Wireless Personal Area Network.
[13] A használt hálózati eszközök saját maguk térképezik fel a hálózat többi tagját és önállóan konfigurálják magukat a hálózat változása esetén is.

Az összehasonlításhoz használt adatok:
Távolság: 30 m
Adatátviteli sebesség: 250 Kb/s
Frekvencia: 2,4 GHz
Honlap: www.threadgroup.org/

WirelessHART (Wireless Highway Addressable Remote Transducer)

Hibrid rendszer, amely mind analóg, mind digitális jeleket használ. A HART Communications Foundation által 2004-ben indított szabvány. Az iparban egyik legkeresettebb technológia a vezeték nélküli szenzorhálózatok területén. Ugyanazokat a vezérlési szolgáltatásokat nyújtja, mint a vezetékes hálózat [14].

Az összehasonlításhoz használt adatok:
Távolság: 30 m
Adatátviteli sebesség: 250 Kb/s
Frekvencia: 2,4 GHz
Honlap: https://fieldcommgroup.org/

ZigBee

A Zigbee Alliance alkotta meg 1998-ban. A szabvány kiadásának éve: 2004. Kis sebességű WPAN-hálózatok számára készült, szöveges adatok átvitelére. Erőssége a kis fogyasztásban és bonyolult ad-hoc hálózat felépítésében rejlik. Felhasználható elsősorban gép-gép kommunikációra (M2M[14]), ahol nincs szükség nagy átviteli sebességre. Gyors és kis erőfeszítésekkel járó hálózatépítést tesz lehetővé [15].

Az összehasonlításhoz használt adatok:
Távolság: 75 m
Adatátviteli sebesség: 250 kb/s
Frekvencia: 2,4 GHz
Honlap: www.zigbee.org/

Z-Wave

A Z-Wave egy alacsony fogyasztású RF kommunikációs technológia, amelyet elsősorban otthoni automatizáláshoz tervezett a Zensys 2001-ben olyan termékekhez, mint a lámpavezérlők és érzékelők. A gigahertz alatti ISM-sávban működik, és nem interferál a WiFi és más vezeték nélküli technológiák 2,4 GHz-es frekvenciájával.

[14] Machine to Machine.

Támogatja a full mesh hálózatokat anélkül, hogy szükség lenne koordinátor-csomópontra. Nagyon jól skálázható, akár 232 eszköz vezérlését is lehetővé teszi [16].

Az összehasonlításhoz használt adatok:

Távolság:	30 m
Adatátviteli sebesség:	100 kb/s
Frekvencia:	900 MHz

Honlap: www.z-wave.com/

DASH7

A protokollt a DASH7 Alliance kezeli a 2011-es indulása óta. Az ISO 18000-7 Active RFID-szabványon alapul. Az épületautomatizáláshoz, az intelligens otthonokhoz, a logisztikához és autóipari felhasználáshoz fejlesztették. A kezdeti 433 MHz frekvenciáról váltott magasabbra, ezzel csökkentve az antenna méretét és növelve az átviteli sebességet. A legtöbb vezeték nélküli hálózattól eltérően nem igényli átjáró vagy csomópontvezérlő működését [17].

Az összehasonlításhoz használt adatok:

Távolság:	1,5 km
Adatátviteli sebesség:	167 kb/s
Frekvencia:	900 MHz

Honlap: www.dash7-alliance.org/

802.11a/b/g/n/ac

A WiFi, a vezeték nélküli protokollok közül a legismertebb. 1997-ben készítette el az eredeti szabványt az IEEE.[15] Azóta folyamatosan frissíti a szabványt. A verziókat új betűjelzéssel különböztetve meg (802.11 b/g/n/ac). Felhasználását tekintve általános célú, ezért is terjedt el a mindennapokban, az otthonoktól kezdve a közlekedési eszközökön át a munkahelyekig.

802.11a: Nagy távolságú pont-pont kapcsolatra használják általában.

802.11b: Régi szabvány, átviteli sebessége kicsi, de régebbi gyártású eszközök még csak ezt támogatják.

802.11g: A 802.11b-hez hasonló felépítésű, az eszközök kompatibilisek vele. Előnye a nagyobb adatátviteli sebesség.

802.11n: Jelenleg a legelterjedtebb WiFi-szabvány. Több adatfolyam összefogása miatt gyorsabb. Jelenleg egy, két, és újabban három adatfolyamos WiFi-routerek és adapterek vannak forgalomban. Az n-es WiFi egyik jelentős újítása az 5 GHz-es frekvencia használata. A 2,4 GHz-es tartomány ugyanis már nagyon telített további WiFi, Bluetooth és egyéb rádiós átvitelt használó eszközök jeleivel, illetve a mikrohullámú sütők is zavarják.

[15] Institute of Electrical and Electronics Engineers.

802.11ac: A megváltozott használati szokásokhoz, mobil készülékekhez igazították. Tovább gyorsult, és növelték a kapcsolat stabilitását [18].

Az összehasonlításhoz használt adatok:
Távolság: a: 120, b: 140, g: 140, n: 250, ac: 350 m
Adatátviteli sebesség: a: 54, b: 11, g: 54, n: 600, ac: 1300 Mb/s
Frekvencia: b,g,n,ac: 2,4 GHz, a, n, ac: 5 GHz
Honlap: www.ieee802.org/11/

802.11af

Az IEEE 802.11af, más néven White-Fi vagy Szuper WiFi a televíziós műsorszórásra kijelölt frekvenciák nem használt spektrumát használja ki. Ez engedélyköteles tartomány, így használatához frekvenciaengedély szükséges. Új keletű szabvány, 2014 februárjában engedélyeztette az IEEE, elsődlegesen a nagy távolságú vezeték nélküli kapcsolatokra optimalizálva [19].

Az összehasonlításhoz használt adatok:
Távolság: 1 km
Adatátviteli sebesség: 26,7 Mb/s
Frekvencia: 54-790 MHz
Honlap: www.ieee802.org/11/

802.11ah

Az IEEE 2017-ben tette közzé ezt a protokollt. A gigahertz alatti ISM-sávok használata lehetővé teszi a nagy hatótávolságú és alacsony teljesítményű vezeték nélküli szenzorhálózatok üzemeltetését. Így IP-alapú WiFi-szerű megoldást biztosít az M2M-alkalmazásokhoz a korábbi WiFi-verziókhoz képest sokkal nagyobb hatótávolsággal [20].

Az összehasonlításhoz használt adatok:
Távolság: 1 km
Adatátviteli sebesség: 40 Mb/s
Frekvencia: 915 MHz és 920 MHz
Honlap: www.ieee802.org/11/

Wi-SUN (Wireless Smart Utility Network)

A Wi-SUN az IEEE802.15.4e szabványon alapuló kommunikációs protokoll. A Wi-SUN Alliance indította 2015-ben és kezeli a mai napig. Megalkotásának célja, hogy megoldásokat kínáljon FAN-ok[16] számára olyan alkalmazásokhoz, mint a fejlett mérési infrastruktúra és az adattovábbítás automatizálása, valamint az okosotthon-megoldások.

[16] Field Area Network.

Ehhez fejleszt okos villamos fogyasztásmérőket, gázmérőket és további különböző mérőberendezéseket [21].

Az összehasonlításhoz használt adatok:
Távolság: 4 km
Adatátviteli sebesség: 40 Mb/s
Frekvencia: 920 MHz
Honlap: www.wi-sun.org/

Zigbee-NAN

Más néven JupiterMesh, a ZigBee Alliance 2016-ban indított kezdeményezése. Ez egy 802.15.4g szabványú protokoll. Robosztus felépítése és rugalmas adatátviteli sebessége lehetővé teszi az optimális vezeték nélküli kommunikációt a közművek és az önkormányzatok számára, intelligens hálózatot és intelligensváros-megoldásokat alkalmazva [22].

Az összehasonlításhoz használt adatok:
Távolság: 10 km
Adatátviteli sebesség: 100 kb/s
Frekvencia: 920 MHz
Honlap: www.zigbee.org/jupitermesh-neighborhood-area-network-nan-announced/

2G

A második generációs vezeték nélküli távbeszélő technológia a távközlési hálózati technológiákra vonatkozik, amelyeket az ITU-R[17] 1991-ben indított a GSM[18]-szabványban. Legfontosabb újítása az első generációhoz képest a telefonbeszélgetések digitális titkosítása és a spektrum jobb kihasználása. Ebben vezették be az első mobil adatátviteli szolgáltatásokat [23].

Az összehasonlításhoz használt adatok:
Távolság: 100 km felett
Adatátviteli sebesség: 57,6 kb/s
Frekvencia: 900 MHz
Honlap: www.gsma.com/

[17] International Telecommunication Union Radiocommunication Sector.
[18] Global System for Mobile Communications.

3G

A 3G, más néven IMT-2000[19]-szabvány 2001-es évi megtervezésekor a mobil multimédiás szolgáltatásokhoz szükséges gyorsabb vezeték nélküli kommunikációra fókuszáltak. A továbbfejlesztett adatátviteli sebesség tette lehetővé a valós idejű mozgókép-továbbítást, illetve a mobiltelefonnal történő internetes böngészés megvalósítását. Ezt követően megnyitotta az utat az okostelefonok megjelenéséhez. Mivel alkalmasabbak voltak mobil weboldalak megtekintésére vagy mobil TV-nézésére. Széleskörű elterjedése 2007-től figyelhető meg [23].

Az összehasonlításhoz használt adatok:
Távolság: 100 km felett
Adatátviteli sebesség: 2 Mb/s
Frekvencia: 900 MHz és 1800 MHz
Honlap: www.3gpp.org/

4G

A 4G szabványokat IMT-Advanced[20] néven jelölik. Célja, hogy megbízhatóan biztosítsa a mobilszolgáltatók számára a 100 Mbps-nál nagyobb adatátviteli sebességet, ami szükséges a HD[21]-minőségű multimédiás tartalmak továbbításához. 2009 szeptemberében két szabványtervezetet nyújtottak be ITU-R-hez: az LTE Advanced-ot és a IEEE 802.16m szabványt. Az első bevezetett technológia a WiMax (IEEE802.16) volt [23].

Az összehasonlításhoz használt adatok:
Távolság: 100 km felett
Adatátviteli sebesség: 300 Mb/s
Frekvencia: 1800 MHz
Honlap: www.3gpp.org/technologies/keywords-acronyms/98-lte/

5G

Az 5G-ConnectedMobility egy speciális hálózati infrastruktúrát és alkalmazási környezetet hoz létre. Elsősorban a jármű-jármű, a jármű-infrastruktúra és a vasút-infrastruktúra kommunikáció számára. A konzorcium alapítótagjai az Ericsson, a BMW-csoport, a Deutsche Bahn, a Deutsche Telekom, a Telefónica Deutschland és a Vodafone, a TU Dresden 5G Lab Németország, a Federal Highway Research Institute [23].

[19] International Mobile Telecommunications-2000.
[20] International Mobile Telecommunications Advanced.
[21] High Definitons.

Az összehasonlításhoz használt adatok:
Távolság: 100 km felett
Adatátviteli sebesség: 1 Gb/s
Frekvencia: 1800 MHz
Honlap: www.3gpp.org/release-15/

LTE-MTC (Long Term Evolution – Machine Type Communication)

A 3GPP[22] szabványügyi testülete dolgozik az MTC-szolgáltatások specifikációinak szabványosításával az LTE-hálózatok részeként. Ezek az eszközök várhatóan alacsony költségű, alacsony adatátviteli sebességgel és késleltetett toleranciával rendelkeznek majd. Ezért a fő fejlesztési irányelv a valós idejű adattovábbítás lett ennek a technológiának a kidolgozásánál [24].

Az összehasonlításhoz használt adatok:
Távolság: 100 km felett
Adatátviteli sebesség: 2 Mb/s
Frekvencia: 900 MHz és 1800 MHz
Honlap: www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/

LoRa

A LoRa-technológiát a SEMTECH vállalat fejlesztette ki 2012-ben. Egy kifejezetten nagy hatótávolságú, kis teljesítményű kommunikációra tervezett vezeték nélküli protokoll. Elsősorban az M2M és az IoT-hálózatokra optimalizálva, lehetővé téve számos, ugyanazon a hálózaton futó alkalmazás csatlakoztatását. A továbbfejlesztésére létrehozták a LoRa Alliancet, hogy szabványosítsa az LPWAN[23]-t az IoT számára. Tagjai között van a CISCO, a MicroChip, az IBM, az STMicro, a SEMTECH, és idén csatlakozott az Antenna Hungária [25].

Az összehasonlításhoz használt adatok:
Távolság: 15 km
Adatátviteli sebesség: 50 kb/s
Frekvencia: 868 MHz és 915 MHz
Honlap: http://lora-alliance.org/

[22] 3G Partnerségi Program.
[23] Low Power Wide Area Networks.

PTC (Positive Train Control)

Vasúti biztonsági rendszer, amelynek célja a vonatközlekedés biztonságának növelése. 1990-ben kezdte meg a fejlesztését az NSTB[24] az USA-ban azzal a céllal, hogy megelőzze a vonatok ütközését, a túlzott sebesség miatti kisiklásokat, és folyamatos vonatkövetést biztosítson. A hatékony PTC-rendszer képes meghatározni a vonatok helyét és sebességét. Ha a személyzet a figyelmeztető jelzésekre nem reagál, akkor automatikusan beavatkozik [26].

Az összehasonlításhoz használt adatok:
Távolság: 100 km felett
Adatátviteli sebesség: 1 kb/s
Frekvencia: 220 MHz
Honlap: www.fra.dot.gov/ptc/

SIGFOX

A Sigfox cég fejlesztette 2009-ben. A protokoll az UNB[25] nevű technológiát használja. Elsődlegesen okosvárosokhoz, programokhoz tervezték. Alacsony adatátviteli sebességet biztosít, ami elegendő a M2M kommunikációra okosmérők, betegmonitorok, biztonsági eszközök, utcai világítás és környezeti érzékelők számára. Európa nagyvárosaiban már jelenleg is tízezer eszköz van felszerelve és csatlakoztatva a hálózathoz. Erőssége a hálózat robusztussága, az energiatakarékossága és skálázhatósága [27].

Az összehasonlításhoz használt adatok:
Távolság: 50 km
Adatátviteli sebesség: 1 kb/s
Frekvencia: 868 MHz és 915 MHz
Honlap: www.sigfox.com/

Neul

2014 óta a Huawei kezelésében van. A Sigfoxhoz hasonlóan a UNB-t használja. A 802.11ah frekvenciájának egy nagyon kis szeletén működik, az 1 GHz alatti ISM-sávban. Előnye a skálázhatóság, a nagy lefedettség, a kis teljesítmény és az olcsó bekerülési költség [28].

Az összehasonlításhoz használt adatok:
Távolság: 10 km
Adatátviteli sebesség: 100 kb/s
Frekvencia: 915 MHz
Honlap: http://neul.com/

[24] National Transportation Safety Board.
[25] Ultra Narrow Band.

Telensa

A Telensa UNB nagy hatótávolságú, kis energiafogyasztású protokoll. Relé üzemmódot biztosít a csomópontok között a teljes lefedettség érdekében. 2005-ben telepítették a Telensával vezérelt első világítási rendszert. Azóta kibővült a teljes intelligens város infrastruktúrájának felügyeletét ellátó alkalmazásra. Heterogén hálózati közegben is alkalmazható. Különböző interfészeket kínál más szabványú érzékelők, hálózatok, az alkalmazások és az adatplatformok számára [29].

Az összehasonlításhoz használt adatok:

Távolság:	16 km
Adatátviteli sebesség:	1 kb/s
Frekvencia:	868 MHz és 915 MHz

Honlap: www.telensa.com/

Összegzés

Az IoT hatalmas és szerteágazó terület, rengeteg felhasználási móddal. A megvalósítandó feladatok sok különböző és sokszor egymásnak ellentmondó követelményeket támasztanak. Ezért nem lehet egyértelműen kijelenteni egyik vagy mások protokollról, hogy az a legjobb. Legtöbbször csak a legkisebb vagy a legelőnyösebb kompromisszumot lehet megtalálni az elvárások között.

Az érintési távolságban használható RFID- és NFC-protokollok megférnek egymás mellett, mert más célt szolgálnak. Az RFID automatikus azonosításra tervezett, egyirányú kommunikációra képes. Éppen ezért csak a leolvasó egységnek szükséges mindenképpen áramforrás a működéshez. Az NFC ezzel szemben kétirányú kommunikációt tesz lehetővé. Viszont minden eszköz áramellátásáról gondoskodni kell.

A rövid hatótávú kommunikációra alkalmas protokollok már sokkal változatosabbak. Jellemzően 30 m és 100 m az áthidalható távolság. A rövidebb távra az EnOcean, a Thread, a WirelessHART és a Z-Wave ajánlott. Ezek közül a választást a megoldandó feladat sajátossága határozza meg. Az EnOcean előnye az ultraalacsony fogyasztás. Belső architektúrája az ipari rendszerekhez, azok érzékelő, vezérlési, felügyeleti és jelzőrendszer feladataihoz megfelelő. A Thread az intelligens otthoni hálózat eszközeinek kommunikációja. IP-alapú, támogatja az IPv6-ot és a már meglévő WiFi-hálózatot kiegészítve, ahhoz csatlakozva üzemel. Ezért a használatához WiFi-hálózat is szükséges lehet. A WirelessHART ipari szenzorhálózatok meghatározó protokollja. Előnye a többi protokollal szemben, hogy nemcsak digitális, hanem analóg jelek feldolgozására is alkalmas. A ZigBee M2M kommunikációra tervezett, kis energiaigényű, kis adatátviteli sebességű protokoll. Kimondottan szöveges adatok átvitelére alkalmas. A Z-Wave egy otthoni rendszerekhez tervezett, vegyes felhasználású protokoll. Támogatja a szenzorok és vezérlők kezelését, mint az EnOcean és a WirelessHART. Támogatja a mesh-hálózatokat, mint a Thread. A többitől eltérően nem a 2,4 GHz-es ISM-sávot használja, hanem a 900 MHz-et. Más hullámterjedés jellemző rá és kevésbé zavarja más hálózatok működése.

A rövid/közepes hatótáv sokkal egységesebb. A 802.11 protokollcsalád, azon belül is a WiFi különböző verziói a piacvezetők a maximum 1 km távolságú összeköttetésekben. Persze ez csak irányszám, hiszen Magyarországon is van példa 50 km feletti pont-pont WiFi-kapcsolatra. A 802.11 a/b/g/n/ac a visszamenőleges kompatibilitás miatt a legelterjedtebb vezeték nélküli hálózatiprotokoll-csoport. A folyamatos fejlesztés eredményeként az elérhető adatátviteli sebesség és a hatótáv is folyamatosan növekedett. Előnye, hogy szinte minden informatikai eszköz kompatibilis vele. Hátránya is az elterjedtségéből adódik. Kevés számú elérhető csatornán kell osztozni nagyszámú hálózatnak. A sáv túlzsúfoltsága miatt zavarják egymást a szomszédos hálózatok. A 802.11af szabványt részben a régi technológiák eltűnése hozta létre. Az analóg műsorszóró TV-adók megszűnésével felszabadult frekvenciákat újrahasznosítják adattovábbításra. Kevésbé elterjedt, mert használata engedély- és díjköteles. A 802.11ah protokoll subgigahertz ISM-sávokat használ. Részben kompatibilis az IP-alapú WiFi-protokollokkal, ami egyszerűbb vegyes hálózatok kialakítását teszi lehetővé az M2M alkalmazásokhoz. A DASH7 a többi megoldáshoz képest kis adatátviteli sebességű protokoll, ezért olyan ipari rendszerekhez ajánlott ahol nincs nagy továbbítandó adatmennyiség. Előnye a többi protokollhoz képest, hogy nem igényel egyéb kiépített hálózati infrastruktúrát, mint például átjáró vagy csomópontvezérlő. A Wi-SUN és a ZigBee-NAN még egy mérettel nagyobb hálózatokhoz tervezett protokollok. Mindkettő már az okosvárosok koncepciójába illeszkedik. Tervezett felhasználóik a közműszolgáltatók és az önkormányzatok. Jelentős különbség az elérhető adatátviteli sebességben van. Ahol szükséges a nagyobb adatátviteli sebesség, ott a Wi-SUN ajánlott. Ahol elég a kisebb is, de fontos szempont a nagyobb hatótáv, ott a ZigBee-NAN lehet a jó választás.

A hosszú távú kommunikációhoz, főleg a látóhatáron túlihoz már komoly infrastruktúrára, kiépített bázisállomásokra, relékre és átjátszókra van szükség. Az ilyen kereskedelmi rendszerek között a legismertebbek a 2G/3G/4G/5G hálózatok. Használatukhoz előfizetői szerződés szükséges és díjfizetés ellenében történik. Nem kizárólagos használói vagyunk a hálózatnak, így az adatátviteli sebesség változhat a többi felhasználó által generált forgalom miatt. Az LTE-MTC a GSM-rendszerekhez hasonló, illetve azzal közös hálózatot használ, de kimondottan M2M-kommunikációra fejlesztett protokoll. Fő jellemzője az alacsony adatátviteli sebesség és a kis késleltetés. A LoRa gigahertz alatti ISM-sávot használ, független a GSM-rendszerektől. elsősorban M2M-kommunikációra és IoT-hálózatokhoz tervezték. Ezért kis energiaigényű, kis adatátviteli sebességű protokoll. A PTC speciális vasúti biztonsági rendszer. Kimondottan ennek a feltételrendszere alapján fejlesztették. A SIGFOX, a Neul és a Telensa hasonló célból létrehozott protokollok. Elsődlegesen okosvárosok kiépítésének megoldására. A SIGFOX és a Telensa kis adatátviteli sebességet biztosít, a Neul két nagyságrenddel nagyobbat. A SIGFOX erőssége a nagyobb hatótáv, a Telensáé a heterogén hálózatban is alkalmazhatóság. Más szabványú érzékelőkhöz is rendelkezik interfészekkel.

Ahogy a fogyasztók megismerik az intelligensotthon-megoldások és az IoT előnyeit, úgy fog robbanásszerűen növekedni a népszerűségük. Nem lesz ritka, hogy számos vezeték nélküli protokoll fog párhuzamosan működni az otthonokban. Pontosan úgy, ahogy a mai mobiltelefonok is zökkenőmentesen támogatják – akár egy időben – a 3G/4G, WiFi és Bluetooth kapcsolatot.

A mai IoT-szegmensben még nem dúl ádáz harc az egyeduralomért. Nem egyetlen vezeték nélküli technológia fog teret hódítani. Sokkal inkább az látszik, hogy a fejlesztők megtalálják a vezeték nélküli kommunikációk megfelelő kombinációját, hogy az IoT-termékeik zökkenőmentesen kommunikáljanak egymással, a kapcsolódó hálózatokkal, a felhőszolgáltatásokkal és nem utolsósorban a felhasználóval.

Ennek a kombinációnak az összeállításához ad segítséget a tanulmány. Áttekintést nyújt az elérhető megoldásokról, és az ábrák segítségével megkönnyíti a megfelelő hatótávú és adatátviteli sebességű protokollok kiválasztását.

Hivatkozások

[1] K. Kovács és J. Katona, „Vezeték nélküli protokollok az Internet of Things világában," *elektro-net.hu,* [Online]. Elérhető: www.elektro-net.hu/konstruktor/6641-vezetek-nelkuli-protokollok-az-internet-of-things-vilagaban (Letöltve: 2018. 02. 20.)

[2] Zs. Haig és I. Várhegyi, *Hadviselés az információs hadszíntéren.* Budapest: Zrínyi Kiadó, 2005.

[3] I. Négyesi, „Informatikai rendszerek és alkalmazások a védelmi szférában," *Dunaújvárosi Főiskola Közleményei,* (2010), In: Szerk.: Cserny László Informatika Korszerű Technikái Konferencia 2010. Dunaújváros: Dunaújvárosi Főiskola (DF), 2010. pp. 1–10.

[4] S. Szőlősi, „Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében," Doktori (PhD) értekezés, ZMNE, Budapest, 2008.

[5] M. S. Mahmoud and A. Mohamad, A Study of Efficient Power Consumption Wireless Communication Techniques/ Modules for Internet of Things (IoT) Applications, *Advances in Internet of Things (AIT)*, vol. 6, no. 2, 2016. január. [Online]. DOI: https://doi.org/10.4236/ait.2016.62002

[6] I. Négyesi, „Die überprüfung der voraussetzungen von COTS systemen," *Hadmérnök,* 7. évf. 2. sz. pp. 371–376, 2012.

[7] I. Négyesi, „COTS rendszerek alkalmazási lehetőségeinek vizsgálata," *Hadtudományi Szemle,* 4. évf. 4. sz. pp. 111–116, 2011.

[8] NFC Forum, „Technical Specifications" *NFC Forum,* [Online]. Elérhető: https://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/ (Letöltve: 2018. 03. 11.)

[9] D. M. Dobkin and T. Wandinger, "A Radio-Oriented Introduction to RFID–Protocols, Tags and Applications," *High Frequency Electronics,* August, pp. 32–46. 2005. [Online]. Elérhető: www.highfrequencyelectronics.com/Aug05/HFE0805_RFIDTutorial.pdf

[10] "Your Health & Fitness Partner, What is ANT+," *thisisant.com,* [Online]. Elérhető: www.thisisant.com/consumer/ant-101/what-is-ant/ (Letöltve: 2018. 03. 21.)

[11] "Radio Versions," *bluetooth.com,* [Online]. Elérhető: www.bluetooth.com/bluetooth-technology/radio-versions (Letöltve: 2018. 03. 26.)

[12] Enocean alliance, "EnOcean Wireless Standard," *Enocean alliance* [Online]. Elérhető: www.enocean-alliance.org/what-is-enocean/enocean-wireless-standard/ (Letöltve: 2018. 03. 29.)
[13] "What is thread?" *threadgroup.org,* [Online]. Elérhető: www.threadgroup.org/What-is-Thread/Overview (Letöltve: 2018. 04. 06.)
[14] "WirelessHART – How it works," *fieldcommgroup.org,* [Online]. Elérhető: https://fieldcommgroup.org/technologies/hart/hart-technology (Letöltve: 2018. 04. 09.)
[15] Zigbee Alliance, "Zigbee is the only complete IoT solution, from the mesh network to the universal language that allows smart objects to work together," *Zigbee Alliance,* [Online]. Elérhető: www.zigbee.org/zigbee-for-developers/zigbee-3-0/ (Letöltve: 2018. 04. 08.)
[16] Z-wave, "Smart home products with Z-Wave inside work together, use just one app to connect and control your smart home from anywhere." Z-wave, [Online]. Elérhető: www.z-wave.com/learn (Letöltve: 2018. 04. 09.)
[17] "Why DASH7?" [Online]. Elérhető: dash7-alliance.org/product/dash7-alliance-protocol-specification-v1-2/ (Letöltve: 2019. 10. 11.)
[18] S. Sendra, P. Fernandez, C. Turro, and J. Llorret, "IEEE 802.11a/b/g/n Indoor Coverage and Performance Comparison," In Proc. 6th International Conference on Wireless and Mobile Communications, 2010. DOI: https://doi.org/10.1109/icwmc.2010.46
[19] A. B. Flores, R. E. Guerra, E. W. Knightly, P. Ecclesine, and S. Pandey, "IEEE 802.11af: a standard for TV white space spectrum sharing," *IEEE Communications Magazine*, vol. 51, no. 10. 2013. DOI: https://doi.org/10.1109/MCOM.2013.6619571 https://ieeexplore.ieee.org/document/6619571/ (Letöltve: 2018. 04. 16.)
[20] S. Aust, R. V. Prasad, and I. G. M. M. Niemegeers, "IEEE 802.11ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi," In Proc. IEEE International Conference on Communications (ICC), 2012. DOI: https://doi.org/10.1109/ICC.2012.6364903
[21] WiSun Alliance, "Comparing IoT Networks at a Glance," *WiSun Alliance,* [Online]. Elérhető: www.wi-sun.org/index.php/tcwp-en/file (Letöltve: 2018. 04. 22.)
[22] Zigbee Alliance "JupiterMesh® Neighborhood Area Network (NAN) Announced," *Zigbee Alliance,* [Online]. Elérhető: www.zigbee.org/jupitermesh-neighborhood-area-network-nan-announced/ (Letöltve: 2018. 04. 24.)
[23] "The Evolution of Mobile Technologies: 1G, 2G, 3G, 4G LTE," [Online]. Elérhető: www.qualcomm.com/media/documents/files/download-the-evolution-of-mobile-technologies-1g-to-2g-to-3g-to-4g-lte-qualcomm.pdf (Letöltve: 2018. 04. 27.)
[24] GSMA, "Long Term Evolution for Machines: LTE-M," *GSMA,* [Online]. Elérhető: www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/ (Letöltve: 2018. 05. 05.)
[25] LoRa Alliance, "About the LoRaWAN™ Specification," *LoRa Alliance,* [Online]. Elérhető: https://lora-alliance.org/lorawan-for-developers (Letöltve: 2018. 05. 08.)
[26] Cisco, "Positive Train Control," *Cisco,* [Online]. Elérhető: www.cisco.com/c/dam/en_us/solutions/industries/docs/trans/ptc-aag.pdf (Letöltve: 2018. 05. 10.)
[27] Sigfox, "Sigfox Technology Overview," *Sigfox,* [Online]. Elérhető: www.sigfox.com/en/sigfox-iot-technology-overview (Letöltve: 2018. 05. 13.)

[28] Neul, “News,”*Neul,* [Online]. Elérhető: http://neul.com/neul-news/ (Letöltve: 2018. 05. 15.)
[29] “Mass scale smart city technology,” [Online]. Elérhető: www.telensa.com/ (Letöltve: 2018. 05. 17.)

HADMÉRNÖK
FÓRUM
14. évfolyam (2019) 3. szám 147–158.
DOI: 10.32567/hm.2019.3.12

Forgó Veronika[1]

A campylobacteriosis detektálási lehetőségei az élelmiszer- és vízbiztonsági rendszerekben

Possibilities of Detecting Campylobacteriosis in Food and Water Safety Systems

Az élelmiszerek által közvetített megbetegedések átfogó ismerete elengedhetetlen, hogy a nemzet biztonságát megóvjuk. A biztonság megőrzéséhez ismerni kell az előre nem látható, illetve a szándékos jogellenes magatartások veszélyforrásait, és rendelkezni kell a megfelelő védelmi stratégiával a potenciális és a bekövetkezett események elhárításához. Az élelmiszer- és vízbiztonsági rendszerek jelenleg nem alkalmasak az élelmiszerfertőzések, köztük a Campylobacter-fertőzés korai felismerésére. Léteznek különböző módszerek, amelyek megkönnyítik a kórokozók identifikálását, azonban ezek nem korszerűek, nem az élelmiszerbiztonsági monitorozó- és védelmi rendszerek részét képezik. Szükséges monitoring kidolgozása, hogy megfelelő módon kezelhető legyen a felmerülő kockázat.

Kulcsszavak: élelmiszerbiztonság, vízbiztonság, campylobacteriosis, védelmi rendszerek, biztonságtechnika

The comprehensive knowledge of food-borne diseases is indispensable to protect the nation's security. For one's safety, one must know the dangers of unforeseen or deliberate unlawful behaviour and provide for the prevention of potential and occurring events with an appropriate defence strategy. The food and water safety systems are currently not suitable for early detection of food infections, including Campylobacter infection. Nowadays, there are various methods to facilitate the identification of pathogens, however, they are not modern, not part of food safety monitoring and protection systems. It is necessary to develop monitoring to manage the risk in an appropriate manner.

Keywords: food safety, water safety, campylobacteriosis, protection systems, safety

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: vercsy.forgo@gmail.com, ORCID: https://orcid.org/0000-0002-0188-9898

Bevezetés

A biztonság, mint fogalom megjelenik az élet minden területén, ahogyan a biztonságtechnikában, úgy az élelmiszer- és vízbiztonságban egyaránt.

A biztonság megőrzéséhez, ismerni kell az előre nem látható, illetve a szándékos jogellenes magatartások veszélyforrásait, és rendelkezni kell a potenciális- és a bekövetkezett események elhárításához megfelelő védelmi stratégiával.

Felmerül a kérdés, hogy mennyire ismerjük az élelmiszerbiztonságot veszélyeztető élelmiszer-fertőzéseket és azok hatásait?

Napjainkra, az élelmiszerkereskedelem globalizálódásával egyidejűleg az élelmiszer és ivóvíz eredetű fertőzések a gyártóhelytől és közvetlen vonzáskörzetétől eltérő régiókban történő megjelenésének kockázata megnövekedett. Szinte havi rendszerességgel jelennek meg hírek egy-egy minőségileg nem megfelelő, esetleg egészségre kockázatot jelentő élelmiszeripari termék polcokról történő kivonásáról. Az egyre hatékonyabb élelmiszeripari minőségbiztosítási rendszerek bevezetése ellenére is előfordulhat biológiailag szennyezett termék piacra kerülése, ami a globális élelmiszeripari láncok hálózatán keresztül széles néptömegeket érhet el, egymástól távol eső területeken, veszélyeztetve az egészséget, valamint gazdasági károkat okozva a gyártónak. A különböző súlyosságú megbetegedéseket okozó kórokozók belekerülhetnek élelmiszereinkbe technológiai hiba, gondatlanság, illetve szándékos magatartás révén is.

A biológiai fegyverek, mint a *szándékos jogellenes magatartások veszélyforrásai,* nem csak az emberek és állatok megbetegítésére képesek, hanem anyagok, élelmiszerek és a víz fertőzésére, károsítására is alkalmasak. Előfordulásukat tekintve lehetnek élő kórokozók vagy azok anyagcseretermékei, illetve harcanyagok [1].

Míg a kormányok és a biztonsági ügynökségek jobban szervezettek a fenyegetés ellen mint valaha, a világ még mindig felkészületlen a bioterrorista-támadásra. A terroristák tudatában vannak annak, hogy biológiai fegyver egyetlen alkalmazása több ezer áldozatot követelhet. Egyesek úgy vélik, hogy az ilyen fegyverek létrehozásának technikai nehézségei miatt a pusztító támadás esélye jelenleg kicsi, de akár egy betegség szándékos terjesztésének következményei is katasztrofálisak lehetnek [2].

A biológiai fegyverek nemcsak a lakosság megbetegítésére alkalmasak, hanem gyengíthetik a haderő képességét, nagy kiterjedésű fertőzésre képesek, komplikációt okozhatnak a mezőgazdaságban és az iparban, valamint a gyógyszer-, a víz- és az élelmiszerellátásban. Ezáltal fontos ismerni a biológiai fegyverként használható patogének[2] megjelenési formáit, emellett az általuk okozott tüneteket, hogy a biológiai veszély minél gyorsabban elhárítható legyen. Az elmúlt 10 évben megnőtt az élelmiszerek és víz által okozott Campylobacter-fertőzések száma az EU-ban és Magyarországon egyaránt.

A Katasztrófavédelmi Tudományos Tanács 2012. évi pályázata kapcsán egy tanulmány figyelmet fordít az élelmiszer és víz eredetű problémákra, amelyben már akkor megemlíti a Campylobacter-fertőzések fontosságát is [3]. A Centers for Disease Control and Prevention (CDC), illetve a 61/1999. (XII. 1.) a biológiai tényezők hatásának

[2] Kórokozó.

kitett munkavállalók egészségének védelméről szóló EüM rendelet is kiemelt figyelmet fordít a kórokozóra, a Campylobactert, B, azaz 2-es kategóriájú bioterrorista szerek közé sorolja [4], [5].

Megfogalmazódik, hogy a napjainkban alkalmazott biztonságtechnikai rendszerek mennyire korszerűek, a fertőzések korai felismerésére és megelőzésére alkalmasak-e?

Az élelmiszerellátás ilyen jellegű kritikus pontjai lehetnek a növénytermesztés, az állattenyésztés létesítményei, emellett a vízellátás bázisai és létesítményei, valamint a logisztikai és kereskedelmi folyamatok, a termőföldtől az asztalig [6].

Jogi szabályozás

Az élelmiszerjog általános elveiről és követelményeiről szóló 178/2002/EK rendelet értelmében, élelmiszer minden olyan termék, amely feldolgozott, részben feldolgozott vagy feldolgozatlan anyagot tartalmaz, emberi fogyasztásra szánják és emberek fogyasztják. A rendelet kitér arra, hogy az élelmiszer definíció magába foglalja az italt, a rágógumit, valamint azokat az anyagokat, amelyeket az előállítás, feldolgozás és kezelés során szándékosan a termékhez adtak, köztük a vizet is [7]. Magyarországon a 4/1998. (XI. 11.) EüM rendelet az élelmiszerekben előforduló mikrobiológiai szennyeződések megengedhető mértékéről kimondja, hogy a Campylobacter-fajok, fogyasztásra kész élelmiszerek esetén a vizsgált mintákban nem fogadhatók el, határértékük 0 [8].

A vízbiztonság, akárcsak az élelmiszerbiztonság meghatározzák az egészség minőségét. A 201/2001. (X. 25.) Korm. rendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről kimondja, hogy a víz, abban az esetben ivóvíz minőségű, ha nem tartalmaz a szabályozásoknak megfelelő mennyiségben vagy koncentrációban olyan anyagot, mikroorganizmust, parazitát, fizikai, kémiai anyagot, amely veszélyeztetné az egészséget [9]. A vizet érintő minőségromlás esetén, a vízhasználat korlátozása mellett, szükséges a fertőző forrást eltávolítani, fertőtlenítést és vízkezelést végezni, emellett a megelőzés lehetőségeire nagyobb hangsúlyt fektetni. A 201/2001. (X. 25.) Korm. rendelet szabályozásai leginkább a kémiai határértékeket érintik, a mikrobiológiai határértékek jelenleg nem térnek ki a Campylobacter-speciesek által okozott fertőzések követelményeire, vízminőségi paramétereire és feltételeire. Amennyiben az élelmiszerekből és a vízből származó fertőzések száma az évek folyamán tovább emelkedik, állásfoglalásom szerint, rendeletmódosításra lesz szükség, amelyben kitérnek a Campylobacte-fajok határértékeire is.

A campylobacteriosis humán vonatkozásai

A minőségi termékfeldolgozás hiánya, a nem megfelelő higiéniai eljárások, a népesség immunrendszerének változása, a nemzetközi kereskedelem, illetve a fokozott gyógyszerfogyasztás, amely a rezisztencia kialakulásához vezetett, szignifikánsan[3] megnövelte az élelmiszerekből eredő humán megbetegedések kialakulásának a számát.

[3] Jelzésértékűen.

Az utóbbi években Európában jelentős a Campylobacter-fajok által okozott kórképek megjelenése. Az emberi megbetegedést okozó fajok, a C. jejuni, a C. coli, a C. fetus és a C. upsaliensis [10]. A legtöbb élelmiszerfertőzés kialakulását a Campylobacter jejuni és a Campylobacter coli okozza. A Campylobacter-fajok többsége megtalálható a normál humán flórában, az emlősállatok, mint a kutya, a macska, a rágcsálók, illetve a madarak kommenzális[4] bélflórájában. A terjedés módja történhet közvetlen módon emberről emberre, vagy közvetetten, szennyezett tárggyal, piszkos kézzel, közvetítő közeg útján, vízzel vagy élelmiszerrel (tej, baromfi-, sertéshús, saláta, burgonya, paprika, gomba, petrezselyem). A baktérium a szaporodásához 3–5%-os oxigént és 2–10%-os szén-dioxidot igényel. A baktérium szaporodási hőmérsékleti optimuma 42°C [11], [12].

Az otthonokban nem megfelelően tartott háziállatok, mint a kutya és a macska, valamint az állatsimogatás után és étkezés előtt nem kellően megtisztított kéz is lehet a fertőzés forrása a betegség kialakulásához. A baktérium a vízbe és az élelmiszerbe ürülékkel is bekerülhet. A helytelen személyi higiénés szokások – emellett a nem megfelelő hőkezelés – és a konyhatechnológia az, ami a legnagyobb problémát okozza. A betegség lappangási ideje 3–5 nap, amelyet követően koleraszerű tünetek alakulnak ki, véres-vizes hasmenéssel, lázzal és hányással, ritkán vakbélgyanús tünetekkel. Rizikófaktornak[5] tekinthetők az immunszupresszált[6] betegek, az idősek, a gyermekek, és a várandós nők.

A campylobacteriosis alakulása 2013 és 2017 között Európában és Magyarországon

Az EFSA[7] és az ECDC[8] adatait feltárva az elmúlt 10 évben folyamatosan növekedett a campylobacteriosis megjelenése [13], [14]. Az elmúlt 5 év adatait tekintve 2013–2017-ig mind az Európai Unió országaiban, mind Magyarországon ingadozó a Campylobacter-speciesek által okozott élelmiszerfertőzések száma.

Az 1. táblázat adatai azt mutatják, hogy 2013–2017-ig, az utolsó vizsgált 5 évben, mekkora volt a népességszám az Európai Unióban, illetve Magyarországon. Megfigyelhető, hogy míg az EU-ban a népességszám szignifikáns emelkedést mutat, ehhez képest Magyarországon ez a szám folyamatosan csökken [15].

[4] Normál baktériumflóra tagja.
[5] Betegség kialakulásának valószínűségét növelő tényező.
[6] Immunrendszer védekezőképessége csökkent.
[7] European Food Safety Authority – Európai Élelmiszerbiztonsági Hatóság.
[8] European Centre for Disease Prevention and Control – Európai Betegségmegelőzési és Járványvédelmi Központ.

1. táblázat

Népességszám 2013–2017-ig az EU-ban és Magyarországon (a szerző szerkesztése [16] alapján)

	Népességszám (fő)	
	Európai Unió	**Magyarország**
2013	505 163 008	9 908 798
2014	507 011 330	9 877 365
2015	508 540 103	9 855 571
2016	510 277 177	9 830 485
2017	511 521 686	9 797 561

A 2. táblázat adataiból megfigyelhető, hogy az EU-ban 2014 és 2015 között, valamint 2016 és 2017 között kismértékben csökkent a campylobacteriosisos esetek száma. Elmondható, hogy Magyarországon ugyanezen időszak alatt is csökkenés figyelhető meg a fertőzés kialakulásának esetszámában. Azonban összességében, a 2013-as adatokhoz képest a 2017-es adatok esetszámai nagymértékű növekedést mutatnak.

2. táblázat

Megerősített élelmiszer-eredetű campylobacteriosisban megbetegedettek száma Európában és Magyarországon (beleértve a vízzel terjedő járványokat is) (a szerző szerkesztése [13] alapján)

	Megerősített élelmiszer eredetű megbetegedések száma (fő) (campylobacteriosis)	
	Európa	**Magyarország**
2013	214 710	7247
2014	236 818	8444
2015	232 134	8342
2016	246 917	8556
2017	246 158	7840

Az átlag népességszám és a megbetegedések középértékének meghatározása mind az EU-ban, mind Magyarországon a 3. táblázat adatai alapján történt.

Az Európai Unió népességszámát tekintve az 5 év vonatkozásában az átlag népességszám S1 = 508 502 661 fő volt. Ez idő alatt az élelmiszer-eredetű Campylobacter-fertőzések számának középértéke az EU-ban, amely tartalmazza a vízzel terjedő fertőzések számát is, S2 = 235 347 fő.

Magyarország átlag népességszáma 2013–2017-ig S3 = 9 853 956 fő volt. Az élelmiszer és víz által okozott fertőzések számának középértéke Magyarországon, erre az időszakra vonatkoztatva, S4 = 8086 fő.

3. táblázat

Módszer a középérték meghatározásához a népesség és a fertőzések számát tekintve
[a szerző szerkesztése]

Megnevezés	Érték	Átlag (S1, S2, S3, S4)
Népességszám EU	E1, E2, E3, E4, E5	$S1 = \frac{E1 + E2 + E3 + E4 + E5}{5}$
Megbetegedés szám EU	M1, M2, M3, M4, M5	$S2 = \frac{M1 + M2 + M3 + M4 + M5}{5}$
Népességszám Magyarország	e1, e2, e3, e4, e5	$S3 = \frac{e1 + e2 + e3 + e4 + e5}{5}$
Megbetegedés szám Magyarország	m1, m2, m3, m4, m5	$S4 = \frac{m1 + m2 + m3 + m4 + m5}{5}$

Ahol:

- Népességszám EU: E1, E2, E3, E4, E5 megegyezik az 1. táblázat soronkénti népességszámával az Európai Unióban, évenkénti lebontásban.
- Megbetegedés szám EU: e1, e2, e3, e4, e5 megegyezik az 1. táblázat soronkénti népességszámával Magyarországon, évenkénti lebontásban.
- Népességszám Magyarország: M1, M2, M3, M4, M5 megegyezik a 2. táblázat soronkénti megerősített élelmiszer-eredetű megbetegedések számával az EU-ban, évenkénti lebontásban
- Megbetegedés szám Magyarország: m1, m2, m3, m4, m5 megegyezik a 2. táblázat soronkénti megerősített élelmiszer-eredetű megbetegedések számával Magyarországon, évenkénti lebontásban.

A népességszám középértékének és a fertőzésszámok középértékének hányadosaként megállapítható, hogy az Európai Unióban, átlagosan, 2013 és 2017 között minden 2161. személy betegedett meg élelmiszer vagy víz által okozott Campylobacter-fertőzésben.

Hazánkban, a vizsgált időszakban átlagosan minden 1219. ember betegedett meg valamely Campylobacter-kórokozó által.

Ahogyan Magyarországon, úgy a szomszédos EU-országokban is megfigyelhető az ingadozás, a fertőzés számának kialakulásában a kórokozóra vonatkozóan. Mindent összevetve azonban a 2013-as campylobacteriosis esetszámhoz képest 2017-ben

nagymértékű a változás a fertőzést illetően a szomszédos országok tekintetében. A jövőben, amennyiben ez a tendencia növekedést mutat, felmerül a kérdés, hogy milyen megelőző intézkedéseket kell bevezetni annak érdekében, hogy elkerülhető vagy csökkenthető legyen azok kialakulása.

Élelmiszer- és vízbiztonsági vonatkozások

Az élelmiszerek által közvetített megbetegedések átfogó ismerete elengedhetetlen. Ugyanis az élelmiszer- és ivóvízszennyezéssel nemcsak a termékminőség romlik, hanem könnyen irreverzibilis egészségkárosodás okozható. Az Európai Unió országaiban az élelmiszer-előállítás szabályai közötti különbségek magukkal vonják azt, hogy a Magyarországra importált és a Magyarországon gyártott élelmiszerek biztonsága és minősége sokszor kifogásolt. Az áruk szabad áramlásával előtérbe kerültek a bio- és az új élelmiszerek,[9] amelyek a magyarországi gyártókat háttérbe szorították. Ahhoz, hogy a hazai gyártók fenn tudják tartani a versenyképességüket a forgalmazott termékekkel szemben, sokszor minőségromlást von maga után. A szándékosság a másik fontos tényező, amelyet figyelembe kell venni, ebben az esetben fokozott egészségkockázattal kell számolni.

A víz a populáció számára nélkülözhetetlen élelmiszerforrás. Népegészségügyi szempontból kulcsfontosságú, hogy megfelelő minőségben használják fel, mind önmagában fogyasztva, mind élelmiszer-, gyógyszer-előállításnál, valamint konyhatechnológiai eljárások során. A vízbázisok különböző járványok terjesztőközegei lehetnek, amennyiben nem biztonságos azok üzemeltetése és védelme, nem megfelelő a vízkezelési technológia. Elengedhetetlen, hogy a fogyasztásra szánt víz fertőtlenítése megfelelő hatékonyságú legyen, az ne okozzon a fogyasztónak reverzibilis/irreverzibilis egészségkárosodást. A kontaminált víz, amelynek kontaminációja eredhet gondatlanságból, szándékosságból, az egyik legnagyobb járványügyi veszélyforrás, mivel a szennyezéssel vagy mérgezéssel romlik az élelmiszer-alapanyagok és az élelmiszerek minősége. Az ivóvíz biológiai, mikrobiológiai, fizikai, kémiai biztonságát meg kell őrizni. Ahhoz, hogy ez megfelelően működjön, szükségszerű feltárni a víz biztonságát érintő potenciális kockázatokat és veszélyeket. Ezáltal, valamint a feltárt adatok alapján, értékelni kell az egészségkárosító hatások kockázatát és azok élelmiszerbiztonsági kapcsolatát, valamint szükséges rangsorolni a feladatokat, kidolgozni a megelőzés és az egészségkárosító hatások könnyebb azonosítását, monitorozását és csökkentésének módozatait.

Élelmiszerbiztonsági, -védelmi rendszerek

Az élelmiszerek biztonságának megőrzéséhez ismerni kell az előre nem látható, szándékos jogellenes magatartások veszélyforrásait, és rendelkezni kell a potenciális és a bekövetkezett események elhárításához megfelelő védelmi stratégiával.

[9] Azok az élelmiszerek, amelyeket nem fogyasztottak az EU-ban 1997 előtt.

Az első védvonal a mechanikai védelem. Ahhoz, hogy a termék biztonságát megőrizzük, hangsúlyt kell fektetni a termelőobjektum és a termék védelmére. A második az elektronikai jelzőrendszerek, mint riasztórendszerek, felügyeleti rendszerek, higiénés kapuk rendszerei, monitorozó rendszerek, elektronikus áruvédelmi rendszerek, amelyek kiemelt fontosságúak az élelmiszerbiztonság területén. A beléptetőrendszer biztosítja, hogy egy adott területre csak az arra illetékes személy léphessen be. Itt megtörténik a személy azonosítása és a jogosult személy áthaladásának biztosítása is egyben [17], [18].

Az élelmiszervédelmi rendszerek következő eleme a higiéniai kapu. A higiénés kapukon akkor engedélyezett a technológiai tér felé az áthaladás, ha mindkét kéz átesett a fertőtlenítésen, illetve a csizmamosás is megtörtént, amelyhez egy beépített infraérzékelő vezérli a tisztítókeféket, illetve indítja be a fertőtlenítőszer és a víz elegyének adagolását. A gyártótér elhagyása is ugyanezen a metóduson keresztül történik, azonban itt kihagyható a kézfertőtlenítés.

Az áruvédelmi rendszerek között megemlítendő a fémdetektor, amely a fémszennyezett termékek azonosítására alkalmas. A fémdetektor a kiegyensúlyozott tekercsek hurokelvén működik, amelynek egyik formáját az ömlesztett vagy csomagolt termékek esetén a szállítószalaghoz kapcsolva helyeznek el. A rendszer fém eredetű, rozsdamentes vagy mágnesezhető szennyezéskor jelez és leállítja a szállítószalagot [19]. Az áruvédelmi rendszerek között fontos kiemelni a röntgensugaras vizsgálórendszereket is, amelyek alkalmasak a csomagolt, az üvegedényes, illetve a konzervdobozos termékek vizsgálatára. A termékvizsgálati rendszerek az üveg-, a fém-, a műanyag- és a csontmaradványok azonosítását végzik a technológiai folyamat kezdeti szakaszán, hogy minél hamarabb detektálható legyen a hibás termék [20], [21].

Az objektumvédelem magába foglalja a vízbiztonsági rendszerek védelmét is. Ezáltal meg kell őrizni a közműszolgáltatások, mint az ivóvíz- és csatornahálózat biztonságát. A természeti eredetű veszélyek mellett a civilizációs és a technológiai veszélyek, valamint az ártó jellegű cselekmények azok, amelyek veszélyforrást jelentenek. Ezért a kritikus infrastruktúrák védelmére olyan technológiát kell kialakítani, ahol könnyen felismerhetők a behatolási kísérletek, emellett megelőzhetők a biológiai és mikrobiológiai ágensekkel való előreláthatatlan vagy szándékos fertőzések. Ehhez a védelmi rendszer megtervezésekor fel kell tárni a potenciális veszélyeket, meg kell határozni a veszélyforrásokat, majd kockázatelemzést kell végezni, végül ki kell alakítani a védelmi tevékenységet [22].

Felmerül a kérdés, hogy a jelenleg alkalmazott, veszélyes anyagok jelenlétét monitorozó rendszerek mennyire korszerűek? Képesek az újonnan megjelenő fertőzések detektálására és a biológiai jellegű veszélyhelyzet azonosítására?

Az élelmiszerbiztonsági rendszerek jelenleg nem alkalmasak az élelmiszerfertőzések, köztük a Campylobacter-fertőzés korai felismerésére. Léteznek gyorstesztek és real time módszerek, amelyek megkönnyítik a kórokozók identifikálását,[10] azonban ezek nem korszerűek, nem automatizáltak, nem az élelmiszerbiztonsági monitorozó- és védelmi rendszerek részét képezik.

[10] Azonosítás.

A vízbázisok területén a monitorozórendszerek ellenőrzési pontjai és mérései magukba foglalják a mezőgazdasági, az állattartási és egyéb emberi tevékenységre kiterjedő szennyezőforrásokat. Az ellenőrző tevékenység magába foglalja a fizikai, kémiai, biológiai vízvizsgálatokat a nyersvíz és a tisztított víz vonatkozásában. Ebben az esetben is, ahogyan az élelmiszervizsgálatoknál, ellenőrző vizsgálatokkal validálják,[11] ha a vizsgált paraméterek megfelelőek. Eltérés esetén, ha elérik a kritikus határértéket, be kell avatkozni a rendszerbe, így elkerülhetők a vízminőségi károk [23]. A víz által közvetített fertőzések tovaterjedésének megelőzésére a vízbiztonság védelmi rendszerei között szerepelnek az UV-berendezések, amelyek feladata a fertőtlenítés és a kórokozó mikroorganizmusok elpusztítása. A vízbiztonsági rendszerek sem automatizáltak működésüket tekintve, ugyanis a mikrobiológiai vizsgálatokat előre meghatározott pontokon végzik, ellenőrző mérésekkel, ezáltal küszöbölhető ki egy esetleges veszély [24].

Következtetések

Az élelmiszerbiztonságot fokozni hivatott intézkedések és minőségbiztosítási rendszerek, valamint a gondos ellenőrzési tevékenység, sorra hozzájárulnak egészségünk védelméhez, biztosítva az élelmiszerrel terjedő fertőzések minimalizálását. A megfelelően alkalmazott biztonságtechnikai eszközök képesek hatékonyan támogatni az élelmiszerbiztonsági törekvéseket, azonban azok háttérrendszereinek technológiai fejlődése újabb és újabb feladatokat teremt számunkra a biztonsági lehetőségek növelése mellett. A közelmúltban az okoseszközök világméretű terjedése lehetővé teszi, hogy nemcsak az otthonunkban, hanem az ipari termelés bármely területén fokozzuk a termék- és a vagyonbiztonságot.

A nemzet biztonságának megőrzése szempontjából rendkívüli jelentőségű a betegségek megelőzése, a kóros állapotok, valamint a víz- és az élelmiszerfertőzések korai felismerése.

Komoly veszélyt jelenthetnek a biológiai anyagokhoz történő hozzáférési jogosultsággal bíró illetékes személyek részéről elkövetett visszaélések is, amelyek ellen a biológiai biztonság, a biológiai védelem egyes komponensei mellett, szándékos visszaéléssel szembeni védelem elemeit is fejleszteni kell, beleértve a bioetikát is [25].

A biztonságtechnikai műveletek a tevékenységük során kiemelt figyelmet fordítanak a szabotázs megakadályozására. A megelőzés és az információ hangsúlyozza az elővigyázatosság értékjellegét. Szükséges olyan monitoring kidolgozása, amely segítséget nyújt abban, hogy megfelelő módon kezelhető legyen a felmerülő kockázat. Nagyobb hangsúlyt kell fektetni a védelmi és megfigyelőrendszerek hatékonyságára, annak érdekében, hogy egy esetleges krízishelyzet minél könnyebben elhárítható legyen.

Szükséges azt megvizsgálni, hogy az új technológiák mennyire alkalmasak arra, hogy a víz- és élelmiszerbiztonságot fokozzuk. Ehhez felül kell vizsgálni a jelenleg alkalmazott technológiákat, meg kell vizsgálni az újonnan fellépő kockázatokat, be kell vezetni az új technológiai megoldásokat, illetve meg kell határozni a kritikus

[11] Érvényesít.

szabályozási pontokat. Az alkalmazást követően bizonyítani kell, hogy az új technológiák alkalmasak az élelmiszerbiztonság növelésére és a felmerülő veszélyek és kockázatok csökkentésére.

Hivatkozások

[1] G. Faludi, „A biológiai fegyver és az ellene való védelem – biovédelem (orvosi) kérdései," Doktori (PhD) értekezés, ZMNE, Bolyai János Hadmérnöki Kar, Hadmérnöki Doktori Iskola, Budapest, 2012. [Online]. DOI: https://doi.org/10.17625/NKE.2012.001

[2] R. Pellérdi és T. Berek, "Redefining the CBRN risk assessment," *AARMS,* vol. 8, no. 1, pp. 159–172, 2009. [Online]. Elérhető: www.researchgate.net/publication-/268394543_A_A_R_M_S_Redefining_the_CBRN_risk_assessment (Letöltve: 2019. 03. 18.)

[3] Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság, „A XXI. század biztonsági kihívásainak sajátosságai és megválaszolásuk lehetőségei – Humán egészségügyi kihívások vizsgálata a klímaváltozásban – kiemelt figyelemmel a járványügyi kritikus szektorokra," *Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság,* 2012. [Online]. Elérhető: www.katasztrofavedelem.hu/letoltes/tudomany/Klima.pdf (Letöltve: 2019. 02. 06.)

[4] Massachusetts Department of Public Health, "Massachusetts Department of Public Health Guide to Surveillance, Reporting, and Control: Campylobacteriosis," Bureau of Infectious Disease and Laboratory Sciences, 2016. [Online]. Elérhető: https://webcache.googleusercontent.com/search?q=cache:I6r5HqXfC1oJ:https://www.mass.gov/files/documents/2016/08/qf/campylobacter-enteritis.rtf+&cd=2&hl=hu&ct=clnk&gl=hu (Letöltve: 2019. 02. 16.)

[5] 61/1999. (XII. 1.) EüM rendelet a biológiai tényezők hatásának kitett munkavállalók egészségének védelméről, [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?-docid=99900061.EUM (Letöltve: 2019. 02. 16.)

[6] A. Horváth, „Az élelmiszerellátási lánc kritikus infrastruktúrái, terrorfenyegetettségének jellemzői," *Hadmérnök,* 4. évf. 2. sz. pp. 437–449, 2009. [Online]. Elérhető: http://hadmernok.hu/2009_2_horvatha.pdf (Letöltve: 2019. 02. 16.)

[7] Az Európai Parlament és A Tanács 178/2002/EK rendelete az élelmiszerjog általános elveiről és követelményeiről, az Európai Élelmiszerbiztonsági Hatóság létrehozásáról és az élelmiszerbiztonságra vonatkozó eljárások megállapításáról, [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32002R0178. (Letöltve: 2019. 02. 13.)

[8] 4/1998. (XI. 11.) EüM rendelet az élelmiszerekben előforduló mikrobiológiai szennyeződések megengedhető mértékéről. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=99800004.EUM (Letöltve: 2019. 02. 13.)

[9] 201/2001. (X. 25.) Korm. rendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről, [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A0100201.KOR (Letöltve: 2019. 02. 13.)

[10] T. Pál, „Az orvosi mikrobiológia tankönyve," *tankonyvtar.hu,* 2013. [Online]. Elérhető: www.tankonyvtar.hu/en/tartalom/tamop425/2011_0001_524_Mikrobiologia/ch03s03.html (Letöltve: 2019. 02. 14.)
[11] T. Deák, G. Kiskó, A. Maráz és C. Mohácsiné Farkas, „Élelmiszer-mikrobiológia," *tankonyvtar.hu,* 2006. [Online]. Elérhető: www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_521_Elelmiszer-mikrobiologia/ch04s02.html#id540276 (Letöltve: 2019. 02. 14.)
[12] N. Schweitzer, „Termofil Campylobacter-fajok genetikai és epidemiológiai jellemzése" Doktori (PhD) értekezés, Szent István Egyetem Állatorvos-tudományi Doktori Iskola, 2011. [Online]. Elérhető: www.huveta.hu/bitstream/handle/10832/169/SchweitzerNoraDissertation.pdf;jsessionid=18ECF44C20643F6F499683033757C2E5?sequence=1 (Letöltve 2019. 02. 18.)
[13] EFSA, ECDC, "The European Union summary report on trends and sources of zoonoses, zoonotic agents and food-borne outbreaks in 2017," *EFSA, ECDC,* 19. November 2018. [Online]. DOI: https://doi.org/10.2903/j.efsa.2018.5500
[14] EFSA, ECDC, "The European Union summary report on trends and sources of zoonoses, zoonotic agents and food-borne outbreaks in 2013," *EFSA, ECDC,* 28 January 2015. [Online]. DOI: https://doi.org/10.2903/j.efsa.2015.3991 Elérhető: https://ecdc.europa.eu/sites/portal/files/media/en/publications/Publications/EU-summary-report-trends-sources-zoonoses-2013.pdf (Letöltve: 2019. 02. 13.)
[15] K. S. H., „Eurostat statikus táblák – Népességszám (2008–2019)," *K. S. H.,* [Online]. Elérhető: www.ksh.hu/docs/hun/eurostat_tablak/tabl/tps00001.html (Letöltve: 2019. 02. 13.)
[16] Eurostat, "Population on 1 January," *Eurostat,* [Online]. Elérhető: https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tps00001 (Letöltve: 2019. 02. 13.)
[17] L. Berek, T. Berek és L. Berek, „A biztonság, az őrzés és a védelem, valamint a biztonságtechnika értelmezése – Az őrzés és a védelem formái, valamint azok komplex alkalmazása", pp. 14–68 in *Személy- és vagyonbiztonság,* Budapest: Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Óbudai Egyetem, ÓE-BGK-3071, 2016. p. 173.
[18] T. Berek, „Adaptációs lehetőségek az éghajlatváltozás következményeihez a biztonságtechnikában a közszolgálat területén", in *Adaptációs lehetőségek az éghajlatváltozás következményeihez a közszolgálat területén,* J. Berek, T. Csurgai, A. Farkas, L. Földi, L. Halász, H. Hegedűs, J. Hornyacsek, L. Kohut, R. Kuti, A. Márton, J. Mika, M. Monosi, és Á. Restás szerk., Budapest: Nemzeti Közszolgálati Egyetem, 2019, pp. 625–686. [Online]. Elérhető: https://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/11183/adaptacios_lehetosegek_az_eghajlatvaltozas_kovetkezmenyeihez_a_kozszolgalat_teruleten.pdf?sequence=1&isAllowed=y (Letöltve: 2019. 03. 30.)
[19] Marker Bt., „A fémdetektálás alapjai," [Online]. Elérhető: www.muszeroldal.hu/measurenotes/femdetektalas.pdf (Letöltve: 2019. 03. 21.)

[20] Mettler Toledo, „Safeline röntgenes termékvizsgálati rendszerek," *Mettler Toledo,* [Online]. Elérhető: www.mt.com/hu/hu/home/products/Product-Inspection_1/safeline-x-ray-inspection.html?cmp=sea_10010614&bookedkeyword=r%C3%B6ntgeng%C3%A9pek&matchtype=b&adtext=59673687307&placement=&network=g (Letöltve: 2019. 02. 18.)
[21] L. Kálmán, „A csomagvizsgálati röntgenberendezés alkalmazási lehetősége," *Hadmérnök,* 10. évf. 3. sz. pp. 15–31, 2015. [Online]. Elérhető: http://hadmernok.hu/153_02_kalmanl.pdf (Letöltve: 2019. 02. 18.)
[22] L. I. Rácz és T. Berek, „Vízbázis, mint nemzeti létfontosságú rendszerelem védelme," *Hadmérnök,* 8. évf. 2. sz. pp. 120–133, 2013. [Online]. Elérhető: www.hadmernok.hu/132_11_berekt_rli.pdf (Letöltve: 2019. 02. 18.)
[23] T. Berek és Zs. Dávidovits, „Vízbiztonsági terv szerepe az ivóvízellátás biztonsági rendszerében," *Hadmérnök,* 7. évf. 3. sz. pp. 14–25, 2012. [Online]. Elérhető: http://hadmernok.hu/2012_3_davidovits_berek2.pdf (Letöltve: 2019. 02. 18.)
[24] T. Berek és R. Pellérdi, „ABV (CBRN) kihívásokra adott válaszlépések az EU-ban," *Bolyai Szemle,* 20. évf. 2. sz. pp. 55–72, 2011. [Online]. Elérhető: http://hdl.handle.net/11410/1922 (Letöltve: 2019. 03. 18.)
[25] Zs. Dávidovits és L. Berek, „Vízbázisvédelem, ivóvízbiztonság," *Bolyai Szemle,* 21. évf. 2 sz. pp. 27–38, 55–72, 2012.

HADMÉRNÖK
FÓRUM
14. évfolyam (2019) 3. szám 159–166.
DOI: 10.32567/hm.2019.3.13

Németh József Lajos[1]

Stratégiai kommunikáció – szakirodalmi áttekintés

Strategic Communication – Literature Review

Napjainkra a „stratégiai kommunikáció", mint kifejezés és sajátos gondolkodásmód és eljárási rendszer divatos szakkifejezéssé vált a nemzetközi kapcsolatokban csakúgy, mint a hadtudományokban. A szerző a cikkben bemutatja és csoportosítja az eddigi kutatásai során felkutatott forrásokat, azzal céllal, hogy elősegítse a témához kapcsolódó további kutatásokat és kiindulási pontokat nyújtson a téma könnyebb értelmezéséhez.

Kulcsszavak: **stratégiai kommunikáció, szakirodalom, áttekintés**

Today, "strategic communication" as a term and a specific way of thinking and procedural system has become a "buzzword" in international relations, as well as in military sciences. In this article, the author presents and groups the literature resources that have been researched so far in order to facilitate further research on the topic and provide a starting point for a more readable interpretation of the topic.

Keywords: **strategic communication, literature, overview**

Bevezetés

Jelen cikk tárgya az üzleti életből eredeztethető stratégiai kommunikáció, amelynek – mint komplex elgondolásnak és eljárási rendszernek – megjelenése a biztonságpolitikában (így a hadtudományokban is) a 2001. szeptember 11-ei terrortámadásokat követően vált markánssá oly módon, hogy annak rendkívüli jelentőségét mind az Észak-Atlanti Szerződés Szervezete (North Atlantic Treaty Organization – a továbbiakban: NATO) mind pedig az Európai Unió (European Union – a továbbiakban: EU) felismerte

[1] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, egyetemi docens, e-mail: nemeth.jozsef@uni-nke.hu, ORCID: https://orcid.org/0000-0003-2819-7362

és hangsúlyozza mind szervezeti, mind eljárási értelemben.[2] A téma szomorú, de fontos időszerűségét adják ugyanakkor a hidegháború vége (1989–1991) óta lezajlott úgynevezett „kis háborúk" tapasztalatai, valamint a nemzetközi terrorizmus elleni küzdelemben – különösen 2001. szeptember 11-e óta – megjelent hadviselési módok és formák, amelyekben kiemelt szerephez jutottak a szembenálló felek célkitűzéseinek erősítésére és/vagy gyengítésére törekvő kommunikációs stratégiák. A szerző az alábbiakban az általa eddig elvégzett vonatkozó kutatások alapján adja közre az általa legfontosabbnak vélt hazai és nemzetközi forrásokat, és egyúttal kutatásmódszertani segítséget is igyekszik biztosítani a témában elmélyülni szándékozók számára [1: 167.].

Bár az elmúlt években számos kísérlet történt a stratégiai kommunikáció definiálására, azonban ezek tartalmát illetően kevés egyetértés mutatkozik *a szakértők* között; pontosabban *abban értenek egyet, hogy miben nem értenek egyet* az egyes tartalmi kérdéseket illetően. A vonatkozó szakirodalom tüzetes áttanulmányozása után és a különböző meghatározási kísérleteket összevetve érdemes kiemelni Peter O'Malley felfogását, aki üzleti szempontok alapján közelítette meg a fogalmat: a stratégiai kommunikáció „olyan vállalati és intézményi kommunikációs elemeket és/vagy eszközöket használ, amelyek a »cél- vagy kulcshallgatóság« (célcsoport) körében kedvező véleményt alakít(hat)nak ki a vállalati és intézményi célkitűzések lehető leghatékonyabb elérése érdekében" [1: 167.], [2].

Magyar nyelvű források

Hadtudományi szakcikkek, könyvek: csekély eredmény

Az elvégzett forráskutatás alapján jelenleg (2019. április) az állapítható meg, hogy a stratégiai kommunikációval foglalkozó magyar nyelvű hadtudományi szakcikkek, tanulmányok alig találhatók, azonban megjegyzendő, hogy a mégis felleltek döntően a szerző korábbi munkái közé sorolandók [1], [3]. Mivel a stratégiai kommunikáció kapcsolódik az információs hadviseléshez, így ebben a témában magyar nyelvű forrást keresve meg kell említenünk Haig Zsolt *Információs műveletek a kibertérben* című könyvét, amiben többször is említi a könyv szerzője a témakört [4]. Ugyanakkor megállapítható, hogy a lehetséges szakirodalmi források között a stratégiai kommunikációt hadtudományi megközelítés alapján tárgyaló könyv (monográfia) jelenleg még nem található.

Katalógusok és adatbázisok

Kutatásmódszertani szempontból fontos és hasznos (de napjainkban szinte már kötelező) az online katalógusok és adatbázisok használata, amelyek nem csak munkánkat

[2] Lásd: a NATO Stratégiai Kommunikáció kiválósági Központját (NATO Strategic Communications Centre of Excellence), amit 2014-ben hoztak létre a lettországi Rigában [22], vagy az EU által 2015-ben létrehozott úgynevezett Kelet Stratégiai Kommunikáció Munkacsoportot (EU East StratCom Task Force) [23].

könnyíthetik meg, hanem újabb érdekes összefüggésekkel, akár eredményekkel is szolgálhatnak.

A Nemzeti Közszolgálati Egyetem online elérhető OPAC könyvtári katalógusában [24] a „stratégiai kommunikáció" kifejezés címben történő – magyar nyelvű – keresésre több találatot is kapunk, amelyek nagyban árnyalják a korábban bemutatott kissé lehangoló képet, hiszen ily módon 5 tétellel is találkozunk, amelyek közül:

- egy szlovák nyelvről magyarra fordított könyv – rendkívüli tudományossággal és olvasóbarát felfogással – gazdasági (vállalkozási) megközelítésből vizsgálja a témakört [5],
- egy, 2010-ben a Budapesti Corvinus Egyetemen elkészített szakdolgozat a magyar felsőoktatási intézmények stratégiai kommunikációját vizsgálja [6],
- egy tanulmány pedig a „szervezeti vakság" szempontjából vizsgálja a témakört [7],
- további két publikáció (tanulmány) pedig a hadtudományi területhez kapcsolható.

A Nemzeti Közszolgálati Egyetem online elérhető könyvtári adatbázisaiban az alábbi eredményeket kapjuk az adatbázisok szerint történt keresésben [25]:

- Az Akadémiai Kiadó által nyújtott Magyar Elektronikus Referenciaművek Szolgáltatásában végzett „stratégiai kommunikáció" kulcsszavakra történt, bármilyen szövegrészben megjelenő keresés 153 (!) találatot eredményezett, amelyek megoszlása[3] [26] az orvostudományoktól kezdve a társadalomtudományokon át egészen a műszaki tudományokig megfigyelhető. A korábban megfogalmazottokat figyelembe véve meglepőnek mondható, hogy az *Orvosi Hetilap* című periodika 72 közleményében található meg a fenti kulcsszó.

  Az orvostudományoknál maradva meg kell említenünk Forgács József publikációját, aki a *Magyar Pszichológiai Szemle* 2000. évi 2–3. számában az érzelem, és a stratégiai kommunikáció kapcsolatát vizsgálja [8]. Munkájában a szívességkérés eltérő hangulati hátterét értékeli, és rámutat az eltérő stratégiák maximalizálásának eltérő formáira. Forgács a jó vagy rossz hangulatú kísérleti személyekkel folytatott kísérletek során igazolja azt a modellt, amely szerint az előbbi hangulatú személyek „kevésbé udvariasan" kérnek, mint azok, akik rossz hangulatban vannak, és ezek az egyéni stratégiákban is kimutathatók.

  Az Arcanum Digitális Tudománytár online adatbázisában a „stratégiai kommunikáció" teljes szövegű keresésére történt beállítás már 6360 (!) találatot eredményezett, amelyek megoszlása a különböző, folyóiratok, gyűjtemények vonatkozásában széles lefedettséget mutat [27].

  Tárgyalt témánkhoz közvetlenül kapcsolva említést kell tennünk Csizmadia Sándor az ideológia, a kommunikáció és a terrorizmus összefüggéseit tárgyaló 1987-ben megjelent publikációjáról, amelyben a szerző több, napjainkban is időszerű megállapítást tesz [9]. A középkor sajátos kommunikációs viszonyait tárgyalja (azokat megengedett és tiltott kategóriákba sorolva) Novák Veronika az *Aetas* folyóirat oldalain 2002-ben megjelent tanulmányában [10].

[3] Az úgynevezett MERSZ az alap- és referenciaművek folyamatosan bővülő elektronikus gyűjteménye.

Angol nyelvű források

Az idegen – elsősorban angol – nyelvű források feltárása a bevezetésben említett okok miatt is kézenfekvő, azonban a könnyebb eligazodás és felhasználás érdekében érdemes ezeket is csoportosítanunk.

Kézikönyvek és monográfiák

A Routledge brit akadémiai könyvkiadó által 2015-ben először megjelentetett *Stratégiai kommunikáció kézikönyve* bevezetőjében az áll, hogy a kiadó az abban bemutatott tanulmányokat a tárgyalt téma multi- és interdiszciplináris megközelítése alapján adja közre [11].

Christopher Paul katonai, valamint biztonságpolitikai szempontok alapján tárgyalja részletesen könyvében a stratégiai kommunikáció eredetét, valamint egyes koncepcióit és a kapcsolódó vitákat [12].

A stratégiai kommunikáció történelmi hátterét mutatja be az első világháború kontextusában Jonathan Reed Winkler, aki munkájában kiemelt figyelmet szentel a kommunikáció műszaki megközelítésének, így a kiemelkedően fontos tenger alatti összeköttetés stratégiai fontosságának [13].

A téma történelmi (és az oly fontos nyilvános diplomáciai) szempontú megközelítését mutatja be a Rhonda Zaharna által szerkesztett kiadvány [14].

A hatalom és meggyőzés kiindulópontjaira helyezkedve a stratégiai kommunikáció „művészetét" tárgyalja könyvében James P. Farwell [15].

Bár tárgyalt témánkhoz csak közvetve kapcsolódik, mégis érdemes említést tennünk Elizabeth Losh *VirtualPolitik* című könyvéről, amelyben a szerző részletesen bemutatja az amerikai kormányzati retorikát a virtuális térben kiemelten olyan témákra koncentrálva, mint a háborúk, a botrányok, illetve a különböző katasztrófák [16].

Patrick Sellers pedig a stratégiai kommunikáció egyes jellemzőiről ír, könyvében az amerikai kongresszus működésébe betekintést nyújtva [17].

A hatékony üzleti stratégiai kommunikáció tervezéhez nyújt segítséget könyvében Laurie J. Wilson és Joseph D. Ogden [18].

A megfelelő narratíva kiemelkedő fontosságát tárgyalja katonai megközelítésből Mari K. Eder [19].

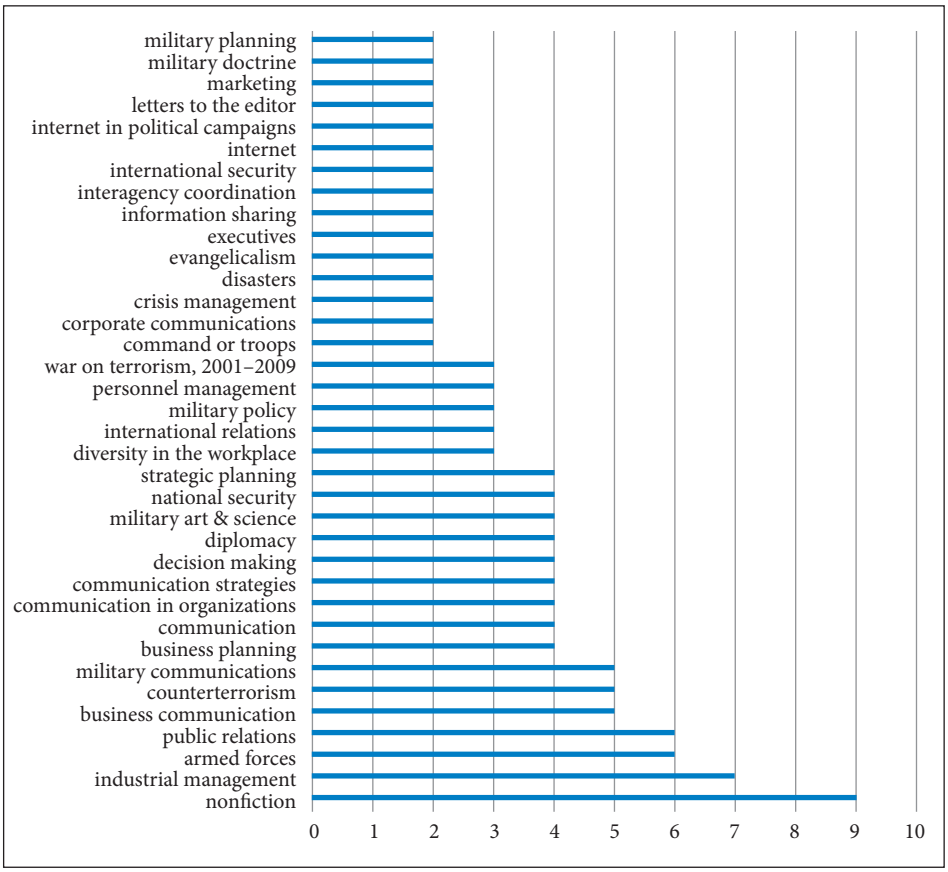
A stratégiát vizsgálja az információs és befolyásolási kampányok kontextusában Jarol B. Mannheim [20].

A kommunikáció történetében bekövetkezett markáns változásokat, azokat „forradalmaknak" nevezve ad átfogó képet számunkra Bill Kovarik [21].

Angol nyelvű cikkek és publikációk feltérképezése adatbázis segítségével

A Metropolitan Egyetem Könyvtárában elérhető EBSCO-adatbázisban 2019. január 29-én elvégzett angol nyelvű források tudománymetriai vizsgálata, a „strategic

communication" kulcsszóra, valamint teljes szövegre történő, minden forrást figyelembe vevő keresés alapján mintegy 95 találatot eredményezett.



1. ábra

A tudománymetriai vizsgálat eredményei [Metropolitan Egyetem Könyvtára által biztosított EBSCO-adatbázis, az adatfelvétel dátuma: 2019. január 29.]

Az 1. ábrán jól látható, hogy azok számos témakört ölelnek fel, ugyanakkor a biztonságpolitikai és katonai jellegű megközelítések dominálnak. Fontos hangsúlyoznunk, hogy az adatbázis az 1998–2015 közötti időszakra mutatott találatokat, így arra következtethetünk, hogy 1998 előtt nem jelentek meg a stratégiai kommunikációt közvetlenül vagy jelentős mértékben tárgyaló publikációk.

A nemzetközi szervezetek honlapjain található források

Az eddigi kutatások alapján jól kimutatható és bizonyítható, hogy a stratégiai kommunikációt számos nemzetközi szervezet is fontosnak tartja. Vizsgálódásunk szempontjából

megemlítendő az Észak-Atlanti Szerződés Szervezete (NATO) és az Európai Unió (EU), amelyek felismerték és hangsúlyozzák a stratégiai kommunikáció fontosságát mind szervezeti, mind eljárási értelemben. A NATO korábban már említett Kiválósági Központ weboldalán (www.stratcomcoe.org) egy online könyvtárban az alábbi csoportosításban találhatjuk meg a vonatkozó információkat:

- könyvek;
- kutatási és más típusú jelentések;
- periodikák;
- szakpolitikai dokumentumok;
- kézikönyvek;
- cikkek.

Az Európai Unió dedikált szervezetének honlapján (https://euvsdisinfo.eu/) a vonatkozó híreken kívül értékeléseket és egy további olvasásra javasolt gyűjteményt találunk, de az oldalon feliratkozhatunk egy hetente érkező e-mail-csatornára is.

Számunkra fontos és megemlítendő nemzetközi szervezet az ENSZ, ami ugyancsak foglalkozik a kérdéskörrel: A szervezet erre vonatkozó honlapján az alábbi témákra vonatkozóan találhatunk megfelelő információkat [28]:

- béke és biztonság;
- fenntartható fejlődés;
- Palesztina, dekolonizáció és emberi jogok;
- Afrika.

Végezetül fontos megjegyeznünk, hogy az Európai Biztonsági- és Együttműködési Szervezettel kapcsolatban(EBESZ-OSCE) is találhatunk annak a stratégiai kommunikációra vonatkozó tevékenységével összefüggő információkat.

Következtetések

A fentiek alapján kimutatható, hogy napjainkban már létezik a stratégiai kommunikáció hazai és nemzetközi szakirodalma, azonban ez előbbi még némi lemaradásban van a nemzetközi trendekhez és eredményekhez képest. Levonható az a következtetés is, hogy a stratégiai kommunikáció témaköreit nemcsak történeti megközelítésben, hanem módszertani szempontok alapján is vizsgálhatjuk, továbbá nem elhanyagolhatók annak személyi (emberi) tényezői csakúgy, mint a műszakiak is. A szerző határozott meggyőződése az, hogy a téma további magyar nyelvű feldolgozásához elegendő forrás és kiindulási pont áll rendelkezésre.

„Ez a publikáció az Emberi Erőforrások Minisztériuma Únkp-18-4-Nke-107 kódszámú Új Nemzeti Kiválóság Programjának és Az MTA Bolyai János Kutatói Ösztöndíj támogatásával készült."

This article is Supported BY the ÚNKP-18-4-NKE-107 New National Excellence Program of the Ministry of Human Capacities and Supported by the János Bolyai Scholarship of the Hungarian Academy of Sciences.

Hivatkozások

[1] L. J. Németh, „A stratégiai kommunikáció interdiszciplináris megközelítésben," *Hadtudományi Szemle,* 12. évf. 1. sz. pp. 167–174, 2019. DOI: https://doi.org/10.32563/hsz.2019.1.11

[2] P. O'Malley, "Strategic Communication Planning," [Online]. Elérhető: http://real.mtak.hu/25066/1/131.pdf (Letöltve: 2013. 01. 15.)

[3] J. L. Németh, „A (stratégiai) kommunikáció és a háború kapcsolata napjainkban," *Hadtudomány,* 23. évf. 1–2. sz. pp. 129–139, 2013.

[4] Zs. Haig, *Információs műveletek a kibertérben.* Budapest: Dialóg Campus Kiadó, 2018.

[5] S. Kassay szerk., *Vállalat és vállalkozás III. kötet: Stratégiai kommunikáció.* Budapest: Gondolat, 2015.

[6] Á. Szilágyi, *A magyar felsőoktatási intézmények stratégiai kommunikációja napjainkban.* Budapest: BCE KIK Kommunikációs Tanszék, 2010.

[7] V. Both, „Stratégiai kommunikáció és szervezeti vakság – amikor nem látjuk a fától az erdőt," in *Konvergencián innen és túl – digitális jövőképek:* [írások az internet és a média világából], Á. Csermely, Szerk.: Budapest: Prime Rate Kft., 2004.

[8] J. Forgács, „Az érzelem és a stratégiai kommunikáció: az érzelem hatása a szóbeli kérések megfogalmazására és értelmezésére," *Magyar Pszichológiai Szemle,* 55. évf. 2–3. sz. pp. 145–178, 2000. DOI: https://doi.org/10.1556/MPSzle.55.2000.2-3.1

[9] S. Csizmadia, „Ideológia, kommunikáció, terrorizmus," *Valóság,* 30. évf. 1. sz., pp. 38–48, 1987.

[10] V. Novák, „Gyanús viszonyok: Megengedett és tiltott kommunikáció a középkor végi Franciaországban," *Aetas,* 17. évf. 4. sz. pp. 29–51, 2002.

[11] D. Holtzhausen és A. Zerfass, szerk., *The Routledge Handbook of Strategic Communication.* New York, London: Routledge, 2015. DOI: https://doi.org/10.4324/9780203094440

[12] C. Paul, *Strategic Communication: Origins, Concepts, an Current Debates.* Santa Barbara, California: Praeger, 2011.

[13] J. R. Winkler, *NEXUS: Strategic Communications and American Security in World War I.* Cambridge, Massachusetts, London, England: Harvard University Press, 2008. DOI: https://doi.org/10.4159/harvard.9780674033900

[14] R. Zaharna, *Battles to Bridges: US Strategic Communication and Public Diplomacy After 9/11*. UK: Palgrave Macmillan, 2010. DOI: https://doi.org/10.1057/9780230277922_2

[15] J. P. Farwell, *Persuasion and Power: The Art of Strategic Communication*. Washington, D.C.: Georgetown University Press, 2010.
[16] E. Losh, *VirtualPolitik: An Electronic History of Government Media-making in a Time of War, Scandal, Disaster, Miscommunication, and Mistakes.* England: The MIT Press, 2009. DOI: https://doi.org/10.7551/mitpress/7966.001.0001
[17] P. Sellers, *Cycles of Spin: Strategic Communication in the U. S. Congress.* New York: Cambridge University Press, 2009. DOI: https://doi.org/10.1017/CBO9780511642289
[18] L. J. Wilson and J. D.Ogden, *Strategic Communications: Planning for effective Public Relations & Marketing.* Dubuque, Iowa, USA: Kendall/Hunt Publishing Company, 2008.
[19] M. K. Eder, *Leading the Narrative: The Case for Strategic Communication.* Annapolis, Maryland: Naval University Press, 2011.
[20] J. B. Mannheim, *Strategy in Information and Influence Campaigns.* New York, London: Routledge, 2010.
[21] B. Kovarik, *Revolutions in Communication.* London, Oxford, New York: Bloomsbury Publishing Inc., 2017.
[22] Nato Strategic Communications Centre of Excellence, "Annual Report," *Nato Strategic Communications Centre of Excellence,* 2014. [Online]. Elérhető: www.stratcomcoe.org/report-period-1-october-2014-31-december-2014, (Letöltve: 2019. 02. 01.)
[23] European Union External Action, "Questions and Answers about the East StratCom Task Force," [Online]. Elérhető: https://eeas.europa.eu/headquarters/headquarters-Homepage/2116/questions-and-answers-about-east-stratcom-task-force_en, (Letöltve: 2019. 02. 01.)
[24] Nemzeti Közszolgálati Egyetem, „Egyetemi Központi Könyvtár és Levéltár elektronikus katalógusa," *Nemzeti Közszolgálati Egyetem,* [Online]. Elérhető: www.uni-nke.hu/konyvtar/katalogus, (Letöltve: 2019. 03. 31.)
[25] Nemzeti Közszolgálati Egyetem, „Online adatbázisok," *Nemzeti Közszolgálati Egyetem,* [Online]. Elérhető: www.uni-nke.hu/konyvtar/adatbazisok, (Letöltve: 2019. 03. 31.)
[26] Nemzeti Közszolgálati Egyetem, „Online adatbázisok," *Nemzeti Közszolgálati Egyetem,* [Online]. Elérhető: www.uni-nke.hu/konyvtar/adatbazisok (Letöltve: 2019. 03. 31.)
[27] Arcanum Digitális Tudománytár, [Online]. Elérhető: https://adtplus.arcanum.hu/hu/ (Letöltve: 2019. 03. 31.)
[28] United Nations, "Strategic Communications" United Nations, [Online]. Elérhető: www.un.org/en/sections/departments/department-global-communications/strategic-communications/index.html, (Letöltve: 2019. 03. 31.)