BOLYAI SZEMLE

2016/1. SZÁM

A NEMZETI KÖZSZOLGÁLATI EGYTEM KATONAI MŰSZAKI TUDOMÁNYÁGI FOLYÓIRATA

XXV. évfolyam, 2016/1. szám

BOLYAI SZEMLE

A NEMZETI KÖZSZOLGÁLATI EGYETEM
KATONAI MŰSZAKI TUDOMÁNYÁGI FOLYÓIRATA

A borítón Prof. dr. Berek Lajos ny. ezredes, Mednyánszky László-díjas szobrászművész *Bolyai János, a hadmérnök* című szobra látható

A lapban megjelenő írásokat lektoráltatjuk. A közlésre szánt tanulmányokat a bolyaiszemle@uni-nke.hu címre kérjük megküldeni magyar és angol címmel, valamint magyar és angol összefoglalóval ellátva.

Kiadja: NKE Szolgáltató Nonprofit Kft.
Felelős kiadó: Hegyesi József ügyvezető igazgató
Tördelés: Tordas és Társa Kft.
ISSN 1416-1443

Tartalom

E számunk szerzői

BALOG KÁROLY, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola

ESTÓK SÁNDOR, PhD (hadtudomány, logisztika), közgazdász, logisztikai magiszter, nyugdíjas alezredes

FATALIN LÁSZLÓ, Nemzeti Közszolgálati Egyetem, HHK KLI Természettudományi Tanszék, egyetemi docens

HAJDU VERONIKA, Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, doktorandusz

HORVÁTH ISTVÁN, Nemzeti Közszolgálati Egyetem, HHK KLI Természettudományi Tanszék, tanszékvezető egyetemi tanár

KOMJÁTHY LÁSZLÓ, Nemzeti Közszolgálati Egyetem, óraadó ny. egyetemi docens

KÓRÓDI GYULA, dr., tű. alezredes, Nemzeti Közszolgálati Egyetem, Katasztrófavédelmi Intézet, Katasztrófavédelmi Műveleti Tanszék, egyetemi docens

KOVÁCS ZOLTÁN, PHD, Nemzeti Közszolgálati Egyetem, egyetemi docens, alezredes, HHK Műveleti és Támogató Tanszék

SOLYMOSI JÁNOS, okleveles villamosmérnök, okleveles munkavédelmi szakmérnök, Óbudai Egyetem, Biztonságtechnikai Doktori Iskola, doktorandusz

TAR CSABA, Nemzeti Közszolgálati Egyetem, hadnagy, HHK KLI Haditechnikai Tanszék, gyakorlati oktató

TEKNŐS LÁSZLÓ, dr., Nemzeti Közszolgálati Egyetem, Katasztrófavédelmi Intézet Katasztrófavédelmi Műveleti Tanszék, egyetemi tanársegéd

VÉCSEY ALEXANDRA, Óbudai Egyetem, Biztonságtudományi Doktori Iskola, doktorandusz

VEDÓ ATTILA, rendőr őrnagy, Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, doktorandusz

VÉG RÓBERT LÁSZLÓ, dr., Nemzeti Közszolgálati Egyetem, HHK Katonai Logisztikai Intézet, Haditechnikai Tanszék, egyetemi docens

Hajdu Veronika

A befolyásolás művészete mint a pszichológiai műveletek és a marketing eszköze

A pszichológiai műveletek (PSYOPS) célja, hogy jól megtervezett módon, megfelelő információk birtokában, különböző eszközökkel és módszerekkel befolyásolja egy meghatározott célközönség érzelmeit, attitűdjét annak érdekében, hogy a műveleti célok kivitelezése sikeressé váljon. A modern hadviselés lehetőséget teremtett arra, hogy a szemben álló felek széles spektrumú megközelítést alkalmazhassanak az ellentétek és konfliktusok rendezésére. Mindennek az alapja a befolyásolás, amely nem különbözik napjainkban sem a Clausewitz által meghatározott állásponttól, azaz akaratunk rákényszerítése az ellenségre. Tanulmányomban többek között a befolyásolás szerepét vizsgálom meg, kitérve a kommunikációban és a média területén játszott szerepére is, a marketingkommunikációs szempontok figyelembevételével.

Kulcsszavak: pszichológiai műveletek, marketingkommunikáció, média, befolyásolás

Bevezetés

Nem kérdés már, hogy a 21. században mekkora jelentősége van annak, hogy ki milyen minőségű és mennyiségű információt birtokol. Az új típusú társadalom, a globalizáció megköveteli magának a szabad információáramlást földön, vízen, vagy akár levegőben egyaránt, legyen az normál polgári, civil élethelyzetben, vagy épp egy katonai művelet során. A technológia fejlettségével és folyamatos fejlődésével pedig lehetővé is válik a minél szélesebb körű és gyorsabb információhoz való jutás képessége.

A katonai képességeket jelentősen befolyásolja bizonyos információk birtoklása, vagy épp annak megakadályozása, hogy az az ellenfél birtokába jusson. [1] Éppen ezért rendkívül fontos az információs fölény megszerzése és megtartása, ezáltal a szemben álló fél információs képességeinek korlátozása, hiszen megfelelő információk nélkül a katonai vezető nem tud objektív, pontos döntést sem hozni.

Amikor megtörténik az információ cseréje, akkor elindul egy kommunikációs körfolyamat, melynek során a feladótól eljut a vevőig az ismeretanyag. Az információ ismeret, az ismeret tudás, a tudás pedig hatalom! [2; 20.] Az információ, szerepét tekintve egy ter-

melési tényező, hiszen ugyanúgy van értéke és piaca, adni, venni lehet, aki pedig birtokolja azt, vezető pozícióba kerül. [3; 44.]

Az információs műveletek egy az Amerikai Egyesült Államokban 2012-ben kiadott katonai doktrína (JP 3–13) szerint minden olyan információval kapcsolatos képesség integrált alkalmazása, amelyek segítségével befolyásolhatja, megzavarhatja, leronthatja, vagy épp korlátozhatja a szemben álló fél döntéshozatali képességét, illetve megvédi saját hasonló képességeit. [4] A pszichológiai műveletek az információs műveletek támadó fajtájú tevékenységében kap létjogosultságot, míg a PSYOPS részét képező ellenpropaganda a védelmi képességeket erősíti. [3; 187.]

2010-ben a PSYOPS megnevezése Military Information Support Operations lett, ami magyarul Katonai Információs Támogató Műveletekként fordítható le.1 Azaz olyan katonai művelet, amely az információs műveletek céljainak kivitelezésében működik közre oly módon, hogy segíti a katonai tevékenységek elfogadtatását, valamint biztonságos műveleti környezetet teremt. Teszi ezt a megfelelő célcsoportok kiválasztásával és beazonosításával, a kultúrák, szubkultúrák tekintetbevételével, és minden egyéb tényező figyelembevételével, melyek nem megfelelő kezelése esetén gátolhatják az üzenet célba juttatását. [5]

A tanulmány során bemutatásra kerül a pszichológiai műveletekhez és a marketinghez kapcsolódó olyan képesség, amely a műveleti célok kivitelezéséhez szervesen járul hozzá olyan hatástényezők2 segítségével, melyek a kommunikáció és az ahhoz – napjainkra különösen jellemző – kapcsolódó média szerepkörén keresztül érvényesülnek. [3; 189.]

A kommunikáció a befolyásolás köntösében

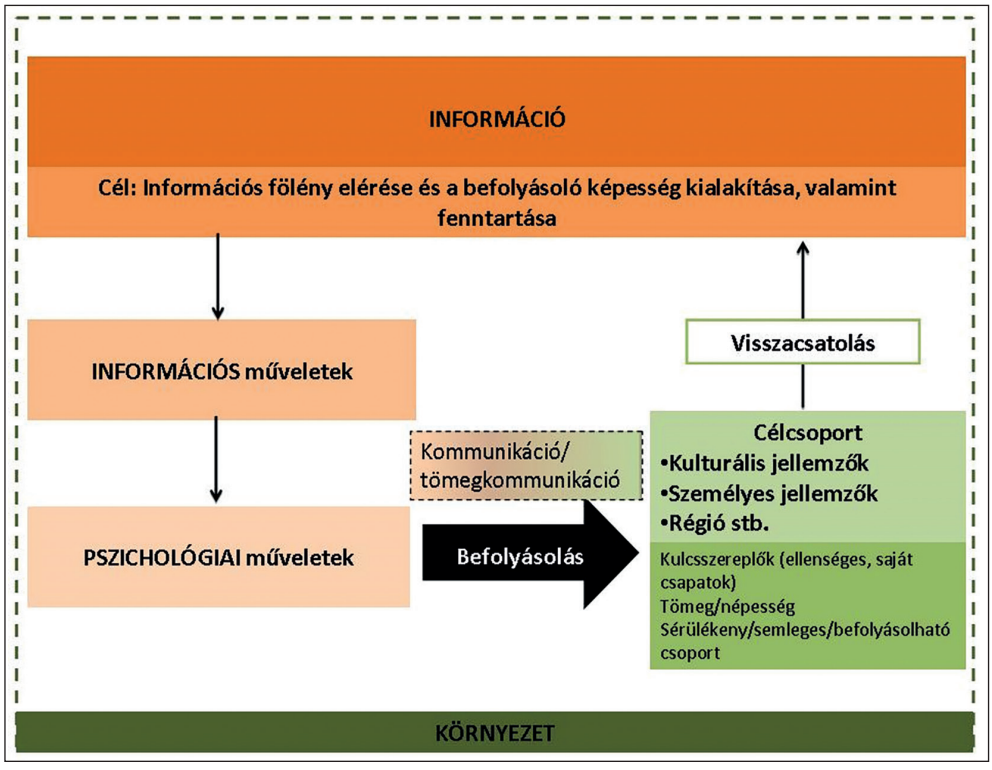
A célcsoportok elérésénél vitathatatlanul fontos tényező a kultúra, hiszen a szokások, normák révén ugyanazt a tényt az eltérő társadalmi rétegek/célcsoportok, illetve egyének más és más értelmezési kontextusba helyezik. Ebből kifolyólag gyakran egyértelműnek szánt üzenetek másképp kerülnek kódolásra a befogadók által. Így a kultúrák közti különbségek kommunikációs különbségként is jelentkezhetnek. [6; 59.]

Az információtovábbítás, azaz a kommunikáció során döntő fontosságú szerephez jut az üzenettovábbítás módja, illetve az, hogy milyen egyéb információval együtt jut el a befogadó(k)hoz. Azzal, hogy mit hangsúlyozunk az üzenetben, már meghatároztuk, hogy milyen szempont szerint kell értelmezni az üzenet tárgyát (azaz a tényt), vagyis befolyásoltuk a célcsoport viszonyulását egy adott irányba. Mind a pszichológiai műveletek, mind a civil életben a marketingkommunikáció és annak eszközeként a tömegkommuni-

1 A pszichológiai műveleteknek számos elnevezése van: PSYOPS, PSYWAR, lélektani hadviselés, MISO, propagandatevékenység, de az egyszerűség kedvéért a tanulmány során a pszichológiai műveletek, illetve ennek rövidített változata, a PSYOPS kerül használatra. 2010 óta a MISO (Military Information Support Operations) nevet viseli.

2 Ilyen hatástényező lehet: tájékoztatás, befolyásolás, meggyőzés stb.

káció arra törekszik tevékenysége során, hogy célcsoportját befolyásolva elérje a vezetők által kitűzött célokat olyan módon, hogy az attitűdváltozásban és viselkedésmódosulásban teljesedjen ki. A befolyásolás egy olyan erő, illetve képesség, amelynek révén hatást gyakorolunk a másik félre (célcsoportra). [7] Nincs olyan szituáció egyik oldalon sem, ahol ne a helyzet irányítására törekednének a felek. A közlő célja minden esetben az, hogy a befogadót rávegye valamilyen – a műveleti céloknak megfelelő – cselekedetre, de azt nem nyílt módon teszi. Ennek a folyamatnak a leegyszerűsített bemutatása az 1. ábra.



1. ábra: Az információ szerepe a befolyásolás folyamatában (saját szerkesztés [2] alapján)

Az információ megléte nagyban hozzájárul a katonai műveletek egyik sikerességét meghatározó részeredményéhez, azaz a célcsoport – amelyeknél különböző szempontok érvényesülnek – befolyásolásához. A befolyásolás képessége nagyban függ bizonyos attribútumoktól, amelyek sok esetben kulturális módon épülnek ki, illetve be a csoportokba. [8; 100.] Ezek a csoportok a műveleti célok szerves részét képezik, ugyanis az eseményekhez történő viszonyulásuk nagyban meghatározza a sikeres művelet végrehajtását. A kulcsszereplők révén a műveleti terület biztonságosabbá tehető – saját csapat moráljának és harci szellemének emelésével, a szemben álló fél csapatainak demoralizálásával –, a tömeg, népesség irányultságának sikeres módosítása révén pedig akadálytalan munkafo-

lyamat mehet végbe. Mindez egy meghatározott környezetben megy végbe, ami vagy akadályozhatja, vagy megkönnyítheti a befolyásolás eszközének, a pszichológiai műveletek módszerének, a tömegkommunikációnak a hatékonyságát. A további sikeres tevékenység lényege pedig a visszacsatolás, vagyis az új információk révén kialakult ismeretanyag, annak alkalmazása és felhasználása járul hozzá ahhoz, hogy kialakulhasson az információs fölény és a befolyásoló képesség fenntartható legyen. A lényege pedig, hogy egy körfolyamatként folyamatosan új információk segítsék a katonai műveleti tevékenységet.

Jellemző, hogy minden közleményben implicit információk vannak elrejtve, amelyek a csoport ítéletét a saját célok irányába befolyásolják. [6; 169.] Ez nehezen átlátható, hiszen, tárgyilagosak ezek az üzenetek és a kommunikációs csatornák is nagyban hozzájárulnak ahhoz, hogy őszintének és igaznak tűnjenek. Ilyen „őszinte" információtovábbításra alkalmas mód a word of mouth, azaz a szájreklám, amely esetében láncként terjed a közlemény. Itt barát barátnak, ismerős ismerősnek, csoport csoportnak, közösség közösségnek adja tovább az üzenetet, megteremtve ezzel a bizalmi alapot, hiszen ismert forrású üzenetről van szó.

Ennek modern változata a viral-marketing, azaz a vírusmarketing,[3] amely egy olyan marketingstratégia, ahol az információk minél gyorsabb, és minél szélesebb körben való terjesztése a cél egy konvencióktól mentes környezetben, civil/polgári személyek között egy bizonyos termék, szolgáltatás, illetve eszme kapcsán az interneten keresztül. [9] Az üzenetet azok továbbítják, akiknek szól. Hatékonyan teremt újfajta kommunikációs módot, különösen az internet társadalma felé. Ha elindul, vírusként, emberről emberre terjed tovább, és megállíthatatlan. A terroristák módszere leginkább az ilyen jellegű üzenettovábbítás. Gondoljunk csak az Iszlám Állam videóira. Propagandaként használják ezeket a videóformában közölt üzeneteket, amelyekben a félelemkeltés, figyelmeztetés, felhívás és új emberek toborzása a cél. Jelszavakkal és célokkal kecsegtetik az újonnan érkezetteket. Ezekben a videókban olyan képi, hang és tárgyi adatokat közölnek, amely a semleges érintettek csoportjára nagy hatással bírhatnak. A közösségi média „erejét" használják ügyük megnyeréséhez. Ugyanakkor Amerika ellen – illetve 2015. november 13. óta ténylegesen Európa ellen is[4] – hadjáratot folytatnak lélektani hadviselés terén is. Egy 2015 novemberében közzétett videójukban kijelentik, hogy míg Amerikában örülnek a sikeres légicsapások általi eredményeknek, addig ők tovább „kísértenek" az amerikai katonák elméjében és félelmet lopnak a szívükbe (1. kép). [10]

3 A vírusmarketing a gerillamarketing egyik alfajtája, melynek lényege a nem hagyományos (konvencionális) eszközök, illetve technikák alkalmazása a marketingstratégia során. Lényege, hogy olcsó, kreatív, ötletes, valamint széles befogadó réteget és szűk, a hagyományos módszerekkel megközelíthetetlen csoportokat is el lehet érni.

4 2015. november 13.: Párizsban történt merényletsorozat, amelyet az Iszlám Állam katonái követtek el.

1. kép: Az Iszlám Állam videoüzenetéből származó képrészlet (Forrás: [10])

A videóban kiemelésre kerül a katonák öngyilkosságára vonatkozó statisztika, valamint olyan gyengeséget említenek, ami meggátolja Amerikát, hogy a földjükre lépjenek, ezzel akadályozva a sikerességüket.

Napjainkban tehát teret áthidaló kommunikációról beszélhetünk, amelynek nem szabhat gátat már az információs technológia sem. Jellemzően pedig átitatja az egész kommunikációs körfolyamatot a befolyásolás szándéka. Az információs társadalom napjainkban jóval több, mint 3 milliárdos létszámú internetes felhasználójával a virágkorát éli. Az információs technológia fejlettségi szintje pedig bárkinek lehetőséget biztosít a digitális művészet világában, legyen az hirdetés, vagy épp propagandaanyag az üzenetek célba juttatására. Látható azonban, hogy az új módszerek egyaránt jó és rossz célokra is alkalmazhatók, így a média szerepe egyaránt kényes kérdésnek bizonyulhat.

A média szerepe és befolyásoló képessége

Aronson meghatározása szerint a rábeszélés legáltalánosabb hordozóeszköze a média. Egyben a meggyőzés kiváló eszköze is, mely mind a civil, mind a katonai oldalt segítheti céljai megvalósításában. [11] A meggyőzés révén a valóság sajátosan kerül értelmezésre – a meggyőző szándékainak megfelelően. A kognitív dimenzió, azaz a tudat kerül a folyamat során átszervezésre, melynek célja egy elv elfogadtatása, vagy éppen egy új nézet kialakítása (attitűdváltozás elérése). [12; 68.] Ahhoz, hogy ezek az elvek kifejezésre juthassanak, számos módszer kínálkozik. Lehet logikailag, illetve érzelmileg megközelíteni a

célcsoportot, vagy félelem és terrorfenyegetés motívumaira építkezni, ami a mostani események tükrében aktuális elem lehet. Gondoljunk csak a 2015. év erőszakos támadásaira, a párizsi merényletekre, 2011. szeptember 11-re, a World Trade Center támadására, vagy éppen a 2005-ös év londoni merényletére. Ezekre az eseményekre megfelelő módon kell tudni reagálni. A sokkos állapotban lévő polgárokat meg kell tudni nyugtatni ilyen esetekben. Fontos a kommunikátor szerepe, akinek pontosan meg kell határoznia, miben áll a fenyegetés, és hogyan kerülhető el a katasztrófa. A lényeg minden helyzetben, hogy elfogadható bizonyítékokon kell alapulnia a közleménynek. [13; 101.] Manapság minden krízis, válsághelyzet, illetve konfliktus reflektorfényben zajlik. A média mindenhol ott van, és a fejlett kommunikációs technológia révén gyakorlatilag azonnal hozzá lehet jutni minden információhoz. A közösségi média pedig gondoskodik arról, hogy a lehető leggyorsabban és legtöbb emberhez eljusson a hír. Az internet révén bárki, bármikor, bármilyen információhoz hozzáférhet korlátlanul. Az innen szerzett híreket, ha még kritikusan is, de releváns információként fogadja el az olvasó. Nem egy alkalommal ismerőstől, baráttól származnak azok az információk, így elhiszik annak tartalmát. Hajlamosak akár annak a személynek a véleményére adni is. Arról nem is beszélve, hogy a fejlett mobiltechnológia segítségével azonnali információtovábbításra van lehetőség. Így tudnak terjedni korlátlanul, és hihetetlen mennyiségben a rémhírek, vagy épp az olyan információk, amelyek a befolyásolást, vagy épp szélsőséges esetben a megtévesztést szolgálják. McLuhan szerint a média például maga az üzenet, a kiterjesztett tudat, amely képes lehet arra, hogy változásokat idézzen elő. [14]

Az első világháborút megelőzően született meg a lövedék elmélet, amely nagyban meghatározta a közgondolkodást.[5] Az elmélet szerint a média nagy befolyással bír a közönségre, oly módon, hogy a rádióból, nyomtatott sajtóból, valamint a televízióból származó üzenetek úgy csapódnak a célcsoport elméjébe, mint a lövedék a testbe, ezáltal „sérülést", maradandó nyomot hagyva bennük. [15] Ezt az elméletet Harold Lasswell határozta meg 1927-ben megjelent a Propaganda Technique in the World War c. könyvében a legteljesebb formájában, amelyben azt vizsgálta meg, hogy a háborúban részt vevő nemzetek miként voltak képesek a különböző propagandatechnikák által feltüzelni Európát. [16] A célcsoportot egy összefüggő tömegnek írja le, amelynek tagjai egyformán reagálnak a záporozó üzenetekre. A korabeli társadalomban tényként kezelték a háborús helyzetből fakadó bizalmatlanságot, a nép nem kellő tájékozottságát az eseményekről, az identitás felbomlását, amelyek rendkívüli módon kiszolgáltatottá tették az embereket a média hatásainak. Lasswell külön fejezetben írta le a befolyásolás sikertényezőit, az ellenség demoralizálását, valamint azt, hogy hogyan lehet a győzelem illúzióját fenntartani. A rákövetkező évek Lasswell elméletét látták bizonyítani, hiszen valóságos propagandaháború indult meg – különösen a német és a szovjet birodalomban – a kornak megfelelő

5 Lövedékelmélet, amelynek idegen nyelvű megnevezése: magic bullet theroy vagy hypodermic-needle theory.

modern eszközök alkalmazásával (rádió, televízió). [17] Az elmélet hiányossága volt azonban, hogy a tömeget egyneműként kezelte, ami már a kulturális és szubkulturális különbségekből fakadóan sem helytálló megállapítás.

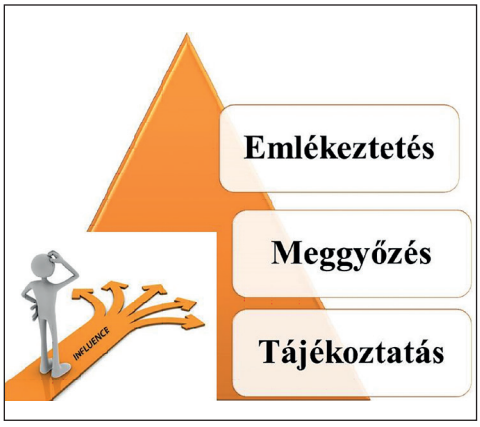
Meghatározó példaként szolgálhat azonban a médiahatás extrém formájára az Amerikai Egyesült Államokban, 1938-ban sugárzott H. G. Wells Világok harca c. művére alapozott rádiójáték, melynek során pánik tört ki azon hallgatók körében, akik nem hallották a műsor elején elhangzott bevezetőt, így valósnak vélték a marslakók támadását. [18] A modern tömegkommunikációs eszközök megjelenésével tehát lehetővé vált a célközönség azonnali és szélesebb körben való elérése. Érzelmek tömegesen történő kiváltására nyílt lehetőség. Olyannyira, hogy az első világháború folyamán a tömegek lelkesen meneteltek a halálba, a hátországban maradottak pedig mégannyira lelkesen támogatták a nemzetért harcolókat, amelyben a sajtónak igen nagy szerepe volt.

A médiahatások tekintetében a 20–21. század folyamán a világháló révén kiszélesedett közösségi oldalak, blogok, hirdetési felületek adnak lehetőséget a tömegek elérésére, és az extrém hatások kiváltására, mint ahogy azt a vírusmarketing esetében is láthattuk az előzőekben.

A befolyásolás szerepköre hazai és nemzetközi vonatkozásban

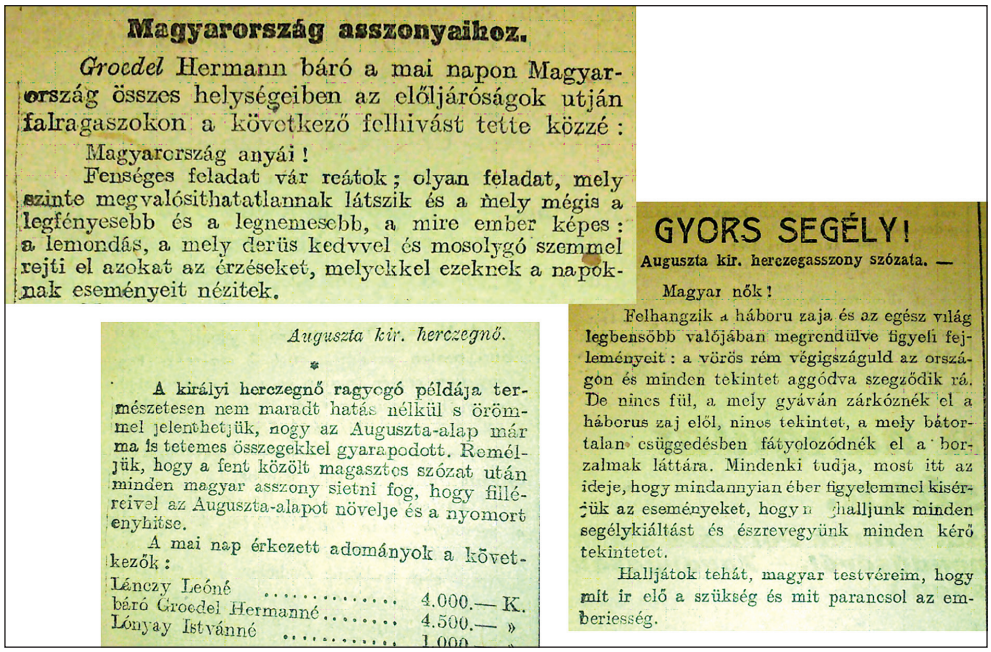
Magyarországon az első világháború során szintén jellemző volt a harci kedv, valamint a lelkesedés és a támogatás megnyerésére szolgáló módszerek alkalmazása. Nem lehetett ugyanis győzelemről beszélni egy egységes nemzet támogatásának hiányában, a vezetőség pedig nem rendelkezhetett egységes nemzettel annak tudatmódosítása nélkül. Ennek pedig legjobb módja volt akkoriban a különböző sajtóanyagok, röplapok és tárgyi eszközök alkalmazása, melyek révén a hírek és lényeges információk az otthonokba is eljutottak. Mindezek közül azonban előtérbe került a sajtó, harcias és buzdító üzenetekkel elárasztva a népet.

Annak vizsgálatára, hogy a média által hogyan vál(ha)t meggyőzhetővé az elérni kívánt célcsoport, egy, a marketingkommunikációban alkalmazott hármas szempontrendszeren keresztüli bemutatásra törekedtem, még mindig az első világháború eseményeihez kapcsolódva. Ennek felosztása a 2. ábrán látható.



2. ábra: A marketingkommunikáció céljai
(Forrás: [19])

A különböző részek – tájékoztatás, meggyőzés, emlékeztetés – esetében más-más a feladat. Meg kell erősítenünk az emlékeztetésnél például azt, hogy miért is jó a magyar népnek a háború? Miért is küzdenek? Mi a szerepe az egész folyamatban? Miért lehetnek jobbak az ellenséggel szemben? Fontos a hajlandóságot növelni, hogy a nép az ügy mellé álljon, és lelkesítse a hátországból az arcvonalon levő katonákat, szellemi és anyagi támogatássá váljon a politikai céloknak megfelelően. Ez az első világháborúban úgy működött, hogy a Pesti Hírlap[6] különböző rovataiban egy-egy célközönség felé irányultak a hírek, felszólítások, javaslatok. A specializáció lényege az volt, hogy egy-egy célcsoport különböző igényeire hatva igyekeztek eredményt elérni a propagandisták.[7] A következő képen néhány rovat látható az említett napilapból, mely szerves részét képezte a tájékoztatásnak és a meggyőzésnek, ezen keresztül pedig a befolyásolásnak.



Magyarország asszonyaihoz.

Groedel Hermann báró a mai napon Magyarország összes helységeiben az előljáróságok utján falragaszokon a következő felhivást tette közzé:

Magyarország anyái!

Fenséges feladat vár reátok; olyan feladat, mely szinte megvalósithatatlannak látszik és a mely mégis a legfényesebb és a legnemesebb, a mire ember képes: a lemondás, a mely derüs kedvvel és mosolygó szemmel rejti el azokat az érzéseket, melyekkel ezeknek a napoknak eseményeit nézitek.

Auguszta kir. herczegnő.

*

A királyi herczegnő ragyogó példája természetesen nem maradt hatás nélkül s örömmel jelenthetjük, hogy az Auguszta-alap már ma is tetemes összegekkel gyarapodott. Reméljük, hogy a fent közölt magasztos szózat után minden magyar asszony sietni fog, hogy filléreivel az Auguszta-alapot növelje és a nyomort enyhitse.

A mai nap érkezett adományok a következők:

Lánczy Leóné	4.000.— K.
báró Groedel Hermannné	4.500.— »
Lónyay Istvánné	1.000.— »

GYORS SEGÉLY!

Auguszta kir. herczegasszony szózata. —

Magyar nők!

Felhangzik a háboru zaja és az egész világ legbensőbb valójában megrendülve figyeli fejleményeit: a vörös rém végigszáguld az országon és minden tekintet aggódva szegződik rá. De nincs fül, a mely gyáván zárkóznék el a háborus zaj elől, nincs tekintet, a mely bátortalan csüggedésben fátyolozódnék el a borzalmak láttára. Mindenki tudja, most itt az ideje, hogy mindannyian éber figyelemmel kisérjük az eseményeket, hogy n halljunk minden segélykiáltást és észrevegyünk minden kérő tekintetet.

Halljátok tehát, magyar testvéreim, hogy mit ir elő a szükség és mit parancsol az emberiesség.

2. kép: Részletek a Pesti Hírlap 1914-es évfolyamából (Forrás: [20])

Ezek a cikkek főként adománygyűjtésre, a hadszíntéren lévő katonák támogatására, vagy épp csak buzdításra vonatkoztak, további adományozást és támogatást igényelve gyakorlatilag.

6 1878. december 25-én Légrády Károly indította el az első egyértelműen üzleti alapon álló, mérsékelten konzervatív tömeglapot, a Pesti Hírlapot. A Pesti Hírlap célja a programadó vezércikk szerint: A magyar közönségnek egy jól és fürgén szerkesztett, minden hírt gyorsan közlő, olcsó napilapot nyújtani."

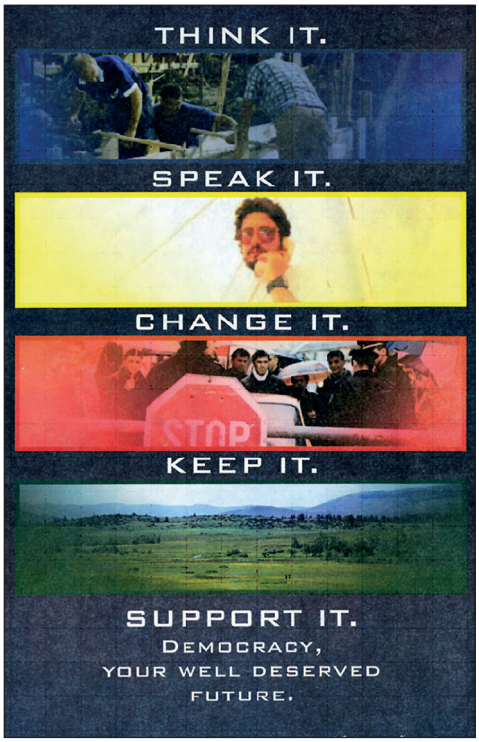
7 Az igények sokfélék lehetettek, de ezeknek az igényeknek a kielégítésével a nők például úgy érezhették, hogy támogatják, segítik férjük, fiuk, apjuk ügyét azáltal, hogy hósapkát vagy derékmelegítőt kötnek, lelkesen fogadják őket a vasútállomásokon, és még lelkesebben integetnek utánuk, buzdítva őket.

A háború tehát durva szóval élve sokfajta igényt kielégített, és célzott meg. A kereskedők is bőven hasznot húztak belőle, termékeiket a jó ügy érdekében reklámozták, ajánlották, a katonák pedig nem egyszer népszerűsítették azt. Emellett persze léteztek hirdetések és társadalmi felhívások, illetve adományok gyűjtésére vonatkozó rovatok is.

Ez a hármas meghatározás érvényes napjaink konfliktushelyzeteiben is. A pszichológiai műveleti tevékenységek ugyanis csak úgy érhetnek célt, ha világos tényeket közölnek, annak helyességét, illetve valóságtartalmát igazolják, valamint emlékeztetnek ennek megfelelően a „helyes" viselkedésmódra.

Jó példa erre a hármas egységre még az SFOR Bosznia-Hercegovinában 1998-ban terjesztett röplapja, amely a demokrácia jelentőségét hangsúlyozza. Tájékoztat és gondolkodásra buzdít, meggyőz a változtatás jelentőségéről, továbbá emlékezteti a népet arra, hogy a megérdemelt jövőért küzd. A röplap a 3. számú képen látható.

A fent elmondottak alapján így nem meglepő, hogy a média napjainkra könnyűszerrel válhatott az elsődleges információk megszerzésének forrásává és eszközévé egyaránt. Éppen ezért lehet veszélyes „fegyver" is, ha arról van szó, hogyan is nyerjük meg magunknak a közvéleményt. Ismeretes ugyanis, hogy a különböző csoportok véleménye, attitűdje, bizonyos viselkedésmódja egy-egy esemény, katonai művelet során döntő fontosságú lehet a műveleti célok kivitelezésében. A vietnami háború ennek a döntő fontosságnak az iskolapéldája. Az 1964–65-ös években még a társadalom jelentős hányada a háborút támogatta az Amerikai Egyesült Államokban, éppen ezért igyekeztek az eseményekről széles körű tájékoztatást adni, és ennek hatásaként az amerikai közvélemény támogatását megnyerni. A sajtó vezető híreként szerepelt a vietnami háború, a haditudósítók korlátlanul közölhették le az ott történteket. A háború azonban elhúzódónak bizonyult, és jellegéről olyan információk is kiszivároghattak, amelyek szándékukkal ellentétes véleményeket váltottak ki. A sajtó szerepe korlátozva lett, de így sem lehetett megakadályozni, hogy kiszivárogjanak az 1968-as My Lai-i események, ahol több száz polgári lakost – főleg nőket, gyerekeket és öregeket – mészároltak le amerikai katonák. Ez megingatta és felháborította a közvéleményt, akik elvesztették hitüket az igazságos ügyben. [22]



3. kép: Az SFOR által terjesztett szórólap (Forrás: [21])

Következtetések

Az embert beszéde szervesen meghatározza, amely háromféle módon teljesedik ki: kinyilvánítás, az információ továbbítása, valamint a meggyőzés, illetve ezek együttműködése. [23; 31] Az ember természetéből kifolyólag mindenhez jelentéseket társít. Ezt főként saját szociális és kulturális környezetének meghatározottsága tekintetében teszi meg. Így a közös nézőpont kialakítása, és maga a befolyásolás számos akadályba ütközhet, és a folyamat kivitelezése mind a marketing-, mind a pszichológiai műveletek szempontjából nagyfokú éleslátást, széles látókört és kreativitást követel meg.

Három olyan fejlődési tendencia adja azt a lehetőséget, ami a PSYOPS eszközeit és módszereit sikeresen kivitelezhetővé teszi [24]:

– az információs technológia fejlődése;
– a tömegmédia, tömegkommunikáció fejlődése;
– a társadalomtudományok fejlődése, amelyek az emberi viselkedést kutatják.

A befolyásolás alkalmazása, a célcsoport attitűdváltoztatásra való késztetése számos etikai problémát vet fel. Fontos szempont azonban az, hogy mi az a cél, amelynek érdekében a kommunikáció és a média eszközeit használjuk. Lényeges, hogy ne idegenítsék el a társadalmakat és a célcsoportokat hazugságokkal és álhírekkel, hiszen a bizalom elvesztése akár a művelet sikerességét is gátolhatja.

Gyakorlatilag két fronton folyik a háború: a hadszíntéren, és az emberi agyban a kommunikáció, a média és így a propaganda eszközével. Az új típusú konfliktusok, valamint a modern hadviselés meg is követeli ezt a felosztást.

A nyilvánosságra kerülő információk áramlása a média és az új technológiai eszközök közvetítésével sokkal nagyobb folyamatot alkot, mint amit a hagyományos kommunikációs stratégiákkal ellenőrizni lehetne. Gondoljunk csak abba bele, hogy ha bármilyen erőszakos cselekmény történik a világban, az okostelefonok és okoseszközök révén azonnal hír lesz belőle, és villámgyorsan szétterjedhet az internet révén az egész világban. Walter Lippman, volt amerikai politikus, író szerint háborús helyzetben a szemben álló fél propagandatevékenységet folytat, míg a saját oldal az igazság és tisztesség jegyében keresztes hadjáratot vív a békéért. [25] Mindenki mást lát a saját oldalán, más szemszögből nézi az eseményeket, a lényeg azonban az, hogy miként valósul meg a befolyásolás célja, azaz a műveleti cél, és az a pszichológiai műveletek támogatása során miként kerül alkalmazásra. Bernard Cohen politológus úgy vélte, *„nem mindig sikerül az emberek szájába rágni, mit gondoljanak, de azt igen, hogy miről gondoljanak valamit. A világban az emberek aszerint tájékozódnak, hogy milyen térképet rajzolnak számukra az általuk olvasott újságok írói, szerkesztői és kiadói."* [26]

Irodalomjegyzék

[1] Munk Sándor: Az információs műveletek típusai és modelljei. *Hadtudomány,* 2002 (1), www.zmne.hu/kulso/mhtt/hadtudomany/2002/1-/z-02/chapter1.htm (a letöltés ideje: 2015. október 21.)

[2] Haig Zsolt: *Információ – társadalom – biztonság.* NKE, Budapest, 2015, 291. (ISBN 978-615-5527-08-1)

[3] Dr. Haig Zsolt – Dr. Várhegyi István: *Hadviselés az információs hadszíntéren.* Zrínyi Kiadó, Budapest, 2005, 286. (ISBN 963-327-391-9)

[4] Information Operations. Joint Publication 3–13, 20 November 2014, www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (a letöltés ideje: 2015. november 21.)

[5] Joint Publication 3–13. 2 Military Information Support Operations December 2011, 103., publicintelligence.net/jcs-miso/ (a letöltés ideje: 2014. október 13.)

[6] Kapitány Ágnes – Kapitány Gábor: *A tömegkommunikáció szimbolikus üzenetei. Kommunikáció, demokrácia, média.* MÚOSZ Bálint György Újságírói Iskola kiadása, Budapest, 1998, 222. (ISBN 963-7115-22-6)

[7] Cambridge Dictionaries Online, dictionary.cambridge.org/dictionary/english/influence (a letöltés ideje: 2015. december 1.)

[8] Manuel Castells: *Az identitás hatalma. Az információ kora. Gazdaság, társadalom és kultúra II. kötet.* Gondolat–Infona, 2006, 546. (ISBN 963-9610-43-7)

[9] Dictionary.com, dictionary.reference.com/browse/viral-marketing (a letöltés ideje: 2014. december 20.)

[10] Trey Sanchez: *ISIS Propaganda Video Taunts USA, 'Bring It On,' Mocks Soldier Suicides.* "We will drown all of you in blood." www.truthrevolt.org/news/isis-propaganda-video-taunts-usa-bring-it-mocks-soldier-suicides (a letöltés ideje: 2015. november 30.)

[11] Elliot Aronson – Anthony R. Pratkanis: *A rábeszélőgép – Élni és visszaélni a meggyőzés mindennapos mesterségével.* Ab Ovo Kiadó Kft., 2012, 212. (ISBN 978-96378-530-36)

[12] Dr. Szabó István: *Bevezetés a szociálpszichológiába.* Nemzeti Tankönyvkiadó, Budapest, 1998, 122.

[13] Elliot Aronson: *A társas lény.* Akadémiai Kiadó, Budapest, 2008, 504. (ISBN 978-963-05-8628-3)

[14] Marshall McLuhan: *Understanding Media: The Extensions of Man.* New York, McGraw Hill, 1964. (ISBN 978-0262631594)

[15] Bajomi-Lázár Péter: *Manipulál-e a média?* Médiakutató oldal, 2006. nyár, www.mediakutato.hu/cikk/2006_02_nyar/04_manipulal-e_a_media/ (a letöltés ideje: 2015. október 3.)

[16] Harold D. Lasswell: *Propaganda Technique in the World War.* London, Kegan Paul, Trench, Trubner & Co. Ltd., 1927, 233.

[17] Communication Theory, communicationtheory.org/lasswells-model/ (a letöltés ideje: 2015. október 23.)

[18] The War of the Worlds panic was a myth. *The Telegraph,* Culture/Radio, www.telegraph.co.uk/radio/what-to-listen-to/the-war-of-the-worlds-panic-was-a-myth/ (a letöltés ideje: 2015. október 13.)

[19] Philip Kotler – Kevin Lane Keller: *Marketingmenedzsment.* Akadémia Kiadó, 2006, 986. (ISBN 963-05-8345-3)

[20] Pesti Hírlap, 36(1914)/151–211.

[21] www.psywar.org/product_1998SFORSDP.php (a letöltés ideje: 2015. december 11.)

[22] My Lai Massacre, www.history.com/topics/vietnam-war/my-lai-massacre (a letöltés ideje: 2015. december 13.)

[23] Philippe Breton: *A manipulált beszéd.* Helikon Kiadó Kft., 2000, 210. (ISBN 963-208-676-7)

[24] Commander Randall G. Bowdish: Information-Age Psychological Operations. *Military Review,* December 1998 – February 1999, 28–36., www.c4i.org/bowdish.pdf (a letöltés ideje: 2015. október 13.)

[25] John Long: Propaganda. *The Voice of Visual Journalist,* nppa.org/page/9148 (a letöltés ideje: 2015. december 12.)

[26] Szabó Ferenc: Háború és média. *Jelek* (virtuális folyóirat), 2006/4., jelek.hu/index.php?cid=89 (a letöltés ideje: 2015. december 12.)

The Art of Influence as a Tool of Psychological Operations and Marketing

Hajdu Veronika

The aim of psychological operations (PSYOPS) is to influence a specific target audience's emotions, attitudes with relevant information and different techniques and methods in a well-planned manner to reach operational objectives. Modern warfare provides the opportunity for the opposing parties to apply a broad-spectrum of approaches to settle conflicts and controversies. It is all about influencing, which echoes Clausewitz's opinion: forcing our will on the enemy. In this study I examine the role of influence, addressing the role of communications and media while also taking into account marketing communications.

Keywords: psychological operations, marketing communication, media, influence

Vég Róbert László

A Nemzeti Közlekedési Hatóság „B" és „C" kategóriás gépjárművezető képzésének műszakielőírás-változásai

A műszaki oktatás jelentős része az elméleti oktatás során teljesül, és a számítógépes tesztes vizsgával többnyire véget is ér (főleg a „B" járműkategóriában). A műszaki oktatás fontosságát alátámasztja, hogy a jelen kori nagy teljesítményű és nagy menetsebesség elérésére alkalmas járművekkel történő közlekedéskor egy műszaki hiba bekövetkezte, vagy az azokat megelőző hibajelenségek fel nem ismerése ugyanolyan gyorsan baleset forrásává válhat, mint egy közlekedési szabály be nem tartása. A közlekedési hatóság részletesen meghatározza a műszaki ismeretek oktatásának ismeretanyagát, de az oktatás során a képző szervek csak csekély időt szánnak a tényleges oktatásra, vagyis a meghatározott követelmények nem teljesülnek teljes mértékben. A cikk elhelyezi és értékeli az oktatásban és a közlekedésben betöltött szerepének megfelelően a műszaki oktatást, a közlekedési hatóság előírásait és annak változásait.
Kulcsszavak: gépjármű, közlekedés, műszaki, oktatás, képzés

A „B" és „C" járműkategóriás képzések célja, tartalma

A tanfolyam célja a jelentkezőket olyan járművezetőkké képezni, akik képesek önállóan, biztonságosan, kulturáltan, a szabályokat betartva, a környezetet kímélve közlekedni, és a megszerzett vezetői engedély birtokában járművezetőként szerzett tapasztalataikat felhasználva továbbfejlődni. [1]

A képzés során kiemelt célként kell figyelembe venni a gépkocsivezető vonatkozásában a közúti közlekedés mai kornak megfelelő követelményrendszerét. Tudatosítani kell a gépkocsivezető személyes felelősségét, a közlekedésben rá háruló feladatokat, különös tekintettel a tehergépkocsi sajátosságaira. [2]

A tanfolyam feladata olyan ismeretek tanítása, amely lehetővé teszi:

– a közlekedés zavartalanságának elősegítése érdekében a jogszabályok helyes alkalmazásának az elsajátítását;
– a közúti közlekedésben rejlő veszélyek felismerését és helyes megítélését;
– a jármű feletti uralom birtokában a folyamatos és biztonságos közúti közlekedést és az elsődlegesen kialakuló veszélyhelyzetre a megfelelő módon való reagálást;

– a közlekedési partnerek biztonságának szem előtt tartását;
– a jármű jogszabályban előírt ellenőrzését, a közlekedésbiztonságot veszélyeztető műszaki hiba felismerését és a továbbhaladás lehetőségéről való helyes döntést.

A gépjárművezető a járművével köteles úgy közlekedni, hogy a személy- és vagyonbiztonságot ne veszélyeztesse, másokat közlekedésükben indokolatlanul ne akadályozzon, és ne zavarjon. [3] Valamennyi gépjármű vezetőjének minden pillanatban rendelkeznie kell a 24/2005. (IV. 21.) GKM rendelet 7. számú melléklet C) fejezetben meghatározott, a gépjárművek vezetéséhez szükséges ismeretekkel, jártassággal és magatartással.

Képesnek kell lennie a vezetőnek:

– a forgalmi veszélyhelyzeteket felismerni és felmérni azok veszélyességének mértékét;
– megfelelő mértékben az irányítása alatt tartania a járművet, hogy ne okozzon veszélyes helyzeteket, és az ilyen helyzetben megfelelően tudjon reagálni;
– a közúti közlekedés szabályait betartani;
– a járműben minden jelentősebb műszaki meghibásodást észlelni, különösen azokat, amelyek biztonsági veszélyforrást jelentenek, és azokat megfelelő módon meg tudja javíttatni;
– számításba venni a vezetői magatartást befolyásoló minden tényezőt;[1]
– a többiek iránti tiszteletadással elősegíteni valamennyi közúti közlekedő, különösen a leggyengébbek és a legvédtelenebbek biztonságát. [4]

Nem könnyű dolog minden jelentős műszaki meghibásodást felismerni, még egy gyakorlott vezetőnek sem, pedig ezt a képességet a tanulónak el kell érnie a forgalmi vizsgáig.

A „B" járműkategóriánál a képzés közlekedési alapismeretekből, a járművezetés elméletéből, szerkezeti és üzemeltetési ismeretekből, valamint a vezetési gyakorlat alap- és főoktatásából áll. Az elméleti tantárgyak előírt minimális óraszáma 28 óra. A „B" járműkategória elméleti vizsgája számítógépes tesztlapkitöltéses vizsgával valósul meg, ahol a közlekedési ismeretek tesztekbe be vannak építve a műszaki kérdések is. A vizsgakérdéssor végén található öt kérdés vonatkozik a szerkezeti és üzemeltetési ismeretekre.

A „C" járműkategóriánál a képzés közlekedési alapismeretekből, a járművezetés elméletéből, szerkezeti és üzemeltetési ismeretekből, munkavédelmi, tűzvédelmi, szállítási, biztonsági ellenőrzési és üzemeltetési ismeretekből, valamint a vezetési gyakorlat alap- és főoktatásából áll. Az elméleti tantárgyak előírt minimális óraszáma 54 óra, amihez hozzá kell még venni a biztonsági ellenőrzés és üzemeltetés mint gyakorlat 14 óráját. A „C" járműkategória elméleti vizsgája szintén számítógépes tesztlap-kitöltéses vizsgával valósul meg, de itt már mind a munkavédelem, tűzvédelem, szállítás ismereteknek mind a szerkezeti és üzemeltetési ismereteknek külön vizsgakérdéssor van biztosítva. A biztonsági ellenőrzés és üzemeltetés szóbeli gyakorlati vizsgaként valósul meg.

1 Például: alkohol, fáradtság, gyenge látás.

A kötelező elméleti képzésnek a jogszabályok szerint két formája lehet, az egyik a hagyományos tantermi oktatás, a másik az elektronikus formában, számítógéppel teljesíthető e-tanfolyam. [5]

A „B" és „C" járműkategóriás műszaki oktatás problematikája

2015 januárjában a különböző vezetői engedély kategóriák kérdésadatbankja lényeges megújuláson esett át. A megújulás szükségességét az adta, hogy a kérdések ismertek voltak a tanulók számára, valamint a kérdések mennyisége és sajnos minősége nem segítette elő a valós tudásszint felmérését. A képzésre szigorú szabályok vonatkoznak, de a problémát az elméleti képzés esetében a vizsgacentrikus megközelítés okozza. Az elméleti képzés nem kényszerítette rá a tanulókat arra, hogy ne a vizsgára, hanem a valós közlekedésre készüljenek fel.

A tanulók jelentős részét a sikeres vizsgaeredmény megszerzése motiválta, aminek érdekében az összetett tanulás helyett a vizsgakérdések betanulása volt a céljuk. Az autósiskolák nagy része is alkalmazkodott ehhez a helyzethez, és kevés óraszámban csak azokat az ismereteket adta át, amelyek a sikeres vizsgához szükségesek voltak. [6]

Az elavult műszaki kérdéseket valóban használható és korszerű technikai kérdések váltották fel, amelyek megfelelnek a jelen kori műszaki szintnek. Az új kérdésbank az alapkérdések tekintetében közel négyszeres, a variációs lehetőségeknek megfelelően pedig közel tízszeres kérdésmennyiséggel rendelkezik. Ez a hatalmas kérdésszám biztosítja, hogy ne lehessen bemagolni őket, és a tanulók a vizsgakérdések helyett valóban a Nemzeti Közlekedési Hatóság (NKH) által előírt ismeretanyagot tanulják meg. Az új kérdések bevezetésével lényegében nem változtak a vizsgázók eredményességi mutatói. Az új kérdésbank biztosítja az elméleti tananyag tényleges elsajátítását. [7]

A hatékony gyakorlati oktatás csak szilárd elméleti alapok letétele után képzelhető el. A gyakorlati oktatásnak nem az elméleti alapok átadása a célja, hanem azok készségszintű alkalmazásának az elsajátíttatása. [8]

A „B" járműkategóriás szerkezeti és üzemeltetési ismeretek tantárgy követelményrendszerének változásai

A különböző járműkategóriák elméleti tantárgyi ismereteit részletesen meghatározza a Nemzeti Közlekedési Hatóság kiadott tantervi és vizsgakövetelménye. A tanterv felsorolja azokat az ismeretanyagokat, amelyeket a képzés során ismertetni kell a tanulókkal. A tanterv szerint az elméleti tananyagnak a gyakorlatra kell irányulnia, és az üzemeltetési tud-

nivalóknak kiemelt jelentőséget kell biztosítani. Minden oktatott téma során ki kell térni a környezet védelmével kapcsolatos feladatokra, és a teljes tantárgy tanítását át kell hatnia a környezetvédő szemléletmódnak.

A szerkezeti és üzemeltetési ismeretek tantárgy követelményrendszerének vizsgálatakor három különböző évben kiadott tantervi útmutatót hasonlítok össze, a 2007, 2013 és a 2015-ös évekét. Távolabbi évekkel nem foglalkozom, mert azok már nem feltétlenül a jelen technikai kort tükrözik. A mai technikai szintbe már nem fér bele a kétütemű benzinmotor és a részletes karburátor témakörök. A különböző tantervek felépítése minimális eltérést mutat, de az egységesség szem előtt tartása miatt a 2015-ben szereplő felosztást veszem alapnak.

Ismeretanyag	2007	2013	2015
A gépkocsi felépítése, főbb szerkezeti egységek.	×	×	×
A motorok felépítése és működése, a motorok hűtése, kenése.	×	×	×
Keverékolajozás.	×	–	–
A motor üzemanyag-ellátása (benzin, dízel). A szívó- és kipufogó berendezés, a katalizátor. A hideg motor indítása.	×	×	×
A karburátor működési elve.	×	–	–
Alternatív üzemanyagok. Elektromos és hibrid hajtás.	–	–	×
Az akkumulátor, generátor és indítómotor. A jelzőberendezések működése, előírások. A pótkocsi (utánfutó, lakókocsi) villamos berendezései.	×	×	×
A gyújtóberendezések feladata, a vezetékhálózat.	×	–	–
A fedélzeti számítógépek jelzései.	–	–	×
A világítóberendezések működése és hatósági előírások (távolsági és tompított fényszórók, helyzetjelző lámpák, rendszámtáblát megvilágító lámpa, belső világítás, ködfényszórók és a hátsó helyzetjelző lámpa).	×	×	×
Nappali menetjelző lámpa, bekanyarodási lámpa.	–	–	×
Az erőátviteli berendezések feladata, elrendezési módok. Tengelykapcsoló, mechanikus sebességváltó. Automata sebességváltó kapcsolója, üzemmódok.	×	×	×
Szabadonfutó szerkezet.	×	–	–
A kerekek, a gumiabroncsok felépítése, fajtái és jelölésük. A gumiabroncsok megfelelősége, rendellenes kopások.	×	×	×
Gumiabroncs nyomásfigyelő rendszerek (TPSM). Pótkerék, szükségpótkerék, abroncsjavító készlet.	–	–	×

Ismeretanyag	2007	2013	2015
A kormányzás geometriája. A szervokormány, a pótkocsi kormányzása.	×	×	×
A fékberendezések feladata, hatósági előírások. Hidraulikus üzemi fékberendezés, vákuumos fékrásegítő berendezés, blokkolásgátló.	×	×	×
A rögzítőfék felépítése, működési elve. A pótkocsi fékezése.	×	×	×
Üzemeltetés télen (hideg időben), kiegészítő felszerelések, hólánc használata, a gépkocsik megelőző karbantartása. Ápolási munkák, ellenőrzések, beszabályozások.	×	×	×
Az elromlott jármű vontatása, a gépkocsi kötelező műszaki felülvizsgálata.	×	×	×
A sebességtartó berendezés (tempomat), a kipörgésgátló (ASR).	×	×	×
Tolatóradar, automata parkolórendszer, sávtartó rendszer.	–	×	×
Elektromos menetstabilizáló program (ESP), adaptív sebességtartó automatika (ACC), fékasszisztens (BAS), ütközéselkerülő rendszer (ABA), holttérfigyelő rendszer, követési távolságot szabályozó rendszerek, visszagurulás-gátló, lejtmenet-szabályozó.	–	–	×

1. táblázat: Szerkezeti és üzemeltetési ismeretek tantárgy ismeretanyagai különböző években a „B" járműkategóriánál

A 2007-es évben még voltak előírások (keverékolajozás, szabadonfutó szerkezet), amelyek közvetlenül a kétütemű benzinmotorra vonatkoztak, viszont ekkor már alig voltak jelen ezek a gépjárművek (kétütemű Trabant, Wartburg) a közúti forgalomban. Ezek a témakörök a korábbi évekből maradtak vissza, és ebben a formában már teljesen feleslegesek voltak, mert az oktatás csak a négyütemű motorokra korlátozódott. A karburátorok működési elve és a gyújtóberendezések című témák már sokat veszítettek jelentőségükből, mert ekkor zömében már benzinbefecskendező rendszerekkel szerelték fel a gépjárműveket. A karburátor önmagában olyan nagy téma, hogy az oktatásának semmi értelme sincs, ha nem tudjuk ráfordítani a kellő időt. Ha túlságosan felületesen oktatjuk, akkor ezt a témát inkább jobb kihagyni, mint ahogyan a későbbi években tették is. A 2015-ös évektől már megjelenik a fedélzeti számítógép mint ismeretanyag, ez teljesen helyénvaló, mert a mai járművek már rendelkeznek ilyennel. Nehéz a közúti forgalomban olyan járművet találni, amely ne lenne ellátva egy vezérlőegységgel, és az egyszerűbben vagy bonyolultabban ne kommunikálna a gépjármű vezetőjével. Több műszakilag előremutató ismeretanyag is megjelent (elektromos és hibrid hajtás, bekanyarodási lámpa, TPMS, tolatóradar, sávtartó rendszer, ESP, BAS, ABA, stb.), amelyek még csak elterjedőben vannak, de egyre nagyobb lesz a jelentőségük. Célszerű foglalkozni ezekkel a műszaki fejlesztésekkel, mert a gépjárművekben egyre nagyobb számban fordulnak elő, már alapfelszereléskénti a korszerű járművezetést segítő rendszerek.

A „C" járműkategóriás szerkezeti és üzemeltetési ismeretek tantárgy követelményrendszerének változásai

A „C" járműkategóriánál a szerkezettan tantárgynak meg kell alapoznia a jármű biztonsági ellenőrzését, valamint elő kell segítenie a gépkocsi kezelésének hatékony elsajátítását. Ismereteket kell adni a gépkocsi szerkezeti felépítéséről és működéséről. A tanterv szerint, ahogyan a „B" járműkategóriánál is, az elméleti tananyagnak a gyakorlatra kell irányulnia, és az üzemeltetési tudnivalóknak kiemelt jelentőséget kell biztosítani. Minden téma oktatása során ki kell térni a környezetvédelmi feladatokra is. A pontosabb összehasonlítás érdekében, ahogyan a „B" járműkategóriánál is tettem, itt is ugyanazokban az években kiadott tantervi útmutatókat vizsgálom meg.

Ismeretanyag	2007	2013	2015
Vázszerkezet és a kocsiszekrény. A szellőzés és a fűtés. Ajtók és ablakok. A billenő rakterű járművek billentő szerkezetei. A járműszerelvények kapcsolószerkezetei.	×	×	×
Alvázaknál alkalmazott biztonságtechnikai megoldások. Klímaberendezés.	–	–	×
A négyütemű Otto-motor működése. Keverékképzés és égési folyamat. Karburátoros, befecskendezéses és kipufogógáz turbinás Otto-motorok.	×	×	–
A négyütemű dízelmotor működése. Keverékképzés és égés a dízelmotorban. Közvetlen befecskendezésű és kamrás dízelmotorok. Dízelmotorok kipufogógáz turbinás feltöltővel. A turbófeltöltő ellenőrzése, üzemeltetése.	×	×	×
Töltőlevegő-visszahűtés.	–	–	×
A motor hűtése (a léghűtés, a szivattyús folyadékhűtés, a hűtőfolyadékok). A motor kenése (a motorolajok, olajozási rendszerek, az olajhűtő).	×	×	×
A tüzelőanyagok (benzin, gázolaj). Az Otto-motor tüzelőanyag-ellátása (keverékképzés, karburátoros tüzelőanyag-ellátás, benzinbefecskendezés).	×	×	–
Alternatív tüzelőanyagok, adalékanyagok.	–	–	×
Dízelmotor tüzelőanyag-ellátása (tápszivattyú, gázolajszűrők, befecskendező-szivattyú, nyomócső porlasztó). Elosztó rendszerű befecskendező-berendezés.	×	×	×
Common Rail rendszerek.	–	×	×
Szívó- és kipufogórendszer, a kipufogógázok tisztítása.	×	×	×

Ismeretanyag	2007	2013	2015
Az akkumulátor, áramfejlesztő, indítómotor. Egyéb villamos berendezések (vezetékek, kapcsolók, biztosítók).	×	×	×
Gyújtóberendezések (hagyományos akkumulátoros, elektronikus gyújtás).	×	×	–
Világítóberendezések (távolsági és tompított fényszóró, nappali menetjelző lámpa, helyzetjelző lámpák, hátsó rendszámtáblát megvilágító lámpa, hátrameneti lámpa, ködfényszórók). Jelzőberendezések.	×	×	×
Méretjelző lámpák, bekanyarodási lámpa.	–	–	×
Dízelmotor indítását segítő berendezések (izzógyertya, lángizzógyertya, Startpilot, motort előmelegítő fűtőberendezés).	×	×	×
A tengelykapcsoló. A sebességváltó (mechanikus sebességváltók, félautomata és automata sebességváltók). Összkerékhajtás, osztóművek, mellékhajtóművek. Kardántengely, differenciálmű, differenciálzár, a hajtótengelyek.	×	×	×
Hibrid hajtás, elektromos járművek.	–	–	×
Keréktárcsák, gumiabroncsok (szerkezete, méretei és jelölése). Kerékagyak, a kerekek felfüggesztése és rugózása (laprugó, légrugózás). Az alváz magasságának állítása. Ikertengelyek, segédfutóművek, lengéscsillapító, stabilizátorok.	×	×	×
Gumiabroncs nyomásfigyelő rendszerek (TPMS).	–	–	×
A gépkocsi kormányzása (a kormányzás geometriája, a kormányzott kerekek állása, a pótkocsik kormányzása).	×	×	×
Kormányberendezések (kormányművek, szervokormányművek).	×	×	×
A fékberendezések feladata és a vonatkozó előírások. A kerékfékszerkezetek (dobfék, tárcsafék, a fékberendezések fajtái és a működtetés egységei).	×	×	×
A gépkocsik üzemifék-berendezései (hidraulikus, tisztán sűrített levegős, szerelvények, kombinált üzemi fék, terheléstől függő dinamikus fékerő-szabályozók. A blokkolásgátló berendezés (ABS).	×	×	×
Elektronikus fékrendszerek (EBS).	–	–	×
A rögzítőfék berendezések és szerelvényeik. A tartós lassító fékberendezések. Csővezetékek, csőkötések.	×	×	×
A tachográf készülékek fajtái, kezelése. Az analóg tachográf kezelése, az adatrögzítő lap. A digitális tachográf (gépkocsi-vezetői kártya, ellenőri kártya, műhelykártya, munkáltatói kártya).	×	×	×

Ismeretanyag	2007	2013	2015
A gépjárművek üzemeltetése (bejáratás, üzemeltetés hideg időben, a hólánc használata, a jármű üzemen kívül helyezése, a karbantartási rendszer felépítése).	×	×	×
Tankolás, AdBlue adalék utántöltése.	–	–	×
Elektromos menetstabilizáló program (ESP), a kipörgésgátló (ASR).	×	×	×
Sebességkorlátozó, sebességtartó berendezés (tempomat), adaptív sebességtartó automatika (ACC), fékasszisztens (BAS), ütközéselkerülő rendszer (ABA), holttérfigyelő rendszer, követési távolságot szabályozó rendszerek, visszagurulás-gátló, lejtmenet-szabályozó, tolatóradar, automata parkolórendszer, sávelhagyásra figyelmeztető és sávtartó rendszerek, parkolást segítő rendszerek.	–	–	×

2. táblázat: Szerkezeti és üzemeltetési ismeretek tantárgy ismeretanyagai különböző években a „C" járműkategóriánál

A 2013-as évben még oktatni kellett a négyütemű benzinmotort, pedig ekkor már teherautókban szinte alig lehetett megtalálni ezeket a motorokat. Egyértelmű, hogy ez már ki is maradt a 2015-ös évben, és csak a négyütemű dízelmotor lett előírva, mint oktatandó típus. A töltőlevegő-visszahűtés csak a 2015-ös évben jelent meg, pedig ez a technika már elég régi konstrukció, és nagy valószínűséggel a korábbi években a turbófeltöltés oktatásakor ismertetésre is került, ezért inkább ezt csak mint adminisztrációs hibát értékelem, amit a közlekedési hatóság korrigált. Az alternatív tüzelőanyagok oktatása csak az utóbbi évben lett előírva. Már régóta lehet az üzemanyagtöltő kutakon tankolni alternatív üzemanyagokat (LPG, E-85), de ezek felhasználása jelenleg inkább a személygépjárműveknél jellemző. A tehergépjárműveknél döntő többségében gázolajat használnak üzemanyagként. A Common Rail rendszerek 2013-ban már oktatásra kerültek, de szerintem ekkor már lényeges lemaradásban voltak az adott kor technikai színvonalához képest, vagyis sokkal korábban elő kellett volna írni. 2005-ben már megjelent egy Common Rail rendszereket bemutató és feldolgozó szakirodalom, ami azt jelenti, hogy ekkor már ezek a rendszerek nagy számban elterjedtek, és szinte egyeduralkodóvá váltak a gépjárműtechnikában. A közlekedési hatóság jó pár évig nem reagált a technikai kihívásra az oktatás során. 2015-ben a „B" járműkategóriával egyetemben a teherautóknál is megjelent a hibrid hajtás és elektromos járművek tananyag, de ez szerintem még csak egy valószínűsíthető jövő. Ez a technika a személygépkocsiknál is csak az elterjedés fázisában van, és még jó pár évnek el kell telnie, hogy tömegesen jelentkezzenek. Véleményem szerint a „C" járműkategóriánál ez teljesen felesleges ismeretanyag, mert a „B" kategóriánál már úgyis megtanulták, és a teherautóknál ilyen járművekkel még nem találkozni a közutakon. Az elektronikus fékrendszerek oktatása jogos elvárás volt, mert egyre több ilyen járművet üzemeltetnek manapság, ennek az előírása már korábban is megtörténhetett volna. A táblázat alsó so-

rában felsorolt, műszakilag előremutató ismeretanyagokkal és korszerű járművezetést segítő rendszerekkel a „B" járműkategóriánál megfogalmazottaknak megfelelően itt is kell foglalkozni, mert ezen rendszerek egyre nagyobb számban fordulnak elő.

A „C" járműkategóriás biztonsági ellenőrzési ismeretek követelményrendszerének változásai

A tantárgy oktatása során el kell érni, hogy a tanulók felismerjék, és logikusan be tudják határolni a leggyakrabban előforduló hibákat. Ennek érdekében az összes meghatározott feladatot gyakoroltatni kell, az egyes témák átfedése megengedett, ha az az oktatási feladat megvalósítása érdekében szükséges. Az egyes műveletek megkezdése előtt részletesen ismertetni kell a kapcsolódó munka- és tűzvédelmi szabályokat. A vizsgázónak bizonyítania kell, hogy rendelkezik a személygépkocsi biztonságos közlekedéséhez szükséges ellenőrzési ismeretekkel. Végre kell tudnia hajtani a közúti közlekedés szabályaiban előírt indulás előtti ellenőrzéseket, a gépkocsi szerkezeti felépítését a feladatok megoldásához szükséges mértékben ismernie kell. A vizsgázónak a feladatok végrehajtása közben meg kell állapítania az egyes biztonsági berendezések megfelelőségét, illetve hibáját, a megállapításokat néhány mondattal indokolni kell.

Ismeretanyag (elvégzendő műveletek)	2007	2013	2015
A vázszerkezet és a kocsiszekrény ellenőrzése és karbantartása. A motortértető nyitása. Fülkebillentés.	×	×	×
Az analóg (digitális) tachográf működésének ellenőrzése, adatrögzítő lap (adatrögzítő kártya) kezelése. Az ablakmosó és az ablaktörlő ellenőrzése. Az elakadásjelző háromszög felállítása.	×	×	×
A léghűtés ellenőrzése, karbantartása (hűtőbordák, turbóventilátor). A zárt rendszerű folyadékhűtés ellenőrzése, karbantartása. A szivattyús olajozás ellenőrzése (olajszint, utántöltés, olajnyomás, tömítettség).	×	×	×
A motor indítása a hidegindító-berendezések működtetésével. A levegőszűrők karbantartása. A kipufogórendszer ellenőrzése.	×	×	×
A dízel tápszivattyú karbantartása. A főszűrők karbantartása, a betét cseréje. A tüzelőanyag-ellátó rendszer kisnyomású részének légtelenítése.	×	×	×
A befecskendező szivattyú karbantartása, kenése.	×	×	–
Az akkumulátor elektrolitszintjének ellenőrzése, az utántöltés. Az akkumulátor töltöttségének ellenőrzése. Az akkumulátor összekapcsolása az akkumulátor-töltővel. Indítás külső akkumulátorról.	×	×	×

Ismeretanyag (elvégzendő műveletek)	2007	2013	2015
Az akkumulátor-főkapcsoló használata. Gondozásmentes akkumulátor ellenőrzése.	–	–	×
A generátor ellenőrzése (a motort működtetve a töltés ellenőrzése). Az indítómotor ellenőrzése (a csatlakozók megtisztítása, rögzítése).	×	×	×
A világító- és jelzőberendezések működtetése, ellenőrzése. Egy-egy izzó ki- és visszaszerelése. A tompított fényszóró átvilágítási képének ellenőrzése a fényszóró elé tartott fehér papírlapon.	×	×	×
A vezetékhálózat ellenőrzése, a zárlat vagy szakadás elhárítása, biztosítócsere. A dízelmotor indítását segítő berendezések ellenőrzése, karbantartása, az izzógyertyás berendezés hibái.	×	×	×
A tengelykapcsoló ellenőrzése. A pedál holtjátékának ellenőrzése és beállítása. Mechanikus, hidraulikus erőátvitel ellenőrzése, karbantartása.	×	×	×
A sebességváltó, a differenciálmű, egyéb hajtóművek olajszint-ellenőrzése. A kardántengely csavarkötéseinek ellenőrzése.	×	×	–
A kerékpántok és keréktárcsák ellenőrzése és karbantartása. A gumiabroncs állapotának, a mintázat mélységének ellenőrzése. Kerékcsere végrehajtása tehergépkocsi ikerkerekes tengelyén.	×	×	×
Kerékagy, a kerékfelfüggesztés ellenőrzése. A laprugózás ellenőrzése és karbantartása. A hidraulikus szervokormány ellenőrzése (szivattyúhajtás, olajszint, csövek, csatlakozók).	×	×	×
Abroncstöltés a légfékrendszerből.	–	–	×
A kerékfékszerkezetek ellenőrzése, karbantartása (a betétek vastagsága, tisztítása). A hidraulikus üzemifék ellenőrzése, karbantartása (üzemképesség, a folyadékszint, az utántöltés, a légtelenítés).	×	×	×
A légfék berendezés ellenőrzése, karbantartása (légsűrítő, nyomásszabályozók, légtartályok, munkahengerek. A fékvezetékek és főfékszelep tömítettségének vizsgálata. Fékezőnyomás vizsgálata.	×	×	×
Szűrők, fagymentesítő vizsgálata.	×	×	–
Légszárító vizsgálata.	–	–	×
A kombinált fék vizsgálata.	×	×	–
A rögzítőfékek ellenőrzése, karbantartása. A pneumatikus vezérlésű (rugóerőtárolós) fék ellenőrzése. A rögzítőfék oldása, ha a levegő „megszökik".	×	×	×
A lassítófék ellenőrzése, karbantartása.	×	×	×

3. táblázat: A biztonsági ellenőrzési ismeretek tantárgy ismeretanyagai különböző években a „C" járműkategóriánál

A biztonsági ellenőrzés és üzemeltetés témaköreiben lényegesen kevesebb változtatás történt, mint a szerkezeti és üzemeltetési ismereteknél. Az akkumulátor főkapcsoló, a gondozásmentes akkumulátor és az abroncstöltés a légfékrendszerből témakörének megjelenése nem tekinthető új ismeretnek, mert már évekkel ezelőtt elterjedten alkalmazták őket. Ezeket inkább mint hiánypótlást tekintem. A kombinált fék kihagyása egy logikus döntés volt, mert pár, főként speciális alkalmazást tekintve ilyen gépjárművekkel alig találkozni a közúti közlekedésben. A korszerű légfékrendszerekben alkalmazott légszárító témakör fontos ismereteket ad, mert gyakori a használatuk, de a különféle fagymentesítő berendezések elhagyása még korainak tűnik, mert elég sok járműben megtalálhatók, és nem kellő szintű ismeretük komoly üzemzavarokat okozhat a gépjármű fékrendszerében.

Összefoglalás

A közúti gépjárművezetési képzésre adható óraszámot a közlekedési hatóság csak minimumban határolja be, vagyis elvileg az autósiskolák több órát is tudnának fordítani a tananyag elsajátítására, de ez a jelenlegi versenypiacon csak elméleti lehetőség. Az utóbbi években megtörtént a műszaki ismeretek tananyagának korszerűsítése, és így elmondható, hogy most már végre tényleg azt tanulják a leendő gépjárművezetők, amire a valós életben szükségük is lesz. Az ismeretanyag széles körű, minden fontos témát átfed, és kellő részletességgel kibont. A probléma az ismeretanyag nagyságából, bonyolultságából és a rendelkezésre álló csekély időkeret kapcsolatából adódik, vagyis ekkora ismeretanyagot, a közlekedési hatóság által elvárható minőségben a rendelkezésre álló időkeretben szinte lehetetlen feladat leoktatni. Az autósiskolák által biztosított tantermi oktatáson felül nagyon sok időt kell még a tanulóknak ráfordítaniuk a kellő szintű elsajátítás érdekében.

Irodalomjegyzék

[1] Nemzeti Közlekedési Hatóság Tantervi és vizsgakövetelmények a „B" kategóriás járművezető-képző tanfolyamok számára, 3. változat, Nemzeti Közlekedési Hatóság Közúti Gépjármű-közlekedési Hivatal Képzési és Vizsgáztatási Főosztály, Budapest, 2015, 4.

[2] Nemzeti Közlekedési Hatóság Tantervi és vizsgakövetelmények a „C" kategóriás járművezető-képző tanfolyamok számára, 3. változat, Nemzeti Közlekedési Hatóság Közúti Gépjármű-közlekedési Hivatal Képzési és Vizsgáztatási Főosztály, Budapest, 2015, 4.

[3] 1/1975. (II. 5.) KPM-BM együttes rendelet a közúti közlekedés szabályairól, I. rész: Bevezető rendelkezések. A közlekedésben résztvevőkre vonatkozó általános rendelkezések, 3. § (1) bekezdés (C) pont.

[4] 24/2005. (IV. 21.) GKM rendelet a közúti járművezetők és a közúti közlekedési szakemberek képzésének és vizsgáztatásának részletes szabályairól, 7. sz. melléklet, C) a gépjárművek vezetéséhez szükséges ismeret, jártasság, magatartás.

[5] Nem ismerjük kellően a KRESZT? Forrás: www.pecsma.hu/csemege/nem-ismerjuk-kello-en-a-kresz-t/ (a letöltés ideje: 2015. október 16.)

[6] Nem sokat ér a hazai KRESZ-vizsga. Forrás:www.vezess.hu/hirek/semmit-nem-er-magyarorszagi/57058/ (a letöltés ideje: 2015. október 16.)

[7] Új elméleti kérdések a közúti járművezetők vizsgáztatásában. Közlekedésbiztonság, a Nemzeti Közlekedési Hatóság szakmai lapja, 2015/3, Magyar Közlekedési Kiadó Kft., Budapest, 2015, 15. (ISSN 2062-6916)

[8] Sajtóhírek – elméleti képzés és vizsgáztatás. Forrás: szakoe.hu/sajtohirek-elmeleti-kepzes-es-vizsgaztatas/ (a letöltés ideje: 2015. november 10.)

Changes in the Regulation of the National Transport Authority's "B" and "C" Category Driver Training

Vég Róbert László

The majority of technical education is realized during the theoretical education, which ends with a computerized exam (especially in category B). Technical education is important, because in case of high speed and high powered vehicles an engineering problem or the misunderstanding of its preceding signs can lead to serious traffic accidents, similarly to the disobeying of traffic rules. The transport authority specifies the teaching material of the technical education in great detail, but most of the time this material is not fully covered due to the lack of time. This article illustrates the role of technical education in the formation and in transport and evaluates the regulations of the transport authority and its changes.

Keywords: vehicle, traffic, technical, education, training

Tar Csaba

Korszerű irányított páncéltörő rakéták (FGM-148 Javelin és Spike-LR)

A második világháború jellemzően a páncélozott haditechnikai eszközök alkalmazásáról szólt, melyek harcászati jelentősége, szerepe a világháború után sem csökkent. Harctéri megsemmisítésükre a hatékony választ egy olyan „intelligens lövedék" kifejlesztése jelentette, melyet irányított páncéltörő rakétaként ismerünk. Jelen publikációmban célom a fegyverzeti eszközök ezen csoportjába tartozó korszerű típusok (FGM-148 Javelin, Spike-LR) bemutatása a fellelhető szakirodalmi adatok alapján.
Kulcsszavak: irányított páncéltörő rakéták, páncélozott eszközök, anti-tank guided missiles, armoured weapons

FGM-148 Javelin rakétarendszer

Az FGM-148 Javelin típusú hordozható, vállról indítható irányított páncéltörő rakétarendszert (1. kép) az amerikai Raytheon Company és a szintén amerikai Lockheed Martin társaság közös vállalkozásban fejlesztette ki az FGM-77 (M47 Dragon) típusú rakétarendszer leváltására. Rendszerbe állítása 1996-ban történt meg az USA-ban. [1; 1.]

1. kép:. FGM-148 Javelin irányított páncéltörő rakétarendszer (Forrás: [2])

A rendszer harmadik generációs, azaz Fire and Forget (FaF = „tüzelj és felejtsd el") elv alapján működik, melynek lényege, hogy a kezelő a hőképalkotó irányzékon keresztül kiválasztja és rögzíti a célt, majd indítja a rakétát. Az indítás előtti célrögzítést Lock-On-Before-Lunch (LOBF = „rögzítsd indítás előtt") típusú indításnak nevezzük. A rakéta a teljes röppályán önrávezetéssel halad, külső emberi beavatkozás nélkül.

Indítás előtt a kezelő a célra közelítés módját is meghatározhatja, mely lehet felülről támadó (Top Attack) vagy közvetlenül az irányzóvonal mentén támadó (Direct Attack). A Top Attack üzemmód olyan célok ellen alkalmazható, melyek páncélzata felülről sérülékenyebb, illetve ha a cél és az indítóegység között egy viszonylag kis méretű akadály, például egy fa van. A Direct Attack üzemmód a gyengébb oldalpáncélzatú célok leküzdésére szolgál. [3; 2–3.]

A rakéta hatótávolsága 70–2500 méter, harci része tandem HEAT (High Explosive Anti Tank = nagy hatóerejű páncéltörő robbanótöltet) töltetekből áll, vagyis reaktív páncélzattal védett célok megsemmisítésére is alkalmas. Elméleti átütőképessége RHA (Rolled Homogeneous Armour = hengerelt homogén páncélzat) páncélzaton 700 mm.

A rendszer alapfelépítését tekintve az M98A1 típusú indítóegységből, valamint magából a páncéltörő rakétából áll.

Az M98A1 típusú indítóegység (Central Lunch Unit, CLU) tartalmazza a

– nappali irányzékot (optikai),
– az infravörös tartományú éjszakai irányzékot,
– a vezérlőegységet és
– a védőburkolatot.

A terjedelmi paramétereket tekintve, az indítóegység hosszúsága 34,82 cm, magassága 33,88 cm, szélessége 49,91 cm, az össztömege 6,42 kg.

– A nappali irányzék nagyítása max. 4,2-szeres, látószöge pedig 4,8° × 6,4°.
– Az éjszakai irányzék 2 csatornás: a nagylátószögű nagyítása 4,2-szeres, látószöge 4,58° × 6,11°; a kislátószögű nagyítás 9,2×, látószög 2,00° × 3,00°.

A hőképalkotó irányzék kamerája CCD (Charge-Coupled Device = töltéscsatolt eszköz) érzékelős, mely 64×64 darab HgCdTe anyagú – mely a 8–12 μm hullámhossztartományra érzékeny – félvezető pixelből áll (4096 darab), és az optikai gyűjtőlencse fókuszsíkjában helyezkedik el. Terepmegfigyelésre a széles látószög-tartományú optika, célazonosításra pedig a kis látószög-tartományú optika lép működésbe.

A rakéta tartalmazza az

– indítóhajtóművet,
– a gyorsító-menet hajtóművet,
– a stabilizáló síkokat (szárnyak) a rakéta középső részén,
– a kormánysíkokat (lapátok) a rakéta hátsó részén,
– az elő- és főtöltetet (külön-külön detonátorral),
– az I2R típusú IR CCD érzékelőt tartalmazó keresőfejet;
– az irányító és biztonsági elektronikai elemeket.

A rakéta tömege 11,8 kg, hosszúsága 108,2 cm, átmérője 12,7 cm.

A rakéta az indításáig indítókonténerben van elhelyezve, mely biztosítja a tárolás és szállítás közbeni védelmét. A konténer saját tömege 2,86 kg, hosszúsága 121,4 cm, átmérője 14,21 cm. [4; 1–4.]

A rakétarendszer összműködését tekintve a kezelő:

– az indítóegység elektronoptikai képalkotóján keresztül megfigyeli a terepet (az irányzási szögtartomány horizontálisan: 0–360°, vertikálisan: 0–90°; felderíti és kiválasztja a célt;
– aktiválja a rakéta keresőfejét, amely rááll a kiválasztott célra; sikeres detektálás esetén a kereső visszajelzést ad a CLU megjelenítőjére;
– a szálkereszttel kijelöli a keresőfej részére a cél referenciaponját (tömegközéppontját), mellyel a célkiválasztás véglegesítése végrehajtásra kerül;
– meghatározza a rakéta röppályájának típusát (Top Attack vagy Direct Attack);
– indítja a rakétát.

Majd ezt követően

– a rakéta indítóhajtóműve kiveti a rakétát az indítókonténeréből;
– az indítókonténertől kb. 65 méterre a rakéta gyorsítómenet hajtóműve működésbe lép: a rakétát felgyorsítja a menetsebességre, majd becsapódásig ezen a sebességen tartja;
– a rakéta a teljes röppályán önrávezetéssel halad, külső emberi beavatkozás nélkül;
– a rakéta becsapódásakor az előtöltet berobbantja a harckocsi reaktív páncélzatát (ha van), majd a főtöltet koncentrált kumulatív sugara áthalad a harckocsi alappáncélzatán.

A teljes komplexum szállítását 1 raj (3 fő) végzi, ebből 1 fő az indítóegységet és 1 db rakétát, a másik két fő pedig 2-2 db rakétát szállít.

A rakéta harchelyzetbe történő állítása 30 másodperc, újratöltési ideje 20 másodperc. A rakéta indítható: fekvő, ülő (törökülés; felhúzott térd), térdelő, féltérdelő és álló testhelyzetből.

A rakétarendszer előnyei:

– Mivel a konstrukció nem háromlábú állványhoz kötött, ezért a harc- és menethelyzetbe állítási idő rövid, az irányzási szögtartománya pedig maximális.
– Mozgékonyság: a Fire-and-Forget rendszer lehetővé teszi a kezelő számára az indítás utáni azonnali tüzelőállás-változtatást, mely jóval nagyobb biztonságot nyújt a kezelőnek egy SACLOS (= Semi-Automatic Command to Line Of Sight = félautomata parancs az irányzóvonalhoz) típusú rakétához képest.
– Hatóerő: a dupla kumulatív töltet előtöltete megsemmisíti a páncélozott harci eszköz reaktív páncélzatát, ami után a főtöltet képes áthatolni az alappáncélzaton. Top Attack módban pedig a legkevésbé védett helyen támadja a harcjárművet, biztos megsemmisítést biztosítva ezzel.

– Lágy indítás: az indításkor hátrafelé ható lökőfázis alacsony energiájú, mellyel nemcsak harcászati, de taktikai alkalmazásra is bevethető (városi, épületharcászati alkalmazás).

A rakétarendszer hátrányai:

– Hőképes irányzék: az üzemi hőmérsékletre történő lehűléshez gyártói információ szerint kb. 30 másodperc szükséges, de ez nyilván függ a környezeti hőmérséklettől is, mely ezt az időt könnyen meghosszabbíthatja (akár 2,5-3,5 perc is lehet).
– Indítás után a kezelőnek már nincs lehetősége a rakéta irányítására a röppályán.
– A rakéta hivatalos hatótávolsága 2500 méter, amelyet több alkalmazásban lévő irányított páncéltörőrakéta-típus is meghalad.
– Értékesítési ára relatíve nagy. 2009-es adat szerint 1 darab indítóegység 142 ezer USA dollárba, míg 1 darab rakéta 126 ezer USA dollárba került.

Spike-LR (long range) rakétarendszer

A Spike-LR rakétarendszert (2. kép) az izraeli Rafael Advanced Defense Systems fejlesztette ki és gyártja a SACLOS rendszerű FGM-77 (M47 Dragon) rakétarendszer leváltására. Az 1990-es évek elején került rendszeresítésre Izraelben. [5; 1.]

2. kép: Spike-LR irányított páncéltörő rakétarendszer (Forrás: [6])

A rendszer 4. generációs üzemmódban is alkalmazható, mert a Fire and Forget üzemmód mellett a Non Line of Sight (NLOS = nem irányzóvonalas) működési elvet is képes használni (külön-külön), melynek során a kezelő nem egy konkrét célt, hanem egy célkörzetet választ ki, ahová indítja a rakétát. A röppályán haladó rakéta elektronoptikai képalkotójának valós idejű videoképeit széles sávú optikai kábelen keresztül küldi az indítóegység videokijelzőjére, melynek valós idejű értékelése alapján a kezelő kiválaszt(hat)

ja a konkrét célt, melyet a rakétának meg kell semmisítenie. A célkiválasztás ezen üzemmódját nevezik még Fire, Observe and Update (FOU = „tüzelj, figyelj és frissíts"), illetve Lock-On-After-Lunch (LOAL = rögzítsd indítás után) üzemmódnak is.

A rakéta hatótávolsága 75–4000 méter, harci része szintén tandem HEAT töltetekből áll, vagyis reaktív páncélzattal védett célok megsemmisítésére is alkalmas. Elméleti átütőképessége (RHA páncélzaton) 750 mm.

A rendszer alapfelépítését tekintve szintén egy indítóegységből, valamint magából az indítókonténerben lévő rakétából áll. [5]

Az indítóegység tartalmazza:

– a dual CCD-s hőképalkotós irányzékot, mely egyidejűleg képes a nappali és az éjszakai irányzásra,
– a vezérlőegységet,
– a védőburkolatot,
– a háromlábú indítóállványt.

A rakéta felépítése:

– indítóhajtómű;
– gyorsító-menet hajtómű;
– szárnyak;
– kormánylapátok;
– giroszkóp;
– előtöltet, főtöltet (külön-külön detonátorral);
– dual CCD-s irányzék keresőfej;
– irányító és biztonsági elektronikai elemek;
– feszültségtelep;
– felcsévélt optikai kábel (kb. 4000 méter).

A rakéta tömege indítókonténerben 13,5 kg, hosszúsága 120 cm, átmérője 14,21 cm. Gyártói szavatossági idő: 20 év (10 év után felülvizsgálat szükséges).

A rakétarendszer összműködése vázlatosan:

1. FaF üzemmódban: hasonlóan az FGM-148-hoz, kivéve azt, hogy a konstrukció háromlábú állványt tartalmaz, ami az irányzási szögtartományt korlátozza.

A kezelő

– az indítóegység elektronoptikai képalkotó irányzékán keresztül megfigyeli a terepet;
– kiválasztja a célt, melynek digitális képét átküldi a rakéta keresőjének megjelenítőjére;
– kijelöli, hogy a rakéta milyen üzemmódban (FaF vagy NLOS) és röppályán (Top Attack vagy Direct Attack) repüljön;
– indítja a rakétát.
– Majd ezt követően a rakéta

– indítóhajtóműve kiveti a rakétát az indítókonténeréből;
– az indítókonténertől kb. 75 méterre a gyorsító-menet hajtómű működésbe lép: a rakétát felgyorsítja a menetsebességre, majd becsapódásig ezen a sebességen tartja;
– a teljes röppályán önrávezetéssel halad, külső emberi beavatkozás nélkül;
– becsapódásakor az előtöltet berobbantja a harckocsi reaktív páncélzatát (ha van), majd a főtöltet koncentrált kumulatív sugara áthalad a harckocsi alappáncélzatán.

2. NLOS üzemmódban

A kezelő
– az indítóegység irányzékán keresztül megfigyeli a terepet;
– kiválasztja a célkörzetet (tehát nem a konkrét célt), melynek digitális képét átküldi a rakéta keresőjének elektronoptikai megjelenítőjére;
– NLOS üzemmódra kapcsol és meghatározza a röppálya típusát (Top Attack vagy Direct Attack);
– indítja a rakétát.

A rakéta
– indítóhajtóműve kiveti a rakétát az indítókonténeréből;
– az indítókonténertől kb. 75 méterre a gyorsító-menet hajtómű működésbe lép: a rakétát felgyorsítja a menetsebességre;
– önrávezetéssel halad a célkörzet felé, majd azt elérve (vagy akár előbb is) a rakéta által az optikai kábelen az indítóegység részére küldött videoképek alapján a kezelő ki tudja választani a konkrét célt, melyre a rakéta továbbra is önrávezetéssel rávezeti magát;
– becsapódásakor az előtöltet berobbantja a harckocsi reaktív páncélzatát (ha van), majd a főtöltet koncentrált kumulatív sugara áthalad a harckocsi alappáncélzatán.

A rakétarendszer előnyei:
– A rakéta legnagyobb előnye az FaF és az NLOS üzemmódra való képesség, mely a hatékony célkiválasztást és megsemmisítést nagymértékben elősegíti.
– A rakéta hatótávolsága 4000 méter, ami nagyon jó értéknek számít.
– Mozgékonyság: FaF röppálya üzemmódban a rendszer lehetővé teszi a kezelő számára az indítás utáni azonnali tüzelőállás-változtatást, mely jóval nagyobb biztonságot nyújt a kezelőnek egy SACLOS típusú rakétához képest.
– Hatóerő: a dupla kumulatív töltet előtöltete megsemmisíti a páncélozott harci eszköz reaktív páncélzatát, mely után a főtöltet képes áthatolni az alappáncélzaton. Top Attack módban pedig a legkevésbé védett helyen támadja a harcjárművet, biztos megsemmisítést biztosítva ezzel.
– „Lágy indítás": az indításkor hátrafelé ható lökőfázis alacsony energiájú, mellyel nemcsak harcászati, de taktikai alkalmazásra is bevethető (városi, épületharcászati alkalmazás).

A rakétarendszer hátrányai:

– a konstrukció háromlábú állványt tartalmaz, ami az irányzási szögtartományt korlátozza, valamint a harc-, illetve menethelyzetbe való helyezés idejét növeli (az FGM-148 Javelin-hez képest);
– NLOS üzemmódban a kezelő kitettsége természetesen megnő;
– hőképes irányzék üzemi hőmérsékletre történő lehűtéséhez a környezeti hőmérséklettől függően bizonyos időre van szükség.

Irodalomjegyzék

[1] IHS Jane's online adatbázis, Javelin Medium Anti-tank Missile System (az adatbázisba feltöltve: 2013. április 29.)

[2] www.raytheon.com/capabilities/products/javelin/, Javelin Weapon System, gyártói közzététel (a letöltés ideje: 2015. november 9.)

[3] Dr. Gyarmati József: Napjainkban alkalmazott irányított páncéltörő rakétarendszerek összehasonlító elemzése. *Katonai Logisztika*, 20(2012)/3.

[4] *FM 3-22.37 Javelin — Close combat missile system, medium.* Headquarters Department of the Army, Washington DC, 2008.

[5] IHS Jane's online adatbázis, Spike Multi-purpose Precision Weapon Systems (az adatbázisba feltöltve: 2014. július 31.)

[6] www.rafael.co.il/Marketing/343-997-en/Marketing.aspx, Long Range Multi-Purpose Tactical Missile, gyártói közzététel (a letöltés ideje: 2015. november 10.)

Modern Anti-Tank Guided Missiles (FGM-148 Javelin and Spike-LR)

TAR CSABA

The Second World War II basically meant the applying of the armoured military equipments, which tactical importance, after the World War, is not reduced. The effective answer was for their destroying in the battlefield the developing of an „intelligent projectile", what is known as anti-tank guided missile. In this publication my aim is to introduce these weapons' modern representatives (FGM-148 Javelin, Spike-LR) by the available special literature.

Keywords: anti-tank guided missiles, armoured weapons

Horváth István

A gammacsillagászat kezdetei

A gammakitörések a világegyetem máig ismert legnagyobb energiakibocsátással járó folyamatai. Jelen munka a felfedezésüket és korai kutatásukat tárgyalja.
Kulcsszavak: csillagászat;, gammacsillagászat;, gammakitörések;, kutató műholdak

A gammakitörések felfedezése

Hosszas tárgyalások után, 1963. augusztus 5-én a Szovjetunió, az Amerikai Egyesült Államok és az Egyesült Királyság képviselői Moszkvában aláírták a Nemzetközi Atomcsend Egyezményt (Nuclear Test Ban Treaty), amely megtiltotta az atombomba-kísérleteket a légkörben, a világűrben és a víz alatt.[1] Az egyezményhez azóta több mint száz ország csatlakozott, viszont Kína és Franciaország máig sem.

Az egyezmény betartásának ellenőrzésére hozta létre az Egyesült Államok a Vela projektet, és lőtték fel a világűrbe a Vela műholdakat. A Vela szó spanyol eredetű (velar), jelentése őr vagy felügyel. Mivel ezek a műholdak fedezték fel a gammafelvillanásokat, ezért a projektről részletesen kell szólnunk.

A programot 1959-ben indították el, viszonylag csekély költségvetéssel. Összesen tizenkét műholdat indítottak, hatot a Vela Hotel, hatot az Advanced Vela felépítéssel (Klebesadel, 2012). A hat Vela Hotel műhold űrbéli nukleáris robbanások után kutatott, míg az Advanced Vela hagyományos robbanásokat is megfigyelt. A műholdakat a TRW (Thompson Ramo Wooldridge) cég gyártotta.

A hidegháború javában dúlt, az amerikaiak biztosra akartak menni, így a legvadabb elképzeléseket is ellenőrizni akarták. Ma már talán hihetetlennek tűnik, de attól is tartottak, hogy a Szovjetunió a Hold túlsó oldalán robbant kísérleti atomtölteteket (Vedrenne–Atteia, 2009). (2000-ben nyilvánosságra hozták, hogy maga az amerikai légierő is tervezett 1958-ban nukleáris robbantást a Holdon.) Ezek megfigyeléséhez több magas pályán keringő műholdra volt szükség. Végül a műholdakat a Van Allen-féle sugárzási övezet fölé, négyszeres geoszinkron magasságú (120 ezer kilométer magas) pályákra állították [Klebesadel, 2012].

1 Az egyezmény szövege a következő helyen található meg az interneten: www.ctbto.org/fileadmin/content/treaty/treatytext.tt.html

A műholdakat párosával indították, az első Vela Hotel-párt (Vela-1A és Vela-1B) 1963 augusztusában. A második párt (Vela-2A és Vela-2B) 1964-ben, a harmadikat (Vela-3A és Vela-3B) 1965-ben állították pályára, tervezett élettartamuk 6 hónap volt, aminek végül több mint tízszeresét szolgálták ki. A műholdakat 12 külső röntgendetektorral és 18 belső neutron- és gammasugár-detektorral szerelték fel [Klebesadel–Strong–Olson, 1973].

A légköri atom- vagy hidrogénbomba-robbanás a másodperc ezredrészéig tartó gammavillanást produkál, amit a kialakuló tűzgolyó fénysugárzása követ. A műholdak milliszekundumos skálán figyelték a jelenségeket, így több műhold együttes megfigyelése esetén a forrás térbeli helyzete egyszerű háromszögeléses módszerrel, nagyjából 5000 kilométeres pontossággal meghatározható volt a Föld felszínén. Távoli források esetén ez nyilvánvalóan csak iránybeli lokalizációt jelent, amely azonban elegendő a lunáris vagy szoláris források azonosításához. Az irányszög meghatározásának hibája nagyjából 8–15 fok volt.

Az Advanced Vela párokat 1967-ben (Vela-4A és Vela-4B), 1969-ben (Vela-5A és Vela-5B) és 1970-ben (Vela-6A és Vela-6B) indították, de már nem az Atlas Agena rakétákkal, mint az előző párokat, hanem a sokkal erősebb Titan IIIc rakétával, így a tömegük is nagyobb lehetett. Tervezett élettartamuk másfél év volt, de ezek a műszerek is tízszeresen felülmúlták az előzetes terveket. Az utolsó 1984-ig működött. Az Advanced Vela műholdak hat darab cézium-jodid gammadetektorral voltak felszerelve, melyek teljes térfogata kb. 60 cm^3 volt, és 150–750 keV (kiloelektronvolt) közötti energiájú fotonokat voltak képesek észlelni.

A műholdak a megfigyelt adatokat továbbították a Földre. Nukleáris bomba robbanását röntgensugárzás jelezte volna, melyet a gamma- és neutrondetektorok megfigyelése erősített volna meg. A Hold túloldalán történt robbanást közvetlenül nem észlelték volna a Vela műholdak, de a felvert nukleáris por a robbanás erejétől olyan gyorsan tágult volna, melyet a műholdak a robbanás során aktivált atommagok gammasugárzását megfigyelve tudtak volna azonosítani.

Ray Klebesadel a Los Alamos Scientific Laboratory (ma LANL, Los Alamos National Laboratory) munkatársa (aki a Vela műholdak tervezésében és építésében is részt vett) elemezte a megfigyelt adatokat. Azokat a megfigyelési eredményeket is gondosan megőrizték, melyek biztosan nem nukleáris robbanást jeleztek. 1972-ben Ian Strongot kérték meg, hogy Klebesadellel és Roy Olsennel közösen értékeljék ki ezeket az adatokat, akik 16 olyan eseményt találtak, melyek bizonyosan nem földi, szoláris vagy lunáris eredetűek voltak (1969 júliusa és 1972 júliusa közötti jelenségekről volt szó). Gammatartományban olyan jelentős volt az emisszió, hogy ki lehetett zárni, hogy egy röntgenforrás nagyenergiás részéről legyen szó. Ebből az eredményből született meg az első gammakitörés (gamma-ray burst vagy röviden GRB) publikáció [Klebesadel–Strong–Olson, 1973].

Cline és Desai az IMP-6 műhold fedélzetén lévő röntgendetektorral a napflerek megfigyelését végezték. Értesülve a felfedezésről, az elsők voltak, akik megerősítették a gammavillanások létezését [Cline–Desai–Klebesadel–Strong, 1973]. Ezektől függetlenül az OSO-7 műhold gammadetektorai is megerősítették ezt a felfedezést. [Wheaton et al., 1973].

Bolygóközi hálózat

A gammakitörések véletlen felfedezésének hatására az azt követő években több műholdra és műbolygóra gammasugárzást megfigyelni képes műszereket szereltek fel. Az orosz mesterséges égitestekre általában felszereltek gammadetektorokat. Ezek esetében azonban az adatokhoz való hozzájutás okozott problémát. Volt gammadetektor az 1977-ben fellőtt Prognoz 6 és az 1978 októberében felbocsátott Prognoz 7 fedélzetén is. Mindkettő a Föld körül keringett. NaI és CsI gammadetektorok voltak a KONUS [Mazets et al., 1981], az ISEE-3 (International Sun-Earth Explorer) [Anderson et al., 1978] és az SMM (Solar Maximum Mission) [Forest et al., 1980] műbolygókon. Gammadetektorok voltak még a High Energy Astronomical Observatory (HEAO), az International Cometary Explorer (ICE), a Helios 2, a Hakucho, a Hinotorti, a Ginga, a Phobos [Higdon–Lingenfelter, 1990] és az Apollo-16 fedélzetén is [Metzger et al., 1974].

A gammavillanások tisztázatlan eredete miatt fontos lett volna a pontos lokalizáció az esetleges források tanulmányozására. A helymeghatározás egy detektor esetén lehetetlen, hiszen így csak a fotonok beérkezését lehet rögzíteni. Megfelelő elektronikával ez a beérkezés milliszekundumos pontossággal volt rögzíthető. Két egymástól távoli detektor megfigyelése esetén a megfigyelt jelek időkülönbségéből az égi helyzet meghatározható. Pontosabban szólva két független megfigyelésből a számolható pozíció egy vékony körgyűrű az égen. Pontos lokalizáláshoz minimum három egymástól távoli műszer egyidejű megfigyelése szükséges [Atteia et al., 1987]. Itt a hangsúly az egymástól távoli kifejezésen van. Időben fél-egy perc, esetleg több perces eltérés szükséges. Vagyis a megfigyelőhálózat egy eleme keringhet a Föld körül, de a többi már nem. Így legalább két Földtől távoli műszer szükséges. A német Helios 2 műbolygó a Nap körül keringett, fedélzetén gammadetektorral, így kiválóan megfelelt e kutatási célra.

A harmadik tájékozódási pont a Vénusz körül keringő három műhold volt: az orosz Venyera 11 és 12 [Barat et al., 1981] valamint az amerikai PVO (Pioneer Venus Orbiter) [Klebesadel et al., 1980]. Mindhármat szintén 1978-ban bocsátották útjára. Az ún. első bolygóközi hálózat 1980-ig működött.[2] Megfigyelték a gammakitöréseket, majd a már említett háromszögelési módszerrel meghatározták a források irányát (84 kitörésre állapítottak meg égi koordinátákat [Hartmann–Epstein, 1989]). De a kibocsátás helyén még a legnagyobb távcsövekkel sem találtak semmit.

1990-ben felbocsátották az Ulysses műbolygót, majd 1991-ben a Compton Gamma Űrtávcsövet (CGRO, Compton Gamma Ray Observatory) [Fishman et al., 1994], így ismét létrejött egy bolygóközi hálózat [Cline et al., 1991].

2 www.powerset.com/explore/semhtml/InterPlanetary_Network?query=grb

Milyen távol vannak?

A ’80-as évek végéig közel 500 gammafelvillanást észleltek a különböző műholdak [Fishman–Meegan, 2012]. Ezek nagy részét a PVO [Evans–Fenimore–Klebesadel–Laros–Terrel, 1981] és a KONUS [Mazets et al., 1981] figyelte meg, de a felvillanásoknak az eredete még tisztázásra várt. Nem volt ismeretes egy azonosított forrásuk sem, de még azt sem tudtuk, hogy milyen messze lehetnek a források. Tehát az sem volt ismeretes, hogy a forrás milyen erős, ugyanis a mért gammasugárzást okozhatta egy közeli gyenge forrás vagy egy távoli, de ennél sokkal erősebb forrás is.

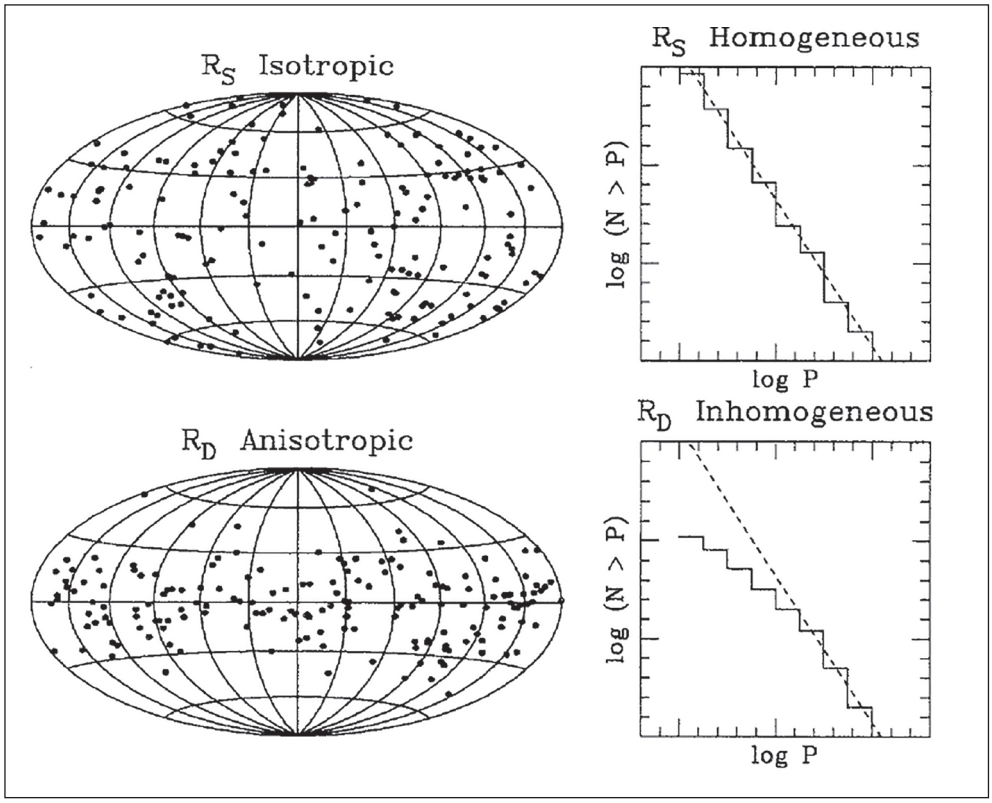
Az egyik elfogadható feltételezés a galaktikus neutroncsillagokból jövő sugárzás volt [Higdon–Lingenfelter, 1990], [Harding, 1994], [Colgate–Li, 1996]. Ez esetben a források a galaxis síkjában vagy a galaktikus haloban helyezkednének el, kiloparszek, illetve 10-20 kiloparszek távolságban.

A különféle asztrofizikai objektumok távolságának a meghatározásában nagy szerepe van az égbolton való eloszlásuknak, elhelyezkedésüknek. Lehetnek a források a Naprendszerben vagy ahhoz közel. Ha például a források a bolygók felszínén vannak, akkor az égen ábrázolva az ekliptika mentén helyezkednének el, korrelálva természetesen a bolygópozíciókkal.

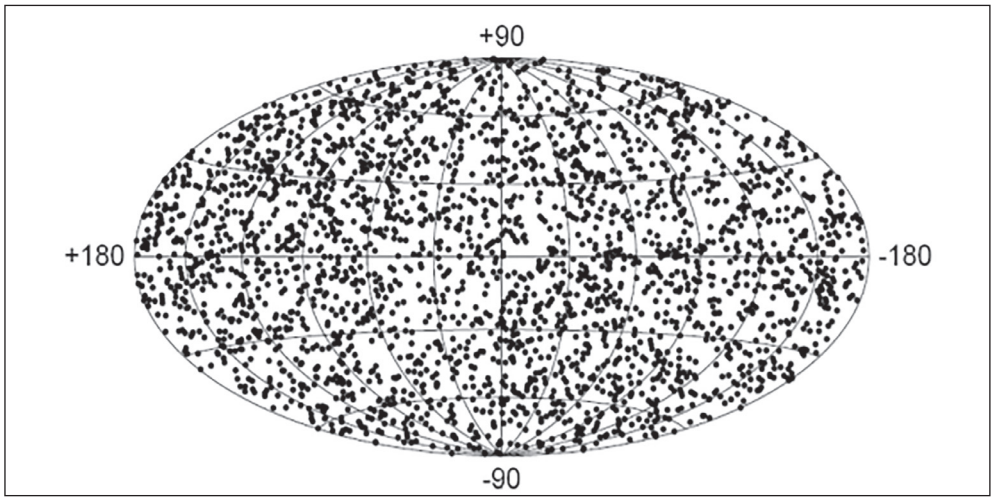
Ha valamely asztrofizikai megfigyelés esetén közeli csillagok lennének a források, akkor a helyük az égre vetítve véletlenszerűen helyezkedne el, tehát betöltenék a teljes eget. Ha egy adott távolságnál közelebb lévő források számát N-nel jelöljük, akkor a kétszer akkora távolságnál közelebb lévő források száma körülbelül 8N lenne, ha a források eloszlása homogén, hiszen a megfigyelt objektumok száma arányos a térfogattal.

Ha a galaxisunkban levő forrásokat figyelnénk a Földről, akkor a kétszer olyan távolságban lévő források száma csak 4N lenne, hiszen a források egy lapos korongban helyezkednek el (pl. az 1. ábra bal alsó ábrája), és a kétszer akkora sugarú kör területe csak négyszer nagyobb.

Tehát a források számának a fényességüktől való függése információt ad a források térbeli elhelyezkedésével kapcsolatban. Nézzünk egy egyszerű példát. Töltsék ki a források a teljes teret egyenletesen, és legyen minden forrás egyforma fényességű. Ez esetben a legfényesebbnek látszó forrás van hozzánk legközelebb. A négyszer halványabb források kétszer messzebb vannak, de mivel a kétszer nagyobb sugarú gömb térfogata nyolcszor nagyobb, ezért a négyszer halványabb források száma átlagosan nyolcszor több. A kitevőben lévő kettes és hármas eredményeképpen a logaritmikus ábrázolásnál a jelenséget egy mínusz háromketted meredekségű egyenes jól közelíti. Ez a híres „–3/2”-es törvény.



1. ábra: A Gamma-ray Bursts kötetben bemutatott ábra szemlélteti, hogy homogén térbeli eloszlás esetén (jobb felső ábra) statikus euklideszi térben az égbolteloszlás egyenletes (izotróp) kell legyen. Amennyiben a térbeli eloszlás nem homogén (jobb alsó ábra), úgy az égbolteloszlás sem az (Forrás: Fishman–Meegan, 2012)]



2. ábra: A gammakitörések eloszlása az égbolton a Compton Gamma Obszervatórium Burst And Transient Source Experiment (BATSE) adatai alapján

A Compton Gamma Ray Observatory (CGRO) műhold egyik nagy tudományos eredménye volt a kitörések égi eloszlásának megmérése. Ez az eloszlás egyenletes eloszlást mutatott az égbolton (lásd a 2. ábrát) [Meegan et al., 1996], [Vavrek et al., 2008]. Ez a megfigyelés kizárta a galaktikus eredetet. Ugyanis ha a források nagy része a teljes galaxisban található, akkor a galaxis síkjának látszódnia kellene az égi eloszláson. Ennek ellenére egészen 1996-ig tartotta magát a kiterjesztett galaktikus halo-eredet hipotézise (extended galactic halo) [Brainerd, 1992], [Podsiadlowski–Rees–Ruderman, 1995].

Ha a források egyenletesen oszlanak el az égen, akkor csak három térrész képzelhető el a források eredetére:

1. A Naprendszer-közeli tér.

2. A fényes csillagokhoz hasonlóan egy néhány tucat, maximum néhány száz parszeknyi térrész.

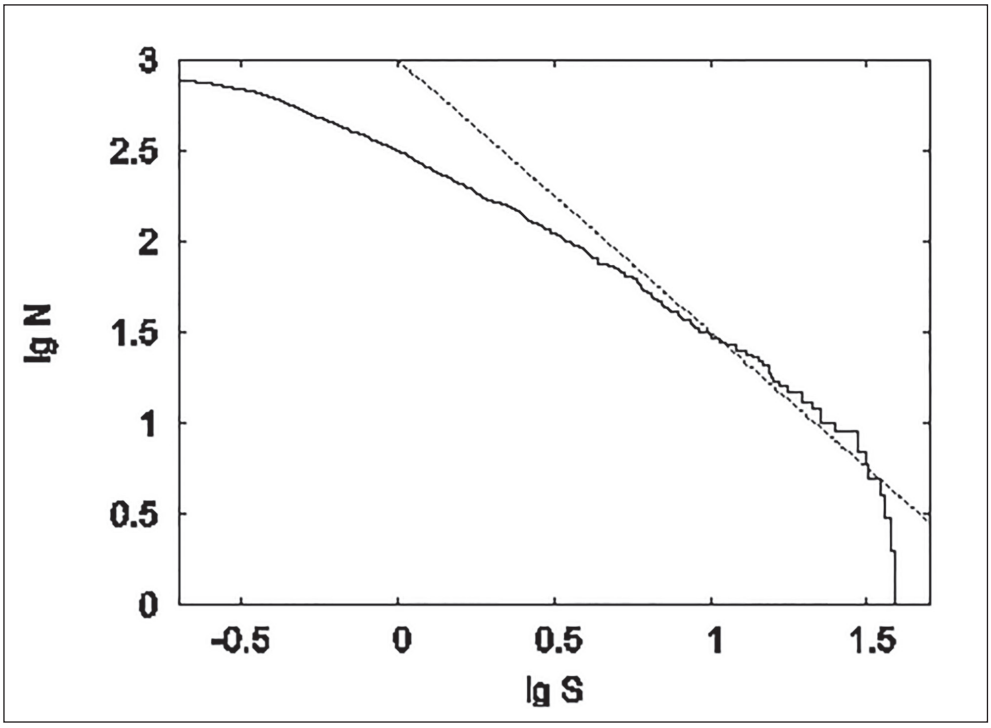
3. Száz megaparszek vagy annál lényegesen nagyobb sugarú tér.

Az elsővel kapcsolatban dolgozták ki az üstökös felhő elméletet, amely a 100–1000 CsE (csillagászati egység = Nap–Föld-távolság) távolságban keringő üstökösöket tekintette forrásnak [Bickert–Greiner, 1993], [White, 1993], [Luchkov, 1994].

A háromféle eredet között segít választani a fényességeloszlás-ábra, az ún. logN – logS diagram [Cohen–Piran, 1995], [Fenimore–Bloom, 1995]. A 3. ábra mutatja közel ezer kitörés látszó fényesség szerinti kumulatív eloszlását [Horváth–Mészáros P.–Mészáros A., 1996]. A függvény értéke azt adja meg, hogy hány kitörést figyeltünk meg adott idő alatt, amely az adott fényességnél (S) fényesebb volt.

Euklideszi tér és homogén térbeli eloszlás esetén a már az előzőekben leírt okok miatt egy körülbelül –1,5 meredekségű egyenest (szaggatott vonal a 3. ábrán) kell kapnunk a log-log ábrán. Ez csak a fényes kitörésekre igaz a gammakitörések esetén [Fishman et al., 1994], [Veres et al., 2010], [Perez-Ramirez et al., 2010]. A halvány kitörések hiányát persze lehetne magyarázni elnyeléssel, de csillagászati megfigyelésekből tudjuk, hogy sem a Naprendszer közelében, sem a néhány száz parszekes környezetünkben nincs lényeges elnyelő anyag. Egy mindent áteresztő, csak gammában elnyelő közeg feltételezése pedig abszurd lenne.

Mindezek alapján nyilvánvalóan csak a harmadik eset lehetséges. Ugyanis valóban euklideszi tér esetén mindig igaz a mínusz másfeles törvény. Tudjuk viszont, hogy a világunk nem euklideszi, hanem riemanni [Riemann, 1854], [Einstein, 1916], [Friedmann, 1922], [Paál–Horváth–Lukács, 1992]. A kozmológiai megoldások ([Walker, 1936], [Peebles, 1993]) valóban megmagyarázhatják a mért logN – logS eloszlást [Cohen–Piran, 1995], [Fenimore–Bloom, 1995], [Horváth–Mészáros P.–Mészáros A., 1996]. Azonban ehhez a kitörések forrásait a legtávolabbi kvazárok távolságáig kell elképzelnünk. Ezt az elképzelést már a hetvenes években felvetették [Usov–Chibisov, 1975], [Prilutskii–Usov, 1975], de csak Paczynski cikke [Paczynski, 1986] után vették többen komolyabban. Pedig az 1. ábráról is világosan látszik, hogy euklideszi tér esetén, egyenletes eloszlásnál a bal felső égi és jobb felső térbeli eloszlást, vagy a két alsó eloszlást figyelhetjük meg. De a gammaki-



3. ábra: A gammakitörések megfigyelt fényességeloszlása (a szerző saját szerkesztése)

törések a bal felső és jobb alsó eloszlásokat követik. Ez csak akkor lehetséges, ha az általuk kitöltött tér nem euklideszi. A nagyon távoli (kozmológiai távolságban levő) objektumok által kitöltött tér nem euklideszi, mert a négydimenziós téridő görbült.

Mindezek ellenére többeknek ez annyira hihetetlennek tűnt, hogy a tudóstársadalom legalább fele inkább az egyre extrémebb kiterjesztett halo elméletek kidolgozásán fáradozott. Tették mindezt egészen 1997-ig, az első gammakitörés-utófény, illetve -forrás azonosításáig, melyet a BeppoSAX műhold tett meg.

Irodalomjegyzék

K. A. Anderson – S. R. Kane – J. H. Primbsch – R. H. Weitzmann – W. D. Evans – R. W. Klebesadel – W. P. Aiello: *X-ray spectrometer experiment aboard the ISEE-C /Heliocentric/ spacecraft,*. IEEE Transactions on Geoscience Electronics, Volume GE-16, 1978, 157–159.

J.–-L. Atteia et al.: A Second Catalog of Gamma-Ray Bursts: 1978–1980 Localizations from the Interplanetary Network,. *The Astrophysical Journal's,* Volume 64, 1987, 305–382.

C. Barat – G. Chambon – K. Hurley – M. Niel – G. Vedrenne – I. V. Estulin – A. V. Kuznetsov – V. M. Zenchenko: The Signe 2 Franco-Soviet interplanetary gamma ray burst experiment network,. *Space Science Instrumentation,* Volume 5, 1981, 229–235. (Centre National d'Etudes Spatiales).

K. F. Bickert – J. Greiner: *Gamma-ray bursts from collisions of primordial small-mass black holes with comets*, AIP Conf. Proc., No. 280, 1993, 1059–1063.

J. Brainerd: Gamma-Ray bursts in the galactic halo,. *Nature,* Volume 355, 1992, 522–524.

S. A. Colgate – H. Li: *Gamma-ray bursts from the interaction of degenerate disks with fast neutron stars* = eds. C. Kouveliotou – M. S. Briggs – G. J. Fishman (eds.): *Gamma-ray bursts: 3rd Huntsville symposium,.* AIP Conference Proceedings, Volume 384, 1996a, 734–738.

T. L. Cline – U. D. Desai – R. W. Klebesadel – I. B. Strong: Energy Spectra of Cosmic Gamma-Ray Bursts,. *Astrophysical Journal,* Volume 185, 1973, L1–L5.

T. L. Cline et al.: *Gamma ray burst source locations with the Ulysses/Compton/PVO Network, Gamma-ray bursts,.* AIP Conference Proceedings, Volume 265, 1991, 72–76.

E. Cohen – T. Piran: The Distribution of Cosmological Gamma-Ray Bursts,. *The Astrophysical Journal,* Volume 444, 1995, L25–L28.

A. Einstein: Die Grundlage der allgemeinen Relativitatstheorie,. *Annalen der Physik,* Volume 49, 1916, 769–822.

W. D. Evans – E. E. Fenimore – R. W. Klebesadel – J. G. Laros, – N. J. Terrel: Gamma-burst observations from the Pioner Venus Orbiter,. *Astrophysics and Space Science,* Volume 75, 1981, 35–46.

E. E. Fenimore – J. S. Bloom: Determination of Distance from Time Dilation of Cosmological Gamma-Ray Bursts,. *The Astrophysical Journal,* Volume 453, 1995, 25–36.

G. J. Fishman – C. A. Meegan: *The BATSE era.* = eds. C. Kouveliotou – R. A. M. J. Wijers – S. Woosley (eds.): *Gamma-Ray Bursts,.* Cambridge University Press, Cambridge, 2012, 19–38.

G. J. Fishman et al.: The first BATSE Gamma-Ray Burst Catalog,. *The Astrophysical Journal Supplement,* Volume 92, 1994, 229–283.

D. J. Forest et al.: The gamma ray spectrometer for the Solar Maximum Mission,. *Solar Physics,* Volume 65, 1980, 15–23.

A. Friedmann: Über die Krümmung des Raumes,. *Zeitschrift für Physik,* Volume 10, 1922, 377–386.

A. K. Harding: Gamma-ray burst theory: Back to the drawing board,. *Astrophysical Journal Supplement Series,* Volume 90, No. 2, 1994, 863–868.

D. Hartmann – R. Epstein: The Angular Distribution os Gamma-Ray Bursts,. *The Astrophysical Journal,* Volume 346, 1989, 960–966.

J. C. Higdon – R. E. Lingenfelter: Gamma-ray bursts,. *Annual review of astronomy and astrophysics,* Volume 28 (A91-28201 10-90), Palo Alto, CA, Annual Reviews, Inc., 1990, 401–436.

Horváth I. – Mészáros P., – Mészáros A.: Cosmological Brightness Distribution Fits of Gamma-Ray Burst Sources,. *The Astrophysical Journal,* Volume 470, 1996, 56–62.

R. W. Klebesadel: *The discovery of the gamma-ray burst phenomenon.* = eds. C. Kouveliotou – R. A. M. J. Wijers – S. Woosley (eds.): *Gamma-Ray Bursts,.* Cambridge University Press, Cambridge, 2012, 1–8.

R. W. Klebesadel – W. D. Evans – J. P. Glore – R. E. Spalding – F. J. Wymer: The Pioneer Venus Orbiter Gamma Burst Detector,. *IEEE Transactions on Geoscience and Remote Sensing,* Volume GE-18, 1980, 76–80.

R. W. Klebesadel – I. B. Strong – R. A. Olson: Observations of Gamma-Ray Bursts of Cosmic Origin,. *The Astrophysical Journal,* Volume 182, 1973, L85–L88.

B. I. Luchkov: A cometary model for cosmic gamma-bursts., *Astronomy Letters,* Volume 20, Issue 2, 1994, 253–255.

E. P. Mazets – S. V. Golenetskii – R. L. Aptekar – Iu. A. Gurian, – V. N. Ilinskii: Cyclotron and annihilation lines in gamma-ray burst,. *Nature,* Volume 290, 1981, 378–382.

C. A. Meegan et al.: The Third BATSE Gamma-ray Burst Catalog,. *The Astrophysical Journal Supplement,* Volume 106, 1996, 65–110.

A. E. Metzger – R. H. Parker – D. Gilman – L. E. Peterson – J. I. Trombka: Observation of a cosmic gamma-ray burst on Apollo 16. I – Temporal variability and energy spectrum,. *Astrophysical Journal,* Volume 194, pt. 2, 1974, L19–L25.

Paál G. – Horváth I., – Lukács B.: Inflation and Compactification from Galaxy Redshifts? *Astrophysics and Space Science,* Volume 191, 1992, 107–124.

B. Paczynski: Gamma-ray bursters at cosmological distances,. *Astrophysical Journal,* Part 2, Volume 308, 1986, L43–L46.

P. J. E. Peebles: *Principles of Physical Cosmology,.* Princeton University Press, Princeton, New Jersey, 1993.

D. Perez-Ramirez et al.: Detection of the ultra-high z short GRB 080913 and its implications on progenitors and energy extraction mechanisms,. *Astronomy and Astrophysics,* Volume 510, 2010, Paper A105.

P. Podsiadlowski – M. J. Rees – M. Ruderman: Gamma-ray bursts and the structure of the Galactic halo,. *Monthly Notices of the Royal Astronomical Society,* Volume 273, Issue 3, 1995, 755–771.

O. F. Prilutskii – V. V. Usov: On the Nature of gamma-Ray Bursts,. *Astrophysics and Space Science,* Volume 34, 1975, 387.

B. Riemann: *Über die Hypothesen, welche der Geometrie zu Grunde liegen. Habilitationsschrift, Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen.* 1854, 13.

V. V. Usov – G. V. Chibisov: Statistics of gamma-ray bursts,. *Astronomicheskii Zhurnal,* Volume 52, No. 1, 1975, 192–194.

Vavrek R. – Balázs L. G. – Mészáros A. – Horváth I., – Bagoly Z.: Testing the randomness in the sky-distribution of gamma-ray bursts,. *Monthly Notices of the Royal Astronomical Society,* Volume 391, Issue 4, 2008, 1741–1748.

G. Vedrenne, – J.–-L. Atteia: *Gamma-Ray Bursts: The Brightest Explosions in the Universe,.* Springer Praxis Books, Springer-Verlag, Berlin, Heidelberg, 2009.

Veres P. – Bagoly Z. – Horváth I. – Mészáros A., – Balázs L. G.: A Distinct Peak-flux Distribution of the Third Class of Gamma-ray Bursts: a Possible Signature of X-ray Flashes? *Astrophysical Journal,* Volume 725, 2010, 1955–1964.

A. G. Walker: On Milne's Theory of World-Structure,. *Proceedings of London Mathematical, Society,* Volume 42, 1936, 90–127.

W. A. Wheaton et al.: The Direction and Spectral Variability of a Cosmic Gamma-Ray Burst,. *Astrophysical Journal,* Volume 185, 1973, L57–L61.

R. S. White: Some requirements of a colliding comet source of gamma ray bursts,. *Astrophysics and Space Science,* Volume 208, Issue 2, 1993, 301–311.

The Beginning of Gamma Astronomy

HORVÁTH ISTVÁN

Gamma-ray bursts are the most powerful explosions known in the universe. In this paper their discovery and some of their early studies are shown.

Keywords: astronomy, gamma astronomy, gamma-ray bursts, searching satellites

Fatalin László

The Classical Representations of the Conceptual Hierarchies with Graphs

Conceptual hierarchies are often presented in graphs. These typical representations or containment or derivation relationships are built. The classic visual depictions seem simple, but several sources of error can cause misunderstanding. This article discusses the logical shortcomings and misinterpretations of these representations through the example of convex quadrilaterals. Mathematical models used in the analysis can be discovered in the flowcharts ambiguities.
Keywords: hierarchical concept structures, flowchart, convex quadrilateral

Hierarchical system

The hierarchical connections of a concept system are often presented with graphs. Various methods are used to illustrate a hierarchical system, which this article intends to demonstrate on an example of structure of convex quadrilaterals.

The mathematical models of the hierarchical knowledge representation set out from the basic set $\mathscr{C}$. The elements of the basic set $\mathscr{C}$ can be the "knowledge units". The knowledge units can be modelled by the classes or by the structured objects. Also the elements of the set $\mathscr{C}$ are called pre-concepts. In this article we demonstrate it on an example of the structure of convex quadrilaterals that can be seen in Figure 1. (The expression of general quadrilateral means a quadrilateral without special characteristics.)

In general a hierarchy of concepts exists on set $\mathscr{C}$ and it is based on an order relation. One order relation can be either a weak partial order relation (reflexive, transitive, antisymmetric) or a strict partial order relation (irreflexive, transitive and asymmetric). From the point of view of didactics, the containment between concepts is primary. There are many conceptions about the formal basic containment relation $\leq$ on the set $\mathscr{C}$. In this paper, we take the binary concept relation $\leq$ for representing this containment relation of the concepts. The set $\mathscr{C}$ of pre-concepts and the relation $\leq$ create a formal concept system among these forms.

We are going to use a *hierarchical system* as the tuple $H := (\mathscr{C}, \leq)$ where $\mathscr{C}$ is a set whose elements are called pre-concepts, and $\leq$ is a binary partial order relation on the set $\mathscr{C}$ (i.e. $\leq \subseteq \mathscr{C} \times \mathscr{C}$ is a reflexive, transitive, antisymmetric relation).

The examined convex quadrilaterals C			
Figure as object	code	Figure as object	code
convex quadrilateral	1	parallelogram	7
general quadrilateral	2	rhombus	8
trapezium	3	rectangle	9
orthogonal trapezium	4	square	10
symmetric trapezium	5	cyclic quadrilateral	11
kite	6	circumscribed quadrilateral	12

Figure 1: The examined convex quadrilaterals with code

The finite hierarchical system can be given by containment table: we write a rectangular table with one row for each pre-concept and one column for each pre-concept, having a ≤ in the intersection of row *g* with column *m* if (sub)-concept *g* is (super)-concept *m* as representation of the knowledge units. The finite hierarchical system can be visualized by a graph with Hasse-convention.

Olosz (2005) gives one concrete inquest through the system of symmetric quadrilaterals. The related containment table is presented in figure 2/a and the graph of this inquest is presented in figure 2/b (Teaching of quadrilaterals in Hungarian elementary schools adopts this construction.)

Containment table			quadrilaterals					
			4	6	7	8	9	10
quadrilaterals	symmetric trapezium	5	≤					
	kite	6		≤				
	parallelogram	7			≤			
	rhombus	8		≤	≤	≤		
	rectangle	9	≤		≤		≤	
	square	10	≤	≤	≤	≤	≤	≤

Figure 2/a: The formal containment table '≤' of symmetric quadrilaterals

The examination of the quadrilateral classes is completed with the additional quadrilateral varieties. *Mitroica (1987)* gives one concrete hierarchical structure diagram of convex quadrilaterals that can be seen in Figure 3/a. (The containment table of this graph is presented in Figure 3/b.)

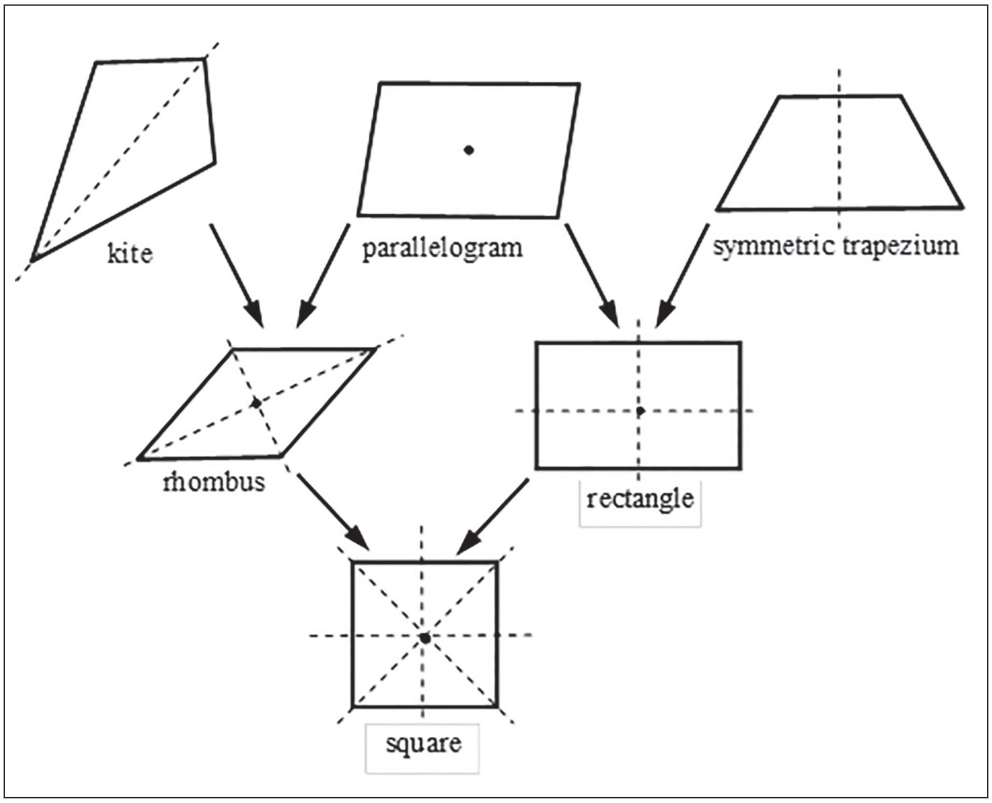


Figure 2/b: The genesis diagram of symmetric quadrilaterals by Olosz (p60)

It's important to observe that this analysis characterizes the examined classes of quadrilaterals only from containment aspect. One of the formal failures of the diagram is that it can lead to false conclusions, because it can be seen from the figure, that the common part of the sets of circumscribed quadrilateral and trapezium is the rhombus i.e.

circumscribed quadrilaterals ∩ *trapeziums* = *rhombuses.*

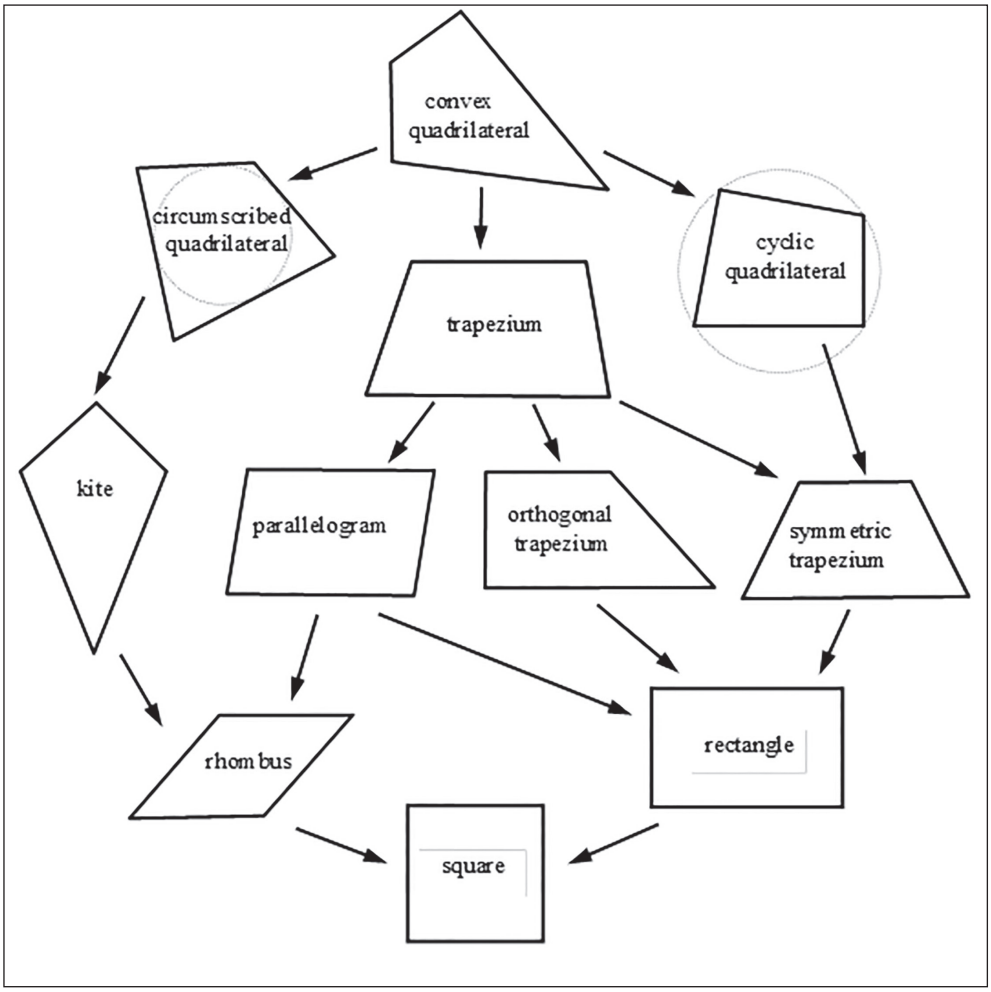


Figure 3/a: The hierarchical structure of the convex quadrilaterals by Mitroica (p58)

This description of the concept has one relevant drawback from the point of view of didactics: this formal model of the pre-concept (as an element of basic set) does not comprehend the objects and the attributes of the concept directly, i.e. a pre-concept has only intuitive content with explicit denomination. As a consequence, this graph does not present the aspect of the concept generalising or specialising, that is a central aspect in teaching.

containment table			quadrilaterals $\mathscr{C}$										
			1	3	4	5	6	7	8	9	10	11	12
quadrilateral $\mathscr{C}$	convex quadrilateral	1	≤										
	trapezium	3	≤	≤									
	orthogonal trapezium	4	≤	≤		≤							
	symmetric trapezium	5	≤	≤	≤							≤	
	kite	6	≤				≤						≤
	parallelogram	7	≤	≤				≤					
	rhombus	8	≤	≤			≤	≤	≤				≤
	rectangle	9	≤	≤	≤	≤		≤		≤		≤	
	square	10	≤	≤	≤	≤	≤	≤	≤	≤	≤	≤	≤
	cyclic quadrilateral	11	≤									≤	
	circumscribed quadrilateral	12	≤										≤

Figure 3/b: The formal containment table of convex quadrilaterals

The content of the convex quadrilaterals

To characterize the convex quadrilaterals the examined features need to be fixed. The mathematical modelling of the characterization sets out from the attributes set $\mathscr{A}$. This paper is based on the Hungarian National Curriculum *[NAT;1995]*, in which the constructions of curriculum are based on symmetrical and metrical properties. The symmetrical and metrical attributes are among the examined features. The attributes of set $\mathscr{A}$ with the code of the attributes are presented in figure 4.

The set of the attributes: $\mathscr{A}$	
Attributes of quadrilaterals	code
(at least) one parallel pair of sides	A
(at least) one equal pair of sides	B
two parallel pairs of sides	C
two equal pairs of sides	D

The set of the attributes: $\mathcal{A}$	
Attributes of quadrilaterals	code
equal sides	E
equal diagonals	F
orthogonal diagonals	G
diagonals bisect each other	H
(at least) one equal pair of angles	I
two equal pairs of angles	J
equal angles	K
central symmetry	L
(at least) one axisymmetry about a diagonal	M
(at least) one axisymmetry about a perpendicular bisectional line	N
two axisymmetries about diagonals	O
two axisymmetries about perpendicular bisectional lines	P
axisymmetry about a diagonal and about a perpendicular bisectional line	Q
circumscribed circle	R
inscribed circle	S

Figure 4: The set of the attributes with code

The cross table of the convex quadrilaterals

The relation $\mathcal{R}$ can be defined between objects set and attributes set on a natural way, that can be written down with a cross table in the simplest format (Figure 5 presents one cross table of the convex quadrilaterals). A cross table is a rectangular table, with one row for each object (the examined quadrilateral class) and one column for each attribute (the examined features of quadrilaterals) per convention. The intersection of row *o* with column *a* contains the information with cross sign whether object *o* has attribute *a.*

It is important to observe that this analysis characterizes the examined classes of quadrilaterals only from containment aspect, i.e.:

– the cross sign in the intersection of row *o* with column *a* means that all elements of quadrilateral class *o* have the attribute *a*,

– the missing cross sign in the intersection of row *o* with column *a* means that *(at*

least) one element exists in quadrilateral class *o*, that does not have the attribute *a*, i.e. this should not be taken to mean that all elements of the quadrilateral class *o* do not have the feature *a*.

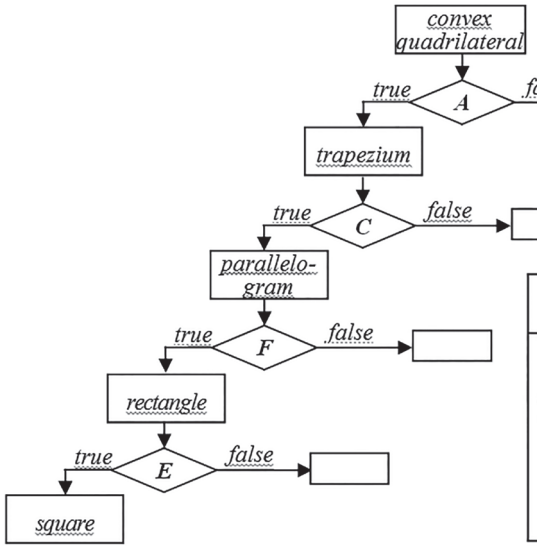
CROSS TABLE $\mathcal{R}$			attribute $\mathcal{A}$																	
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
quadrilateral $\mathcal{O}$	convex quadrilateral	1																			
	general quadrilateral	2																			
	trapezium	3	×																		
	orthogonal trapezium	4	×								×										
	symmetric trapezium	5	×	×				×			×	×				×				×	
	kite	6		×		×			×		×				×						×
	parallelogram	7	×	×	×	×				×	×	×		×							
	rhombus	8	×	×	×	×	×		×	×	×	×		×	×		×				×
	rectangle	9	×	×	×	×		×		×	×	×	×	×		×		×		×	
	square	10	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	cyclic quadrilateral	11																		×	
	circumscribed quadrilateral	12																			×

Figure 5: The cross table $\mathcal{R}$ of convex quadrilaterals by education plan of Hungary

Producing a cross table is a useful starting-point in planning education. The construction of the cross table (the circumscribing of basic sets of objects and attributes, filling of table) requires the mathematical and also the mathematicdidactical competent simultaneously.

The flowchart of the convex quadrilaterals

Plato in the *Sophist* gives one method of the concept definition: The extension of the concept has to be narrowed down with the distinctive attribute step by step. *Ambrus (1995)* presents Plato's idea precisely through the method of specialization of the convex quadrilaterals, i.e. narrowing down the extension of the concept through the intension of the concept. This classical method puts to use the relevant attribute as leading feature (*differentia specific*).



cross table by *Ambrus*			attribute *A*			
			A	*C*	*E*	*F*
convex quadrilateral	convex quadrilateral	*1*				
	trapezium	*3*	×			
	parallelogram	*7*	×	×		
	rectangle	*9*	×	×		×
	square	*10*	×	×	×	×

Figure 6: The hierarchical systematisation of the convex quadrilaterals by Ambrus (p. 60)

Attribute *A* (*parallel pair of sides)* divides the set $\mathscr{C}$ (convex quadrilaterals) into two parts. The first subset (trapezium) has the relevant attribute *A*, the second subset (general quadrilateral) is the complementary set of the first subset, i.e. the elements of the second subset do not have the attribute *A*. The first set (trapezium) can be repeatedly divided in two parts by attribute *C (two parallel pairs of sides)*, etc. This diagram really describes one decision algorithm. Figure 6 presents the diagram of the method by *Ambrus*.

This illustration very accurately depicts the structure of the explicit definitions; it helps to learn the forms of the explicit definition. (For example: The square is a rectangle with attribute *E*, i.e. with equal sides.) The concept is fixed from the next genus (*genus proximum*) with the distinctive attribute (*differentia specific*) in the explicit definition. Important to note that this method has a formal defect, because it can lead to having false conclusion: the next genus (*genus proximum*) exists unanimously. The square can be derived from rhombus, i.e. the square is a rhombus with attribute *K*, i.e. with equal angles.

The defect of the diagram is that the rhombus can not be embedded in this explicit definition chain. The integration method of the rhombus and other convex quadrilateral classes in the diagram has to be generalised.

Pelle (1974) gives an algorithm by which the objects of the quadrilateral classes can be sorted. It can be seen in Figure 7/a. This flowchart describes a method, by which it can be decided if a concrete quadrilateral belongs to one special class of convex quadrilaterals. The activity of the decision (the ranging and the preclusion) is the first function in this method. The decisions are based on the formal logic considerations of the relevant attributes. The relevant attributes can be selected from the set of attributes *E* in several ways, so other flowcharts can also be constructed from a cross table.

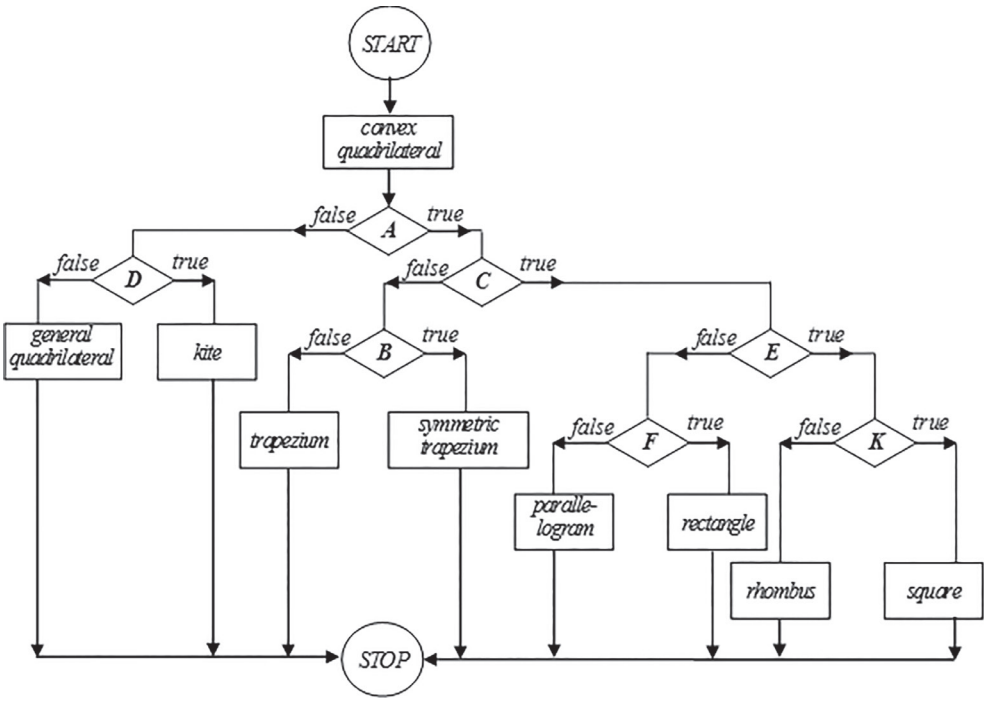


Figure 7/a: The process diagram to categorize the convex quadrilaterals by Pelle

Figure 7/b presents the selected attributes and the used information (with × sign) of cross table 5. In general the construction of an algorithm does not need to employ all information of the cross table. Table 7/b presents also the unused information (as lost information with – sign) of the cross table.

Taking them each individually, it can be read from this algorithm that a concrete class of the quadrilaterals does not have a given attribute. (For example: The kite does not have the attribute *A*, i.e. it does not have parallel pair of sides.) Figure 7/b contains the information from not only true but also false attributes by Figure 7/a. (Table 7/b presents also this misleading information with + sign.) This additional implicit information may lead to a false conclusion, because it can be seen from Figure 7/b, that a kite '*never*' has (at least) one parallel pair of sides (see cell *A6* in the table 7/b), but a rhombus 'always' has at least one pair of parallel sides (see cell *A8* in the table 7/b), i.e. the false conclusion can be drawn:

a rhombus is not a kite.

The problem appears that a net of concept cannot simply be described with a flow-chart.

Information table of figure 7.1			attribute						
			A	B	C	D	E	F	K
quadrangles	convex quadrilateral	1							
	general quadrilateral	2	+			+			
	trapeze	3	×	+	+				
	symmetric trapeze	4	×	×	+			–	
	kite	6	+	–		×			
	parallelogram	7	×	–	×	–	+	+	
	rhombus	8	×	–	×	–	×		+
	rectangle	9	×	–	×	–	+	×	–
	square	10	×	–	×	–	×	–	×

Markings:
***×:** used information*
***+:** misleading information*
***–:** lost information*

Figure 7/b: The information table of Figure 7/a

When preparing such a figure one should pay attention to these errors, because they cause confusions. Right figures are prepared with tools of the formal concept analysis and of trichotomyc concept model. (It must not be forgotten what is illustrated: the relationships between real objects or between their names.)

Bibliography

Ambrus, A.: *Bevezetés a matematikadidaktikába.* Eötvös Kiadó, Budapest, 1995.

Fatalin, L.: Strukturelle Analyse des Lernstoffes = *Neue Sichtweisen in der Didaktik der Mathematik,*. eEds.: Parisot, K. J., – Vásárhelyi, É., Abakus Verlag, Salzburg, 2003, 45–56.

Fatalin, L.: *Hierarchikus fogalmi struktúrák vizsgálata gráfokkal*, 2008,. Source:https://dea.lib.unideb.hu/dea/bitstream/handle/2437/85019/ertekezes_magyar.pdf?sequence=4&isAllowed=y

Mitroica, Gh.: *Din peripetiile rezolvitor de probleme,*. Editura Albatros, Bukarest, 1987.

Olosz, F.: *Mértanfeladatok megoldási stratégiái,*. 2ndConference of Teaching Mathematics, Komárom, 2005.

Pelle, B.: *Geometria,*. Tankönyvkiadó, Budapest, 1974.

Varsics, Z.: Osztályozási modellek – hierarchikus rendszerek,. *Iskolakultúra,* 1993/5., Budapest, 1993.

Fogalmi hierarchiák klasszikus ábrázolásai gráfokkal

Fatalin László

A fogalmi hierarchiákat gyakorta gráfok szemléltetik. E tipikus ábrázolások vagy tartalmazási, vagy származtatási kapcsolatra épülnek. A klasszikus vizuális ábrázolások egyszerűnek tűnnek, de több hibaforrásuk is félreértést okozhat. Ez a cikk ezen ábrázolások hiányosságait, logikai félreértelmezhetőségét mutatja be a konvex négyszögek példáján keresztül. Az elemzésben használt matematikai modellel feltárhatók a folyamatábrák kétértelműségei is.

Kulcsszavak: hierarchikus fogalmi struktúra, folyamatábra, konvex négyszög

Solymosi János

Vajon nyerünk-e a LO-TO-n a munkavédelemben?

A veszélyes technológiáknak – nem véletlenül – külön figyelmet szentel a munkavédelem. Az ilyen technológiák alkalmazása során a súlyos munkabalesetek bekövetkezésének valószínűsége, a sérülések súlyossági foka jelentősen nő. Különösen nagy odafigyelést igénylő területe a munkavédelemnek a veszélyes energiák „kézben tartása" az üzemeltetési és karbantartási munkák végzése során.

A „Lock out – Tag out (LO-TO; magyarul: kizárás-címkézés) rendszert az USA-ban széles körben alkalmazzák, amely gyakorlatilag a munkahelyen használt berendezések karbantartása során a veszélyes energiák berendezésről történő leválasztására és a jogosulatlan visszakapcsolásuk megakadályozására szolgáló biztonsági szabályokat tartalmazza. Jelen cikk szerzője a rendszer lényegét, a karbantartási munkák biztonságára való hatását kívánja ismertetni.

Kulcsszavak: veszélyes technológiák, munkabalesetek, veszélyes energiák, üzemeltetési és karbantartási munkák

Bevezetés

Európai statisztikák szerint a halálos munkabalesetek 10-15%-a történik karbantartási tevékenység közben, és az összes munkabaleset 15-20%-a függ össze karbantartással. E balesetek nagy részének az oka az ellenőrizetlen energiaáramlás. A karbantartási (preventív vagy hibaelhárítás) feladatok közben a gépek, berendezések nem szándékolt mozgása, az elsődleges vagy a felszabadult tárolt veszélyes energia személyi balesetet vagy anyagi kárt okozhatnak.

A rendszeres karbantartás elengedhetetlen a berendezések, a gépek és a munkakörnyezet biztonságosságának és megbízhatóságának fenntartásához. A karbantartás hiánya vagy a nem megfelelő karbantartás veszélyhelyzeteket, baleseteket és egészségügyi problémákat okozhat. Ebből adódóan mind a munkáltatók, mind a munkavállalók jól felfogott érdeke, hogy a karbantartási munkák biztonságosan, az emberi hibázási tényezőket is kizárva legyenek végezhetők.

A LOTO-rendszer lényege

A kizárás-kitáblázás (Lockout/Tagout, rövid nevén LO-TO) az üzemi biztonság vállalati szabályzatban írásban is rögzített, begyakoroltatott rendszere.

A kizárás-kitáblázás lényege, hogy minden olyan esetben, amikor az ipari technológiák normál üzemi működését fel kell függeszteni (karbantartás, hibamegállapítás, beállítás, javítás stb. céljából) és a megfelelő szakembereknek a technológiai eszközök belsejébe vagy közelébe (a veszélyzónába) be kell menniük, az energiaforrások véletlenszerű ki- és/vagy bekapcsolását a szerelvények (szelepek, csapok, kapcsolók, csatlakozók stb.) kizárásával mechanikus eszközökkel, fizikailag akadályozzuk meg minden lehetséges ponton. A LO-TO-rendszer feltételezi a személyi lakatok alkalmazását, hogy minden, a munkaterületeken (veszélyzónában) valamilyen műveletet (karbantartás, hibamegállapítás, beállítás, javítás stb.) végző szakember a saját biztonságáról úgy gondoskodik, hogy a szabályzatnak megfelelő kizárási ponton a kizáró eszközre saját személyi lakatját elhelyezi. A kizáró eszköz feloldása csak a lakat levétele után lehetséges, és az energiaforrás csak ezután szabadítható fel. A LO-TO-rendszer feltételezi a személyi lakatok alkalmazását, ami annyit jelent, hogy minden, a munkaterületeken (veszélyzónában) valamilyen műveletet (karbantartás, hibamegállapítás, beállítás, javítás stb.) végző szakember a saját biztonságáról úgy gondoskodik, hogy a szabályzatnak megfelelő kizárási ponton a kizáró eszközre saját személyi lakatját elhelyezi. A kizáró eszköz feloldása csak a lakat levétele után lehetséges, és az energiaforrás csak ezután szabadítható fel.

A rendszer a következő kockázattípusoknál alkalmazható:

– a berendezések mozgása, gépek működése,
– vegyi kockázat, vegyszer/folyadék/gáz előfordulása csővezetékben,
– villamos áram okozta kockázat,
– egyéb kockázat (pl. időjárási viszonyok).

Veszélyes energiák

A gépeket, berendezéseket működtető villamos, mechanikus, hidraulikus, pneumatikus, termikus energia egyaránt veszélyes lehet a munkavállalók számára. A javítás, karbantartás alatt álló gépek és berendezések váratlan indítás vagy a tárolt energia váratlan felszabadulása (nem megfelelően ellenőrzött, kézben tartott energia) súlyos sérülést vagy halált okozhat a javítást, karbantartást végző munkavállalók számára.

A LO-TO-eljárás megköveteli, hogy a javítást, karbantartást végző személy:

– kapcsolja ki a gépet vagy berendezést,
– szüntesse meg az energiaforrás(ok)hoz történő csatlakozást,
– zárja ki vagy táblázza ki az energialeválasztó eszköz(öke)t,

– ellenőrizze, hogy az energialeválasztás hatékonyan megtörtént,
– tegyen intézkedéseket a tárolt energia felszabadulásának elkerülésére vagy az energia veszélyes szintű újbóli felhalmozódásának megakadályozására.

Veszélyes tevékenységek

A munkavédelemben jártasak számára nem ismeretlen az alapelv, ami a LO-TO-eljárásnak az alapja. A villamos biztonság alapelvként kezeli, hogy villamos berendezéseken (1. ábra) munkát végezni csak azok feszültségmentes állapotában szabad (kivéve egyes beszabályozási, beállítási tevékenységeket, amiket feszültségmentes állapotban nem lehetséges elvégezni, illetve a villamos méréseket).

1. ábra: Villamos berendezés (forrás: http://mohanet.hu/villamos-berendezesek-tavfelugyelete/)

A feszültségmentesítés lépéseit az MSZ 1585:2012 szabvány tartalmazza:
– kikapcsolás, leválasztás,
– visszakapcsolás megakadályozása (lezárás, táblázás),
– feszültségmentesség ellenőrzése,
– földelés, rövidre zárás,
– a feszültségmentes terület fizikai elhatárolása a feszültség alattitól.

A „visszakapcsolás megakadályozása" azt jelenti, hogy a villamos energia kikapcsolása, leválasztása után a kikapcsoló szervet le kell zárni (le kell lakatolni), a kezelőfogantyút le kell szerelni a karbantartás, javítás alatt álló villamos berendezés visszakapcsolásának megakadályozása céljából (2. ábra).

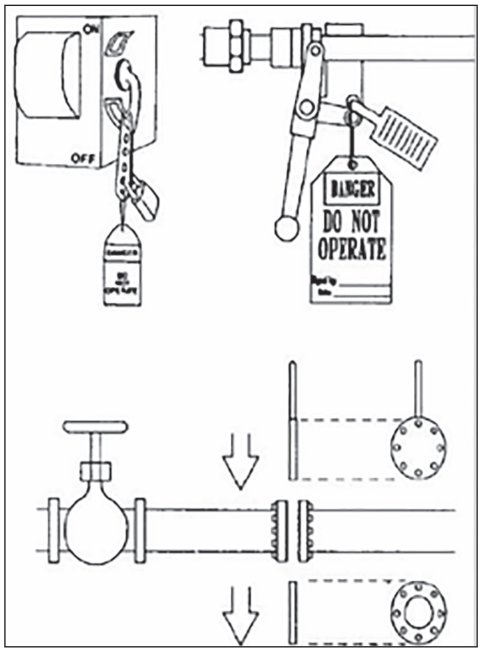
2. ábra: A visszakapcsolás megakadályozása (forrás: www.slideshare.net/magyarvasut/safety-under-ole)

A veszélyes berendezésekbe történő beszállásos munkák során is alkalmazzák a LO-TO-hoz hasonló eljárást. A beszállásos munkák biztonsági szabályait az MSZ-09-57.0033:1990 szabvány tartalmazza. A beszállás (olyan tevékenység, amely a berendezésen behajlással vagy annak belsejében való tartózkodással végezhető, ha ezt a teret emberi tartózkodásra nem tervezték) esetén fellépő alapvető veszélyek:

– veszélyes koncentrációjú, egészségre ártalmas vagy tűz- és robbanásveszélyes gázok, gőzök, porok, maró vagy mérgező anyagok jelenléte,
– oxigénhiány,
– forgó, mozgó belső szerkezetek,
– villamos berendezések,
– radioaktív sugárzás,
– tűzveszély.

Beszállásos munka előtt a veszélyes berendezésnek más veszélyes berendezéssel, csővezetékkel való kapcsolatát úgy kell megszüntetni (leválasztani), hogy a berendezésbe veszélyes anyag ne juthasson. A veszélyes berendezés leválasztását

– csőszakasz eltávolításával és vakkarima alkalmazásával,
– vaktárcsával (vaklencsével),
– kettőzött elzáró szerelvénnyel kell végezni (3. ábra).



3. ábra: Veszélyes berendezés leválasztása; leválasztási módok (forrás: Solymosi János: Beszállásos munkák biztonsága. *Acta Politechnica Hungarica,* Óbudai Egyetem, 2013)

Vaktárcsával (vaklencsével) történő leválasztás esetén a vaktárcsának (vaklencsének) alkalmasnak kell lennie az esetlegesen fellépő (nyomásból, hőmérsékletből, korrozív anyagoktól származó) igénybevé-

telre. Kettőzött elzáró szerelvények alkalmazása esetén a kettő közé olyan szerelvényt kell szerelni, amely nyitott állásban vagy a szabadba, vagy lefuvató rendszerhez csatlakozik. A beszállás előtt a szerelvények belső tömörségét ellenőrizni kell, az elzáró szerelvényekre biztonsági táblákat kell elhelyezni, és a szerelvényeket le kell lakatolni vagy plombálni.

Beszállás előtt a veszélyes berendezésben lévő géprészek (pl. keverők, szállító-berendezések) megindítását megbízhatóan, a villamos meghajtó berendezés feszültségmentesítésével, mechanikus szétkapcsolásával vagy a géprész kiszerelésével kell lehetetlenné tenni, valamint minden csatlakozó villamos berendezést feszültségmentesíteni kell. Megjegyzendő, hogy a villamos feszültségmentesítés nem egyenértékű a kikapcsolással. Villamos feszültségmentesítés esetén a villamos berendezést ki kell kapcsolni, a visszakapcsolását meg kell akadályozni, a feszültségmentességét ellenőrizni kell, a földelés-rövidre zárást el kell végezni, és a feszültségmentes részt a feszültség alattitól jól látható módon el kell határolni.

LO-TO-fogalmak

Érintett személy: Az a személy, aki olyan berendezést működtet, amelyen a LO-TO keretében karbantartás vagy szervizelés folyik, vagy olyan személy, aki a karbantartás vagy szervizelés területén dolgozik. Ez a személy *nem jogosult* a LO-TO elvégzésére.
Felhatalmazott személy: olyan megfelelően képzett személy, aki *jogosult* a veszélyes energia szabályozására (vagyis a LO-TO elvégzésére).

Csoportos LO-TO: minden kizárás-kitáblázási eljárás, amelyben egynél több felhatalmazott személy vesz részt.

LO-TO-eszközök

Kizáró eszközök

A kizáró eszközök az energialeválasztó eszközöket biztonságos vagy kikapcsolt helyzetben tartják. Úgy akadályozzák meg a gépek vagy berendezések energiahatás alá kerülését, hogy kulcsok, esetleg különleges (roncsolást okozó) eszközök használata nélkül nem távolíthatók el.

a) Személyi lakat:
– egy kulccsal rendelkezik,
– nincsenek hozzá mesterkulcsok,
– felhatalmazott személyekhez rendelik hozzá,
– csak személyi kártyával használható (piros),

– maximum egy műszakot használható,
– színe piros (4. ábra).

b) Átmeneti lakat:
– több kulccsal rendelkezik,
– akkor használják, amikor a javítandó gép nem áll aktív munkafolyamat alatt, az üzemeltetés nem biztonságos, vagy a műszakok közötti átadáskor,
– csak átmeneti, sárga kártyával használható,
– a többműszakos használat megengedhető,
– személyvédelemre TILOS használni,
– minden lakathoz külön kártya kell,
– színe sárga.

c) Gyűjtőlakatok, lakattöbbszörözők (5. ábra)

Ha egy berendezésen többen dolgoznak, segítségükkel mindenki elhelyezheti a saját személyi lakatját a kizáró szerelvényen, és a berendezés energia-megtáplálását.

d) Kábeles lakatok (6. ábra)
– Egyetlen eszközzel zárható ki több kezelési pont, azaz kisebb a berendezések költsége.

e) LO-TO-állomások (7. ábra) a LO-TO-eszközök elhelyezésére

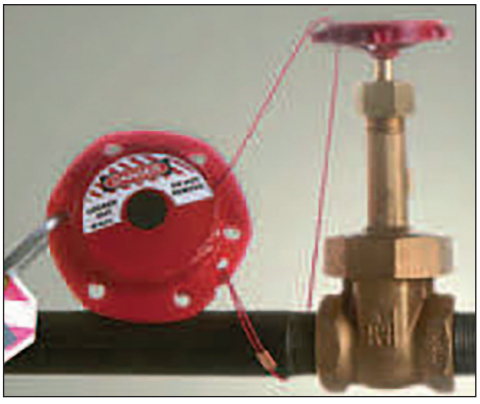
f) Kisautomata kizárók, kismegszakító kizárók (4. ábra)

g) Zsákos kizárók (8. ábra)

Olyan kizárási helyek lezárásához, amelyekhez más eszköz nem alkalmazható. Különböző méretben készülnek.

4. ábra: Személyi lakat (forrás: www.itoto.hu/)

5. ábra: Gyűjtőlakat, lakattöbszöröző (forrás: www.itoto.hu/)

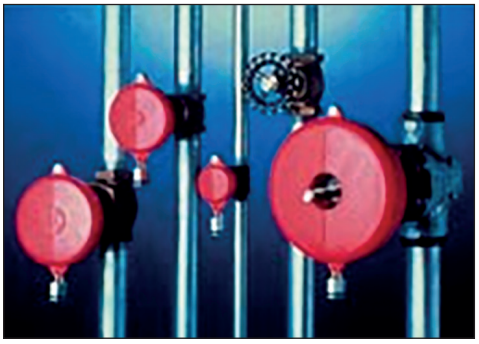


6. ábra: Kábeles lakat (forrás: www.markeref.hu/loto_rendszer.htm)

7. ábra: LO-TO-állomás (forrás: http://brady.hu/termekek/lockout-tagout/kiegesztok/zarhato-boxok-lakat-allomasok.html)

8. ábra: Zsákos kizáró (forrás: www.marker-lock.hu/loto_eszkozok.php)

h) Tolózár kizárók (9. ábra)



9. ábra: Tolózár kizáró (forrás: www.itoto.hu/)

Kitáblázó eszközök

A kitáblázó eszközök figyelmeztető eszközök, melyeket az energialeválasztóra rögzítenek, így figyelmeztetve a dolgozókat arra, hogy ne kapcsoljanak az általuk javított vagy karbantartott gépre veszélyes energiát. A kitáblázó eszközöket könnyebb eltávolítani, és önmagukban nem nyújtanak akkora védelmet a dolgozóknak, mint a lezáró eszközök (10. ábra).

10. ábra: Kitáblázó eszköz (forrás: www.google.hu/search?q=master+lock&biw=997&bih=475&source=lnms&tbm=isch&sa=X&ved=0ahUKEwinjdW5jIXNAhUGOpoKHY3eBVAQ_AUIBigB#imgrc=J6TW78DWzUP93M%3A)

LO-TO-eljárás

Karbantartási tevékenységek elemzése

a) A karbantartási tevékenység lehet:
– Tervezett (időszakos): műszakos, napi, heti, havi, éves
– Nem tervezett (hibaelhárítás, javítás)

b) Végezheti:
– saját dolgozó
– külsős vállalkozó

c) Karbantartói létszám:
– egy fő
– több fő

d) Karbantartás időtartama:
– rövid (max. egy műszak)
– több műszakot érintő

Energialeválasztó szerkezetek felmérése, jelölése

A munkahelyen lévő karbantartandó gépeket, berendezéseket, vezetékeket, azok energialeválasztó szerkezeteit fel kell mérni, és nyilvántartásba kell venni. A nyilvántartás alapján a LO-TO-helyeket meg kell jelölni. A jelölésnek tartalmaznia kell

– a hely azonosító jelzését, pl. 2. gépsor 5. gépe,
– a kizárandó energia fajtáját és jellemzőjét (villamos energia: E ~ 230V; sűrített levegő: SL 6 bar; gőz: G 12 bar stb). Amennyiben több, ugyanaz a fajta energiamegtáplálás van, mindegyiket külön jelölni szükséges, pl. E1 ~ 230 V, E2 ~ 400 V.

Ugyanilyen jelölésekkel el kell látni a gépek, berendezések energialeválasztó szerkezeteit (kapcsoló, elzáró váltó, tolózár stb.) is a fentebb ismertetett jelöléssel, és a gépen, berendezésen jól látható helyen jelölni kell az összes energialeválasztó (kizáró) helyet.

LO-TO belső szabályozás elkészítése

A belső szabályozásnak tartalmaznia kell:

– a célt,
– a hatásköröket,
– a jogosultsági szabályokat,
– a megfelelő kizáró és kitáblázó eszközök fajtáit, kihelyezésük módját,
– a gépek, berendezések energiarendszerről történő leválasztási helyét, módját,
– a kizáró és kitáblázó eszközök kihelyezésének, eltávolításának lépéseit, sorrendjét,
– a LO-TO-rendszer oktatási rendjét, tematikáját.

A belső szabályozást (eljárási utasítást) bevezetése után időszakosan felül kell vizsgálni, a szükséges módosításokat el kell végezni.

A LO-TO oktatása

A felhatalmazott és az érintett személyeket a LO-TO-rendszerből oktatni kell. Ismertetni kell a LO-TO célját, a LO-TO-eszközöket, a jelöléseket, az eszközök használatának módját, a jogosultságokat. A felhatalmazott személyek számára mind elméleti, mind gyakorlati oktatást egyaránt tartani kell, és az oktatásnak vizsgáztatással kell záródnia.

Következtetések

Súlyos munkabalesetek okozói lehetnek az energiák, ártalmas vegyi anyagok váratlan megjelenése a munkavégzés helyén, gépek, berendezések váratlan megindulása. A fentebb leírtakból látható, hogy a munkavédelem csak nyerhet a LO-TO-n, hiszen a rendszer helyes alkalmazása esetén ezek a munkabalesetek megelőzhetők. Nagy értéke a rendszernek, hogy az emberi hiba, tévedés lehetőségét is szinte teljesen kizárja.

Irodalomjegyzék

[1] Európai Munkavédelmi Ügynökség: *Biztonságos karbantartás a gyakorlatban.* Budapest, 2012. (ISBN 978-92-9191-338-1)
[2] loto.hu/ (a letöltés ideje: 2015. október 20.)
[3] Solymosi János: Beszállásos munkák biztonsága. *Acta Politechnica Hungarica,* Óbudai Egyetem, 2013.

Do Employees Benefit from Using the LO-TO System During Maintenance Work?

Solymosi János

The regulation of occupational safety and health, not surprisingly, pays special attention to the use of dangerous technology, since it significantly increases the risk of serious work accidents. Special attention should be paid to the protection of employees while using hazardous energy during operational and maintenance work.
The Lock out – Tag out (LO-TO) system, which is widely used in the USA, contains security arrangements and regulations for the disconnection and unauthorized reconnection of equipment under maintenance to hazardous energy.The author intends to explain the essence of the system and its impact on the safety of maintenance work.
Keywords: dangerous technology, work accidents, hazardous energy, operation and maintenance work

Vécsey Alexandra

Szervezeti biztonság – kit érdekel?!

A szervezeti biztonságnak számos vetülete létezik, amelyek közül a munka iránti érdeklődést vizsgáltam egy 2014-ben publikált felmérés alapján, valamint kerestem a választ arra a kérdésre, hogy miként lehet a szervezeti célok felé irányítani az alkalmazottak érdeklődését. Egyáltalán fontos-e a vállalat alapfunkcióinak biztosításában a munkavállalók munka iránti érdeklődése vagy annak hiánya?
Kulcsszavak: szervezeti biztonság, érdeklődés, motiváció, munkavállalói elkötelezettség

Bevezetés

„Azok a szervezetek, amelyek kihozzák alkalmazottaikból a legtöbbet, rájönnek, hogy az alkalmazottaik hozzák ki a legtöbbet belőlük."

A szervezeti biztonságnak számos vetülete létezik, amelyek közül a munka iránti érdeklődést vizsgáltam egy 2014-ben publikált felmérés alapján, valamint kerestem a választ arra a kérdésre, hogy miként lehet a szervezeti célok felé irányítani az alkalmazottak érdeklődését. Egyáltalán fontos-e a vállalat alapfunkcióinak biztosításában a munkavállalók munka iránti érdeklődése vagy annak hiánya?

Szervezeti biztonság

A szervezeti biztonság nem más, mint „a szervezetek alapfeladata önmaguk fenntartása és a tulajdonosi érdekek kiszolgálása a profittermelés, valamint a vevői érdekek kiszolgálása termékek vagy szolgáltatások előállítása révén. Ezt a feladatot akkor tudják rendeltetésszerűen ellátni, ha az alap- és támogató folyamatok zavartalanul valósulnak meg. Ennek előfeltétele, hogy a szervezet erőforrásainak sértetlensége, rendelkezésre állása, bizalmassága ne sérüljön; fenyegetettségük minimális legyen. Elengedhetetlen feltétele tehát az optimális működésnek a szervezet biztonsága." Arra, hogy miként biztosítják a szervezeti

biztonságot, számos megközelítés létezik: minden kor és vezetési kultúra megteremti a maga elképzelését a szervezet működésének védelmére, a fenyegetettség és a veszélyforrások csökkentésére vonatkozóan. A korai funkcionalista szemlélet szerint kétféle irányzat létezett: a vezetők által működtetett és irányított, az alkalmazottak végrehajtásra szorítkozó vezetői megközelítése, illetve a szervezet minden tagja bevonásával, a vezetői ellenőrzés mellett létrejött emberi erőforrás alapú megközelítés. A később keletkezett biztonsági kultúra elve ennél összetettebb: „A biztonsági kultúra szervezetibiztonság-felfogása szerint egy hatékony és hatásos szervezeti biztonsági rendszer akkor hozható létre, ha a személyes (értékek, attitűdök, hiedelmek, észlelés és felfogókészség) és a viselkedési tényezők (megértés, bizalom, elkötelezettség, motiváció/szándék és az éberség) egyszerre irányulnak a szervezeti biztonság megteremtésére, megtartására."

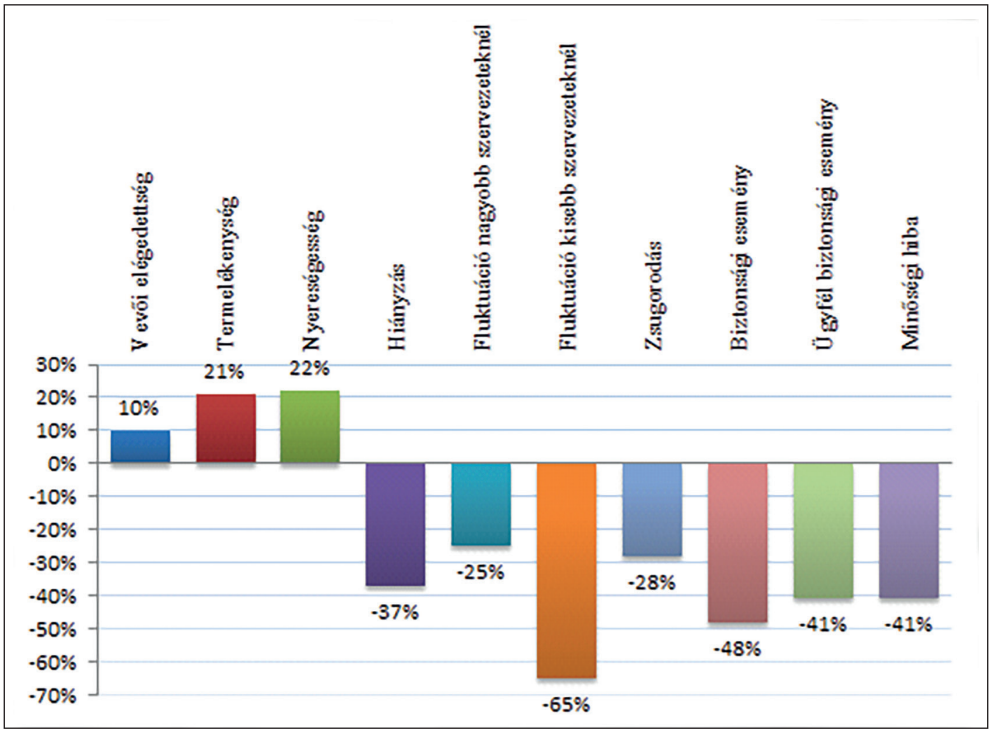
A szervezeti biztonság megőrzésére csak akkor lesznek motiváltak az alkalmazottak, ha fenyegetve érzik a szervezeti biztonságot, és akkor érzik fenyegetve, ha erről a fenyegetettségről tudnak. A teljesítmény a negatív stressz hatására csökken, míg a pozitív stressz hatására nő – nem mindegy, miként értékeli az alkalmazott a fenyegetettség érzékelését. Ha elegendő önbizalma és tudása van a probléma megoldására, akkor problémamegoldóvá válik (pozitív stressz), ellenkező esetben érzelmi alapon a stresszhelyzetet próbálja átértékelni, hogy feloldja azt (negatív stressz). A fenyegetettség folyamatos üzenete csak akkor válik motiváló tényezővé, ha azt pozitív stresszként fogja fel az alkalmazott, és a fenyegetettségből fakadó problémákat megoldja. Ehhez szüksége van a folyamatos képzésre, képességeinek fejlesztésére, és a fenyegetettség csökkentése érdekében rendszerek kidolgozásában való részvételre.

A munka iránti egyéni érdeklődés jelentősége

A Gallup 2012-ben készült globális munkahelyi felmérése szerint mindössze a munkavállalók 13%-át érdekli az, amit dolgozik, még a legjobb eredményeket mutató USA-ban is csak 30%-os ez az arány.

Három fő csoportra oszthatók a munkavállalók érdeklődésük szerint: akiket érdekel a munkájuk, azon munkavállalók szenvedéllyel dolgoznak, innovatívak és előre viszik a vállalatot. Akiket nem érdekelnek a munkaköri feladataik, azok éppen annyit tesznek meg, amennyit elvárnak tőlük, minimális energiabefektetéssel és szenvedély nélkül. Nem ellenségesek a munkájukkal és a vállalattal szemben, de nem is törődnek a vállalat ügyfeleivel, termelékenységével, nyereségességével, a minőséggel vagy a biztonsággal. Gyakorlatilag egész nap a munka végét, egész héten a hétvégét várják... A felmérés szerint ebbe a csoportba tartozik a legtöbb munkavállaló. A harmadik – aktívan érdektelen – csoport viszont nyíltan ellenséges, tönkreteszi az munkatársak munkáját és a cég egészét, kisajátítja a vezető idejét, és elüldözi az ügyfeleket. Ezen munkavállalók aránya is eléri a 10% körüli szintet.

Valódi problémát jelent az ellátott munkakörök iránti érdektelenség. A globális felmérésben azon cégeknél, ahol a feladatuk iránt érdeklődő munkavállalók aránya magasabb, lényegesen jobbak a forgalmi, profit- és teljesítményadatok, mint a munkájuk iránt legkevésbé elkötelezett munkavállalókkal dolgozó vállalatoknál.



1. ábra: A munka iránti érdeklődés hatása a kulcsfontosságú üzleti eredményekre. A felső negyedben elhelyezkedő munkahelyek teljesítménye az értékek szerint felülmúlja a legalsó negyedét [1]

Az 1. ábrát elemezve első ránézésre látszik, hogy a munka iránti érdeklődés két számjeggyel leírható különbségeket képes generálni a legfelső és a legalsó negyedben a vizsgált mintában. A 20% feletti nyereség- és termelékenység-különbség kifejezetten jelentősnek mondható, de ami még inkább szembetűnő – és e cikk szempontjából releváns: 48%-kal kevesebb szervezeti biztonságot gyengítő káresemény (biztonsági esemény) következik be az elkötelezett munkavállalókkal dolgozó cégeknél, szemben azokkal, ahol a munkavállalók jellemzően érdektelenek. Azaz közel feleannyi… Hasonló az arány az ügyfeleknek okozott károk esetében: 41%. Közvetetten a nagyarányú fluktuáció is hatással van a szervezeti biztonságra, hiszen ha a vállalat az alapvető képességét adó munkatársait veszíti el, akkor az az egész vállalat létét kérdőjelezi meg rövid távon, különös tekintettel a kisebb szervezeteknél – például a kis- és középvállalkozások körében –, ahol ez az arány 65% a fent hivatkozott felmérés szerint.

A fentiek alapján tehát kijelenthető, hogy a szervezeti biztonságra közvetlenül és közvetetten is jelentős hatással bír a munkához való hozzáállás: érdekli-e a munkavállalót munkájának minősége, megtesz-e feladatkörében mindent, amellyel biztosítja a szervezeti biztonság feltételeit a saját területén? Amennyiben a rendszerben hibát észlel, képes és hajlandó-e a hibát jelezni, vagy nem érdekli, és a vezetőtől várja a megoldást? Képes és hajlandó-e javaslatot tenni annak érdekében, hogy a hibák bekövetkezésének valószínűsége csökkenjen? Hiszen ő az, aki a hibát nap mint nap megtapasztalja. Hajlandó-e részt venni a biztonsági rendszerek javításában? Kap-e egyáltalán lehetőséget, munkájában, szakértelmében megerősítést, vagy „cserélhető alkatrészként" tekintenek a munkavállalóra annak hangsúlyozásával, hogy senki sem pótolhatatlan, illetve akinek nem tetszik a vállalat, annak kívül tágasabb. A szervezeti biztonság humán oldalról végső soron a munkavállalók egyéni érdeklődésén, és az alkalmazott motiváció hatékonyságán múlik.

Hogyan viszonyulunk a munkához?

Korábban a képességeknek tulajdonítottak elsődleges fontosságot, és a munkának képességei alapján legjobban megfelelő embert keresték. Később a kutatások során fény derült arra, hogy a jobb teljesítmény eléréséhez az érdeklődés az, amely elsősorban meghatározó a munkavállalóban. Tágabb értelemben „az érdeklődés az a tulajdonságunk, ami alapján kiválasztjuk a környezetünkből a számunkra fontos tárgyakat, személyeket, tevékenységeket. Ebből a meghatározásból is láthatjuk, hogy olyan személyiségjellemzővel van dolgunk, amely érzelmi viszonyulástól nem mentes, hanem érzelemmel átitatott."

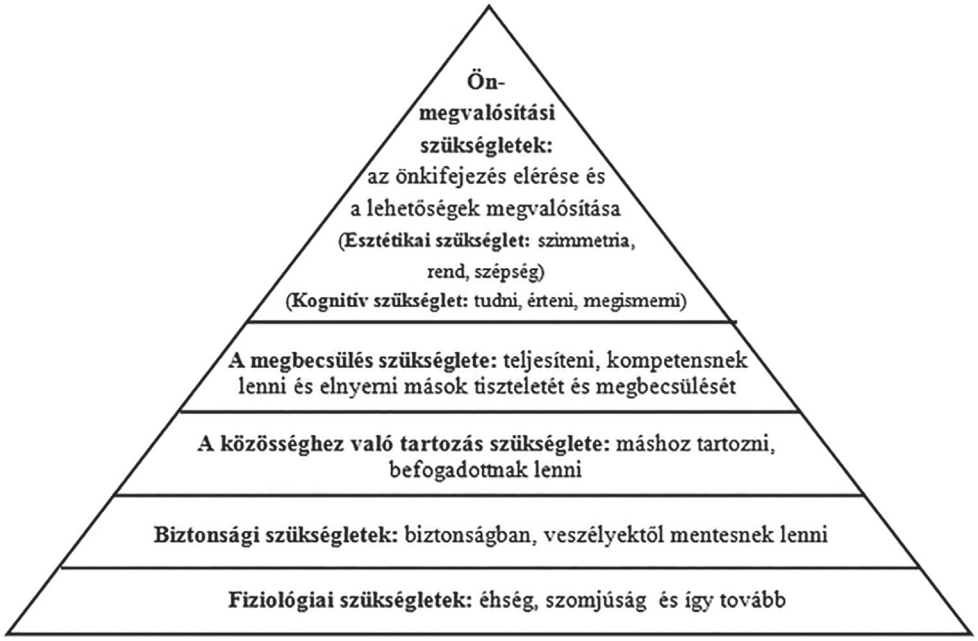
Az érdektelenség problémaköre kevésbé hangsúlyozott, annak ellenére, hogy a szakmai érdeklődés jelentősége egyre nő, ahogy a gondolkodást nem igénylő feladatköröket átveszik a gépek – hiszen a monoton, egyszerű munkafolyamatok esetén valóban nem beszélhetünk szakmai érdeklődésről, de szakmai fejlődésről sem. Ki képes inkább eredményeket elérni a munkahelyén, például egy mérnöki munkakörben? Az, akinek azt mondták, hogy legyen mérnök, és az egyetemet kötelességtudóan kijárta – de nem érti, mit keresett ott; vagy az, aki gyermekként szétszedte a játékát, kamaszkorában már önálló eszközöket fabrikált, felnőttként diplomájával a kezében még szabadidejében is szakirodalmat olvas, és érdeklik a legújabb megoldások? Ki fog inkább fejlődni? Egyértelműen az, akit érdekel, mert fejlődést csak az egyéni érdeklődésen át lehet elérni.

A munkavállaló munkához való hozzáállását alapvetően két dolog határozza meg: érdeklődési köre és azzal összefüggésben a munkához fűzött érzelmei.

Motiváció

„Munkával kapcsolatos motivációról akkor beszélhetünk, ha egyéni szükségleteink kielégítésére törekedve hajlandóak vagyunk a szervezeti célok megvalósítása irányába mutató erőfeszítésekre." Az előző fejezet szerint adott tehát a munkavállaló, aki attól függően viszonyul a munkához, hogy a munka tárgyköre egybevág-e érdeklődési körével vagy sem, illetve milyen érzelmekkel viszonyul a munkavégzéshez. És adott a vezető, akinek feladata, hogy az alkalmazottakat rávegye arra, hogy munkájukkal a szervezeti célok eléréséhez járuljanak hozzá. Számos motivációs elmélet született az évszázadok során, ebből most a szervezeti biztonság szempontjából leginkább szemléletes Maslow-féle szükséglethierarchiát emelném ki.

Abraham Maslow a szükségletek egymásra épülését vázolva állította, hogy csak akkor fordul az ember magasabb szintű szükségletei kielégítése felé, ha az alacsonyabb szintű – legalább részben – már beteljesült, de abban az esetben többé már nem lesz fontos számára, és az új szintek felé fordul (lásd 2. ábra).



2. ábra: A Maslow-féle szükségletpiramis [8]

Maslow elmélete több szempontból is érdekes. Egyrészt ha a vezető tisztában van azzal, hogy beosztottai a piramis mely szintjén vannak, annak megfelelően választott motivációs eszközzel hatékonyan lehet a szervezeti célok felé irányítani az alkalmazottakat. (1. táblázat)

Szükséglet	Néhány hozzá kapcsolható ösztönző eszköz
Fiziológiai	pénz (alapfizetés) munkahelyi étkező munkafeltételek (fűtés, világítás)
Biztonsági	pénz a munkavégzés biztonsága, orvosi ellátás hosszú távú foglalkoztatás, biztos munkahely nyugdíjpénztár
Szeretet/kapcsolat	jó csoportlégkör összetartó munkacsoportok, szakmai közösségek közvetlen, jó vezető-beosztott kapcsolat
Megbecsülés/elismertség	előléptetés, előmenetel kitüntetés, más elismerések teljesítményprémium szolgálati autó, státusznövelő kiegészítő juttatások státusszimbólumok munkakör-szélesítés, rotáció
Önmegvalósítás	munkakör-gazdagítás, nagyobb döntési felelősség kihívó, kreatív feladatok személyes továbbképzés és fejlődés lehetősége önálló munkavégzés önellenőrzés

1. táblázat: A Maslow-féle szükségletekhez kapcsolható ösztönző eszköz [8]

Másrészt a biztonsági szükségletek szintje a szervezeti biztonság szempontjából is lényeges: ahogy azt korábban említettem, az alkalmazott saját indíttatásból is hajlandó tenni a szervezeti biztonságért, ha fenyegetettségben érintett, ha azonban a veszély elmúlt, a szervezeti biztonság már nem lesz fontos számára.

Maslow megközelítésére rímel McGregor elmélete, amely szerint minden vezető döntését a benne kialakult emberkép határozza meg: Miként gondolkodik munkavállalóiról, milyen hiedelmei, sztereotípiái vannak? A klasszikus menedzsment felfogásban az emberi természetről alkotott hiedelmeket az X emberképben írja le. Eszerint az ember természeténél fogva kerüli a munkát, a vezetés szerepe ennek ellensúlyozása. Kényszeríteni kell a szervezetnek hasznos munka végzésére, vezetni, irányítani és negatív eredmény esetén büntetni. Ezzel szemben az Y emberkép szerinti ember szívesen végzi a munkáját, képes elkötelezni magát a szervezeti céloknak, nem pusztán a külső kényszer veszi rá erre, de megfelelő ellentételezés is növeli az elkötelezettség mértékét. Az Y embernek az alkotókészség, a kreativitás veleszületett képessége, szellemi képességeit azonban csak részben használják ki. Tulajdonképpen az X ember a piramis alacsonyabb szintjein, míg az Y a magasabb szintjein helyezkedik el. Figyelemre méltó, hogy mindkét típusú vezetői várakozás,

amely meghatározta a vezetői stílust, egyben önbeteljesítő jóslatként is szolgált: Ahol a vezetők előzetesen úgy vélekedtek a munkavállalókról, hogy X, ott valóban így kezdtek el viselkedni, ahol Y, ott az vezetett eredményre.

Fejlesztési lehetőségek

Joggal merül fel a kérdés: vajon eleve elrendeltetett lenne egyes munkavállalói csoportok besorolása? Különösen az utolsó X és Y típusú emberek esetén világosan látszik, hogy nem, mert a vezetői hozzáállás határozza meg a szervezet jellemző viselkedését, tehát megfelelő motivációs eszközökkel hatékonyabbá tehető a munkavégzés. Ezzel együtt persze el kell fogadni, hogy különbözőek az emberek, és adott pillanatban egy szervezetben megtalálható X és Y ember is, azaz alacsonyabb és magasabb szintű szükségletekkel rendelkező munkavállalók egyaránt. A kihívás tehát abban van, hogy a menedzser tisztában legyen azzal, ki melyik szinten helyezkedik el a piramisban, és a rendelkezésre álló eszközeivel terelje inkább az Y felé a munkavállalókat. Robyn Reilly, a Gallup senior tanácsadója szerint a munka iránti érdeklődés fokozható a menedzserek képzésével, megfelelő kiválasztásával, amelynek segítségével a vezető belátja, hogy az egyén sikere a vállalat sikere. Tisztában van a beosztottak gyengeségeivel és erősségeivel, lehetőséget ad, fejlődést biztosít, és felelőssé tehető a beosztottak hozzáállásáért.

Szervezeti biztonság szintjén ennek megfelelően kell cselekedni: Míg az X emberekkel a szabályok, előírások betartatására a funkcionalista megközelítést kell alkalmazni, addig az Y emberekkel a biztonsági kultúrát lehet megvalósítani, amelynek ők is aktív részesei és megalkotói.

A munka iránti érdektelenség problémájának forrását a jelenleg jellemző oktatásnál érdemes keresni. Sir Ken Robinson „Az alkotó tér" című könyvében kifejti, miként rombolja a világ bármely részén jelenleg jellemző oktatási rend a gyermek természetéből adódó érdeklődést és kreativitást – ezt itt nem ismertetem bővebben. Pár gondolata az oktatásról mégis idekívánkozik: Az oktatás célja egyrészt személyes: egyéni képesség és tehetség fejlesztése; másrészt kulturális: a világ megértését szolgálja; harmadrészt pedig gazdasági: a tanulás hozzásegít ahhoz, hogy később képes legyen eltartani magát az ember. A tehetség azonban sokszínű, a tanulás pedig személyes dolog, differenciált hozzáállást igényel, a rendszerek átgondolásával, a technológiák és módszerek kreatív használatával személyessé tehető. Megfelelő oktatás megléte esetén a munkába állók nagyobb aránya lesz tisztában saját képességeivel, tehetségével és lesz kiforrott érdeklődési köre, amelyben a munkáját örömmel és odaadással tudja végezni. Bízom benne, hogy ez nem utópia, hanem gyermekem jövője.

Konklúzió

A szervezeti biztonságnak számos vetülete létezik, amelyek közül a munka iránti érdeklődést vizsgáltam egy 2014-ben publikált felmérés alapján. A világ számos országára és munkahelyére kiterjedő statisztika megdöbbentő arányokat mutat: a munkavállalók átlagosan csupán 13%-a tekinthető elkötelezettnek, és 10% körüli azok aránya, akik tevőlegesen ártanak a cégnek, ahol dolgoznak. A felmérés egyértelművé tette számomra az addig is sejthetőt: a munkavállalói érdeklődés és érzelmi elköteleződés hiánya jelentősen rontja a vállalat pozícióit minden területen, kiemelten a szervezeti biztonság területén. Tenni lehet és kell is ellene, erre az általam felhasznált szakirodalom többféle választ ad: cégen belül az elkötelezettség fontosságának hangsúlyozásával, a menedzserek megfelelő kiválasztásával és képzésével, az alkalmazottak egyéni sikereinek és céljainak támogatásával fejleszthető a pozitív hozzáállás. Hosszabb távon pedig az oktatás személyessé tételével, a 21. századi technológiák adta lehetőségek kiaknázásával, az érdeklődés és kreativitás megőrzésével várható a munkája iránt érdeklődő, azt örömmel végző és abban fejlődni tudó generáció megszületése.

Irodalomjegyzék

[1] Robyn Reilly: Five Ways to Improve Employee Engagement Now. *Business Journal,* 7th January, 2014. www.gallup.com/businessjournal/166667/five-ways-improve-employee-engagement.aspx (a letöltés ideje: 2016. január 2.)

[2] C. K. Prahalad -– Gary Hamel: The Core Competence of the Corporation,. *Harward Business Review.* From the May–June 1990 Issue. Forrás: https://hbr.org/1990/05/the-core-competence-of-the-corporation

[3] Lazányi Kornélia: A biztonsági kultúra. *Gazdálkodás- és Szervezéstudományi Folyóirat – A Virtuális Intézet Közép-Európa Kutatására közleményei,* Szeged, 7/1–2., 398–405.

[4] Lazányi Kornélia: *Szervezeti biztonság és a munkahelyi stressz kapcsolata.* IX. Régiók a Kárpát-medencén innen és túl – Nemzetközi tudományos konferencia, Kaposvár, 2015. október 16.

[5] Kenderfi Miklós: *Pályaorientáció.* 4.1 fejezet, Szent István Egyetem, Gödöllő, 2011, www.tankonyvtar.hu/hu/tartalom/tamop41-2A/2010-0019_palyaorientacio/ch04.html

[6] Lazányi Kornélia: Érzelmi munka és elkötelezettség. *Munkaügyi Szemle,* 54(2010)/2., 24–34.

[7] Bakacsi Gyula: *A szervezeti magatartás alapjai.* 3. fejezet, Gondolat Kiadó, www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_543_07_A_szervezeti_magatartas_alapjai/ch06.html

[8] Roóz József – Heidrich Balázs: *Vállalati gazdaságtan és menedzsment alapjai.* 4.2.1 fejezet, 38. ábra, Budapesti Gazdasági Főiskola, 2013.

[9] Bakacsi Gyula: *A szervezeti magatartás alapjai.* 3. fejezet, Gondolat Kiadó, www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_543_07_A_szervezeti_magatartas_alapjai/ch06.html

[10] Sir Ken Robinson: *Az alkotó tér.* HVG Kiadó Zrt., Budapest, 2011, 350.

Organizational Safety – Who cares?!

Vécsey Alexandra

Organizational safety can be examined in several ways. This article is based on a report about employee engagement published in 2014. I tried to answer the question how managers can turn their employees interest to organizational goals? Is the employee's engagement really relevant in organizational safety?

Keywords: organizational safety, interest, motivation, employee's engagement

Kovács Zoltán

Physical perimeter security of military facilities

Permanent and temporary military facilities are extremely endangered by different violent attacks, e.g. armed, explosion, CBRN. The author shortly introduces the improvised explosive devices as the main weapons of blast attack, and highlights only a segment of the military facilities' physical security system: presenting the perimeter barriers and their application those may be used primarily to deny or hinder entering the vehicle born improvised explosive devices into the territory of a military facility.
Keywords: military facility, security, physical protection, perimeter protection, barriers, improvised explosive device, IED, VBIED

Introduction

Physical security includes those protective measures that are designed to deny unauthorized access to different facilities, installations, equipment, resources and documents, and to protect the personnel and property from damage or harm.

These measures include fieldworks, facility construction, detection and procedural elements. Procedural elements are the protective measures required by different military regulations or standing operating procedures and provide the basis for developing the other three elements. The construction method of the facility may include reinforced and blast resistant walls, doors, windows and roofs, whilst detection elements include technical segments like sensors, cameras, detectors and a human segment like armed security guards, operators. Fieldworks can be realized in the area surrounding the facility and technically includes perimeter barriers, landforms and standoff distances.

Improvised explosive devices

The Improvised Explosive Device (IED) is "a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract."[1]

The IED can take any form and be activated in a variety of ways. It may be constructed out of any available material and may range in size from a box of matches to a large vehicle. The only limitations are the availability of resources, personal ingenuity and the degree or extent of "know how" required for construction. The IED is usually fabricated from common materials, military or non-military components. It may be static in a fix location and detonated as an observed device when the moving target (e.g. a military convoy) is in the ideal position and distance from the device; or it may be a mobile bomb delivered near to or into a static, fix target (building, military base or military camp).

The most common explosives used for an IED are military explosives, such as C4 or SEMTEX plastic explosives, trinitrotoluene (TNT), commercial explosives, such as ammonium nitrate fertilizer and fuel oil compound (ANFO). However, some IEDs may contain homemade explosives (HME), which are kitchen-mixtures of different chemicals. Common hardware, such as ball bearings, bolts, nuts or nails can be used to enhance the fragmentation and cause more lethal or serious injuries in crowded places.[2]

The triggering mechanism may be victim operated, command controlled or time delayed. Generally, the most common version is the mechanical trigger, when the target gets into direct physical contact and push, pull, remove or release something that ignites the detonator. Time delayed constructions (clockwork, electric or chemical timers) independently operate the device after the pre-set time without any impact of the target. The command operated IED responds to a signal received via a hard wire or a radio frequency (wireless doorbells, car alarms, radio controlled toys, cell phones may be used).

For a successful attack it is very important to hide the device. Depending on its dimensions it may be covered in a harmless object such as a small tin or a paper bag, while bigger devices, which are mainly used against constructed military infrastructure, especially buildings, military bases or camps, can be hidden in the boot of a car or truck. These are the so called Vehicle Born Improvised Explosive Devices (VBIEDs), which are very effective, because they are an expedient method for transporting hundreds of kilograms of explosives to a great distance and can inflict severe damage on any military facility.

Basically, there are two common ways to use a vehicle as an explosive device. The stationary VBIED is when someone parks a truck or a car with full of explosives near to

1 STANAG 3680 NATO Glossary of Terms and Definitions (AAP–6), NATO Standardization Agency (17 November 2015), 431.

2 Kovács Zoltán: Az improvizált robbanóeszközök főbb típusai (Important types of improvised explosive devices),. *Műszaki Katonai Közlöny,* 22(2012)/2, 37–52.

the facility and detonates the IED by either wireless command or time delay. The mobile (movable) VBIED is when someone tries to break through perimeter barriers, drives the vehicle into the facility's territory and then detonates the IED and oneself. This is a suicide attack using a so called Suicide Vehicle Born Explosive Device (SVBIED).

Physical security system

It is fundamental to develop an integrated physical security system for the protection of a military facility. For comprehensive protection, the physical elements should be integrated with other security components and options, based on the features of the site and the identified threats.

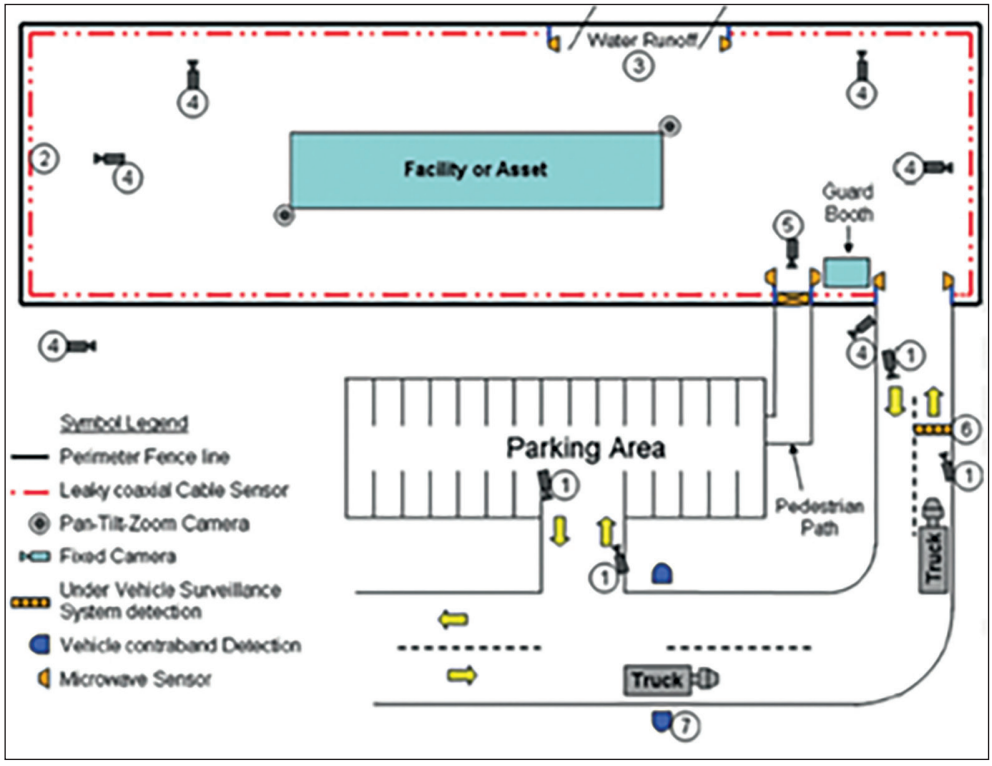


Figure 1: Combined security system[3]

3 *FEMA–426/BIPS–06: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings: Buildings and Infrastructure Protection Series*, Edition 2. U. S. Department of Homeland Security (October 2011), 514. Source: https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf

If risk assessment made before constructing a permanent military facility shows that an IED attack is surely expectable, the frame of the planned building should be reinforced and the glazing should be made of blast resistant glass. Structure of existing buildings also has to be hardened: carbon fibre polymers may reinforce concrete structures, side plates may reinforce steel trusses, different energy absorbing panels and synthetic coating can be used for absorbing and reducing blast effects. The existing and planned temporary military facilities (e.g. military camps) may also require special aspects to consider for reinforcement and hardening, blast and CBRN security or protection of public utilities, etc.[4]

Any reinforcement within the territory of a permanent or a temporary facility amplifies the function and effects of the first security zone, which is the perimeter around in standoff distance. The standoff distance is the maintained distance between an endangered facility and the place where a VBIED is allowed. The initial goal should be to make that distance as far from the target facility as practical, because the bigger the VBIED explosive load the greater the standoff distance necessary for reducing or minimizing the effects of the explosion.

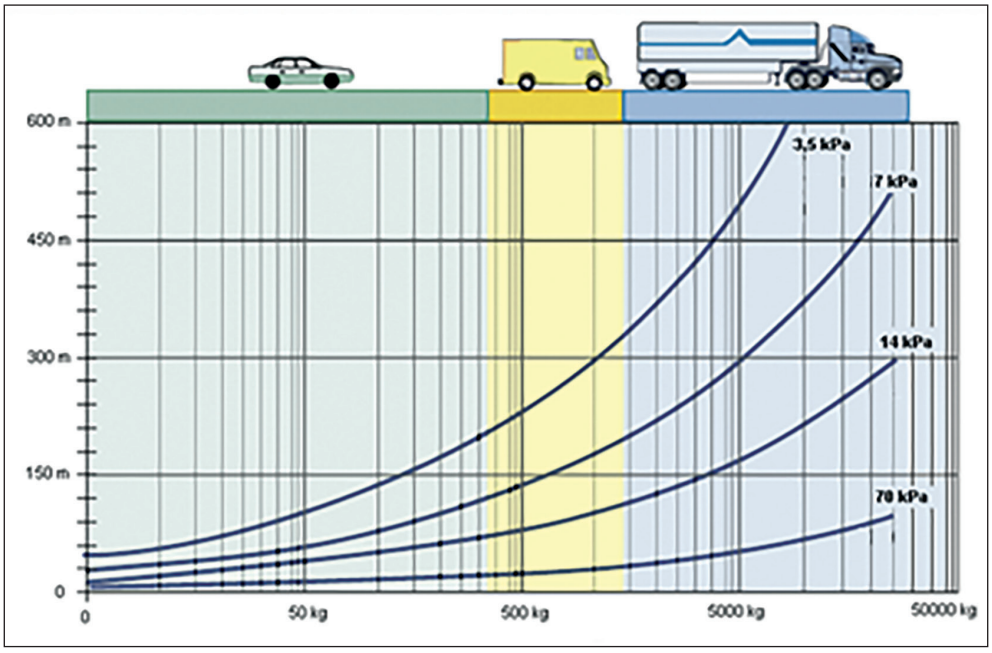


Figure 2: Standoff distance versus TNT weight[5]

4 Berek Tamás – Pellérdi Rezső: ABV (CBRN) kihívásokra adott válaszlépések az EU-ban. (Answers of EU for CBRN challenges),. *Bolyai Szemle,* 20(2011)/2, 55–72.; Kovács Tibor: A katonai táborok biztonsági rendszereinek kialakítása, különös tekintettel a robbantásos merényletek megelőzésére, azok hatásai csökkentésére. (Security system of military camps, with especial regard to prevention of blasting attempts and reduction of their effects),. *Műszaki Katonai Közlöny,* 22 (2012)/3, 70–83.; Dénes Kálmán: Aspects of water supply and sewage systems in military camps,. *Bolyai Szemle,* 20(2011)/1, 163–172.

5 FEMA–426/BIPS–06…, op. cit.

When a military camp is located on an open area, it is easy to provide considerable space for standoff, therefore conventional construction with minor modification on terrain may reach an acceptable level of protection against a VBIED blast. But in many cases, it is very difficult to achieve and maintain the required standoff distance. As the chart above shows, a small change in standoff distance can make a large difference in the blast loadings: bigger distance reduces the peak pressure and the impulse of blast.

If distance is less than necessary, other protective elements should be improved, like structural hardening or reinforcement, more perimeter barriers, high-tech detection devices. The required security standards for each threat levels concerning military camps or buildings are declared in different documents and handbooks.[6]

Financial resources determine and even terminate all the conception, this is why engineers and security experts should find balance between the costs and quantity/quality of protection elements necessary to reach the required security level. If standoff distance increases, the perimeter should be longer around the territory, which requires more barriers, fences and detection equipment increasing the costs of perimeter security.

On the other hand, increasing the distance means that other security elements may be reduced, which requires less investment. During searching the balance always remember that standoff is the best friend and perimeter barriers are primarily for denying unauthorized access, they do not perfectly protect against blast effects!

Perimeter security barriers

The difference between movable and stationary VBIED tactics is that the aggressor using the moving vehicle bomb will attempt to crash through the perimeter; the aggressor using the stationary vehicle bomb will not.

Once the standoff distance for a facility has been established (based on the expected amount of explosives and acceptable damage level), the threat vehicle should not be allowed to get closer to the facility where a greater level of damage could occur.

The moving vehicle produces kinetic energy that must be absorbed by the perimeter barrier to effectively stop the vehicle. This energy can be calculated by the weight and speed of the vehicle. It is very important to control the speed of the vehicle approaching the barrier, because the energy from a vehicle that a barrier must stop increases quadratically as

6 STANAG 2280 (Edition 1) Design Threat Levels and Handover Procedures for Temporary Protective Structures, NATO Standardization Agency (18 December 2008), 28.; Field Manual 3–19.30 Physical Security. HQ U. S. Department of the Army (8 January 2001), 317.; Unified Facilities Criteria (UFC 4-022-02) Selection and application of vehicle barriers, Change 1, US Department of Defense (9 August 2010), 101.; Unified Facilities Criteria (UFC 3–340–02) Structures to Resist the Effects of Accidental Explosions, U.S. Department of Defense (5 December 2008), 1943.; Unified Facilities Criteria (UFC 4–010–01) Minimum Antiterrorism Standards for Buildings, Change 1, U.S. Department of Defense (1 October 2013), 111.

its speed increases. The best way to limit a vehicle's approach speed to perimeter barriers is to place obstacles in all potential approach paths. The vehicles are forced to reduce speed when going around these obstacles placed in a serpentine pattern on the road. If the vehicle hits the obstacles instead of going around them, they are still slowed down. Curved roads and roadways with chicanes, road humps or sharp turns where a vehicle is forced to make a short radius turn before impacting the barrier will also effectively reduce its speed.

Perimeter barriers designated to stop or hinder vehicles may be categorized as either active or passive. Both of them can be fixed or movable, depending on how they are made, operated or used. An active barrier requires some action, either by personnel, equipment, or both to permit entry or exit of a vehicle. Active barriers include barricades, bollards, beams, gates, and active tire shredders.

The passive barrier has no moving parts, their effectiveness relies on their ability to absorb and transmit the energy to their foundation. Jersey walls, bollards or posts, guard-rails, ditches and reinforced fences are good examples of passive barriers.

The fixed barrier is installed permanently and requires heavy equipment to dismantle (e.g. concrete or steel barriers, fences), the movable barrier can be relocated from place to place but it may also require heavy equipment to assist in the transfer.

Fences should not be considered as protection against a moving VBIED attack. Most wire fences can be easily penetrated by a vehicle and will resist impact only if some reinforcement is added. The true value of a perimeter security fence comes in its association with other components of the security system. They are primarily used to provide a legal boundary by defining the outermost limit of the military facility. However, they may also assist in controlling and screening authorized (vehicle) entries into a secured area and providing a "clear zone" for installing lighting, intrusion detection equipment and cameras. Fences are frequently combined with barbed concertina wires to prevent human trespassing, too.[7]

As the perimeter for permanent military facilities a strong masonry wall made of brick, concrete or reinforced concrete blocks is the best solution against VBIED attack. For temporary military camps the HESCO bastions and DEFENCELL system should be appropriate as perimeter protection. Their elements filled with soil, gravel or sand allows raising even a 5–6 meters high protective wall around the base.

If very high walling is not necessary due to lower VBIED threat, the 2-meter-high Jersey-wall elements interlocked together may also be appropriate for protection. These barriers can provide protection through their mass (a 3-meter-long Jersey barrier weighs approximately 1.8 tons) but when placed on the ground surface, they may be ineffective against heavy vehicular attack. Therefore, they need to be embedded and include vertical anchorage of steel reinforcing through the barrier.

7 Padányi József: Műszaki zár a határon (Engineer barrier at the border). *Műszaki Katonai Közlöny,* 25(2015)/3. 21–34.

At permanent facilities the protective walling can be supplemented with other types of barriers as fix bollards and beams made of steel or concrete. At a temporary facility the triangular or rectangular log cribs, log hurdles, ditches, steel or concrete hedgehogs and tetrahedrons, concrete cubes, 200-liter drums filled with sand may also be parts of the perimeter security system. Spacing between these barriers should not exceed 1–1.2 meters, depending on the expected threat.

Figure 3: DEFENCELL protective wall[8]

Whilst passive barriers mentioned above are normally used for perimeter security, the active vehicle barriers are mostly located at facility entrances, entry points (gates) or selected interior locations (entrances to restricted areas).

As one of the active barriers of permanent facilities, the retractable bollard system consists of one or more rising bollards operating independently or in groups of two or more units. Bollards can be raised or lowered by a buried hydraulic or pneumatic power unit, controlled remotely. Typical retractable bollards are 30–35 centimetres in diameter, up to one meter high, and are usually mounted 0.8–1.0 meter apart, depending on expectable VBIED threat. The bollard operating time is adjustable and ranges from 3 to 10 seconds. Emergency operating systems can raise bollards in 1.5 seconds.

Another active element, the rising wedge barrier can be surface mounted or mounted in a shallow excavation. Raised heights are from about 0.5 to 1.2 meter and the standard width is 3 meters. In surface-mounted installations all components are above ground and no cutting or excavation is required on concrete or asphalt surfaces.

8 *DefenceCell: Advantages.* Source:, http://www.defencell.com/advantages_home.html (11.03.2016)

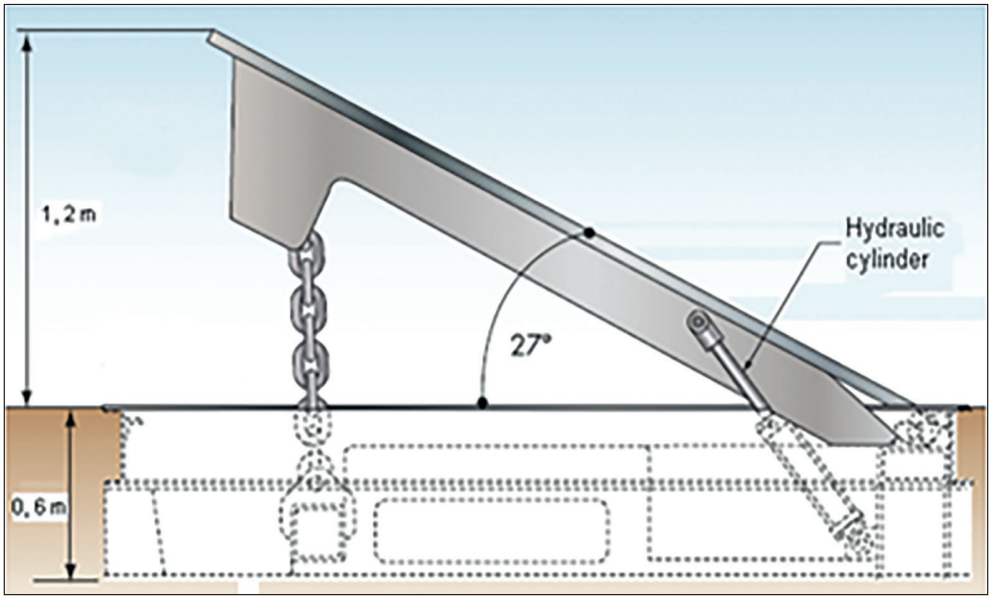


Figure 4: Rising wedge barrier[9]

The rotating wedge is similar in action to the rising wedge barrier but it has a curved front face providing a better appearance, and is embedded to a greater depth. The height of this obstacle is between 0.5 and 0.8 meter, the standard width is 3 meters. It is operated hydraulically by heavy duty rams, and the operating time is about 2–3 seconds per movement.

Besides the active barriers introduced above, crash beams and gates should function as a barrier, too. Beams are usually counterbalanced and lift at one end to allow vehicle access. This system is frequently used for low impact conditions when vehicle speed can be limited and as an interior barrier after a primary high impact barrier. The crash gates include both sliding and swinging styles, the clear opening range is from 4 to 9 meters and the typical height is between 2 and 3 meters.

The constructed active barriers above are mostly used at permanent military facilities and buildings. The active barriers for a temporary military facility (e.g. a camp) may include blocks in different shapes and made of steel or reinforced concrete. They should have handles for relocation and also require a heavy equipment to assist in the transfer.

9 FEMA–426/BIPS–06..., *op. cit.*

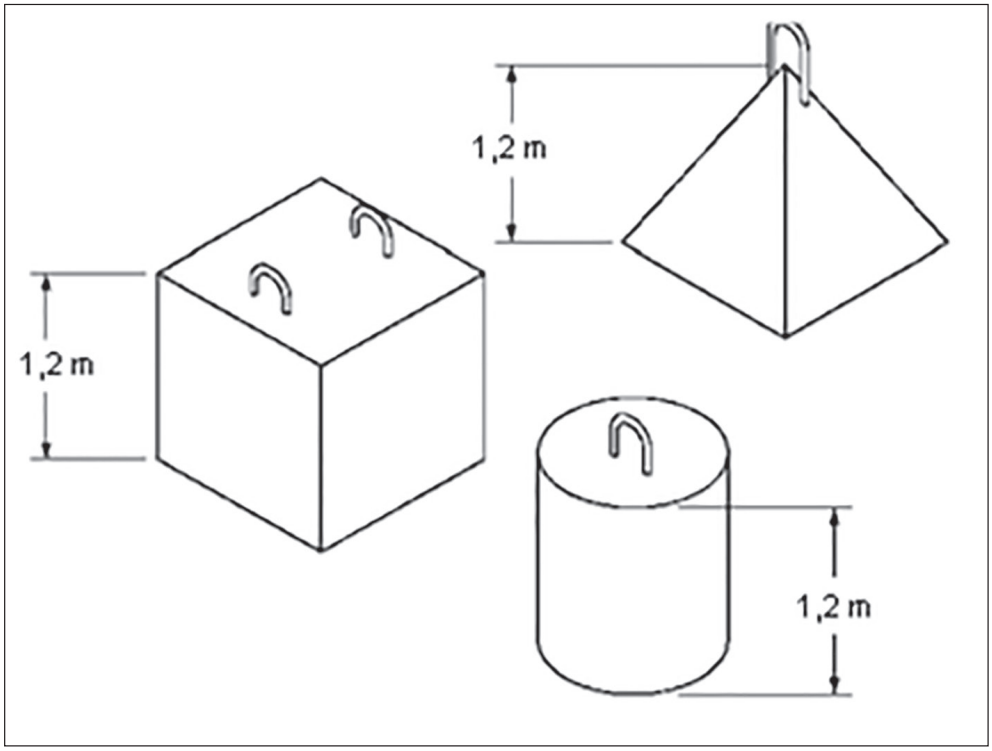


Figure 5: Reinforced concrete blocks[10]

Bars and gates used at entrances of military camps are weaker constructions than those used at a permanent facility. They are operated by hand, since hydraulic or electric sources are usually not available. Movable tire shredders causing flat tire can be also used against wheeled vehicles, forcing them to slow down.

Mobile wedge barriers which can be moved into position by a truck in a few minutes also exist. These can form an effective element of a planned temporary barrier system to respond to a heightened VBIED threat.

10 Unified Facilities Criteria (UFC 4-022-02)..., op. cit.

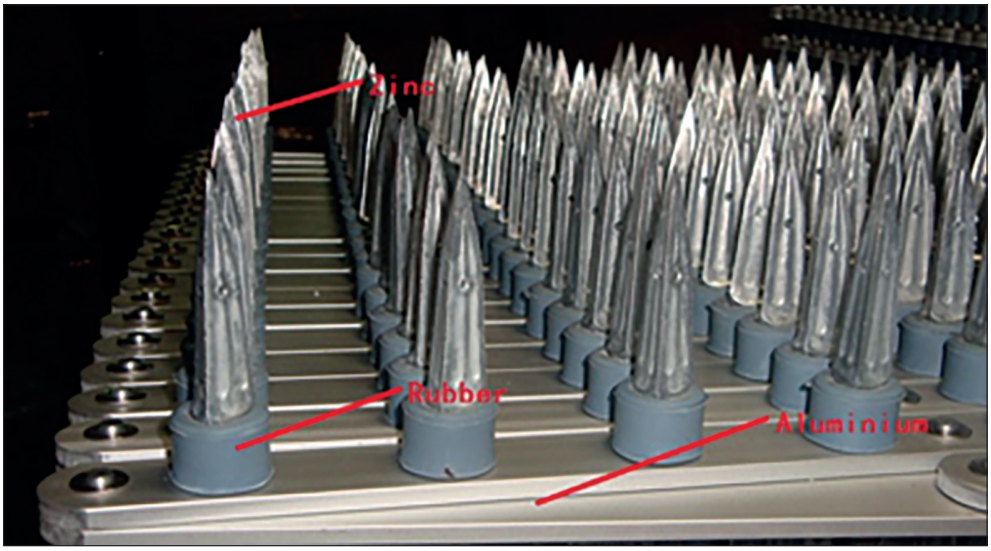


Figure 6: Tire shredder[11]

Summary

Military facilities are highly endangered by terrorist blasts. Basically, there are three ways to perpetrate an IED-attack against a military facility. First, when someone hidden from view tries to take a bomb into the facility, second when detonates outside, near to the facility perimeter and third when tries to break through the perimeter with a vehicle. The first case may be prevented with strict explosive detection, the second one with appropriate standoff distance, the third one with strong walling and perimeter barriers.

Inflicting serious damage on a military facility requires adequate quantity of explosives, and vehicles are the perfect method for transporting these explosives. A movable VBIED can appear anywhere and may cause higher threat than a stationary one.

Vehicle barriers for a movable VBIED must be capable of stopping the moving vehicle at the perimeter. For a stationary vehicle bomb, vehicle barriers must only mark the perimeter of the standoff zone, but they are not required to stop the moving vehicle.

The number of gates and perimeter entrances must be the minimum required for safe and efficient operation of the facility. When closed, gates and entrances must provide a barrier structurally comparable to their associated barriers.

The most important segments for security are keeping adequate standoff distance around the facility, forcing moving vehicles to slow down before they impact the barriers and having a well-designed, strong, effective physical security system.

11 Source: http://img.alibaba.com/img/pb/835/261/370/370261835_473.jpg (11.03.2016)

References

Berek Tamás – Pellérdi Rezső: ABV (CBRN) kihívásokra adott válaszlépések az EU-ban. (Answers of EU for CBRN challenges)., *Bolyai Szemle,* 20 (2011)/2.

DefenceCell: Advantages, . Source: http://www.defencell.com/advantages_home.html (11.03.2016)

Dénes Kálmán: Aspects of water supply and sewage systems in military camps,. *Bolyai Szemle,* 20(2011)/1

FEMA–426/BIPS–06: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings: Buildings and Infrastructure Protection Series, Edition 2. U. S. Department of Homeland Security (October 2011)., Source: https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf

Field Manual 3–19.30 Physical Security. HQ U. S. Department of the Army (8 January 2001)

Kovács Tibor: A katonai táborok biztonsági rendszereinek kialakítása, különös tekintettel a robbantásos merényletek megelőzésére, azok hatásai csökkentésére. (Security system of military camps, with especial regard to prevention of blasting attempts and reduction of their effects),. *Műszaki Katonai Közlöny,* 22(2012)/3.

Kovács Zoltán: Az improvizált robbanóeszközök főbb típusai (Important types of improvised explosive devices),. *Műszaki Katonai Közlöny,* 22(2012)/2 .

Padányi József: Műszaki zár a határon (Engineer barrier at the border),. *Műszaki Katonai Közlöny,* 25(2015) /3.

STANAG 2280 (Edition 1) Design Threat Levels and Handover Procedures for Temporary Protective Structures, NATO Standardization Agency (18 December 2008), 28.

STANAG 3680 NATO Glossary of Terms and Definitions (AAP–6), NATO Standardization Agency (17 November 2015): 431 p.

Unified Facilities Criteria (UFC 4-022-02) Selection and application of vehicle barriers, Change 1, US Department of Defense (9 August 2010).

Unified Facilities Criteria (UFC 3–340–02) Structures to Resist the Effects of Accidental Explosions, U.S. Department of Defense (5 December 2008).

Unified Facilities Criteria (UFC 4–010–01) Minimum Antiterrorism Standards for Buildings, Change 1, U.S. Department of Defense (1 October 2013).

Katonai létesítmények fizikai védelme

KOVÁCS ZOLTÁN

Az állandó és ideiglenes katonai létesítmények rendkívül veszélyeztetettek a különböző támadások (fegyveres, robbantásos, ABV) által. A szerző röviden bemutatja a robbantásos cselekmények fő eszközeit, az improvizált robbanószerkezeteket, valamint a katonai létesítmények fizikai védelmi rendszerének egyik szegmensét: azokat az eszközöket és alkalmazásuk lehetőségeit, melyek elsősorban a gépjárműben elrejtett robbanószerkezetek katonai létesítménybe történő bejutását, bejuttatását hivatottak megakadályozni, megnehezíteni.

Kulcsszavak: katonai létesítmény, biztonság, fizikai védelem, határvonal védelem, akadályok, improvizált robbanószerkezet, IED, VBIED

Balog Károly

Digitális PMR-ek támadási és védelmi lehetőségei

Napjainkban az engedélyhez kötött és engedély nélkül is üzemeltethető PMR[1] rádiótechnológia a mobiltelefonoknál már megtapasztalt paradigmaváltáson megy keresztül. Újfajta digitális PMR rendszerek és egyedi készülékek kezdenek elterjedni a gyakorlatban, melyek frekvenciaengedélyhez nem kötött változatai ráadásul olcsók, bárki számára hozzáférhetők, és mozgásuk sem korlátozott. Mivel ezek az eszközök a hagyományos távközlési infrastruktúrákat kikerülhetik, ebben az esetben felderítésük, ellenőrzésük kizárólag a rádiófelderítés eszközrendszerével történhet. Természetesen a más kommunikációs infrastruktúrához is kapcsolódó rendszerek nem csak a rádiócsatornán keresztül támadhatók. Cikkemben áttekintem és összefoglalom mind az egyedi készülékek, mind a rendszerek támadási vektorait, valamint a PMR készülékekben és rendszerekben alkalmazható védelmi megoldásokat is.

Kulcsszavak: digitális professzionális/magán mobilrádió, rádiófelderítés, rejtjelzés, titkosítás, elektronikai védelem, információbiztonság

Bevezető

Kutatási témámban a nemzetbiztonsági rádiófelderítésen belül annak viszonylag új célterületével, az engedélyhez kötött és engedély nélkül is használható PMR eszközök digitális változatainak felderítési ellenőrzési kérdéseivel foglalkozom. Annak eredményeként, hogy az analóg PMR rádiótechnológia a mobiltelefonoknál már megtapasztalt paradigmaváltáson megy keresztül, neves európai, amerikai és japán gyártók szabványos digitális rendszerei és készülékei egyre jobban kezdenek elterjedni a gyakorlatban. Emellett azonban jelentős népszerűségnek örvendenek a kínai cégek olcsó, de a szabványok kereteit gyakran átlépő készülékei is.

Mivel az ilyen eszközök teljes mértékben kikerülhetik a hagyományos távközlési infrastruktúrákat, ebben az esetben felderítésük és ellenőrzésük kizárólag rádiós úton, a rádiófelderítés eszközrendszerével történhet. Másrészt viszont az engedélyhez kötött rendszerek esetében egyre elterjedtebb, a trönkölt rendszerek esetében pedig általános, hogy

1 PMR: Professional/Private Mobile Radio – professzionális/magán mobilrádió. A felhasználók által saját maguknak nyújtott, zárt körű rádióalkalmazások gyűjtőneve.

ezek valamilyen egyéb távközlési infrastruktúrához is kapcsolódnak, a legtöbb esetben valamilyen IP alapú hálózathoz történő csatlakozással. Ebben az esetben viszont a hálózati oldalról is támadhatóvá válnak a rendszerek.

Ezek az új típusú digitális eszközök a professzionális rendszerekhez hasonló megoldásokat tartalmaznak, azonban ezeket többféle eltérő szabvány formájában valósítják meg. [1] Ezért a hagyományos analóg felderítő berendezésekkel felderítésük csak részben, azonban ellenőrzésük (dekódolásuk) egyáltalán nem valósítható meg. Ehhez egyfajta paradigmaváltás szükséges az ellenőrző eszközök megoldásaiban is. A célom, hogy megvizsgáljam a rendszerek rádióspektrumon keresztüli sebezhetőségét, másrészt a hálózati infrastruktúra felőli támadásának lehetőségeit is. Ehhez szükséges a készülékek és rendszerek biztonsági fenyegetéseit, sérülékenységeit, és ezek kockázatát is feltérképezni (Risk Management) az ilyen rendszerek evolúciója során. A védelmük lehetséges megoldásait is célszerű körüljárni az elektronikai védelem, valamint az információbiztonság (Information Assurance) szemszögéből is, melyek rendkívül fontosak a kritikus infrastruktúrákban (repülőterek, erőművek stb.) alkalmazott PMR-eknél, vagy kiemelten fontos pl. kiscsoportos taktikai kommunikációra történő alkalmazásánál.

Az információbiztonság több mint titkosítás

Ebben a részben megvizsgálom, hogy az IP-hálózatokhoz is kapcsolódó, de alapvetően rádiós, tehát összességében hibrid rendszerek milyen biztonsági kockázatokkal rendelkeznek a korábbi hagyományos rádiós rendszerekhez képest. Ez utóbbinál kézenfekvő kockázatot egyedül a rádiócsatornán keresztüli lehallgatás (zavarás – elektromágneses sugárzás révén megvalósuló információszerzés vagy az információtovábbítás korlátozása, akadályozása), továbbá a fizikai pusztítás jelent. Az ezek elleni védekezés az *elektronikai védelem*[2] módszereivel lehetséges. Ehhez járul még hozzá a berendezések fizikai védelme, valamint esetlegesen a redundáns kialakítás a folyamatos működés biztosítására. Azonban a hibrid rendszereknél gyakorlatilag az infokommunikációs, így több más között az informatikai komplex rendszerekre jellemző (külső és belső) fenyegetésekkel és az ezeket lehetővé tevő sérülékenységekkel is foglalkozni kell. Mivel a hibrid rendszerek műveleti tartománya az RF spektrum mellett a vezetékes hálózati infrastruktúrát is magába foglalja, így a hibrid PMR rendszerek a kibertérben működnek, azaz a támadásukra a kibertéri műveletek, védelmük során pedig a komplex kibervédelmi vagyis elektronikai- és számítógéphálózat-védelmi eljárások alkalmazhatók. [2] Ez utóbbi komplex megvalósítására a civil rendszerek esetében napjainkban az információbiztonság (IA –Information Assurance) ad választ. Vizsgáljuk meg a következőben a két összetevőt külön-külön.

2 EPM: Electronic Protective Measures. Elektronikai védelem, amelyik biztosítja az elektromágneses spektrum saját részről történő hatékony használatát.

Az elsődleges kérdés az RF spektrumon keresztüli támadás lehetősége, azaz a *rádiófelderítés:* a technikai, tartalmi és geolokációs adatok megszerzése, illetve az *elektronikai támogatás*[3]*:* az elektronikai helyzet feltérképezése a zavarás vagy megsemmisítés szempontjából. Mindkét típusú felderítésnél, mind analóg és digitális átvitelnél egyaránt lényeges a használt elektromágneses spektrum, átviteli eljárás és protokoll ismerete, azonban lehallgatásnál az alkalmazott titkosítás ismerete, és ennek visszafejtési módszere is lényeges, hiszen a tartalmi hozzáféréshez ez a meghatározó kulcstényező. A zavarás szempontjából a frekvenciatartományok, a teljesítmények, és a fizikai elhelyezkedés a fontosabbak. Természetesen ezek a tartalom megszerzéséhez szintén fontos adatok, melyek alapvetően befolyásolják az adatszerzés sikerességét. A fenti szándékos tevékenységek elleni védekezésre az *elektronikai védelem* adja meg a választ.

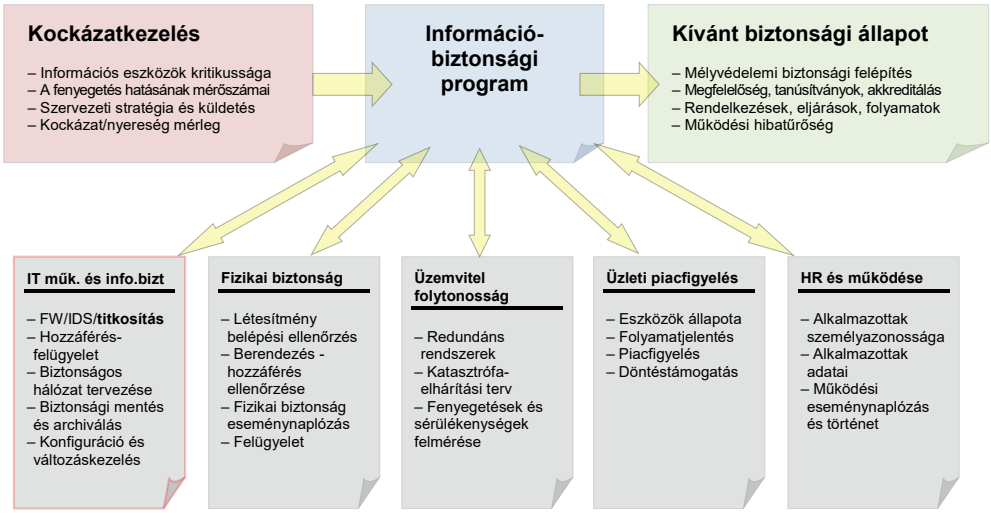
A második kérdés az információbiztonság, melynek alapvető objektumait elsősorban a *biztonságot fenyegető veszélyeztetések*, másodsorban a védelmi megoldások, rendszabályok képezik. A biztonságot fenyegető veszélyeket itt alapvetően a kiberműveleteken belüli *számítógép-hálózati műveletek* támadó részei jelentik. Azaz hardveres vagy szoftveres úton történő behatolás a PMR rendszerek kapcsolódó hálózataiba. Ez a hálózat struktúrájának feltérképezését, a hierarchikus működési sajátosságok feltárását, a hálózati adatáramlás tartalmának regisztrálását, a hálózatokban folyó megtévesztő, zavaró tevékenységet, a célobjektumok program- és adattartalmának megváltoztatását, megsemmisítését jelentik. [2] Természetesen ezek hibrid PMR rendszerek esetében konkrét hálózati elemekhez, objektumokhoz, és adott rendszerekben megvalósuló konkrét folyamatokhoz köthetőek.

Az információvédelem az információbiztonság kialakítására és fenntartására – a biztonság összetevőinek érvényesülésére – irányuló tevékenységek és rendszabályok összessége. Egy adott objektum biztonsága elleni fenyegetések csökkenthetők, elháríthatók az objektumot fenyegető szereplőkre, jelenségekre, továbbá a védendő rendszer elemeire irányuló tevékenységekkel is. Védelmi intézkedések közé tartozik mindenekelőtt a biztonságot fenyegető szereplőkre, jelenségekre vonatkozó információk megszerzése, valamint a képességeiket, lehetőségeiket csökkentő, célzottan „rájuk irányuló" ellentevékenység is. [3]

A PMR/LMR[4] rendszerek esetében is az általánosan elfogadott kockázatalapú üzleti és információbiztonsági elméletek szerint a kockázatelemzésnek megfelelően kialakított információbiztonsági program, azaz a komplex védelmi intézkedések együttesének alkalmazásával érhető el a kívánt biztonsági állapot. [4] Ennek döntési folyamatát és a szervezetre gyakorolt hatásait mutatja be az 1. ábra.

3 ESM: Electronic Support Measures. Elektronikai támogatás.

4 LMR: Land Mobile Radio, a PMR fogalmának amerikai megfelelője, de fogalmilag ugyanazt a kategóriát jelenti.



1. ábra: Az információbiztonság döntési folyamata és hatása a szervezetre (Forrás: [4])

A biztonság kockázatalapú megközelítése abból indul ki, hogy a biztonság egy dinamikusan változó, kedvező állapot, azonban tökéletes biztonság a gyakorlatban szinte sohasem érhető el, mindig számolni kell valamilyen kockázattal. A védelmi intézkedéseket a kockázatok elemzésére kell építeni. A kockázat egy ismert negatív hatású, adott valószínűségű jövőbeli esemény, melynek bekövetkezése függ a sebezhetőségtől is. A kockázatmenedzsment feladata, hogy a fenyegetések azonosítására és kiküszöbölésére – hatásuk felmérésére alapozva – költséghatékony megoldásokat alkalmazzon. Ehhez tisztában kell lenni a sebezhetőségekkel, a fenyegetésekkel, valamint azzal, hogy ezeket milyen védelmi intézkedésekkel lehet mérsékelni. [5]

Az 1. ábrából látható, hogy általánosságban az információbiztonságnak a PMR rendszerek esetében, az informatikai biztonság mellett számos aspektusa van, így a fizikai biztonság mellett az üzemvitel-folytonosság, az üzleti piacfigyelés, valamint az emberi erőforrásokkal történő gazdálkodás szempontjait is figyelembe kell venni. Az egyes területeknek önmagában is jelentős szakirodalmuk van, így a jelen cikk kereteiben csak a kutatási témámhoz szorosabban kapcsolódó, technikai úton történő adatszerzés lehetőségeivel foglalkozom leginkább.

Ennek kérdései az információbiztonság területén belül az informatikai biztonság témaköréhez kapcsolódnak alapvetően, és a sérülékenységekhez kötötten általában szándékosságot feltételeznek a támadó részéről (lásd a számítógép-hálózati műveletek támadó jellegét fentebb). Tehát a nem rádiós úton történő technikai hozzáférés aspektusát az informatikai hálózatokon keresztüli (távoli) hozzáférés veszélyei jelentik. Így elsődlegesen az informatikai rendszer határvédelmét biztosító tűzfal (FW – Firewall), behatolásdetektáló rendszerek (IDS – Intrusion Detection Sytem) védelme mellett a biztonságos háló-

zattervezés és ehhez történő hozzáférés-felügyelet játszik kiemelkedő szerepet. Mindezek mellett pedig adminisztratív feladatok is vannak, melyek az adatbiztonság témakörébe tartoznak, úgymint a rendszeres archiválás, és a rendszerváltozások folyamatos nyomon követése, felügyelete.

Természetesen a bevezetett rendszabályok és folyamatok érvényesülését folyamatosan ellenőrizni kell, amire a különféle minőségbiztosítási szabványok (pl. ISO/IEC 27001,[5] NIST 800) szolgálnak, melyek alapján elvégezhető az információs rendszer tanúsítása. Ha ezeket megfelelő módon alkalmazzák a gyakorlatban, akkor elérhető az elvárt biztonsági állapot, ami egy tervezett mértékű kockázatot tartalmaz.

A következő részekben áttekintem a PMR rendszerek típusait, és megvizsgálom, hogy ezek rendszerfelépítésük okán alapvetően hogyan különböznek támadási lehetőségek és a szükséges védelmi megoldások tekintetében is.

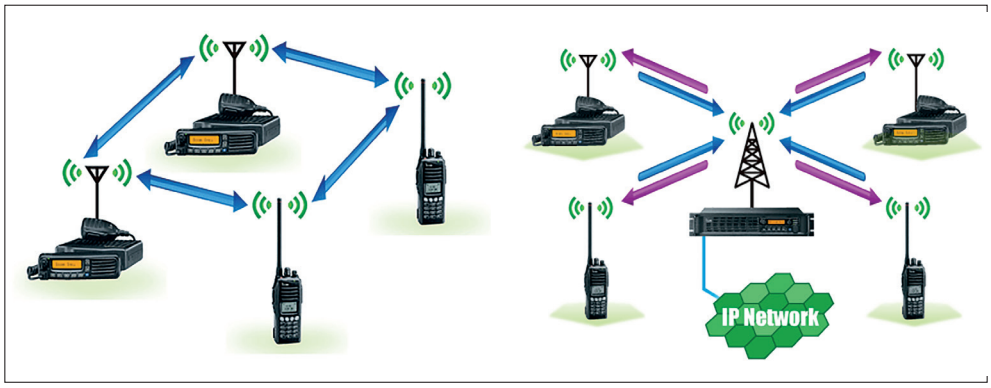
A PMR rendszerek támadási és védelmi szempontú csoportjai

Az ilyen típusú rendszerek támadási és védelmi lehetőségeinek vizsgálatakor a biztonság alanyából, azaz a védendő információból és az azt továbbító PMR/LMR rendszerek típusaiból kell kiindulnunk. [5]

Így a legegyszerűbb direkt kommunikációt alkalmazó rendszerek (2. ábra bal oldala) támadhatók a legkisebb felületen, kizárólag a rádiócsatornán keresztül, mivel ezek nem rendelkeznek semmilyen infrastruktúrával, egyedül a kommunikációban részt vevő készülékekkel. A rádióknak saját tápellátásuk van, így ha ezekből még tartalékkal is rendelkezünk, az egyik leghibatűrőbb kommunikációs módozatot kapjuk, melyet egyedül véletlen vagy szándékos zavarással tudunk hatástalanítani. A felderítésük, ellenőrzésük pedig kizárólag a rádiófelderítés eszközrendszerével lehetséges. Ezeket felfoghatjuk katonai terminológiában egyfajta harcászati hálózatnak is, mivel nem helyhez kötöttek, bárhol bevethetők, nincs infrastruktúra-igényük, így ha a rádió-össze-köttetés nem akadályozott és a rádiók működnek, összehangoltak, létrejöhet az összeköttetés. Az egyedüli probléma a korlátozott földrajzi lefedettség, amely azonban a rádiók teljesítményének növelésével jelentősen kiterjeszthető. A védendő eszközök köre egyedül a kommunikációban részt vevő rádiókat jelenti. A védendő információk köre ezeknél a rádióknál az átvitt beszédinformáció mellett valamilyen jelzésinformáció. Ezek analóg rendszernél valamilyen szelektív hívásjelzés, digitális esetben pedig ezeken felül valamilyen szabványfüggő formátumú lassú

5 Az ISO/IEC:27001 szabvány alapvető célja az Információbiztonsági Irányítási Rendszer létrehozása és működtetése. A szabvány felhasználóinak a biztonsági követelményeket, intézkedéseket a szervezet üzleti céljaiból és stratégiájából kell levezetniük. A szabvány megfelelőségi és ellenőrzési követelményei alapján elvégezhető az informatikai (információs) rendszer tanúsítása.

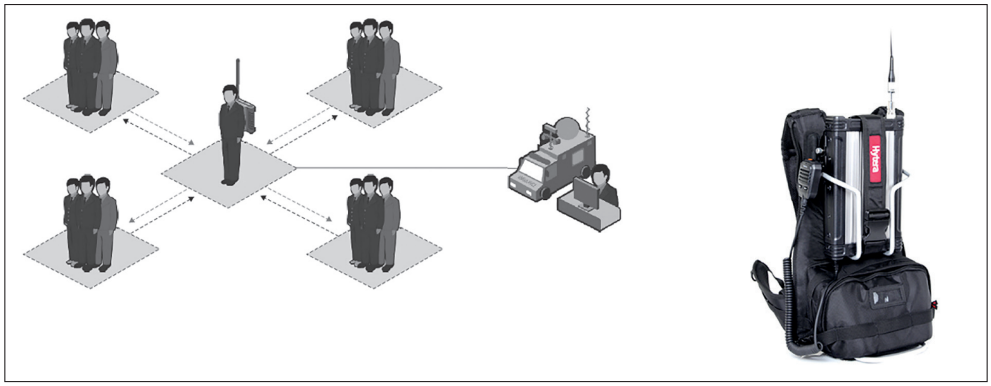
adat, amelyik általában valamilyen státusz- vagy rendszer-, illetve rövid szöveges üzenet, pozícióinformáció, valamint egyéb jelzést és azonosító információkat hordozhat. [1]



2. ábra: Direkt kommunikáció és helyszíni, vagy diszpécser típusú rendszer (Forrás: [6])

Ha nagyobb területi lefedettség szükséges, átjátszót alkalmaznak a hatótávolság növelésére. Ekkor a kommunikáció a PMR terminálok között nem direkt módon, hanem egy átjátszó állomáson keresztül jön létre (2. ábra jobb oldala) ezek az ún. helyszíni vagy diszpécser típusú rendszerek, melyek nagyon elterjedtek a gyakorlatban, a kiskereskedelemben, üzletekben, raktárakban, gyárakban, építkezéseken, kikötőkben, tömegközlekedésben, repülőtereken, taxi-, biztonsági és futárszolgálatok kommunikációja biztosítására.

A technológiai fejlődés eredményeként már rendelkezésre állnak olyan különleges hibrid taktikai megoldások is, amelyek egy hátizsákban hordozható kisméretű átjátszó alkalmazásával, komplex módon terjesztik ki egy korlátozott területen a lefedettséget pl. épületen belül, vagy egyéb infrastruktúra-hiányos területeken (3. ábra). Egy ilyen rendszer bár nem direkt kommunikációt alkalmaz, de a mobilitásával taktikai körülmények között biztosíthatja a diszpécser rendszerek kiterjesztett hatótávolságát és menedzselhetőségét.

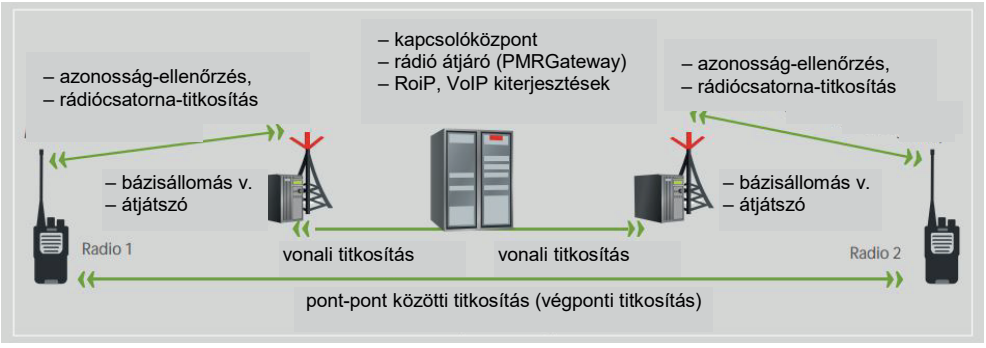


3. ábra: Hordozható taktikai diszpécser típusú rendszer (Forrás: [7])

A harmadik típus a dedikált trönkölt rendszerek csoportja, melyek a mobilhálózatokhoz hasonlóan bázisállomás-rendszert, kapcsolóközpontokat és központi adminisztrációt alkalmaznak, akár egy országot is átfogó területi lefedettség és a szolgáltatások biztosítására.

Látható, hogy a diszpécser, a hibrid taktikai és a trönkölt rendszereknél a rádiókészüléken kívül a rendszerek nagyságától és komplexitásától függő járulékos infrastruktúrával is számolni kell. Ezekben a modern rendszerekben szükség szerint integrálhatnak több kommunikációhordozót, így létrehozva egy olyan kommunikációs hálózatot, amely megfelelően összekapcsolja a területet és a háttér irodai hálózatot a nagyobb hatékonyság és a zökkenőmentes felhasználói élmény érdekében. [8] A helyszíni/diszpécser típusú és trönkölt rendszerek, valamint az IP-alapú vezetékes és vezeték nélküli hálózati technológiák kombinálásával eltérő nagyságú és topológiájú hálózatok építhetők, melyek a VoIP[6] és RoiP[7] megoldások alkalmazásával változatos, az igényeknek megfelelő rendszerek létrehozását teszik elérhetővé.

Ezek további sérülékenységeket, és egyben komplexebb támadási lehetőségeket jelentenek. A védendők köre ezeknél kiterjed az átjátszó vagy bázisállomásokra, kapcsolóközpontokra, diszpécser állomásokra, az ezek elhelyezésére, valamint a rendszer felügyeletére-vezérlésére kiépített objektumokra, továbbá az ezekhez kapcsolódó hálózatképző elemekre, informatikai eszközökre, vezetékes vagy vezeték nélküli átviteli utakra egyaránt. A védendő információk köre tekintetében pedig a rádiócsatornán átvitt információkon felül az összekötő felhordó hálózatokon átvitt beszéd és jelzés információkra is kiterjed az adatok védelme, ahogyan ez a következő ábrán látható.



4. ábra: Átviteli utak lehetséges védelme PMR rendszereknél (Forrás: [9])

A 4. ábra az átviteli utak összes lehetséges védelmi és azonosítási eljárását ábrázolja, de ezek adott rendszerekben skálázva vannak, azaz a teljesen titkosítatlan és azonosság-ellenőrzés nélküli esettől (többnyire analóg) egészen a végponti titkosításig, ami a legnagyobb biztonságot jelenti.

6 VoIP: Voice over Internet Protocoll: beszédátvitel internetprotokoll segítségével.
7 RoIP: Radio over Internet Protocoll.

A fentiekből következik, hogy napjainkban a legegyszerűbb rádiókommunikációs technológia is összetettebb, mint az elődei, így sokkal sérülékenyebb is azoknál. Ez a tény azonban nem mindig tükröződik az egyes alkalmazók rendszer-felügyeleti gyakorlatában. [4] Napjaink internethez kapcsolódó rendszerei nem csak a rádiós alrendszer, de a hálózati infrastruktúra oldaláról is támadási felületet nyújtanak, így adott esetben sokkal sérülékenyebbek, mint az ezektől elszigetelt rendszerek.

Ezt a tényt már számos gyakorlati példa is bizonyította, hiszen akár szándékos háborús pusztítás vagy természeti katasztrófa sújtotta térségekben nemegyszer az infrastruktúra-független direkt kommunikációs rádiórendszerek maradtak az egyetlen működőképes kommunikációt biztosító megoldások, ahogyan ez a legutóbbi nepáli földrengésnél [10], de más korábbi katasztrófák vagy háborúk (pl. délszláv, iraki, afganisztáni) során is bekövetkezett. Az egyedi készülékekből álló, hagyományos infrastruktúrát nem használó készülékek autonóm csoportjai biztosítják az egyetlen működőképes és viszonylag jól használható kommunikációs módot, a hagyományos infrastruktúrák kiesése és működésképtelenné válása esetében (ha nem számolunk a meglehetősen drága, tehát a polgári lakosság számára elérhetetlen műholdas globális megoldásokkal).

Az átvitt információ fontosságát azonban nem a rendszer felépítése határozza meg, így a direkt kommunikációt alkalmazó (adott esetben taktikai célú) rendszereknél is lehet kiemelt fontosságú az átvitt közlésinformációk védelme. Természetesen itt is mérlegelni kell a kockázatot, és ennek megfelelően lehet döntést hozni az alkalmazott titkosítás erősségéről illetve szükségességéről. Az átvitt információk érvényességi ideje alapján történő szelektálás is szempont lehet a védendő információk meghatározásának körében, ahogyan ez a következő NATO-dokumentumból is kiderül. [11, 5–2. o.] Ebben megállapítják, hogy városi körülmények között, a harcászati kommunikáció legalacsonyabb szintjén az információk érvényessége olyan rövid idejű, hogy nem szükséges titkosítás alkalmazása, mivel ez jelentősen kisebb előnnyel járna, mint az igen magas bekerülési költsége. Ezenfelül annak a veszélye is reálisan fennáll, hogy egy végpont elfogásával esetleg az egész titkosítási rendszer kompromittálódik. Továbbá indokként hozza fel a dokumentum a nemzetközi együttműködés nehézségeit is az együttműködő koalíciós partnerek között, a titkosításból adódó inkompatibilitások elkerülése érdekében. Látható módon a katonai harcászati rendszereknél is alkalmazzák a kockázatelemzés módszerét és az anyagi szempontok, és a kockázatok együttes figyelembevételével állapítják meg a titkosítás szükséges mértékét adott esetben.

Összességében megállapítható, hogy a direkt kommunikációt alkalmazó rendszerek kizárólag a rádiócsatornán keresztül támadhatók. A helyi/diszpécser típusú és a trönkölt rendszerek ezen felül a hálózati infrastruktúra felől is sérülékenyek. Ez utóbbiaknál ezek fizikai objektumainak és az ezekben elhelyezett berendezéseknek, továbbá a hálózatok további más hálózatok irányába kiterjesztett kapcsolódásainak és ezek hálózatképző elemeinek sérülékenységével is számolni kell. Megállapítható, hogy minél nagyobb és bo-

nyolultabb rendszerről beszélünk, annál több a támadási lehetőség, azonban ezzel párhuzamosan nőhet a rendszerekben alkalmazott védelmi, azonosítási és titkosítási eljárások száma, és vélhetőleg hatékonysága is. A konkrét rendszerek általában mind egyedi, személyre szabott megoldásokat tartalmaznak, így a sérülékenységük a támadó számítógép-hálózati műveleteken belül a hálózat struktúrájának feltérképezésével, a hierarchikus működési sajátosságaik felderítésével tárható fel (távoli technikai adatszerzések esetén).

PMR rendszerekkel kapcsolatos sérülékenységek, támadások áttekintése

Az általam vizsgált rendszereknél a támadásokat 4 fő kategóriába sorolhatjuk, úgymint passzív, aktív, külső és belső támadások. A passzív támadás lehet a rádiófelderítés ezen belül az információ lehallgatása, dekódolása, rögzítése, a kommunikációban részt vevő felek azonosítása, a kisugárzás irányának valamint helyének meghatározása, a kommunikáció forgalmi analízise, annak eloszlása, továbbá az egyes készülékek RF újlenyomatának azonosítása is ide sorolandó. Ez utóbbi a digitális rendszerek esetében veszített jelentőségéből, mivel ha az információtartalmat vissza tudjuk fejteni, akkor az [1]-ben leírtak szerint a digitális rendszerekben az egyes eszközök azonosítóit, egyedi címeit még titkosított esetben is ismerjük egy rádióhálózaton belül, ami adott környezetben azonosítja őket. Aktív tevékenységek közé tartozik a kommunikáció zavarása, és a fizikai pusztítás, továbbá a rádiós út speciális aktív támadási formája a közbeékelődéses (MitM[8]) támadás, ami a rádiótelefonok esetében alkalmazott támadási eljárás, a titkosítás eliminálása érdekében, de megfelelő feltételek esetén szerintem PMR hálózatok esetében is alkalmazható. A hálózati infrastruktúrán keresztüli támadás szintén aktív tevékenység.

A rádiófelderítés, zavarás, fizikai pusztítás és a hálózati oldalról történő hozzáférés egyaránt külső támadásnak minősül, azonban egy hálózat belülről is támadható, viszont itt már jelentős szerepet játszik a fizikai biztonság is, amivel azonban nem foglalkozom, de megemlítem a fontosságát. Összességében a továbbiakban a külső támadásokra koncentrálok, ami lehet passzív és aktív is. Így tulajdonképpen két részre osztható a vizsgálat, ami nagyjából az ilyen rendszerek főbb részeit is jelenti. Az egyes LMR/PMR rendszereknél a biztonsági fenyegetések és sebezhetőségek vizsgálata szempontjából egy mai rendszert a következők kombinációja jellemzi:

– rádiós alrendszer és sérülékenységei;
– Voice-over-IP (VoIP) alrendszer és sérülékenységei.

Korábban az analóg rádiórendszerek esetében általában elszigetelt hagyományos rádióhálózatokkal álltunk szemben, ahol ha valami zavar volt az egyik csatornán, ideig-

8 MiTM: Man in the Middle, azaz közbeékelődéses támadás, amikor az adatforgalom rajtunk keresztül bonyolódik a hálózatban a rádiócsatornán vagy a csatlakozó hálózati infrastruktúra vezetékes részén.

lenesen áthangoltak egy tartalékra. A modern helyszíni/diszpécser típusú vagy trönkölt rendszerek esetében azonban a rendszer meghibásodása már nem korlátozódik egyetlen csatorna elvesztésére, hanem akár a teljes rendszer üzemképtelenségével is járhat. Amerikai tapasztalatok alapján több száz, de akár több ezer felhasználóra is kihatással lehetnek pl. a természeti katasztrófák, ahogyan a közelmúltban Detroitban ez bekövetkezett. Másodszor, a hardveralapú platformok erősen függenek a számítógépektől és a rajtuk futó szoftverektől. Az instabil operációs rendszerek rendszerhibákat okozhatnak az esetleges lefagyásokkal, a helytelen paraméterbeállításokkal, és így tovább.

Harmadszor, a helyi vagy diszpécser, illetve a trönkölt típusoknál a legnagyobb erőfeszítések ellenére sem beszélhetünk teljesen elszigetelt rendszerekről. Így a modern rádiós rendszerek a következő (többnyire) szándékosságot feltételező sérülékenységekkel rendelkeznek:

- A rádiós alrendszer (RF site) problémája (fizikai és informatikai egyaránt):
  - helyi hozzáférés a RF vezérléshez, az IP-címének elfogása vagy behatolás a hálózatba;
  - távoli hozzáférés az RF vezérléshez, belépési ponton keresztüli támadás a hálózati kapcsolókon vagy vezérlőkön keresztül;
  - rádiófrekvenciás interferencia nem szándékos előidézése/kialakulása, szándékos interferencia okozása, azaz zavarás;
  - hamis/lopott készülékazonosítóval hozzáférés a rendszerhez, támadás a vezérlőcsatorna jelzésátvitelén keresztül;
  - készülékbe integrált beszéd- és adatátviteli képességek felhasználása belépő pontként a hálózat vagy programok elleni támadásra;
  - az információk szándékos lehallgatása a rádiócsatornán, azaz a rádiófelderítés;
  - titkosítás esetén a kulcskezelő rendszer biztonsági problémái.
- IT biztonság problémája (megosztott kapcsolatokkal és szolgáltatásokkal):
  - szoftverfüggő hibák: vírusok, kompatibilitási problémák, szoftverfrissítések;
  - hálózati elemeken keresztüli távoli támadás lehetősége a vezérlő és menedzsment platformokhoz, a diszpécser állomások hardver- és szoftver- (többnyire Windows-alapúak) sérülékenységeinek távoli támadása;
  - a felhasználói fegyelem problémája (a számítógép-terminálok illegális/nem megfelelő felhasználása), saját programok futtatása, fertőzött adathordozók csatlakoztatása;
  - egyre nagyobb függőség a rendszeren kívüli összeköttetésektől (adatbázisok, és egyéb adatátviteli alkalmazások, illetve perifériák).
- A fizikai biztonság problémája (közös helyiségek):
  - szándékos behatolás a rendszerbe, helyi eléréssel;
  - lopás/elvesztés (számos modern rádiórendszerben a készülékek lehetővé teszik a használat megkezdése előtti felhasználói azonosítás lehetőségét, amely lehet akár egy kódsorozat beütése, de manapság akár biometrikus azonosítás is; a rádió ello-

pása/elvesztése esetén a digitális eszközöknél az egyedi azonosítók miatt lehetőség van a diszpécserállomáson keresztül a készülékek tiltására a rendszerben, mely később újra aktiválható);
– a fenti rádiós, illetve IT-infrastruktúra elemei és ezek elhelyezésére szolgáló objektumok elleni fizikai támadások.

További nem szándékos kockázati tényezők PMR hálózatok esetében a következők:
– áramellátás zavarai, környezeti tényezők hatása;
– berendezéshibák, antennarendszer hibái;
– az emberi erőforrás vétlen biztonsági kockázatai.

A rádiós alrendszer támadási lehetőségei

A rádiókommunikáció kezdeti formáinak kialakulása óta alapvető igényként jelent meg az átvitt üzenethez (kommunikáció tartalmához) való hozzáférés, azaz a *rádiófelderítés*, megvalósítása. A lehetőség kézenfekvő volt, hiszen egy rádióadás elektromágneses jeleit tetszőleges számú rádiókészülékkel vehetjük anélkül, hogy az eredeti jelre az bármilyen hatással lenne, azaz gyakorlatilag észrevétlenül, passzív módon. A jelek vétele mellett a kisugárzás irányának és fizikai helyének megállapítása is ide tartozik. A modern digitális rádióknál ezt akár maguk a rádiók is közölhetik, a beépített GPS-ek adatait továbbítva, amit vissza lehet fejteni. A lehallgatás megvalósítása a különféle rádióvevőkkel, vevőrendszerekkel és a hozzákapcsolt antennákkal lehetséges. Az aktív megoldások tekintetében számításba vehető a rádiók és rendszerek *zavarása*, melyet ezeknél az eszközöknél célzottan keskeny sávon, de akár egy adott szélesebb tartományt lefogva is el lehet végezni. A rádiós alrendszer hálózati elemei (melyek a rádiós alrendszer távvezérlésére szolgálnak) az IT-sérülékenységeken keresztül támadhatók, hasonlóan más hálózati elemekhez.

A *titkosított információk visszafejtésére*, tehát az analóg scrambling eljárások és a digitális titkosítások támadására, törésére, eliminálására irányuló megoldások ismertetése, azok titkosítási eljárásainak bemutatása előtt értelmetlen lenne, ezért analóg esetben ennek bemutatása az analóg beszédtitkosítási eljárások (scrambling) után, a védelem résznél közvetlenül azokhoz kapcsolódva kerül ismertetésre. A digitális rádiók titkosításáról mégis itt kell néhány szót ejteni előzetesen, mert az egyik *legújabb támadási vektor ezek kulcsainak megszerzésére vagy eliminálására irányul*.

A digitális kódolások visszafejtésének napjainkban külön tudománya van, a kódtörés. Ahhoz azonban, hogy feltörjünk egy kódolást, be kell azonosítani, hogy milyen módszerrel készült a titkosítás. Ezután lehet kipróbálni a kulcsokat. A PMR rádiók titkosítására napjainkban elterjedt AES,[9] egy szimmetrikus kulcsú rendszer, azaz ugyanaz a kód szükséges

9 AES: Advanced Encryption Standard. Fejlett titkosítási szabvány, 2001-ben szabványosították az USA-ban.

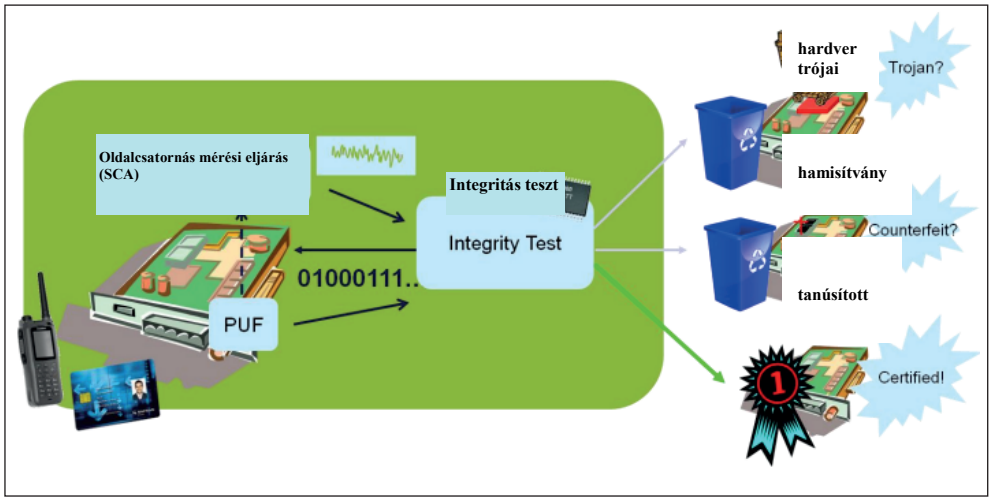
az üzenet titkosításához, mint a dekódoláshoz. Itt a kulcsok nem nyilvánosak, ellentétben az ún. aszimmetrikus vagy nyilvános kulcsú rendszerekkel, mint az RSA,[10] aminél két eltérő kulcs van. A titkosító kulcs nyilvános, de a dekódoláshoz szükséges második kulcs csak az üzenet vevőjénél áll rendelkezésre, megfelelően biztonságosan tárolva. Azaz bárki küldhet nekem titkosított üzenetet, de csak én tudom visszafejteni. A legjobb módszer az üzenet megfejtésére, ha azt számítógépen rögzítjük, és valamilyen matematikai elmélet és az eljárás valamilyen gyengeségének kihasználásával igen erős hardvertámogatás mellett próbálkozunk a lehetséges kulcsok kiszámolásával. Az erős titkosítások esetén azonban ez véges, tehát műveletileg használható időn belül általában nem vezet eredményre. Azonban ha a titkosítási eljárásba mesterségesen hibát visznek, a kulcs feltörhető. Természetesen a legkézenfekvőbb megoldás a nem nyilvános kulcsok megszerzése lenne mindkét fenti esetben, amivel bármilyen kommunikáció visszaállítható eredeti formájában.

A titkosítási rendszernek alapvetően 3 eleme van. A kódolás és dekódolás algoritmusa (a mód, ahogyan az információból kódolt üzenet lesz, majd megint információ), a titkosító kulcs, valamint a rendszer kulcskezelési megoldása. Mivel egy adott eszköz esetében a titkosítási rendszer és az algoritmus nem változik, ezért az integritás megőrzése érdekében a titkosító kulcsokat kell változtatni adott időnként. A kulcskezelési (key management) megoldások erre szolgálnak, azaz előállítják, tárolják, szétosztják, kiválasztják, továbbá megsemmisítik vagy archiválják az egyes kulcsokat. A probléma általában a kulcsmenedzsment kivitelezése, azaz hogyan juttassuk el a kulcsokat a felhasználókhoz. Ez a kérdés már a korai katonai célú digitális harcászati rendszerek esetében is felmerült [12], mivel ellenséges környezetben nagyobb a veszélye egy kulcs kompromittálódásának. Ekkor dolgozták ki a rádiócsatornán keresztüli kulcscsere eljárását, az OTAR[11] technológiát, amelyet azóta számos vezeték nélküli rendszerben alkalmaznak, így pl. trönkölt, de akár helyi vagy diszpécser típusú PMR rádiórendszerek esetében is. Így ezzel már meglehetősen nagy biztonság érhető el a kulcsok kompromittálódásának megelőzése terén.

Napjainkban azonban a fentiek miatt megjelent egy új lehetőség, amelyik a rendszerben lévő *biztonsági áramkörök hardverelemeken keresztüli fertőzésével* (hardver trójai – HT[12]), próbálja meg a kommunikáció visszafejtéséhez szükséges kulcsokat megszerezni, vagy azokat gyengíteni. Ezek pl. a később említett AES blokktitkosító modulokat (8. ábra) támadják. Egyre növekvő az aggodalom, hogy a hardverelemek hamisítása drámaian növekszik. Napjainkban a piacokon kapható alkatrészek mintegy 5-20%-a hamisított alkatrészként kerül forgalomba. Továbbá a fenyegető „trójai" programok, vagy az integrált áramkörök (IC) rejtett funkciói az elméletből egyre inkább a gyakorlati megvalósítás mezejére léptek.

10 RSA: Rivest, Shamir, Adleman, azaz a kifejlesztőinek kezdőbetűiből elnevezett, nyílt kulcsú titkosítási eljárás.
11 OTAR: Over The Air Rekeying, azaz rádiócsatornán keresztül kivitelezett kulcscsere eljárás.
12 HT: Hardware Trojan. Hardver trójai program, ami az eszközökben már gyári állapotban is megtalálható a hamisított alkatrészek miatt, így gyárilag hordozza az ilyen alkatrészekből összeszerelt rádiók sérülékenységét.

A probléma annyira valós, hogy az EU kutatási projektet indított a fentiek megoldására a hetedik keretprogramon belül, több mint 5 millió euró támogatással. [13] A HINT projekt 2013. májusban megjelent publikációjában [14] smart ID card és PMR kézi készülékeken demonstrálják a HT detektálását az általuk kidolgozott módszer segítségével, ahogyan ez az 5. ábrán látható.



5. ábra: A HINT projekt hardverintegritás-tesztje (Forrás: [14])

A HINT projekt a fenti új kihívásokkal foglalkozik, innovatív technológiák kifejlesztését kutatja annak ellenőrzésére, hogy a vizsgált rendszer eredeti és nem módosították. E technológiák támogatják egy adott rendszerben használt hardverelemek (integrált áramkörök, amelyek lehetnek ASICS[13] áramkörök, hagyományos COTS[14] alkatrészek csakúgy, mint a legmodernebb átprogramozható eszközök, CPLD[15]/FPGA[16] áramkörök egyaránt) biztonságának, hitelességének és integritásának megállapítását. Erre az ún. PUF[17] alapú aláírást és azonosság-ellenőrzést valamint az SCA[18] eljárást alkalmazzák, amelyek lehetővé teszik a fenti hardverelemek hatékony és biztonságos ujjlenyomatának megállapítását és az ezekhez képesti eltérések detektálását. A fenti projekt kutatói a [15] bevezető publikációjukban a HT által egy PMR készülékben előidézhető eseményeket a következőkben aposztrofálták:

13 ASICS: Application Specific Integrated Circuits. Alkalmazásorientált integrált áramkörök, amelyek adott speciális célra, adott feladatra készülnek.
14 COTS: Commercial Off-The-Shelf. Hagyományos, általános célra készült kereskedelmi forgalmú alkatrészek.
15 CPLD: Complex Programmable Logic Device. Komplex átprogramozható logikai eszköz.
16 FPGA: Field Programmable Gate Array. Átprogramozható kapuáramkörtömbök adott, pl. rádiós funkciók hardveres végrehajtására.
17 PUF: Physically Unclonable Function. Fizikai másolásvédelmi funkció.
18 SCA: Side Channel Analysis. Oldalcsatorna alapú azonosság-ellenőrzés; egy hardverkomponens viselkedésének elemzésén alapuló eljárás, amellyel megállapítható az eredeti specifikációtól való eltérés.

1. Szolgáltatás-megtagadás előidézése: a készülékben alkalmazott cryptoASIC és a hardver kriptoprocesszor között. A cryptoASIC-ba implementált HT képes a két eszköz közötti busz kommunikációját gátolni, továbbá képes ún. kill switch állapotba kapcsolni a kriptoprocesszort, ami ezután csak újraindítással hozható ismét működésbe. Ezután két lehetőség van: a HT csak ideiglenesen működött és visszaáll a normál működésre a HT következő betöltődéséig, vagy a HT hatása folyamatos, és az eszköz nem működik többé, azaz tönkremegy.

2. Információszivárgás: érzékeny információk kiszivárgása, pl. a titkosító kulcs. Ezzel lehetőség van az érzékeny védendő információk megszerzésére, lehallgatására csakúgy, mint a PMR hálózat 4. ábrán jelölt rádiócsatornán keresztüli azonosság-ellenőrzésének (authentication) kijátszására. Erre kétféle lehetőséget látnak.

Direkt szivárgás esetén a fertőzött terminál közvetlenül elküldi a titkosító kulcsokat a készülék I/O kimenetén vagy a rádiócsatornán, vagy áltitkosító algoritmus számolása mellett a titkosítandó üzenetet (plain text) titkosítatlanul küldi a rádiócsatornán, azaz eliminálja a titkosítást. Ez könnyen észrevehető, ezért a következő eljárás sokkal kifinomultabb.

Indirekt szivárgás esetén a titkosító kulcs visszanyerésére alkalmas információkat szivárogtat ki az eszköz ideiglenesen vagy véglegesen, Pl. órajelváltozás, áramfelvétel, feldolgozási idő változtatása formájában, mintegy titkos jelzésátviteli csatornaként. Ez az ún. SC vagy oldalcsatorna, melynek a megmérésére dolgozott ki eljárásokat a projekt, mind az eszköz elektromágneses kisugárzásának megmérésével, mind az eszközhöz közvetlen hozzáféréssel kivitelezve. Ezeken felül elképzelhető, hogy a HT egy hibát injektál a ciphertextbe, ami a titkosított adat. Egy hibás és egy jó ciphertext közötti különbségből matematikai módszerrel: különbségi hibaanalízissel (DFA – Differential Fault Analysis) akár egyetlen hibás ciphertext injektálásával is megtörhető az AES, vagy az RSA algoritmus. Az ilyen támadások könnyen kivitelezhetők a criptoASIC módosításával, pl. minden OTAR kulcscsere során újra elküldve az oldalcsatornán az új kulcsot, amint a HT érzékeli annak megjelenését a criptoASIC bemenetén.

3. Áramköri meghibásodás: Eltérően az első pontban leírtaktól, a fertőzött eszköz tovább működik, csak hibásan. Ekkor pl. a HT bizonyos belső kapcsolatokat, vagy a memóriatartalmat változtatja meg, amely nem okoz információszivárgást, de működési problémát idéz elő egy rendszerben. A hatás itt is lehet átmeneti és állandó egyaránt. Egy másik módszernél a HT nem engedi alvó (energiatakarékos) üzemmódba a készüléket, miáltal az igen hamar lemerül. A terminál használója nem gondol HT-ra, csak az akkumulátor hibájára. Egy harmadik módszernél egy rejtett vezetékes kapcsolatot hoznak létre pl. egy CPLD és egy cryptoASIC között. Ezt szinte lehetetlen észrevenni, de fizikai hibát képes előidézni, pl. egy vezeték túlterhelődésével. Ez szikrákat idézhet elő, ami adott környezetben robbanást okozhat. A hiba csak a HT betöltésével aktiválja a kapcsolatot, így pl. ATEX[19] robbanásbiztos minősítésű rádiók tanúsítása során sem derül rá fény, így idézve

19 ATEX: Az EU-ban és Magyarországon is érvényes robbanásbiztonsági direktíva francia nevéből: utilisés an Atmosphéres Explosives.

elő akár valódi robbanásokat is a később ilyen körülmények között fokozottabban használt rádiók esetében.

4. Szabotázs előidézése: A támadó a HT segítségével módosítja a PMR biztonsági funkcióit. Pl. a készülékben alkalmazott véletlenszám-generátor (RNG – Random Number Generator) kimenetét állandóan nullára állítja, ami jóval kisebb biztonsági szintet eredményez, mint a véletlen adatokból generáltak. Az RNG kimenetét általában egy online teszterrel folyamatosan ellenőrzik, pl. FIPS 140-2 vagy AIS-31 tesztekkel, azonban egy kifinomult HT a teszt eredményét is képes módosítani, vagy annak hatását eliminálni. És végül lehetséges olyan módosítás alkalmazása a HT segítségével a készülékben, hogy egy lejárt titkosító kulcs esetében az új megküldött érvényes kulcs nem kerül alkalmazásra, ahelyett a régi marad érvényben.

5. Érzékeny adatok megváltoztatása: A fenti 4 veszélyt a [14]-ben kiegészítették egy ötödikkel is. Ennél a HT megváltoztathatja a belső csomópontok és egyes áramkörök memóriatartalmát, ahol azok tárolódnak vagy feldolgozzák őket. Az összes ilyen érzékeny adat (pl. kulcsok, jelszavak, PIN kódok, vagy egyéb felhasználói adatok) megváltoztatása jelentős hatással van a készülék által nyújtott szolgáltatásra.

A VoIP alrendszer támadási lehetőségei

Az IP-hálózatok jól ismert előnyei mellett az IP-protokollok, -platformok és -szolgáltatások nyitottsága, révén ez egyben jelentős új biztonsági réseket jelent az ezeket alkalmazó PMR hálózatok működésére és a kritikus infrastruktúrák környezetében. Az IP-hálózatok robbanásszerűn megnövekedett aszimmetrikus fenyegetettségei nem kezelhetők a hagyományos biztonsági és kockázati megközelítésekkel. A hagyományos fenyegetési modellek szimmetrikusak, és jól definiált határok mentén mozognak. Azonban napjainkban a fizikai és a kiberhadviselés határai elmosódottak a globális társadalompolitikai fenyegetések fejlődése és a nagymértékben szerteágazó vállalati számítástechnikai modellek eredményeként.

Az aszimmetrikus fenyegetések esetén nem beszélhetünk határozott peremvonalakról és feltételekről, amik mentén a támadások zajlanak. Ezek a következőket jelentik:

– külső és belső védelmi vonalak támadása;
– kifinomult automatikus támadási módszerek alkalmazása a technology stack (pl. OSI 7 rétegű modell) alsóbb vagy felsőbb rétegeiben;
– kevert támadások alkalmazása a fizikai és a kibertámadások szabad kombinálásával;
– a hálózati rendszerek és a kritikus infrastruktúrák kapcsolódásának kihasználása;
– az emberi tervezés és a bennfentes részvétel lehetőségeinek kiaknázása.

Az új típusú, IP-alapú PMR hálózatok a számos előnyük mellett jól ismert protokollokat, szolgáltatásokat és felületeket alkalmaznak a hálózati és IT-infrastruktúra különböző szintjein, amelyek a sebezhetőségek gazdag tárházát kínálják.

A fenyegetések matematikája, azaz a fenyegetettség + sérülékenység = kockázat képlete szerint, a fentebb leírt fenyegetésvektorok viszonylag ártalmatlanok lennének, ha nem lennének jelentős emberi és technológiai hiányosságok az IT-függő szervezetekben. A tapasztalt biztonsági mérnökök szerint azonban a legtöbb kereskedelmi és kormányzati IT-infrastruktúrákban találhatók súlyos sérülékenységek. Ezek a következők lehetnek: Hiányzó megfelelő határvédelem és forgalom-ellenőrzés. A fizikai hozzáférés hiányos ellenőrzése. Frissítetlen és rosszul beállított eszközök. Gyenge vagy hiányzó jelszavak. Nem megfelelő biztonsági jelentések. Gyenge antivírus-védelem a rosszindulatú programok ellen. Emberi hibák a rossz képzés és szakmai fejlődés hiányosságai következtében. Adatszivárgás, az információk nem szándékos közzététele.

De ha a fentiek mind rendben lennének, akkor is elmondható, hogy szinte naponta fedeznek fel eddig ismeretlen sérülékenységeket, melyekkel az eddig biztonságosnak hitt rendszerek is kompromittálhatóak (lásd példaként az alkatrészeket fertőző hardver trójai esetét). Az emberi és rendszerhibák ajtót nyitnak a jogosulatlan hozzáférések, szolgáltatás-megszakítások és adatszivárgások széles skálájának. Átfogó információbiztonsági megközelítés nélkül a támadók, terroristák és bűnözők válnak egyre sikeresebbé.

A PMR hálózatok, készülékek védelmi lehetőségei

A rádiós alrendszer esetében a védelem bizonyos részmegoldását az elektronikai védelem biztosíthatja, ezen belül is főleg az *elektronikai felderítés elleni tevékenység* megoldásai, amelyek nem csak az elektronikai támogatás, de a rádiófelderítés ellen is segítséget nyújthatnak. A másik az *elektronikai ellentevékenységgel szembeni védelem*, amelyik gyakorlatilag a szándékos vagy véletlen zavarok, illetve az elektronikai pusztítás ellen is biztosíthat megoldásokat. [2] Mindezek kivitelezése esetében természetesen figyelembe kell venni az ellenfél felderítő és elektronikai hadviselési képességeit, eszközeinek színvonalát.

Az *elektronikai ellentevékenységgel szembeni védelem* esetében a nem szándékos interferenciák – rádiózavarok – megszüntetésére adminisztratív és mérőszolgálati módszerek alkalmazhatók, melyekre hazánkban a polgári rendszerek esetében az NMHH[20] jogosult. Ez a hatóság rendelkezik az ilyen rendszerek zavarásának megmérésére alkalmas országos rendszerrel, és hatáskörrel a bemért zavarások megszüntetésére.

A *felderítés elleni tevékenység* magában foglalja az elektromágneses kisugárzások korlátozását (passzív rendszabályok) és a felderítés előli kitérés különböző módozatait (aktív, az adóberendezések paramétereit megváltoztató, észlelhető rendszabályokat), amelyek úgymond elrejtik az elektromágneses jeleket és eszközöket az ellenséges felderítés, helymeghatározás és azonosítás elől. Ide tartozik továbbá a felderítő berendezések és adataikat

20 NMHH: Nemzeti Média és Hírközlési Hatóság.

továbbító híradó eszközök megsemmisítése, megrongálása vagy zavarása is (békeidőben ezek nem alkalmazhatók). A kisugárzások korlátozása jelentheti a szükséges legrövidebb kommunikáció alkalmazását, a terjengősség mellőzését az információcserénél, de a szándékos rádiócsend alkalmazását is a lehallgatás felmerülő veszélye esetén. Ezek PMR-ek esetében szerintem jól alkalmazhatók. Az aktív rendszabályok azonban már az adófrekvencia és üzemmód változtatását, a kisugárzott teljesítmények minimalizálását jelenthetik például. Megjegyzem, hogy ez az eljárás szerintem polgári rendszerek esetében korlátozottan alkalmazható, hiszen ezek engedélyhez kötött frekvenciákon és üzemmódokban, meghatározott teljesítménnyel működhetnek. Azonban a direkt kommunikációt alkalmazó frekvenciaengedélyhez nem kötött eszközök, vagy az engedély nélkül illegálisan használt rádiók esetében ezek a célnak megfelelően alkalmazhatók, és a bűnözők és terroristák vélhetőleg alkalmazzák is ezeket a felderíthetőség csökkentésére.

A fentiek ellenére azonban a rádióadások megfelelő módszerekkel békeidőben legtöbbször felderíthetők, így a *híradó-biztonsági előírások* segítségével magát az információt is védeni kell a felderítés ellen. Ez lehet csoportos vagy egyéni védelem. Ennek nyílt adások esetén kézenfekvő megoldása a rövidítések, kulcsszavak alkalmazása, azonosítás, hitelesítés kérése az eszköz alkalmazásakor. Azonban a legkézenfekvőbb megoldás a titkosítás alkalmazása, melynek napjainkban elterjedt megoldásait az alábbiakban tekintem át.

Titkosítási eljárások

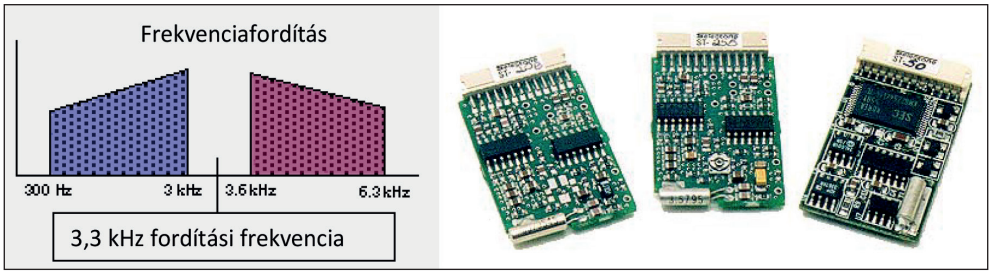
Már a rádiózás hőskorában is felmerült az információ védelmét biztosító eljárások kidolgozása. A kezdeti jelzésátviteleknél erre megfeleltek az offline módú eljárások, pl. morzeátvitelnél, különféle kulcskönyvek, sifre táblázatok stb., azonban az élő beszédkommunikáció megjelenésével online, valós idejű eljárások kidolgozása vált szükségessé az azonnali információátvitel megvalósításához. A beszédátvitelre alkalmazott kommunikációvédelmi megoldásokra eltérő eljárásokat dolgoztak ki analóg és digitális rádiók esetében. Természetesen a digitális rádiórendszereknél megjelenik a natív adatátvitel lehetősége is, azonban ezeknél a hagyományos adatátviteli eljárásokra jellemző jeltitkosítások alkalmazhatóak. A szakirodalomban általában szinonimaként használják a rejtjelzés (scrambling) és a titkosítás (encryption) fogalmát, azonban ezek kivitelezése technikailag jelentősen eltér egymástól. A rejtjelzés analóg jeleknél használt szűréssel, vágással, keveréssel módosított frekvenciaspektrumú jelátvitelt jelent, amely relatíve kisebb biztonsági szinttel és még rosszabb hangminőséggel párosul. Ezzel szemben a digitális titkosítás az alkalmazott algoritmus szerint megváltoztatja az átvitt jel információ- vagy adattartalmát. Ez normál esetben digitális jelekkel működik, tehát digitális PMR-ek esetében, illetve analóg esetben is, ha előtte digitalizáljuk a beszédet.

A gyakorlatban ez azt jelenti, hogy el kell döntenünk, hogy egy adott feladatra adott konfigurációban használandó rádiós rendszer esetében milyen kommunikációvédelmi eljárást alkalmazunk a rádiócsatornán, ha egyáltalán alkalmazunk bármilyet.

Analóg eljárások

Az analóg rádiós rendszerekben a védelem alkalmazására az eredeti hang néhány paraméterét bizonyos algoritmus szerint megváltoztatják, így az eredetitől eltérő hanginformáció továbbítódik a rádiófrekvencián. Ezt a folyamatot angolul „scrambling"-nek nevezik, amire a legjobb magyar megfelelő talán a rejtjelzés kifejezés. A vevő oldalán csak a descrambling algoritmus ismeretében dekódolható az eredeti jel. Az analóg jelkódolás két csoportra osztható: (egyszerű) frekvenciafordítás és dinamikus frekvenciafordítás.

A frekvenciafordítás nagyon egyszerű, a bemeneti jelet egy előre meghatározott frekvenciára tükrözik (6. ábra). Az emberi hang spektruma 300 és 3000 Hz közé esik, elegendő csak ennek a sávnak a változását figyelemmel kísérni. A tükrözött hang 3,6 és 6,3 kHz között, az eredeti frekvenciákhoz tartozó jelerősség fordított sorrendjével kerül átvitelre, ezáltal érthetetlen lesz az átvitt beszéd.

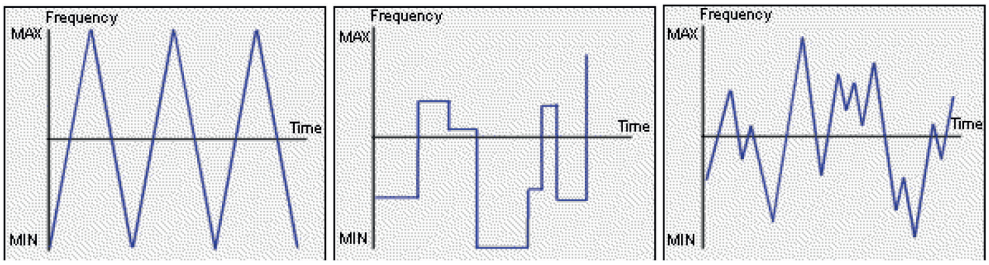


6. ábra: Egyszerű frekvenciafordítás elve és titkosító modulok (Forrás: [16])

Ehhez az átviteli módhoz gyártanak scrambling modulokat erre szakosodott cégek, pl. Selectone [16], Norcomm [17], MX-Com (jelenleg CML Microcircuits USA) [18], Transcript Ltd., Motorola, Kenwood stb., ahol az egyes gyártók általában szabványos fordító frekvenciákat alkalmaznak, de a modernebb titkosítók tükrözési frekvenciája, pl. a CML programozható. A PMR készülékeket gyártó cégek a felsoroltakon kívül még számos gyártó cégtől, illetve saját fejlesztésből is szerezhetnek be készülékeikbe titkosító modulokat.

A dinamikus frekvenciafordítással végzett titkosítás alapelve megegyezik az egyszerű (előzőekben részletezett) frekvenciafordítással, azonban a fordító frekvenciát időnként vagy folyamatosan megváltoztatják, ahogyan ezt a 7. ábra szemlélteti. A dinamikus eljárásnál alapvetően 3-féle változatot különböztetünk meg az algoritmusaik szerint. Ezek a következők:

– *Pásztázó frekvenciás rendszer (7/a. ábra):* A fordító frekvencia előre meghatározott minimum- és maximumérték között változik. A frekvencia emelkedésének és esésének mértéke állandó.
– *Ugró frekvenciás rendszer (7/b. ábra):* Az algoritmus a fordító frekvenciát lépteti változó időközönként. Itt a visszafejtésnél segítség lehet a hosszabb ideig folyamatosan egy frekvencián álló fordító frekvencia.
– *Álvéletlen pásztázó frekvenciás rendszer (7/c. ábra):* Az előző két módszer előnyös tulajdonságait használja fel, ez a típus a legnehezebben visszakódolható.



a) pásztázó frekvenciás *b) ugró frekvenciás* *c) álvéletlen pásztázó frekvenciás*

7. ábra: Dinamikus frekvenciafordítás változatai (Forrás: [19])

Mindhárom dinamikus frekvenciafordítású módszerre jellemző, hogy szükségük van szabályos időközönként szinkronizáló jelre, amit az adás mellett továbbítanak. Az ugró frekvenciás és az álvéletlen pásztázó frekvenciás kódolásnál a váltások tulajdonságait egy szoftveresen felprogramozott kód segítségével lehet beállítani. A komolyabb scrambling szinthez kötődő bonyolultabb elektronika meglehetősen drágává teszi az ilyen scrambling modulokat, ezért a telekommunikáció ezen árérzékeny szegmensében, a PMR rádiókban nem terjedt el az utóbbi módszer alkalmazása. A különböző gyártók készülékei, az eltérő scrambling módszerek és alkalmazott frekvenciák miatt nem kompatibilisek egymással. Azonban egy adott gyártó különböző típusú készülékei általában egyforma scrambling eljárást alkalmaznak.

Az ilyen módon megváltoztatott hanganyagok dekódolására az interneten is találhatunk segítséget. Az itt megtalálható programokkal lehetőség van a frekvenciafordítással kódolt adások azonnali vagy utólagos visszafejtésére. A programban a fordító frekvencia folyamatosan állítható, ezzel megkereshető az éppen használt tükrözési frekvencia. Az ilyen programok szabadon letölthetők az internetről, pl. a következő oldalról [20]. Egy ilyen program gyakorlatilag az inverz műveletét végzi el a scrambling folyamatának, azaz a frekvenciatükrözésnek, a sávfordításnak, az amplitúdóváltoztatásnak vagy az időbeli jelszétosztásnak. Itt nem beszélhetünk kulcsokról, hanem a scrambling paramétereiről, pl. a tükrözési frekvencia értékéről. A paraméterek megtalálása a kulcsa a descramblingnek.

A dinamikus frekvenciafordítással kódolt adások visszafejtésére a fenti program nem használható. Kézi állítással nem kereshető meg és nem követhető a gyorsan változtatott tükrözésifrekvencia-érték. A mai modern DSP jelfeldolgozási algoritmusokkal azonban ezek paramétereinek gyors visszafejtésére is lehetőség van, megfelelő szakértelemmel kiegészítve.

Digitális eljárások

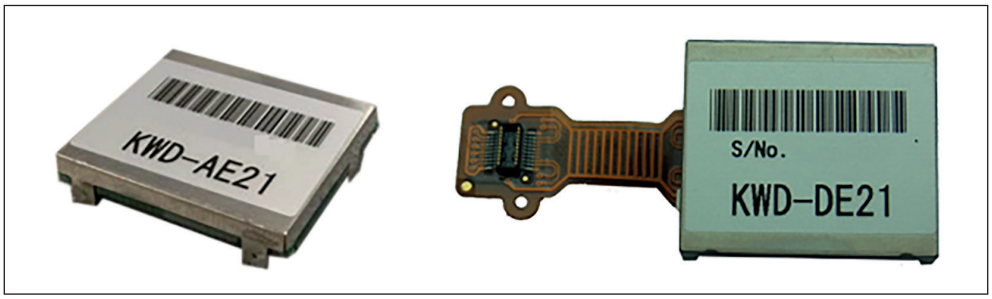
Az analóg rádiós rendszerekben is alkalmazható digitális titkosítási eljárás, azonban ez gyakorlatilag az analóg hanginformáció digitalizálásával jár, ami ezután már mint digitális jelfolyam titkosítható. Ezek az ún. időtartományú titkosító modulok, ahol az analóg mikrofon jelet 100–600 ms-os időszeletekre szegmentálják, majd ezeket további blokkokra osztják. A blokkokat ezután pl. a Selectone esetében egy 72 bites algoritmussal blokkonként titkosítják [16].

Manapság a digitális rendszerek esetében a kérdés szintén felmerül, annak ellenére, hogy maga a digitális átvitel már önmagában egy alap biztonságot jelent, a hagyományos rádiós eszközökkel történő hozzáférés ellen. Ez azonban a hamis biztonság érzetét keltheti a döntéshozókban, akik hagyományosan a biztonsági kérdésekre úgy tekintenek, mint egy költségnövelő és a működés szempontjából célszerűtlen tevékenységre, mely megköti a kezeit a felhasználóknak és a folyamatok kezelőinek egyaránt. [4] A fenti kijelentés alátámasztja, miért alkalmazzák a döntéshozók gyakrabban az olcsóbb megoldásokat. Miért tekintenek el egy egyébként is digitális átvitelű megoldásnál pl. a kiegészítő titkosítás alkalmazásától a különféle kisebb méretű helyszíni és diszpécser típusú rendszereknél.

A gyakorlatban a digitális PMR rádiók tekintetében kvázi szabványként terjedt el a AES[21]/DES[22] titkosító modulok alkalmazása, melyek azonban jelentősen megnövelik a készülékek árát, mivel ezek kb. 300–700 $-ba kerülnek, az analóg modulok 100 $ körüli árával szemben. Ilyen modulokat is több cég kínálatában találhatunk, ilyenek pl. a Kenwood cég saját Nexedge rádióiba szánt típusai. A 256 bites AES/DES algoritmusú KWD-AE21, illetve egy gyengébb, 56 bites DES algoritmusú KWD-DE21 panelba illeszthető titkosító modul (8. ábra).

21 AES: Advanced Encryption Standard. Fejlett titkosítási szabvány, az 2001-ben szabványosították az USA-ban.

22 DES: Data Encryption Standard. Adattitkosítási szabvány, az AES elődje, 1976-ben hagyták jóvá az amerikai kormányzati szervek nem minősített kommunikációjának titkosítására a számítógépes és kommunikációs rendszereknél. 1997-ben internetes összekapcsolású gépekkel 84 nap alatt törték fel a kódot, brute force módszerével, majd 1998-ban egy 250 000 dollárból épített célhardveren mindez már csupán 3 napig tartott.



8. ábra: Kenwood cég KWD-AE21 és KWD-DE21 AES/DES titkosító moduljai (Forrás: [21])

Mind a 256 bites, mind az 56 bites modul 1024 kulcs tárolására képes, melyek kulcsfeltöltő szoftverrel változtathatók. Az ilyen titkosító modulok hivatalos beszerzés során exportengedély-kötelesek adott országokban, így csak a megfelelő engedélyek alapján lehet megvásárolni és kivinni őket. Mint a lábjegyzetből látható, a DES kód már a 2000 körüli számítástechnika szintjén is sérülékeny volt, mivel akkortájt már brute force[23] módszerrel is törhető volt. Az AES viszont napjainkban is erősnek számít (brute force ellen).

Az analóg rendszerekhez képest a digitális átvitel már önmagában egy alap biztonságot nyújt a vétlen behallgatás ellen. De természetesen a védendő információk kritikussága függvényében célszerű mind az analóg mind digitális átvitelnél, a kockázattal arányosan alkalmazott titkosítást választani. Az is elképzelhető hogy ennek alkalmazásától el is lehet tekinteni, a kockázatok (pl. az információ érvényességi ideje) [11] és anyagi szempontok függvényében.

A támadás résznél leírtakból látható, hogy a titkosítás alkalmazása esetében a kulcskezelés eljárásai is védendő körbe tartoznak, mivel itt is elképzelhető a hamisított alkatrészeken keresztüli kompromittálódás.

Az iránymérés és helymeghatározás passzív eljárásai ellen a digitális átvitel önmagában nem véd jobban, mint az analóg jelek esetében, azonban a mért adó beazonosítása jóval nehezebb. A két időréses DMR jelek esetében az időosztásos átvitel miatt az iránymérés is gondot jelent, mivel hasonlóan a GSM-hez, az egyes időrések más fizikai helyzetű felhasználókhoz tartoznak, így az egyes időrések méréséhez időbeli szinkronizálás szükséges.

Az olyan új típusú fenyegetés ellen, mint a hardver trójai, csak a [14]-ben kifejtett utólagos módszerekkel, pl. SDA mérésekkel, illetve a megelőzés szintjén az ezeknek megfelelő szervezeti biztonsági szabályok betartásával védekezhetünk, pl. a biztonságos programozással:

– a cryptoASIC, CPLD, FPGA saját programozásával majd ezek megfelelő integritásának biztosításával;
– a rádiók biztonságos megszemélyesítésével: azaz a saját felhasználói algoritmusok, saját adatok belső felprogramozásával;

23 Brute force: a nyers erő módszere, azaz a fizikailag lehetséges összes kulcskód végigpróbálása egyenként egy adott üzenet megfejtésére.

– az érzékeny adatok, szoftver, firmware és kódok védelmével, integritásuk és megbízhatóságuk együttes biztosításával;
– a kriptográfiai algoritmusok olyan módszerű kidolgozásával, hogy az védett legyen az eljárás gyakorlati kipróbálásától és egyéb információszivárgástól egy rosszindulatú támadó számára.

A VoiP alrendszer esetében a védelem megoldása az információbiztonság (IA), rendszabályok, eljárások és folyamatok bevezetésével és betartatásával történik. Ennek alkalmazásával megvédhetjük az információkat és az információs rendszert egyaránt. Ennek során az IA a következők elérését igyekszik megvalósítani:

– rendelkezésre állást (a jogosult felhasználók részére);
– integritást (az adatok védelmét a jogosulatlan módosítástól és a pusztítástól);
– azonosítás- és hozzáférés-ellenőrzést (a hálózathoz és rendszerelemekhez hozzáférő felhasználók egyedi azonosítása valamilyen eljárással: pl. jelszó, PIN kód, biometrikus azonosítás stb.);
– megbízhatóságot (jogosulatlan személy védett folyamatokhoz és eszközökhöz történő hozzáférésének megakadályozása);
– letagadhatatlanságot (az információközlésben részt vevő felek elismerik egymás azonosságát, így bármely tranzakció [átvitel] letagadhatatlan).

Az IA ezenfelül biztosítja a helyreállítást egy sérült vagy kompromittálódott rendszernél, a felderítési, megelőzési és reagálási képességek beépítésével.

A fentiek betartásával megvédhető a hálózaton mozgó, az alkalmazások által kezelt, valamint a digitális formában bármely médiumon tárolt adatok együttese. Azaz a digitális információk bármely állapotú reprezentációja, nem csak az IP-hálózatokon, de bármely hozzá kapcsolódó IT-infrastruktúrán. Ebből következik, hogy az IA meglehetősen adatcentrikus, de érvényessége nem korlátozódik a digitális formájú adatokra, hanem bármilyen tágabb értelmű vállalaton, rendszeren belüli adatokra vonatkozik.

Ha biztonságos PMR rendszert akarunk üzemeltetni, akkor néhány kulcsfontosságú terület együttese által meghatározott szabályokat is be kell tartani. Ezek a területek a következők: szabályozási irányelveknek való megfelelés, IT- és hálózatbiztonság, fizikai biztonság, üzleti folytonosság és katasztrófa utáni helyreállítás, azonosság- és hozzáférés-kezelés, IT életciklus és projektmenedzsment, információgyűjtés és -elemzés.

Az IA által megkövetelt rendszabályok bevezetése alapját képezheti egy akkreditált szabályrendszer bevezetésének, mellyel tanúsítani lehet a rendszabályok megfelelő betartását. Az IA szabályrendszer kidolgozását a működő rendszerhez kell igazítani, tehát a szervezeten belül kell kidolgozni, de számos helyi szabályozásnak és vonatkozó jogszabálynak kell megfelelni. Ehhez egy IA menedzsernek szerteágazó ismertekkel kell rendelkeznie számos területen, pl. az IT kockázatmenedzsment, biztonsági szabványok, hálózati és peremvédelmi biztonsági szabványok, titkosítási szabványok stb., hogy csak a fontosabbakat említsem.

Összegzés, következtetések

A PMR rendszerek, rádiók alkalmazása ideális megoldás a kiscsoportos pont-többpont kommunikációra, így a szervezett bűnözés és a terrorizmus ilyen típusú kommunikációs igényeinek megvalósítására is. A direkt módú (átjátszó nélküli), de akár az egyedi, pl. hordozható átjátszón keresztüli (taktikai) megoldások egyaránt kikerülhetik a hagyományos távközlési infrastruktúrákat, így ellenőrzésük kizárólag passzív rádiófelderítéssel valósítható meg. A hibrid rendszerek esetében azonban a megjelenő új támadási felületek a hálózati oldalról is sebezhetővé teszik a rendszereket. Az ilyen komplex rendszerek a védelem szempontjából is komplex szemléletmódot igényelnek, az aszimmetrikus fenyegetések mentén, hiszen a támadások esetében is eddig nem látott újfajta aktív támadási eljárások megjelenésére is számítani kell. Így a hagyományos rádiófelderítés mellett előtérbe került a számítógép-hálózati aktív támadások lehetősége is, valamint olyan új eljárások is megjelentek, amelyekkel még az erősnek mondott AES titkosítást is képesek eliminálni a támadók, a cikkben említett hardver trójai segítségével. További lehetőségként pedig a készülékek elleni szabotázs kivitelezése is valósággá válhat segítségével.

A gyakorlati tapasztalatom szerint már most jelentős növekedés figyelhető meg (kutatásaim kezdetén a 3 évvel ezelőtti állapothoz képest) a digitális rádiók hazai és nemzetközi elterjedésében és alkalmazásában egyaránt. Az olcsó kínai készülékek tömeges megjelenése ezt a tendenciát csak tovább fogja erősíteni, főleg az engedélyhez nem kötött eszközök vonatkozásában, de akár az ennél magasabb PMR kategóriákban is. Egy professzionális titkosító modul jóval többe kerül, mint a legolcsóbb rádiók ára, így az alsóbb szegmensben nem valószínű ezek alkalmazása, de a felsőbb kategóriákban is meggondolásra készteti a döntéshozókat.

Az alkalmazott titkosítás mértékének meghatározásakor a magasabb biztonság ára, valamint az interoperabilitás megtartása közötti ellentmondást kell leküzdeni. A titkosító modulok 300, de akár 700 dollárral is megnövelhetik egy készülék árát, ami jelentős anyagi megterhelést ró a szervezetekre. Ennek ellenére a [22] szerint az amerikai felhasználók részére a titkosság sokkal fontosabb, mint az interoperabilitás, azonban a [11]-ben leírtak szerint ez nincs mindig így, még a katonai kommunikációban sem. Azonban a digitális átvitel miatt a hagyományos felderítő eszközökkel még titkosítás alkalmazása nélkül sem nyerhető vissza az átvitt beszédinformáció, ahogyan ezt a [1] cikkben elméleti síkon kifejtettem. A viszonylag korlátos frekvenciatartományokban működő digitális PMR rádiók felderíthetőek, és akár iránymérés is végezhető rajtuk a hagyományos eszközökkel, azonban hovatartozásuk ezekkel nem határozható meg. Egy olyan eszköz megalkotása és alkalmazási feltételeinek, körülményeinek kidolgozása szükséges, amely a fenti rendszerekből a digitális átvitelű beszéd, valamint az egyéb járulékos adatátviteli (műveleti) információkat is megfelelően képes kinyerni és felderítési adatokká konvertálni. Ehhez a megfelelő technikai megoldások kidolgozása vagy adaptálása szükséges a berendezésekben, azonban az emberi közreműködés sem nélkülözhető a jobb eredmény elérése érdekében.

Irodalomjegyzék

[1] Balog Károly: Digitális PMR rendszerek összehasonlítása I. *Hadmérnök*, 9 (2014. szept.)/3. www.hadmernok.hu/143_08_balogk.pdf (a letöltés ideje: 2014. 09. 30.)

[2] Haig Zsolt – Kovács László – Ványa László – Vass Sándor: *Elektronikai hadviselés.* NKE HHK Katonai Műszaki Doktori Iskola, Budapest, 2014. (ISBN 978-615-5305-87-0)

[3] Munk Sándor: Az informatikai biztonság rendszertanához. *Bolyai Szemle,* 18 (2009)/4, 157–174., portal.zmne.hu/download/bjkmk/bsz/bszemle2009/4/13_munksandor.pdf (a letöltés ideje: 2015. 05. 20.)

[4] Information Assurance for Private Radio Networks (Motorola White Paper), www.motorolasolutions.com/content/dam/msi/docs/business/product_lines/astro_25_network/encryption/_documents/astro25_information_assurancewhitepaper.pdf (a letöltés ideje: 2015. 05. 23.)

[5] Munk Sándor: Információbiztonság vs. informatikai biztonság. *Hadmérnök,* Robothadviselés 7. Tudományos Szakmai Konferencia különszáma, 2007. november 27., hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.html (a letöltés ideje: 2015. 05. 20.)

[6] Icom IDAS, What is dPMR, why digital? www.icom.co.jp/world/support/download/brochure/pdf/IDAS_dPMR.pdf/ (a letöltés ideje: 2013. 01. 15.)

[7] The world's thinnest & smallest full power digital portable radio, www.hytera.com/productResources.htm?columnId=416&proId=259&resourceType=2#page-index (a letöltés ideje: 2013. 01. 20.)

[8] Tait Communications (whitepaper): Tougher LMR systems, 10 ways to protect and strengthen your LMR system, www.taitradio.com/__data/assets/pdf_file/0014/123503/Tait_Tougher_LMR_Systems_Guide.pdf (a letöltés ideje: 2015. 05. 25.)

[9] Hytera DMR Trunking Products and Solutions, www.dmr-applications.com/15938 (a letöltés ideje: 2015. 05. 25.)

[10] John Ribeiro: *Ham radio attempts to fill communication gaps in Nepal rescue effort,* www.networkworld.com/article/2916374/ham-radio-attempts-to-fill-communication-gaps-in-nepal-rescue-effort.html (a letöltés ideje: 2015. 05. 25.)

[11] NATO Research and Technology Organisation: *Technical Communications In Urban Operations.* RTO Technical Report TR-IST-067, 2010. szeptember, ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-IST-067//$$TR-IST-067-ALL.pdf (a letöltés ideje: 2015. 05. 25.)

[12] Information Assurance for the Tactical Environment, 2002. szeptember, http://trygstad.rice.iit.edu:8000/Policies%20&%20Tools/InformationAssuranceTechnicalFramework3.1/ch09InformationAssuranceForTheTacticalEnvironment.doc (a letöltés ideje: 2015. 06. 05.)

[13] HINT Project, www.hint-project.eu/ (a letöltés ideje: 2015. 06. 05.)

[14] D1.2 Report on Specifications and overall architecture (Holistic Approaches for Integrity of ICT Systems) EU Seventh Framework Programme, www.cspforum.eu/HINT-D1.2-Report_on_specifications_and_overall_architecture-PU-M08.pdf (a letöltés ideje: 2015. 06. 05.)

[15] D1.1 Report on use case and architecture requirements (Holistic Approaches for Integrity of ICT Systems) EU Seventh Framework Programme, www.cspforum.eu/HINT-D1.1-Report_on_use_case_and_architecture_requirements-PU-M05.pdf (a letöltés ideje: 2015. 06. 05.)

[16] Selectone New Product Bulletin, A Private Collection Affordable Voice Encryption, www.comspec.com/selectone/npb/private/private.htm (a letöltés ideje: 2015. 05. 25.)

[17] Norcomm Voice Encryption, www.norcommcorp.com/VoiceEncryption.html (a letöltés ideje: 2015. 05. 25.)

[18] CML Microcircuits: Audio Band Frequency Inversion Scrambler FX/MX 128, www.cmlmicro.com/products/FX/MX128/ (a letöltés ideje: 2015. 05. 25.)

[19] Scrambling and Frequency Inversion, www.cescomm.co.nz/about/scrambling.html (a letöltés ideje: 2015. 05. 25.)

[20] Nino Porchino: Voice descrambler software for windows and soundcard, antoninoporcino.xoom.it/VoiceDescrambler/index.htm (a letöltés ideje: 2015. 05. 25.)

[21] Kenwood Europe: Optional Modules, Units, Brackets and Kits, www.kenwood.eu/comm/accessories/optional/ (a letöltés ideje: 2015. 05. 25.)

[22] Candy Phelps (Hendon Publishing): *Establishing secure, reliable LMR communications.* Public Safety IT, Jan/Feb 2010, www.hendonpub.com/resources/article_archive/results/details?id=1890 (a letöltés ideje: 2015. 05. 31.)

Digital PMRs Attack and Defence Possibilities

Balog Károly

In these days, both the licensed and license-free PMR radio technology is going through a massive paradigm shift as formerly seen at mobile phone technologies. In fact, the new digital PMR systems and individual devices are spreading, the license-free versions of which are cheap, easily accessible for everyone and not limited in their movements. Since these devices completely bypass the traditional telecommunications infrastructure, their detection and control is only possible by communication intelligence. Of course, the systems related to other communication infrastructures may be vulnerable not only through radio channels. In my paper I intend to overview and summarize the attack vectors of unique devices and systems, as well as the security solutions used in PMR devices and systems.

Keywords: digital Professional/Private Mobile Radio, Communication Intelligence, scrambling, encryption, electronic protection, information assurance

Teknős László
Kóródi Gyula

A globális éghajlatváltozás biológiai kockázatainak elemzése, hatásainak vizsgálata a katasztrófavédelemre I.

Az emberiség történetében mindig nagy jelentősége volt a járványoknak, fertőző betegségeknek. Kialakulásukban és terjedésükben nemcsak a kereskedelmi okok játszottak szerepet, hanem a klíma jellege is. Manapság egyre több tanulmány mutat rá a globális éghajlatváltozás és a fertőző betegségek kapcsolatára. Jelen cikk az éghajlat módosulásának egészségügyi hatásaival foglalkozik, kiemelten a járványok, fertőző betegségek keletkezésének, terjedésének lehetőségeit elemezve.
Kulcsszavak: globális éghajlatváltozás, járványok, fertőző betegségek, humánegészségügy, vektorok

Bevezetés

A Föld éghajlatának vizsgálatakor a tudósok egyetértenek abban, hogy a bolygónk éghajlata a földtörténet során folyamatosan változott. A melegebb (interglaciális) és hidegebb (glaciális) időszakok ciklikusan váltották egymást, és ezek a periodikus változások nem veszélyeztették a bioszférát. Az Éghajlatváltozási Kormányközi Testület negyedik és ötödik jelentése (2007, 2013) szerint, az emberiség a természetalakító cselekvései, káros tevékenységei (elsősorban a légkörbe juttatott szennyezések) által a globális klímát befolyásoló természetes folyamatokra hatással vannak, így a bioszféra zavartalansága immár nem lehetséges. Ebben a megállapításban azonban a tudományos világnak nincs egyetértése, de abban igen, hogy a jelenleg tapasztalható környezeti változások komoly nemzetbiztonsági, lakosságvédelmi problémákat eredményeznek. A Föld olyan egyértelmű, globális mértékű veszélyes anomáliákat jelez (szélsőséges időjárás, közvetlen és közvetett egészségügyi hatások, élettérváltozások stb.), amelyek nagymértékben, már most hatással vannak a környezetre és többek között az emberre. Erre példa a fertőző betegségek földrajzi elmozdulása, a közegészségügyi-járványügyi kockázatok folyamatos növekedése, új kórokozók felbukkanása stb.

Jelen cikkben a szerzők keresik azokat a kapcsolódási pontokat, melyek összefüggésbe hozhatók a klíma módosulása és a fertőző betegségek kockázatának növekedésével, illetve vizsgálja a biológiai fegyverekhez használt ágensek és az éghajlati tényezők közötti

kontaktusokat, tanulmányozva, hogy a (természetes) járványokat generáló kórokozók és vektoraik közül melyiket használhatják fel támadásra, kihasználva az éghajlat változásából adódó előnyöket (például a növények és állatfajok elterjedését gátló hőmérsékleti értékek megváltozása).

Az emberiség történetében mindig nagy jelentőségű szerepe volt a járványoknak, népeket irtottak ki, kultúrákat tettek tönkre, harcászati tevékenységek kimenetelét döntötték el stb., így nem csoda, hogy az emberekben félelmet vált ki egy-egy fertőző betegség, járvány kialakulásának a veszélye. A szerzők ezért kísérletet tesznek arra, hogy a mű tartalmában az olvasó olyan érdekes információkhoz jusson, ami a saját védekezési potenciálját nagyban erősítheti, továbbá a veszélyek elleni ismereteit pontos és szakszerű információkkal (tényekkel), adatokkal alapozza meg a saját túlélési esélyeinek növelése érdekében.

A klímaváltozás és a humánegészségügy kapcsolata

A klímaváltozás és az egészségügy kapcsolatának tudományos vizsgálatát az IPCC[1] második jelentése 1996-ban alapozta meg, ahol egy egész fejezeten keresztül kerültek bemutatásra az egészséget károsító hatások.[2] A 2001-ben kiadott harmadik jelentésben aktualizálták a reális egészségre veszélyes kockázatokat, aminek alapját az egyre jobban érvényesülő hőmérséklettel kapcsolatos hatások adták. A nemzetközi szervek, szervezetek (IPCC, WHO,[3] WMO,[4] UNFCCC[5] stb.) ajánlásai, figyelmeztetései nyomán 2000 óta hazai szinten is foglalkoznak a klímaváltozás egészségkárosító hatásának vizsgálatával a Nemzeti Környezet- Egészségügyi Akcióprogram (NEKAP) keretén belül.

A magyarországi kutatások fő koordinátorai és szellemi bázisai a Fodor József Országos Közegészségügyi Központ, Országos Környezetegészségügyi Intézet, az Állami Népegészségügyi és Tisztiorvosi Szolgálat, a Johan Béla Országos Epidemiológiai Központ és az Országos Meteorológiai Szolgálat voltak. A vizsgálatok kiterjedtek a napi átlag, a minimum-, maximum-hőmérséklet, a hőmérséklet-ingadozások, a relatív páratartalom, légnyomás és a napi halálozás összefüggéseire, továbbá általános additív módszerrel kiszámolták az időjárási változók hatását a napi halálozásra. Ezek alapján megállapították, hogy az extrém időjárási események közvetett és közvetlen hatásokat idéznek elő, amire a négy év alatti gyerekek, a 65 év feletti idősek, a túlsúlyos emberek és az ágyban fekvő betegek

1 Éghajlatváltozási Kormányközi Testület, angolul Intergovernmental Panel on Climate Change (IPCC).
2 Az első IPCC értékelő 1991-ben még nem foglalkozott a járványokkal, az éghajlatváltozás egészségügyi hatásaival.
3 Egészségügyi Világszervezet, angolul World Health Organization (WHO).
4 Meteorológiai Világszervezet, angolul World Meteorological Organization (WMO).
5 ENSZ Éghajlatváltozási Keretegyezmény, angolul United Nations Framework Convention on Climate Change.

a legérzékenyebbek.[6] A hőmérséklet esetében a hőhullámok az elsődleges rizikófaktorok, illetve az ökológiai rendszer károsodásának, a környezetváltozás következményeként a vektorok okozta megbetegedések, az allergén növényfajok pollentermelődésének a fokozódása. A hidrológiai anomáliák, melyek évről évre gyakrabban és intenzívebben jelennek meg, olyan katasztrófákat okoznak, ahol megnőnek a sérülések, fertőzések, táplálkozási, pszichológiai és egyéb károsodások kialakulásának a valószínűségei. Az Egészségügyi Világszervezet (WHO) 2002. évi jelentése szerint a klímaváltozásnak tulajdonítható a 2000-ben bekövetkezett összes hasmenéses megbetegedések számának 2,4%-a, és a maláriás esetek 6%-a a közepes jövedelmű országokban (pl. Brazília, Indonézia stb.). [2] A fertőző betegségek a klímaváltozás hatására különböző földrajzi területeken is megjelennek. Bár eléggé valószínű, hogy a globalizáció miatt a kiterjedt személy- és áruszállítás következtében a vektorok könnyebben tudnak szétterjedni szerte a világban. Erre példa az Afrikából hazatérő négy magyar állampolgár esete, akik kullancsláz (rickettsia africae-fertőzés) miatt a Szent László Kórház Fertőző Osztályára kerültek. [3] Ebből is látszik, hogy a hazai viszonylatban új típusúnak számító fertőzések nemcsak a klímazónák eltolódásából adódó élőlényvándorlás miatt jöhetnek létre, hanem az utazások alkalmával is. Ez megnehezíti az ilyen irányú kutatásokat.

Az állatokról emberre terjedő betegségek (zoonosisok) közül a legnagyobb kockázata a Lyme-borreliosisnak (Lyme-kór) van, illetve a kullancsencephalitisnek, a haemorrhagiás láznak, és a tibolának, melyek egyértelműen a kullancsokkal hozhatók összefüggésbe. De jelentős veszélyt jelent az enteralis infekció,[7] mely a szájon át történő bakteriális fertőzést jelenti, például bevitt élelmiszer útján (salmonellosis, campylobacteriosis, yersiniasis). Kullancs, szúnyog vagy bolha mint vektorok jelentős mértékben hozzájárulnak a Francisella tularensis nevű baktérium[8] elszaporodásához, mely úgy Európában, mint Észak-Amerikában széles körben elterjedt. Leginkább fogékonyak rá a vadon élő rágcsálók, a mezei nyúl, egér, ürge, hörcsög, mókus, a háziállatoknál leginkább a juh és szarvasmarha stb. [4] De hasonló a leptospirosis,[9] melyet a leptospira interrogans baktérium okoz, és a rágcsálók vizeletével terjed. A hazai rágcsálóhelyzetet tekintve a magyarországi melegedő klíma egyre jobb feltételeket biztosít (megszokottnál enyhébb téli periódusok miatt) a szaporodásukhoz, túlélésükhöz, mely jelentősen növeli a következő év fertőzésveszélyeztetettségét. Megemlítendő az ornithosis a Chlamydia psittaci baktérium által okozott heveny, fertőző betegség. A kórokozó baktérium a szárnyasokról jut az emberi szervezetbe, és legtöbbször tüdőgyulladást okoz. [5] A szúnyogok által okozott zoono-

6 Magyarországon a betegségterhet főként a krónikus, nem fertőző betegségek alkotják. A korai halálesetekért férfiaknál elsősorban a keringési rendszerek betegségei és a daganatok a felelősek, mely az életmódbeli tényezőkkel hozható kapcsolatba. Magyarország vezeti a daganatos megbetegedések miatti halálozási statisztikát Európában. A daganatkeletkezés kockázata a kor előrehaladtával növekszik. [1]

7 Például fertőző hasmenés.

8 Bőrt, a szemet és a tüdőt támadó fertőző betegséget okoz.

9 Ez a betegség gyakori például a csatornatisztítók és vágóhídi dolgozók körében.

sisok közül a malária az 1950-es évekig endémiás[10] volt Magyarországon is, de a folyószabályozásokkal, a mocsarak lecsapolásával, valamint a DDT[11] permetezésével sikerült a vektort eradikálni (kiirtani), de a klímaváltozás következtében ismét alkalmassá váltak az eredeti tenyészőhelyek a belvizes területeken a földben megbúvó lárvák kifejlődéséhez.

A második Nemzeti Éghajlat-változási Stratégia szerint egyes kórokozók gyakoribbá válnak a szúnyogok, kullancsok, rágcsálók elterjedésével – elsősorban a Lyme-kór, a kullancsencephalitis, hantavírusok, nyugat-nílusi vírus, madárinfluenza, valamint a különböző féregfertőzések. Nőhet a maláriás esetek száma, s jelentős veszély a lepkeszúnyogok által terjesztett leishmaniasis megjelenése, valamint egyéb, Európában a legutóbbi években detektált[12] fertőzések (chikungunya-láz, dengue-láz, Rift-völgyi láz) megjelenése. Növekedni fog az ivóvízzel, illetve a nem megfelelően kezelt élelmiszerekkel terjedő bakteriális, vírusos és protozoon fertőzések[13] gyakorisága (a salmonellosis campylobacteriosis, hepatitis A, cryptosporidiosis). [6]

A fentebb leírtak alapján a globális éghajlatváltozás egészségkárosító hatásai többféleképpen következnek be: [7]

– az időjárási szélsőségek fizikai hatásán keresztül (hőmérséklet, csapadék, szél által okozott fizikai-mentális terhek, fertőzésveszély, vegetációs időszak kitolódása stb.);
– fertőző betegségek növekvő száma alapján (kedvezőbb szaporodási feltételek világszerte, mutáció miatt erősebb törzsek stb.);
– a vízkészlet mennyiségi, minőségi romlása következtében fellépő kihívások;
– élelmiszer-biztonsági problémák (élelmiszer-eredetű megbetegedések);
– a környezeti, klímamenekültek számának drasztikus emelkedésével.

A globális éghajlatváltozás egészségkárosító hatása mind közvetlen, mind közvetett úton valósul meg. A közvetlen, azonnali hatások olyan direkt hatások, melyeket a szélsőséges időjárási események fizikai tényezője okoz (például hőhullámok, UV sugárzás). A közvetett, azaz indirekt hatások közvetetten betegítik meg az egyént (vektorok által terjesztett betegségek).

Járványügyi kockázati tényezők

Az előző fejezetben leírtak alapján elmondható, hogy az éghajlat változása magával hordozhatja a fertőző betegségek terjedésének a lehetőségét. Jelen alfejezet célja, hogy az éghajlatváltozásból adódó fertőző betegségeket, járványok kapcsolódási lehetőségeit elemezze, de nem foglalkozik a járványok kialakító okai közül a háborúkkal, a népsűrűséggel,

10 Az adott fertőző megbetegedés állandóan, tartósan jelen van.
11 Diklór-difenil-triklór-etán, mely erős hatású rovarméreg, melyet betiltottak az élővilág és a környezetre gyakorolt hatásai miatt.
12 Észlelt.
13 Apró egysejtű élősködők, amik többnyire az emésztőrendszerben telepszenek meg.

városiasodással, állatkereskedelemmel, személyszállítással, hulladékgazdálkodással, migrációval.

Amit célszerű elemezni, az a vektorok által terjesztett betegségek, a vízzel és élelmiszerrel kapcsolatos egészségügyi problémák és az időjárásból eredő katasztrófák következtében jelentkező fertőzések, járványok. Ezek közvetve vagy közvetlenül, de összefüggésbe hozhatók az éghajlat módosulásával.

Fertőző betegségnek nevezzük azokat a megbetegedéseket, melyeket speciális fertőző ágens, vagy annak melléktermék hoz létre, és amelyek képesek közvetlenül vagy közvetve emberről emberre, állatról emberre, állatról állatra terjedni. A fertőző ágens olyan élő organizmus (vírus, rickettsia, baktérium, gomba, protozoon, parazita), amely fertőzést képes okozni. [8] A kórokozó mikrobák terjedése lehet direkt és indirekt úton. A direkt azt fejezi ki, hogy a kórokozó közvetlenül jut a fertőzőforrásból a fogékony szervezetbe, így terjednek a nemi betegségek, de lehetséges a légúti csoportban is. A fertőző betegségek nagyobbik része indirekt úton jut a szervezetbe. Ezek alapján lehetnek:

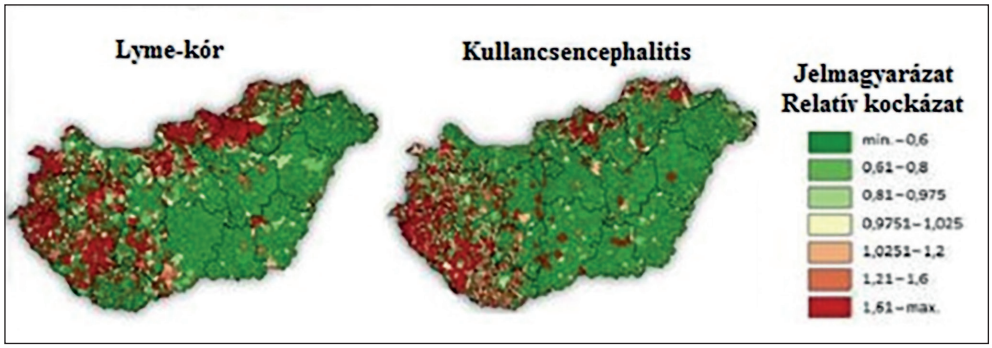
– légúti fertőzések (cseppfertőzés);
– enterális fertőzések (emésztőrendszeri): élelmiszerek, ivó- és fürdővíz, tárgyak, légy, rágcsálók közvetítik a kórokozót;
– haematogén fertőzések (vérfertőző): a forrás vérével a fogékony szervezetébe jut a kórokozó;
– dermatogén: kültakaró sérülései miatt bekövetkező sérülések;
– zoonózis: állatról emberre, emberről állatra terjedő fertőző betegségek.

A hőmérséklet növekedésével járó kockázatok

A melegebb időjárás elősegíti a vektorok szaporodását, és lerövidíti a kórokozó fejlődési ciklusát a vektor szervezetében, viszont a hőtöbblet és a szárazság csökkentik egyes vektorok túlélési esélyeit. Az enyhe telek a rágcsálók életben maradását segítik elő, így a következő évben növekedik a fertőzések terjesztésének veszélye, pl. a kullancsok által terjesztett vírusos agyhártyagyulladás, a bakteriális eredetű Lyme-kór és a hantavírus okozta tüdőmegbetegedés. Egyes rágcsálók által terjesztett betegségek árvizek után válnak gyakoribbá, mint pl. a leptospirozis, tularaemia, vagy a vírusos vérvizelés. A klímaváltozás hatására a hőmérsékleti növekedés következtében megnőnek az élelmiszerekkel kapcsolatos egészségügyi kockázatok is, mivel a mikrobák szaporodási sebességének alapvető meghatározója a hőmérséklet. A hőmérséklet-változás érzékenyen hat az élelmiszer útján terjedő fertőzésekre, úgymint szalmonella, Campylobacter, Listeria stb. Hazánkban az 5°C feletti átlaghőmérsékletű napoknak tulajdonítható a szalmonella incidencia növekedése, ami az ilyen napok számának és intenzitásának hatására emelkedik. Az átlaghőmérséklet egyfokos emelkedése 4,5%-kal megnöveli a szalmonellafertőzések számát. [6]

Az élelmiszer által terjedő fertőzések jelentős megnövekedésére számítanak az Európai Unióban az elkövetkező évtizedekben. A szennyezett élelmiszerek gyakrabban okoznak mérgezést, járványokat, mint a fertőzött ivóvíz, talaj vagy levegő. [9]

Magyarország változó klímája a megfelelő környezeti tényezőkkel (pl. hőmérséklet, páratartalom, alkalmas tenyészőhely stb.) hozzájárul a vektorok, illetve kórokozók életképességének növekedéséhez. A kullancsok változatos klimatikus feltételek között az összes kontinensen megtalálhatók. A világszerte előforduló vérszívó ízeltlábúak humán szempontból legfontosabb fajaik különféle kórokozók (vírusok, baktériumok, protozoonok) vektoraiként számos betegség terjesztői. Magyarországon és Európa északi mérsékelt égövi részén is az Ixodes ricinus[14] fajkomplexbe tartozók (vöröshasú kullancs) okozzák a legtöbb emberi kullancscsípést, és ez az emberre veszélyes két legfontosabb betegség terjesztője is egyben.



1. ábra: A Lyme-betegség és a kullancsencephalitis megbetegedése területi halmozódása Magyarországon 1998–2008 között (Forrás: [6])

A szúnyogok és egyéb ízeltlábúak által terjesztett fertőző megbetegedések

Már közel 100 éve igazolt, hogy egyes fertőző betegségeket (pl. maláriát, sárgalázat, dengue-lázat stb.) terjesztő, így a kórokozóval közvetlen kontaktusban álló vérszívó ízeltlábúak (vektorok) közül a különböző szúnyogfajoknak (Anopheles spp., Aedes aegypti) fertőzést közvetítő szerepe van. A fertőzések átvitelében érintett 25 szúnyogfaj közül az újonnan felismert és esetleg hazánkban is a klímaváltozás hatására megjelenő, fertőző betegségek közvetítésében szerepet játszó egyéb szúnyogfajok jelentőségére is kellő figyelmet kell fordítani. Az éghajlatváltozás hatására a leishmaniasis terjesztője, a lepkeszúnyogfajok elterjedési területe délről észak felé fog húzódni, köszönhetően a jövőben

14 Pókszabású, 1–6 mm-es ízeltlábú, az atkafélék közé tartozik, melyek elsősorban madarak és emlősök, kisebb arányban hüllők vérszívói.

várható enyhébb teleknek és a hosszabb, melegebb vegetációs periódusnak,[15] de a leishmaniasis (lepkeszúnyogok – vektorként terjesztik) endémiássá[16] válhat a Kárpát-medencében, ami komoly kihívást jelenthet mind a humán-, mind az állategészségügy számára. Hasonló kedvezőtlen tendenciák várhatók Európa más, mérsékelt övi területein is. A Culex fajok (szúnyog) vektor szerepének növekedése figyelhető meg, a japán B encephalitis, a nyugat-nílusi láz esetszámai következtében. [10]

A szúnyogok összességében a következő betegségek létrejöttében játszanak közre:

– Malária.
– Chikungunya-láz (előfordul Afrikában, Délkelet-Ázsiában, Indiában és a Fülöp-szigeteken).
– Nyugat-nílusi láz (előfordul Afrikában, Európa déli részein, Közép-Keleten, Indiában és az Amerikai Egyesült Államokban).
– Rift-völgyi láz (előfordul Kelet- és Dél-Afrikában).
– Dengue-láz (csonttöréses láz, előfordul Közép- és Dél-Amerikában, Ázsiában, Indiában, Afrikában).
– Japán B encephalitis (Ázsiában előforduló agyvelőgyulladás).[17]
– Sárgaláz (emésztőrendszeri és májkárosodást okoz, előfordulása: Afrika, Dél-Amerika).
– Leishmaniasis (előfordul a Föld 90 országában, köztük a Földközi-tenger menti országokban is). Három fontosabb klinikai megjelenési formája létezik:
  ◦ Cutan leishmaniasis,
  ◦ Mucocutan leishmaniasis (Espundia),
  ◦ Viscealis leishmaniasis (kala-azar).

Magyarországon (több mint 40 éve) a lakott területeken a közegészségügyi szempontból ártalmas ún. közönséges csípőszúnyogok elleni védekezés megszervezése és kivitelezése elégséges volt. Hazánkban elsősorban az Anopheles maculipennis fajcsoport által terjesztett malária számított nagyobb esetszámú betegségnek, melynek körülbelül 50 éve már csak elvétve vannak esetszámai. Az átlaghőmérséklet-emelkedés és a hirtelen lezúduló csapadékok eddig a főként trópusi területeken honos szúnyogfaj szaporodási feltételeinek hazánkban egyre jobb lehetőséget biztosítanak. Az ízeltlábúak aktivitását a hőmérséklet jelentős mértékben befolyásolja. A klímaváltozása miatt hazánkban a meleg égövi rovarok elérték Baranya, Tolna, Zala megyéket, főként a leishmaniasis betegséget terjesztő lepkeszúnyogok. [11]

15 Márciustól októberig tartó időszak.
16 Egy fertőző betegség egy adott területen tartósan, rendszeresen előfordul.
17 Magyarországon a japán B encephalitis elleni védőoltás (JE-VAX) nem beszerezhető.

Allergén növények elterjedése

Az immunrendszer fokozott működése (túlérzékenységéből adódóan) okozza az allergiás reakciók kialakulását. Az allergia kialakulásában az adott egyén genetikai adottságai mellett a környezeti tényezők és az immunrendszer szabályozó működésének zavarai is szerepet játszanak. A légköri allergénekre érzékeny lakosság becsült számát figyelembe véve az 1,5-2,5 millió allergiás körülbelül 40–70%-a parlagfűre is tüneteket produkál. A parlagfű-allergia becsült prevalenciaértéke[18] Magyarország 10 milliós lakosságára vonatkoztatva 1,2 millió fő. Az összpollenszám emelkedése miatt – 2021–2050 között 28%, 2071–2100 között 93% – a parlagfű-érzékenység 1,68%-kal, illetve 5,58%-kal fog nőni a jelenlegi (pollen) terjedési ütem alapján, ami 2021–2050 között 1,277 millió fő, illetve 2071–2100 között 1,326 millió főnyi növekedést eredményez. Az 1980-as és 1990-es években a hazai időjárás fokozatos felmelegedése, a gyakori enyhe telek hatására egyre több melegkedvelő növényfaj jelent meg és terjedt el az ország területén. Ezek a jövevényfajok szubmediterrán, mediterrán, szubtrópusi és trópusi területekről származnak. A további melegedés hatására az allergén növényfajok virágzásának időtartama meghosszabbodik, emiatt fokozódik az emberek pollenterhelése. Erre példa, hogy az emelkedő légköri CO_2-koncentráció és a melegedő hőmérséklet kitolja a parlagfű pollenjének levegőben történő tartózkodását, s meghosszabbíthatja a parlagfű pollenszezonját.

További komoly kockázati tényező lehet, hogy a mediterrán éghajlaton őshonos és ott jelentős allergénnek számító növények, úgymint az olajfűz, tiszafa, ciprusfélék, melyek már hazánkban is kezdenek elterjedni, és az arra érzékenyeknél allergiás tüneteket okoznak. Ezek a tényezők az allergiás szénanáthában szenvedők kora tavaszi gyulladásos tüneteinek fokozódását, és az allergiás időszak meghosszabbodását jelenthetik. Amennyiben Magyarország éghajlata is fokozatosan tovább fog melegedni, várható, hogy a mediterrán allergén növények megjelennek a Kárpát-medencében is.

Vízzel kapcsolatos problémák

A csapadék egyenetlen eloszlása miatt számítani kell nagy esőzésekre, melyek áradásokhoz vezetnek, és a vízzel terjedő járványok kialakulásának kockázatát eredményezhetik. A szennyvízcsatornák kiömlése nagy területekre kiterjedő vízfertőzést okoz. A vízzel terjedő fertőző betegségek között lehetnek:

– bakteriális kórokozók: Shigellák, szalmonellák, enterovirulens E. coli, Yersinia enterocolitica, Campylobacter, Vibrio cholerae, Pseudomonas aeruginosa, Aeromonas, nem-cholera vibriók, Staphylococcus aureus, Clostridium difficile, illetve perfringens, Enterococcus faecalis, Bacillus cereus, Serratia;

18 Az adott időpontban előfordult esetek arányát jelenti.

– paraziták: Giardia, Cryptosporidium, Entamoeba histolytica, Trichinella spiralis;
– bélférgek;
– vírusok: rotavírus, Norwalk, astro, calici-, corona-, enteralis adenovírusok stb.

A nagy esőzések után valószínű, hogy a csatornarendszer feltöltődik, mely az ivóvízellátó rendszert beszennyezheti. A legismertebb veszélyforrás a Criptosporidium parvum, mely például az Egyesült Államokban okozott már 200 ezres megbetegedést is.

A vízzel történő fertőzés kialakulásában és terjedésében az elégtelen közműállapotok jelentős szerepet játszanak. A magyarországi vízbiztonsági kérdéskört vizsgálva megállapítható, hogy minden települése rendelkezik közüzemi vízművel, az ivóvízbekötéssel rendelkező lakások aránya pedig országos átlagban meghaladja a 94%-ot. A hazai lakosság ivóvízellátása főként felszín alatti vízkészletekből történik. A fejlesztéseket elsősorban vízbiztonsági-vízminőségi területeken kell végrehajtani. Kiemelt feladat a stratégiai tartalékot jelentő távlati vízbázisok védelme, a szolgáltatott ivóvíz minőségének javítása, a vízszennyezők koncentrációjának csökkentése (arzén, bór, nitrit, fluorid, ammónium). A szennyvízkiömlések és bemosódások szennyezhetik a sérülékeny ivóvízbázisokat, és ezzel növelik a fertőzésveszélyt (például a rendkívüli csapadékmennyiség következtében kialakult 2006. évi miskolci vízjárvány, amelyben több mint 3000 ember betegedett meg). Hazánkban főként a karsztvízzel ellátott területek a legveszélyeztetettebbek. A vízjárványokra jellemző, hogy a megbetegedés helye egybeesik a vízellátás területével, hirtelen és egyszerre kezdődik, és nagyszámú ember betegszik meg, az ivóvíz fertőzöttsége megállapítható a kórokozó (esetleg) vízből való kimutatásával, a vízforrás lezárása után tömeges megbetegedés már nem fordul elő (de sporadikusan[19] még számolni kell a visszamaradt ürítők miatt). A vízzel terjedő fertőző betegségek kórokozói közül a leggyakoribbak az E. Coli (O124), Campylobacter jejuni, Cryptosporidium, Giardia lamblia, Salmonella typhi, Shigella flexneri hepatitis A, rotavírus, calicivírus, adenovírus által előidézett megbetegedések. [12]

A hőhullámok idején vagy nagy melegben az állatok és emberek hűsítésként, illetve folyadékbeviteli célból szökőkutakból isznak. A magas hőmérséklet periódusában a kórokozók jobban szaporodnak, így a közvizek fertőzésveszélye megnő. A kutak nem megfelelő karbantartása és tisztításakor fertőzőképes „élőlénybevonat" telepszik meg a külső felszínen, mely 25 °C feletti vízhőmérséklet esetében a mikroorganizmusoknak kiváló szaporodási feltételeket biztosít. A közkutak legelterjedtebb baktériuma a legionella, mely a háztartási melegvízrendszerek 90%-ában, a klímaberendezésekben, a hűtőtornyokban, a párásító berendezésekben, a pezsgőfürdőkben, az akváriumokban, a kerti locsolókban is megtalálható. A nagyobb gondot akkor okozzák, ha vízpermet formájában a tüdő léghólyagocskáiba jutva gyulladást okoznak. Ha a szökőkút állati ürülékkel, vizelettel szennyeződik, akkor több fertőzést okozó mikroorganizmus kerül a vízbe, melynek a leggyakoribb

19 Szórványosan, elszórtan jelentkező.

következménye a szervezetbe jutás után a hasmenés, aminek kitettebb célcsoportja a gyerekek. [13]

A hazai ivóvízbázis-védelem jogszabályi alapját „a vízbázisok, a távlati vízbázisok, valamint az ivóvízellátást szolgáló vízi létesítmények védelméről" alkotott 123/1997. (VII. 18.) Korm. rendelet, továbbá a vizek mezőgazdasági eredetű nitrátszennyezéssel szembeni védelméről szóló 27/2006. Korm. rendelet, továbbá az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről szóló 201/2001. Korm. rendelet, a 147/2010. (IV. 29.) Korm. rendelet a vizek hasznosítását, védelmét és kártételeinek elhárítását szolgáló tevékenységekre és létesítményekre vonatkozó általános szabályokról, [14] a 541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerelemek és vízi létesítmények azonosításáról, kijelöléséről és védelméről szóló jogszabályok biztosítják. A hazai ivóvízbázis-védelem folyamatos ellenőrzésének egyik kulcsszereplője az Országos Környezetegészségügyi Intézet (OKI), mely alapfeladatait tekintve – a teljesség igénye nélkül – foglalkozik az emberi használatra szolgáló vizek (ivóvíz, ásvány- és fürdővizek) minőségét érintő döntések előkészítésével és felügyeli azok végrehajtását. Vizsgálja és értékeli a vizek kémiai és mikrobiológiai minőségét. Közreműködik az emberi használatra szánt vizek vizsgálatára akkreditált, ill. az Országos Tisztifőorvosi Hivatal (OTH) által ivóvízvizsgálatra feljogosított laboratóriumok munkájának minőség-ellenőrzésében, továbbá kezeli a vízbiztonsággal összefüggő országos ivóvíz és természetes fürdővíz adatbázisát stb. [15]

Az Intézet kutatja az időjárási szélsőségekhez történő emberi adaptáció elősegítését, melynek egyik alappillére a Páldy Anna főosztályvezető asszony által vezetett Klímaváltozás-egészséghatás Előrejelzése Csoport. Az osztály szakmailag irányítja a hőségriasztás országos rendszerét, illetve felelős a hőségriasztást megalapozó döntés szakmai előkészítéséért. Folyamatos ismeretterjesztő, tudatosító tájékoztatást ad, és hőhullámok idején, a lakosság felé történő kríziskommunikációban aktívan részt vesz, szakmai tanácsokkal látja el a hatóságokat. A tevékenységeikhez hozzátartozik az UVB sugárzás káros hatásainak megelőzését szolgáló UV riasztás kialakítása, melyet az Országos Meteorológiai Szolgálattal, az MTA Szociológiai Kutató Intézetével és a Magyar Vöröskereszttel közösen hajtanak végre. A tudományos tevékenységüket tekintve részt vesznek több hazai és nemzetközi fejlesztésben, elemzésben, például az egészségkárosodások korai felismerését (prognózisát) szolgáló módszerek, eljárások és eszközök számbavételét és kifejlesztését célzó kutatásokban stb. [16]

Áradásokkal kapcsolatos egészségügyi problémák

A klímaváltozás következtében kialakult extrém időjárási helyzetek, mint például a gyakoribb áradások rendszeres velejárója az ivóvíz elszennyeződése, ami fertőző betegségek terjedéséhez vezethet. A tartósan fennálló hőség különösen az állóvizekben, felszíni víztáro-

zókban, mesterséges tavakban növelheti meg az elsősorban a bélfertőzést okozó (például szalmonella) baktériumok számát. Az árvíz után emelkedik a víz és vektor terjesztette fertőző betegségek előfordulása, úgymint leptospirosis, kolera, dizentéria (vérhas), hepatitis A, hepatitis E stb., de jelentősen megnőhet az enterális fertőzések (hastífusz, szalmonella, hepatitisz A-vírus, calicivírus stb.), a gyomor-bélrendszeri fertőzések (széklettel kiválasztódó kórokozók) kialakulásának az esélye. Kellemetlen vektorként szaporodnak el az ízeltlábúak (főként a szúnyogok), a rágcsálók. Veszélyt jelent a vegyszerek kiömlése, és az elhalt állatok tetemei is. Az árvizes területekről veszélyes állatok menekülhetnek be árvízzel el nem öntött emberi településekre, ilyenkor a harapások, marások esélye növekszik. Fontos biztonsági szempont a kitelepítettek befogadó helyeken történő elhelyezésének közegészségügyi-járványügyi lebiztosítása, mivel a zsúfoltság, a higiéniás szabályok be nem tartása stb. a járvány kialakulásának okozói lehetnek.

2004-ben Bangladeshben (India) több mint 100 000 ember volt kénytelen elhagyni otthonát az árvíz miatt. Az intenzív esőzések következtében több ponton gátszakadás történt több százezer ember halálát okozva. Az utcákat derékig érő víz borította. Az áradás 20 millió embert érintett. Több tízezer embert elzárt a külvilágtól a víz, és az ivóvízellátás is nehézségekbe ütközött. A nem megfelelő minőségű ivóvíz fogyasztása miatt pedig 17 000 ember betegedett meg kolerában. 2004. december 26-án földrengés következtében az Indiai-óceánon cunami keletkezett, mely végigsöpört Szumátra szigetén (Indonézia). A közel 300 ezres halálozási szám mellett jelentős károk érték a közműrendszereket. A cunamit követő két hétben Achen tartomány területéről 106 tetanusz megbetegedést jelentettek. A fertőzöttek közül 20-an vesztették életüket. [17] A Katrina hurrikán 2005. évi tombolása után a kárterületen rekedt lakosság körében kimutatták a norovírust, szalmonellát, kolerát, a hepatitis A-t és a leptospirozist.

A természeti katasztrófák okozta biológiai kockázatok elleni védekezés lehetőségei

Természeti katasztrófák (például árvíz, földrengés) esetén nő a járványügyi veszély, mivel a kialakult helyzet jelentősen eltér a normál életkörülményektől. A lakosság kitelepítése, ideiglenes elszállásolása indokolt lehet. Ebben az esetben meg kell oldani a szállítást, élelmezést, elhelyezést, ahol előfordulhat, hogy a nagy létszámú lakost ideiglenes, kiépített táborokban kell elhelyezni. A fertőzésveszély csökkentése érdekében fontos:

– az ideiglenes szálláshelyeken folyamatos fertőtlenítés megszervezése,
– a lakosság visszatelepítése előtt a kárhelyszín záró fertőtlenítése (a terület elhagyása után a visszamaradt kórokozók elpusztítása).

Árvíz után a fertőtlenítés végrehajtásának célszerű menete:

Az ideiglenes szálláshelyen szükséges fertőtlenítési feladatok:

– az élelmezéssel kapcsolatos eszközök fertőtlenítő mosogatása;
– A mellékhelyiségekben fertőtlenítő kézmosás, illetve takarítás, valamint tartalmának folyamatos fertőtlenítése;
– ágyneműk, hálóruhák, egyéb textíliák fertőtlenítő mosása.

Kárhelyszínen szükséges főbb fertőtlenítési feladatok:
– árvíz után az elöntött helyiségek iszaptartalmának eltávolítása, majd a padlózat, illetve a falak fertőtlenítése;
– indokolt esetben az épületek talajának fertőtlenítése;
– fontos, hogy a fertőtlenítés abban az esetben hatásos, ha a fertőtlenítés a víz visszahúzódása és az iszap eltávolítása után történik.

A fertőtlenítés az alábbi területekre terjed ki:
– ivóvíz fertőtlenítése (vezetékes ivóvíz csak az ÁNTSZ engedélye után használható);
– kutak fertőtlenítése;
– szennyvíz fertőtlenítése;
– árnyékszékek, latrinák fertőtlenítése;
– elöntött házak lakótereinek, az alagsorok, pincék, vízóraaknák fertőtlenítése;
– szemétdob, trágyadomb fertőtlenítése, trágyalé fertőtlenítése;
– fertőző beteget szállító jármű, mentőautó fertőtlenítése;
– talajfertőtlenítés;
– fertőző betegségben elhunytak fertőtlenítése;
– lábbelik fertőtlenítése, fertőzött anyagok, eszközök fertőtlenítése;
– zárt terek, helyiségek légterének, felszerelési-berendezési tárgyainak fertőtlenítése.

Az árvízi esemény lezajlása után, a lakó- és mezőgazdasági ingatlanok, a személyes használati eszközök, és amennyiben szükséges, a vízhálózat szakszerű fertőtlenítését követően is visszamaradhatnak még veszélyforrások, amelyek semlegesítésére nagy gondot kell fordítani. Az ár után hátramaradt hordalék, továbbá a védekezésnél felhasznált anyagok eltávolítása, elhelyezése és esetleges újrahasznosítása szintén a szabályozott feladatok közé tartozik. A gátak megerősítésére használt homok nem alkalmazható közterületek (udvar, kert, játszótér) feltöltésére, csupán építkezéseknél hasznosítható újra, miután a tároló zsákokkal együtt „környezetre ártalmasnak" minősülnek. A kiürített és kiszárított zsákok is csak a hulladék és a szemét gyűjtését, tárolását szolgálhatják.

Az árhullám levonulása után általában belvizes elöntés következik be (domborzati és talajminőségi viszonyoktól függően). A vízzel telt területeken a szúnyogok elszaporodása valószínű, és a klímaváltozással előtérbe kerülő élőhely-elmozdulások miatt a fertőzésveszély növekedni fog. A kockázatszint emelkedése borítékolható (ha a jelenlegi melegedési ütem stagnál vagy növekszik), mivel jelenleg Magyarországon az elsődleges természeti veszélyforrás az árvíz és belvíz. A kiterjedt belvizes területek miatt a rágcsálók az emberlakta területeken kereshetnek menedéket, így az állattal történő közvetlen vagy közvetett érintkezés esélye nagyobb, ezáltal a rágcsálók által terjesztett betegségek leptospirosis,

tularaemia vírusos vérvizelés esetében is több esetszámmal lehet szembesülni. A megbetegedések számát növelheti, hogy a jelenlegi tapasztalatok és a különböző szcenáriók az árvizes, belvizes, sodró árhullámos, nagy csapadékos események számát mutatják a rendkívüli vízjárás, és a szélsőséges időjárás miatti csapadékeloszlás következtében.

A vízzel kapcsolatos esetekből kitűnik, hogy egyrészt a sok csapadék is okozhat problémákat, illetve a sok csapadék miatt kialakult áradások. Az megállapítható, hogy árvizek után a fertőzésveszély nagyobb, illetve a lakossági vízellátást a kiépített rendszerek ellenére meg kell oldani, így az ivóvíz-készletezésre és az ásványvízgyártásra fontos szerep hárul. A klímaváltozás következtében a tengerszint-emelkedés és a kialakult hurrikánok miatt a tengerparti részeken a fertőzésveszély kockázata nagyobb, mint a bentebb levő szárazföldi településeken. Ez a stratégiai tervezéseknél egy prioritást érdemlő kockázatértékelési szempont.

Összefoglalás

Az emberiség történetében mindig nagy jelentősége volt a járványoknak, fertőző betegségeknek. A járványok terjedésének földrajzi korlátai voltak. A hajózás fejlődésével, a kereskedelem széles körű elterjedésével, az utak hálózattá alakításával a fertőző betegségek kontinensekről kontinensekre vándorolhattak, kialakítva ezzel a civilizációs katasztrófák egyik legveszedelmesebb kockázatát. Jelen korban az tapasztalható, hogy a globalizáció adta lehetőségek, úgymint a személyszállítás egész földre kiterjedése mellett az éghajlati módosulás miatt is mód van a járványok terjedésére. A klíma változása magában hordoz több egészségügyi kihívást, melyek a 21. század megoldandó feladatai közé tartozik. Ilyen kockázatot jelent a hőmérséklet esetében a hőhullámok, illetve az ökológiai rendszer károsodásának, a környezetváltozás következményeként a vektorok okozta megbetegedések, az allergén növényfajok pollentermelődésének fokozódása. A hidrológiai, geológiai, meteorológiai anomáliák, melyek évről évre gyakrabban és intenzívebben jelennek meg, olyan katasztrófákat okoznak, ahol megnőnek a sérülések, fertőzések, táplálkozási, pszichológiai és egyéb károsodások kialakulásának a valószínűségei. A második Nemzeti Éghajlat-változási Stratégia szerint egyes kórokozók gyakoribbá válnak a szúnyogok, kullancsok, rágcsálók elterjedésével – elsősorban a Lyme-kór, a kullancsencephalitis, hantavírusok, nyugat-nílusi vírus, madárinfluenza, valamint különböző féregfertőzések jelenthetnek veszélyt. Nőhet a maláriás esetek száma, s jelentős veszély a lepkeszúnyogok által terjesztett leishmaniasis megjelenése, valamint egyéb, Európában a legutóbbi években detektált fertőzések (chikungunya-láz, dengue-láz, Rift-völgyi láz) megjelenése. Növekedni fog az ivóvízzel, illetve a nem megfelelően kezelt – elsősorban rosszul hűtött – élelmiszerekkel terjedő bakteriális, vírusos és protozoon fertőzések gyakorisága (a salmonellosis campylobacteriosis, hepatitis A, cryptosporidiosis).

Magyarországon a 21. században nem voltak a fertőző betegség miatti tömeges elhalálozások, mégis a különböző betegségtípusok alapján elmondható, hogy a biológiai veszélyekkel számolni kell, az új típusú kórokozók megjelenése a klímazónák eltolódása miatt még nem számottevő, főként a személyszállítás miatt történnek megbetegedések. A fertőzés okaiként általában a vízzel és élelmiszerrel kapcsolatos kockázatokat lehet megemlíteni, illetve a szezonálisan jelentkező influenza miatti megbetegedéseket. Mindenesetre a fertőző betegségek ellen a hazai szervezetek fel vannak készülve, jól működő egészségügyi hálózattal rendelkezik az ország, a közművek jelenlegi helyzete és monitorozása csökkenti a fertőzések kialakulásának az esélyét. Amin változtatni kell, az az egészségkultúra fejlesztése, a megfelelő személyi higiénia kialakítása, a vízbázisok védelme, a legális migráció fokozottabb egészségügyi ellenőrzése (munkavállalók, turisták, átutazók stb.), a politikai és környezeti menekültek kérdésköre, a hazai hajléktalanvédelem erősítése stb., melyek olyan vizsgálati szempontokat képeznek, melyek további kutatásokat, elemzéseket, kiértékeléseket követelnek meg a hazai, nemzetközi tudósvilágtól, a katasztrófák elleni védekezésben részt vevő szakemberektől.

Következtetés

Az éghajlatváltozásból adódó előnyök a vektorok szaporodási, túlélési esélyét növelik, így a kapcsolódási pont valószínűleg itt bontakozik ki a biológiai fegyverek és a klímaváltozás között. Az éghajlatváltozás miatti járványügyi kockázatok a folyamatok lassúsága miatt (attól, hogy néhány fertőző vektor kihelyezésre kerül, még nem 100%, hogy az éghajlati viszonyok a kórokozók fertőzőképességeit biztosítani tudják) nem biztos, hogy a klíma változásából adódó lehetőségekkel gyors eredményt tudnak elérni. Egyszerűbb, ha géntechnológiával kifejlesztett erősebb törzs kerül bevetésre zsúfolt, lehetőleg szegényes negyedekben, ahol a személyi higiénia nem megfelelő. Nyilván a megváltozó klimatikus viszonyok a bevetés sikerét fokozhatják, a kórokozók túlélési képességeit növelhetik.

Az urbanizált területeken számos gócpont jelentkezik egy időben és térben, úgymint a hulladékkezelés, szennyvízelvezetés, élelmiszergyártás, piacok, élelmiszer-ellátó egységek, zsúfolt betonépületek egymás mellett, tömegközlekedési csomópontok, bevásárlókomplexumok, melyek mind a biológiai ágensek célpontjaivá válhatnak.

A hőséghullámok idején az emberi immunrendszer a jelentős hőtöbblet miatt le van terhelve, így a biológiai eredetű kórokozóknak nehezebben áll ellen.

Önkéntes, szakképzett mentőszervezetek bevonása (például HUNOR) válhat szükségessé bizonyos betegségek területén (például malária), mivel a nemzetközi segítségnyújtás során ezek a tagok védőoltást kaptak, tehát a védettségük nagyobb, mint a mentőszervezetbe be nem osztott tűzoltótársaiknak.

Irodalomjegyzék

[1] Teknős László: A globális éghajlatváltozás egészségügyi aspektusai – a magyar lakosság sebezhetőségének vizsgálata. *Bolyai Szemle,* (2013)/1, 292. (ISSN 1416-1443)

[2] Páldy Anna et al.: A klímaváltozás egészségi hatásai. *Egészségtudomány,* 48(2004)/2–3., 220–236. (ISSN 0013-2268), www.antsz.hu/data/cms40726/Eutud_PA.pdf (a letöltés ideje: 2016. március 5.)

[3] Háziorvosi fórum: *Fókuszban a zoonosisok,* www.lam.hu/folyoiratok/lam/0702/10.htm (a letöltés ideje: 2016. március 5.)

[4] Radnai István: *A tularaemia*, drradnaiistvan.blogspot.hu/2011/04/tularaemia.html (a letöltés ideje: 2016. március 5.)

[5] Ornithosis (psittacosis, papagálykór), 2012. február, www.egeszseg-portal.hu/egeszsegugyi-tudastar/Betegsegek/Fertozesek-es-parazitak/Ornithosis-%28psittacosis-papagalykor%29-672.html (a letöltés ideje: 2016. március 5.)

[6] Második Nemzeti Éghajlatváltozási Stratégia 2014–2025, kitekintéssel 2050-re, 2013. szeptember, 105., www.kormany.hu/download/7/ac/01000/M%C3%A1sodik%20Nemzeti%20%C3%89ghajlatv%C3%A1ltoz%C3%A1si%20Strat%C3%A9gia%202014-2025%20kitekint%C3%A9ssel%202050-re%20-%20szakpolitikai%20vitaanyag.pdf (a letöltés ideje: 2016. március 5.)

[7] Kohut László: A globális klímaváltozás egészségügyi vonatkozásai. *Repüléstudományi Közlemények*, 24(2012)/2, 697. (HU ISSN 1789 770X), www.repulestudomany.hu/kulonszamok/2012_cikkek/57_Kohut_Laszlo.pdf (a letöltés ideje: 2016. március 7.)

[8] Sipos Ilona Magdolna: *Népegészségügy, járványtani alapismeretek*, www.kepzesevolucioja.hu/dmdocuments/4ap/2_1851_014_101030.pdf (a letöltés ideje: 2016. március 5.)

[9] 96/2009. (XII. 9.) OGY határozat a 2009–2014 közötti időszakra szóló Nemzeti Környezetvédelmi Programról, 75., www.kvvm.hu/cimg/documents/96_2009_OGY_hatarozat_NKP_3.pdf (a letöltés ideje: 2016. március 5.)

[10] Zöldi Viktor: *A „JOHAN BÉLA" Országos Epidemiológiai Központ 2. módszertani levele a szúnyogok elleni védekezésről,* 12(2005. január 31.)/2. különszám, 5., www.oek.hu/oekfile.pl?fid=448 (a letöltés ideje: 2016. március 6.)

[11] Trájer Attila János et al.: *Új vektoriális betegségek megjelenésének lehetősége, és a már őshonos betegségek jelentőségének növekedése a klímaváltozás következtében. A XXI. század egészségügyi és hadászati biztonságát fenyegető hazardok.* 23(2013. május)/elektronikus különszám, 259. (ISSN 1215-4121), unipub.lib.uni-corvinus.hu/1419/1/TA-BFA-BJ-PA_KlimaBizt_hu.pdf (a letöltés ideje: 2016. március 6.)

[12] Sárváry Attila: *A vízszennyeződés okozta ártalmak*, www.tankonyvtar.hu/hu/tartalom/tamop425/0019_1A_Kornyezetegeszsegtan/ch02s03.html (a letöltés ideje: 2016. március 6.)

[13] Szax Anita – dr. Vargha Márta: *A szökőkutak vize, mint potenciális fertőzőforrás,* oki.antsz.hu/hirek/reszletek/70 (a letöltés ideje: 2016. március 7.)

[14] Berek Tamás – Rácz László István: Vízbázis, mint nemzeti létfontosságú rendszerelem védelme. *Hadmérnök,* 8(2013. június)/2, 121–122. (ISSN 1788-1919), www.hadmernok.hu/132_11_berekt_rli.pdf (a letöltés ideje: 2016. március 7.)

[15] Az Országos Környezet-egészségügyi Intézet (OKI) alapfeladatai, oki.antsz.hu/intezetunkrol/alapfeladataink (a letöltés ideje: 2016. március 7.)

[16] Klímaváltozás-egészséghatás Előrejelzése Csoport, oki.antsz.hu/intezetunkrol/klimavaltozas_egeszseghatas_elorejelzese_csoport (a letöltés ideje: 2016. március 7.)

[17] Sztergovai Rebeka: *A járványügy szerepe és jelentősége hazánkban.* Szakdolgozat. Nemzeti Közszolgálati Egyetem, Budapest, 2013, 38.

Analysing the Biological Risks of Global Climate Change and its Impact on Disaster Management I.

Teknős László – Kóródi Gyula

Epidemics, infectious diseases have always been of great importance in the history of mankind. Their outbreak and spread did not only have commercial roots, but climatic as well. Nowadays more and more studies point out the relationship between global climate change and infectious diseases. This article deals with the health impacts of climate change, especially on the possibility of the outbreak and spread of epidemics, infectious diseases.

Keywords: global climate change, epidemics, infectious diseases, human health, vectors

Vedó Attila
Komjáthy László

A Magyar Királyi Csendőrség tűzrendészeti feladatai 1881 és 1945 között

A magyar királyi csendőrség Magyarország vidéki közbiztonsága érdekében 1881-ben létrehozott, rendkívül hatásossága miatt nemzetközileg elismert, katonailag szervezett őrtestület volt. Szolgálatát tekintve a belügyminisztérium, míg tagjai személyes ügyeit tekintve a hadügyminisztérium hatáskörébe tartozott. A szervezet feladata volt működési területén a személy- és vagyonbiztonságot megóvni, a békét és közrendet fenntartani, a törvények, rendeletek és szabályrendeletek megszegését, a gondatlanságból vagy mulasztásból eredő veszélyeket és károkat megakadályozni, a megzavart rendet és békét helyreállítani, az elkövetőket az illetékes bíróságnak vagy hatóságnak átadni. Azonban a testület számos más tevékenységével is óvta a vidéki lakosságot, valamint a köz- és magánvagyont. Ezek közül az eddig még fel nem dolgozott feladatkör a vidéki tűzrendészet ellátása és a tűzrendészeti szabályok betartásában betöltött szerepük. Ennek megértéséhez azonban szükséges annak ismerete is, hogy miként fejlődött a hazai tűzrendészeti szabályozás, milyen konkrét rendszabályok vonatkoztak a megelőzés, a tűzoltás, valamint a tűzvizsgálat végrehajtására ebben az időszakban.
Kulcsszavak: csendőrség, biztonság, tűz, tűzvédelem, vidék

Bevezetés

A Magyar Királyi Csendőrség Magyarország vidéki közbiztonsága érdekében 1881-ben létrehozott, rendkívüli hatásossága miatt nemzetközileg elismert, katonailag szervezett őrtestület volt. Szolgálatát tekintve a belügyminisztérium, míg tagjai személyes ügyeit tekintve a hadügyminisztérium hatáskörébe tartozott. [1]

A szervezet feladata volt működési területén a személy- és vagyonbiztonságot megóvni, a békét és közrendet fenntartani, a törvények, rendeletek és szabályrendeletek megszegését, a gondatlanságból vagy mulasztásból eredő veszélyeket és károkat megakadályozni, a megzavart rendet és békét helyreállítani, az elkövetőket az illetékes bíróságnak vagy hatóságnak átadni. A Magyar Királyi Csendőrség 1881. évi felállításával létrejött a mindenkori kormányzattól függő, egységes közbiztonsági őrtestület, amely komoly eredményeket ért el a bűnmegelőzés és a bűnfelderítés területén, úgyhogy a 19. század utolsó

évtizedére a magyar vidék Nyugat-Európa legbiztonságosabbnak tartott térségeihez tartozott.

Azonban a testület számos más tevékenységével is óvta a vidéki lakosságot, valamint a köz- és magánvagyont. Ezek közül az eddig még fel nem dolgozott feladatkör a vidéki tűzrendészet ellátása és a tűzrendészeti szabályok betartásában betöltött szerepük. Ennek megértéséhez azonban szükséges annak ismerete is, hogy miként fejlődött a hazai tűzrendészeti szabályozás, milyen konkrét rendszabályok vonatkoztak a megelőzés, a tűzoltás, valamint a tűzvizsgálat végrehajtására ebben az időszakban.

Tűzrendészeti szabályozás

A 18–19. században Magyarországon (Habsburg Birodalom, Magyar Királyság, Osztrák–Magyar Monarchia) helytartótanácsi és belügyminiszteri rendeletekkel kívánták szabályozni a tűzveszélyes tevékenységek csökkenését. Az 1723. évi II. dekrétumban a közigazgatás egyik megoldandó feladatául jelölték meg a tűzvédelmet. A következő jelentősebb jogszabály II. József tűzrendészeti pátense volt, ami meghatározta a szakterület felosztását és feladatait. [1] A tűzvédelmi ügyekkel megbízott helytartótanács 1834-ben ajánlotta a vármegyéknek egyik leiratában a lángok ellen védő különböző tűzoltó felszereléseket és eszközöket, köztük az azbesztruhát. [2] 1838-ban újabb tűzrendészeti intézkedések kerültek kiadásra, később belügyminiszteri rendelet szabályozta a tűzrendőrséget. A központi rendelkezések azonban nem érték el a kellő hatást, így a tűzvédelem kellően nem szilárdult meg. Újabb ígéretként 1868-ban a belügyminiszter kilátásba helyezte a tűzrendészet ügyének törvényi rendezését.

A törvényi szintű szabályozásban – annak ellenére, hogy nem született kifejezetten tűzvédelmi rendelkezés – más területeken két törvényben is találhatunk ilyen jellegű előírásokat. A mezei rendőrségről szóló 1840. évi IX. törvénycikkben a mezőgazdasági területek védelme mellett tűzvédelmi büntetőrendelkezések is megjelentek. Ezek értelmében, aki az erdőt vagy tarlót felgyújtja, büntetendő cselekményt követett el. A büntetést az okozott kár és a vétkesség alapján határozták meg. A másik tűzvédelmi jellegű rendelkezést a közmunkák szabályozásáról szóló 1844. évi IX. törvénycikkben találhatjuk. A törvény felsorolja a közmunkák végzésére kötelezetteket, a jobbágyokat, a zselléreket, a nemesi jószágokkal bíró nem nemeseket. Érdekessége, hogy a közmunkára nem kötelezett nemesek is – bizonyos esetekben – hófúvás, más elemi csapás, „tűzi veszély" elhárítása, árvízvédelmi munkák esetén kötelezhetők voltak közmunka végzésére.

A szabadságharcot követően természetesen a tűzoltás szervezésében is történtek változások. A céhes tűzoltóságok korszerűtlenségét sok településen felismerték, és külföldi tapasztalatok alapján megalakították saját tűzoltóságaikat, akiket kezdetben más egyletekhez hasonlóan kezeltek. Egyes források szerint a pesti önkéntes tűzoltó egyesület már

1863-tól fennállt, de működését csak azzal a feltétellel engedélyezték, hogy a tűzvész színhelyén a tűzoltóparancsnok engedelmeskedni tartozik a városi rendőrfőnöknek vagy helyettesének. [3] A kiegyezést követőn megindult gazdasági fejlődés a tűzvédelemben csak lassan éreztette hatását. Az önkéntes tűzoltóságok megalakításának már nem volt akadálya, a tűzrendészet pedig a belügyminiszter hatáskörébe került. A további intézkedésekig a Pátens rendelkezései maradtak érvényben a tűz elleni védekezésben.

Megjelent a „tűzrendőrség" fogalma, amelyet később általánosan használtak a tűzvédelemben. A fogalom a későbbiekben átalakult, 1888-ban a tűzvédelem tárgyában kiadott rendelkezés [4] már a „tűzrendészeti kormányrendelet" elnevezést kapta. A rendelet a tűzrendészetet helyi feladatként fogalmazta meg, tehát az a községek és a városok feladata volt, így a helyi szabályzatokat nekik kellett megalkotni. Lényeges rendelkezés volt továbbá, hogy tűzvész esetében a telkén levő vizet a tűzoltástól senki nem vonhatta meg. Minden, legalább 50 házból álló község köteles volt a rendelet által meghatározott tűzoltószereket beszerezni és azokat biztos, e célra készült helyen jó állapotban tartani.

A tüzek okának kiderítésére is mind nagyobb hangsúlyt fektettek. A tűz oltását követő vizsgálatot a községi elöljáró, vagy ha rendőri erő is jelen volt, a tűzoltást vezető parancsnok azonnal köteles volt elvégezni a tanúk és szakértők közreműködésével. Vizsgálni kellett a tűz keletkezési okát és a személyi felelősséget. Ha valaki törvénybe ütköző cselekményt, mulasztást követett el, a jelentést azonnal az illetékes bírósághoz kellett megtenni. Az 1888. évi rendelet volt az első olyan jogszabály, amely említette a tűzrendészeti hatóságot, mint fogalmat, valamint kötelezővé tette a szakszerű tűzvizsgálatot és annak jegyzőkönyvezését. 1888-tól 1925-ig több mint 30 rendelet kiadására került sor a témában, míg a korábbi szabályozás kiegészítése, módosítása és végrehajtása tárgyában megszületett a 230.000/1925. BM számú új tűzrendészeti kormányrendelet. A tűzrendészeti törvény megalkotására csak 65 évnyi várakozás után, 1936-ban került sor. A törvény végrehajtására pedig kiadták a 180.000/1936. BM-rendeletet. Ezzel a szabályozás egységessé és átláthatóbbá vált. [5]

A csendőrség megelőző tűzrendészeti feladatai

A csendőr kötelessége volt minden veszélyes jelenségre felügyelni, baleseteknél és elemi csapásoknál segítséget nyújtani. Ebből következően a korabeli vélekedés szerint a csendőr kötelessége volt fellépni az események megelőzése érdekében is. [6] A csendőrség tűzrendészettel kapcsolatos szolgálati teendőit három csoportba sorolhatjuk:

– Megelőző tűzrendészet: a jogszabályokban és törvényhatósági szabályrendeletekben rögzített tűzvédelmi szabályok betartásának ellenőrzése.
– A már bekövetkezett tűz helyszínén a tűzoltás vezetése és a rend fenntartása.
– A tűz okának kinyomozása, a tűzvizsgálat.

1. kép: Tűzvédelmi ellenőrzés cséplésekor (Forrás: Magyar Hírlap archív)

A megelőző tűzrendészet feladatait a járőr a napi szolgálata során teljesítette. Ez olyan szabályok betartatásának ellenőrzéséből állt, mint például betakarítás idején a takarmány házak közötti felhalmozása és a lakott területen történő cséplést tiltó rendelkezések, valamint a takarmány és a gabona szállítása, tárolása során a dohányzás és tűzgyújtás tilalma. [7] Ügyelniük kellett arra is, hogy minden háznál és csűrnél álljanak rendelkezésre olyan tűzoltó házieszközök (pl. létra, pemet, csáklya, vasvilla, szikracsapó, fejsze) és tűzoltásra használható víz, melyek meglétét a tulajdonostól keményen számon is kérték. A csendőrnek minden, a községben zajló folyamatot figyelemmel kellett kísérnie, mely alól a gyermekek játéka a gyufával vagy a világításra használt ásványolajak szállítása sem volt kivétel. Aratáskor a boglyákat a terület nagyságától függően 4, 15, és 30 méter széles tűzutakkal kellett elválasztani, a vasút melletti földeken pedig az aratást a vasúti pálya felől kellett kezdeni, és a terményt attól legalább 100 méternyi távolságban lehetett csak elhelyezni.

A csendőr tűzrendészeti ellenőrzése tehát a mindennapi élet tevékenységeire terjedt ki, amely a vármegyei szabályrendeletek betartatását éppúgy magában foglalta, mint a közhasználatú kutak épségét és használhatóságát. Aki ilyen kutat megrongált és a tűzivíz vételezésére alkalmatlanná tette, kihágást követett el. A gépi cséplést kiemelten veszélyes tevékenységnek tartották, így azt a legközelebbi háztól 100 méterre, a szomszéd kazaljától pedig legalább 15 méterre lehetett végezni. A cséplést csak levizsgáztatott gőzgéppel lehetett végezni kiképzett személyzet által, és erősebb szélben abba kellett hagyni.

A munkavégzés környékén tilos volt a dohányzás. [8] Ha a csendőr azt tapasztalta, hogy a cséplőgép mellett működésképtelen „kazalfecskendőt" tartottak és a munkások nem járnak el kellő gondossággal a tűzesetek megelőzése terén, azonnal a községi elöljáróság intézkedését kellett kérnie. A tulajdonost ez esetben a 44.200/1924 BM-rendelet értelmében kihágás miatt fel is jelentette.

A falu utcáin járőröző csendőrök éppúgy felhívták a figyelmet a fedetlen nyári konyhákban való tűzgyújtás tilalmára, mint a legalább havonta esedékes kéménytisztítás kötelezettségére. A gondatlanságból támadt tüzek megelőzése mellett az esetleges szándékos tüzekre is figyelmet fordítottak. A tűzesetek megelőzéshez és felderítéséhez kapcsolódó fontos feladatnak tartották, hogy a csendőr a lakossággal való kapcsolattartása, nyílt információgyűjtése során fordítson figyelmet az újonnan megkötött, nagyobb összegű biztosításokra is.

A csendőrjárőr feladatai a tűzoltás megszervezésében

A szakmai ajánlások szerint a csendőrnek a tűz helyszínén csak a rendet kellett fenntartani, nem az oltásban részt venni. Addig azonban, amíg a tűzoltóság megérkezett, vagy az arra hivatott hatósági személy részéről intézkedés nem történt, gondoskodnia kellett arról, hogy vezetése mellett a lakosság a tűz eloltásához lásson. A járőr az intézkedésre hivatott hatósági személyt és a tűzoltóságot mindenben támogatta, és arra is ügyelt, hogy a lakosság ezek rendelkezéseit teljesítse.

Tűz esetén, ha veszélyeztetett ház lakóinak kilakoltatására volt szükség, a csendőr köteles volt minden veszélyeztetett házba behatolni, a lakókat figyelmeztetni, a ház elhagyására felszólítani. Ekkor elsősorban a gyermekeket, betegeket vagy egyébként gyámoltalanokat kellett mentenie. A járőr elsődleges feladata az volt, hogy a rendet minden körülmények között fenntartsa. A vagyon mentését és megőrzését a tűz elmúlása után is folytatnia kellett.

A nyomozást minden esetben azonnal meg kellett kezdeni annak kiderítésére, hogy a tűz miként keletkezett, és azért terhel-e valakit büntetőjogi felelősség. Ha ilyen nem merült fel, csupán a közigazgatási hatóságnak kellett jelentést tenni. [9]

Aki a tűz oltása során nem engedelmeskedett a hatóság utasításainak, vagy a közveszély elhárításában nem működött közre személyesen vagy háza népének munkájával, szekereinek, hámos lovainak ideiglenes hatósági rendelkezésre bocsátásával, az kihágást követett el. Ugyanis a tűzrendészetről alkotott 1888. évi rendelet értelmében tűzvész idején a lakosság kötelezhető volt az oltás munkájában való részvételre. Ebből következett, hogy a hatóságoknak a közveszély elhárításával kapcsolatos felszólítását a lakosság köteles volt teljesíteni. A komoly ok nélkül ellenszegülőket a megfelelő figyelmeztetés után el kellett fogni, ha ezt a büntetendő cselekményt a csendőr figyelmeztetése ellenére is folytatta.

Az ilyen viselkedés nyilvános botránykeltésnek is tekinthető, így az elfogás jogalapja ez is lehetett. Akár sor került az ellenszegülő elfogására, akár nem, a csendőr kihágás miatt feljelentést tett.

Itt szükséges megemlíteni, hogy a korabeli szakirodalom a tűzrendészeti kihágásokat két csoportba sorolta:

1. a tűzvész kitörését vagy továbbterjedését gátló intézkedések megszegése, vagyis a megelőzés körében elkövethető kihágások.

2. a tűz oltására, a rendre és a biztonságra vonatkozó rendelkezések megsértése voltak. Mindkét jogsértés megállapításának előfeltétele volt olyan miniszteri rendelet, törvényhatósági szabályrendelet vagy eseti jelleggel kiadott hatósági intézkedés megléte, amely a polgárokra a fenti körben kötelezettségeket és tilalmakat írt elő. Ezek súlyos megszegése kihágást valósított meg, ha azonban a tűzrendőri szabályok megszegése miatt tűz keletkezett, a vétkessel szemben már a gondatlan tűzokozás miatt kellett eljárni. Mindezek megállapítására a tűzoltás során, valamint az azt követő tűzvizsgálat alkalmával is lehetőség volt.

Ugyan semmilyen előírásban nem szerepelt, hogy a csendőr az oltásban tevékenyen részt vegyen – főleg azért nem, mert a tűzvizsgálat feladatait már ekkor meg kellett kezdenie –, azonban a szükség néha úgy hozta, hogy a csendőr volt az egyetlen „szakképzett erő" az oltás kezdetekor. Számos esetben előfordult, hogy a mezei munkákhoz készenlétben tartott fecskendőt neki kellett működésbe hozni, hogy a munkások megkezdhessék az oltást. A tűzoltással kapcsolatos műszaki ismereteknek a járőr a napi szolgálatban is hasznát vette. Nem egy esetben neki kellett megítélnie, hogy egy adott tűzoltó eszköz működőképes-e. Az ezzel kapcsolatos gyakorlat megszerzése érdekében a csendőriskolákban nyaranta tűzoltó kiképzést szerveztek. Ez elsősorban a tűzoltás megszervezésére terjedt ki, de gyakorlati ismeretekkel is felruházta a próbacsendőröket. A tanfolyam vizsgával zárult, amely 1927-ben már a követező elemekből állhatott a vizsga helyszínének függvényében [10]:

1. iskolaszerelés kocsi- és mozdonyfecskendővel,
2. kocsi- és mozdonyfecskendő gyorsszerelés,
3. vízvezeték gyorsszerelés egy sugárra, tolólétrán az épület tetejére,
4. horoglétra iskolaszerelés I–III. emeletre,
5. támadási gyakorlat mászóházra,
6. mentési gyakorlat ugróponyván keresztül.

Később az ismeretek átadásának hatékonyságát azzal növelték, hogy a tűzoltók képzésbe történő bevonásán kívül a csendőriskolák oktató tisztjeit és segédoktató altisztjeit az évente megszervezett országos tűzoltó szaktanfolyamra is beiskolázták, ahol a polgári hallgatókkal együtt tanultak.

A tűzvizsgálat lefolytatása

A csendőrség tűzrendészeti feladatai közül a tűzvizsgálat volt az, amely a legnagyobb jelentőséggel bírt. Az itt jelentkező feladatokat egyrészt adminisztratív teendők, másrészt a vizsgálat gyakorlati lefolytatása tették ki. A tűzesetet a Magyar Királyi Központi Statisztikai Hivatalnak az erre szolgáló űrlapon be kellett jelenteni. Ez a jelentés tartalmazta a vármegyét, járást, községet (várost), továbbá, hogy az mikor, kinek a telkén keletkezett. Ha a tűz valamely pusztán, majorban, erdőben, tanyán vagy valamely más, községen kívül fekvő területen történt, akkor azt a községet kellett megjelölni, amelyhez az tartozik.

Az illetékes hatóságnak azt is be kellett jelenteni, hogy milyen kárérték keletkezett, az biztosítva volt-e, milyen összegre, hol és milyen lejárattal. A tűzeseteknél a csendőr elsősorban azt vizsgálta tehát, hogy a Btk. 422–425. § szerinti gyújtogatás, vagy a 382. § szerinti biztosítási csalás megvalósult-e. Nem voltak ritkák az olyan esetek, amikor a tulajdonos idézte elő a tüzet saját otthonában, vagy a kereskedők egymás raktáraiban, üzlethelyiségeiben okoztak károkat. Számos esetben diákok gyújtották fel iskolájukat, de akadt példa arra is, hogy a falusi iskola tanítója volt a tűzokozó, aki ezzel akarta a tető felújítására kényszeríteni a községi elöljáróságot.

A legenyhébb, gondatlanságból elkövetett felgyújtás esetén is a m. kir. járásbíróság volt illetékes, tehát a csendőr akkor is ide tette meg részletes nyomozati jelentését, ha senkit nem terhelt felelősség. A feljelentést tehát minden esetben megtették a bíróság felé, a főszolgabíró felé pedig jelentést tettek az esetről. Annak érdekében, hogy valóban megállapításra kerüljön az esetleges személyi felelősség, nyomozást kellett lefolytatni minden tűzesetnél. A közigazgatási hatóság ennek eredményétől függően állította ki a sértett számára az ún. „ártatlansági bizonyítványt", amellyel biztosítójához fordulhatott. [11]

A tűzvizsgálat gyakorlati lefolytatására számos szakmai ajánlás létezett, amellyel a csendőrségi szaklapok rendszeresen foglalkoztak. A tűzesetek körülményeinek teljes körű tisztázása és a vizsgálati munka segítése érdekében egy 66 kérdésből álló segédlet került összeállításra, melyet először a Csendőrségi Lapokban tettek közzé.

A csendőrségi szakirodalom a tűzesetek okait a következők szerint kategorizálta [12]:

– öngyulladás vegyi folyamat eredményeként,
– öngyulladás rothadás vagy erjedés következményeként,
– gyulladás napsugárzás hatására,
– villámcsapás okozta tűz,
– világítószerek gondatlan kezelése miatt keletkezett tűz,
– rövidzárlat vagy elektromos vezetékek túlterhelése,
– egyéb gondatlanság (pl. gyermekek játéka gyufával),
– robbanás,
– szándékos gyújtogatás.

A fenti lehetőségek mindegyikét vizsgálnia kellett az intézkedő járőrnek. Egy tűzeset helyszínén elsősorban a vizsgálatot végző csendőr tapasztalata és a minden részletre kiterjedő figyelme volt a siker kulcsa. A kor általános vélekedése szerint az a tűzeset, amit fél nap alatt nem lehet kideríteni, nagy valószínűséggel megoldatlan is marad. Ezt arra alapozták, hogy egy tűz után rendszerint olyan kevés értékelhető nyom maradt, hogy azok feldolgozására és a következtetések levonására ennyi idő is elég volt. A helyszínre érő járőrnek ajánlatos volt a bámészkodó tömegben is megfordulni és az ott elhangzottakat megfigyelni. A szakirodalom szerint az itt felvetődő sejtések sokszor jó irányba terelhették a nyomozást. Ha azonban a szándékos gyújtogatás elkövetőjére a helyszínen nem derült fény, akkor azt később csak igen nehezen lehetett felfedni.

Fontos szakmai ajánlás volt, hogy a csendőr minél hamarabb érjen a helyszínre és már az oltás során figyelje meg a helyszínt és annak környékét. Ekkor volt lehetősége az ott talált személyeket tanúként meghallgatni és tisztázni, ki ért először a helyszínre és mit látott. Tanúk hiányában a tűzoltókat kellett meghallgatni, hogy oltás közben mit tapasztaltak, hol mit oltottak el. Tisztázni kellett azt is, hogy a helyszínen oltás közben ki mit mozdított el. Az érdektelen, szemlélődő tanúk vallomásait hitelesebbnek tartották, mint a kárvallottakét, mert őket nem befolyásolták az érzelmeik és az ijedtség.

Már a helyszínen szándékos gyújtogatást kellett feltételezni akkor, ha a tulajdonos főbb értékeivel eltávozott, ha a tűoltószereket megsemmisítették, a kút vizét kimerítették, illetve a tűz egyszerre több helyiségben vagy olyan elzárt, nehezen megközelíthető helyen keletkezett, ahol egyébként éghető anyag nincs. A gyanút erősíthette, ha a tűzoltók más tűzhöz már kivonultak, vagy a gyorsan keletkező lángok hamar csillapodtak. Az önkezűség kizárása érdekében minden esetben tisztázni kellett, hogy a tulajdonosnak volt-e tartozása, mit tett a vagyonmentés érdekében, és hogyan viselkedett az oltás során. Külön figyelmet érdemelt a károsult feleségének magatartása és az, hogy a biztosítási összeg kifizetése körül milyen buzgalommal járt el. A házicselédek és gyermekek kikérdezése is fontos volt annak szem előtt tartásával, hogy hozzátartozóira senki nem volt köteles terhelő vallomást tenni. A károsult haragosainak körét is fel kellett deríteni, de nem szabadott az érzelmeitől vezérelt tulajdonos indulataira hagyatkozni. Ha a gyújtogatással gyanúsítható személlyel szemben nem állt rendelkezésre elegendő bizonyíték, akkor hosszabb távon meg kellett figyelni, hátha elárulja magát.

A vizsgálathoz a csendőr szakértőt is igénybe vehetett, aki tűzoltóparancsnok vagy vegyész-, építész-, gépészmérnök stb. lehetett. A házban lakók elmondása szintén nyomra vezethetett, őket arra vonatkozóan kellett meghallgatni, hogy az elmúlt napokban ki milyen tevékenységet végzett a házban (volt-e kéményseprés, vásároltak-e gyúlékony anyagot, mivel fűtöttek utoljára stb.). Ha lehet, tisztázni kellett milyen volt a szélirány és melyik napszakban, órában, a ház melyik részében keletkezett a tűz. Az oltás során érzett szagok és a füst színe szintén fontos lehetett.

Ha a tüzet elektromos berendezés okozhatta, más szakértőt (mérnököt, villanyszere-

lőt, mozigépészt) kellett igénybe venni, aki a rövidzárlat tényéről nyilatkozott. Az elektromos berendezések által okozott tüzeknél a vizsgálatot végző csendőr elégett vezetéket, megrongálódott szigetelést és az olvadó biztosíték helyére rögzített drótot vagy szeget keresett. Az ilyen tüzeknél a csendőr a biztosítéktáblát lefoglalta és szakértővel vizsgáltatta meg.

A tűz keletkezési helyének megállapítása érdekében először mindig a sértetlenül maradt helyiségeket kellett átvizsgálni, majd a többi helyiségben szisztematikusan a falakat, padlót, mennyezetet, bútorokat, a bútorok alatti területet, tűzhelyek környékét, a szoba elrendezését, a bútorok helyzetét, az ott tárolt tárgyakat kellett számba venni. A tapasztalatokat összevetni a tanúk és a tűzoltók elmondásaival és a ház körül talált nyomokkal.

Tisztázni kellett az öngyulladás lehetőségét is, különösen a mezőgazdasági épületek égése során. A széna öngyulladásának gyanúja esetén tanúkat kellett kutatni, akik a tűz keletkezésének körülményeit láthatták vagy hallhatták. A mezőgazdasági épület tetejét hirtelen, robbanásszerűen áttörő lángok észlelését az öngyulladás következményének tekintették. A helyszínen ilyenkor azt kellett megvizsgálni, hogy az átszakított tető cserepei merrefelé estek, és a tűz a szénarakás közepén vagy a szélén okozott nagyobb pusztítást. A helyszínre érkező csendőrnek ügyelnie kellett arra, hogy a tüzet oltók „bőséges vizet bocsássanak" a széna közepére, így az oltást követően a szénakazal megbontásával megállapítható volt, hogy valóban belülről terjedt-e a tűz. Ha a kazal megbontása után a vizsgálatot végző csendőr elszenesedett szénát talált hamu nélkül, akkor öngyulladásra kellett következtetnie. A hasonló tüzek megelőzésében is szerepe volt a csendőrjárőrnek, hiszen szolgálata során mezőgazdasági területeken haladt át, és észlelhette a veszélyes szénarakásokat. Ha azt tapasztalta, hogy valahol megsüllyedt tetejű, „kozmás" szagú kazal van, értesítenie kellett a tulajdonost.

Összefoglalás

Az eddig leírtakból logikusan következik, hogy a csendőrségnek eddig kevésbé ismert és publikált feladatköre komoly szakmai tapasztalatot, odafigyelést és a szakterület ismeretanyagának önképzés keretében történő elsajátítását igényelte az állománytól. A feladatrendszer komplexitása és illeszkedése a csendőrségi szervezet általános rendeltetéséhez azonban nyilvánvaló. Összességében tehát elmondható, hogy a Magyar Királyi Csendőrség fennállása során jelentős feladatokat hajtott végre a tűzrendészet területén és a tűzoltóságok általános megszervezéséig sok tekintetben elsőszámú letéteményese volt a vidéki területek tüzekkel szembeni védelmének.

A csendőrség állományának szakmai sokoldalúságára jellemző az is, hogy a Magyar Királyi Csendőrség azon őrsei, melyek területileg az országhatárok közelében feküdtek, minden időben bizonyos határvédő feladatokat is elláttak. Kötelességük volt pl. a határ-

vonal jogosulatlan átlépését, áruk, fegyverek, iratok átcsempészését, állami berendezések, határjelek megrongálását, kémkedést megakadályozni, és kapcsolatot fenntartani a határszéli szolgálatot rendszeresen ellátó szervekkel.

Irodalomjegyzék

[1] Parádi József: *A Magyar Királyi Csendőrség. Az első magyar polgári, központosított, közbiztonsági őrtestület 1881–1945,*. Szemere Bertalan Magyar Rendvédelem-történeti Tudományos Társaság, Budapest, 2012, 281. (HU-ISBN 978 963 08 4794 0); A magyar rendvédelem-történet öröksége, 2. (HU-ISSN 2062-8447)

[2] Komjáthy László, – Dr. Gál László: *Szakmatörténet.* eEgyetemi jegyzet. Nemzeti Közszolgálati Egyetem, 2014, 55.

[3] Komjáthy László, – Dr. Gál László: *Szakmatörténet.* eEgyetemi jegyzet. Nemzeti Közszolgálati Egyetem, 2014, 43–45.

[4] 53.888/1888. BM. A tűzrendészeti kormányrendelet kibocsátásáról, MRT, 22(1888), 1727–1741.

[5] 1936. évi X. törvénycikk a tűzrendészet fejlesztéséről; A tűzrendészeti törvény végrehajtására kiadott 180.000/1936. BM számú rendelet MRT LXX. évf., 1936, 789–920; A m. kir. belügyminiszternek 230.000/1925. BM számú körrendelete a tűzrendészetről alkotott 53.888/1888. BM számú rendelet kiegészítése, módosítása és végrehajtása, MRT, 1925, LIX. évf., 249–259.

[6] A tűzrendészet helyi rendészeti teendő, Szut 82. és 89. §.

[7] A m. kir. belügyminisztériumnak 1869. évi junius hó 17-én 3365. sz. alatt kelt körlevele a Magyar- és Erdélyország összes törvényhatóságaihoz; a tűzrendészeti szabályok kezelése iránt.

[8] Toldy Árpád: A községi tűzrendészetről,. *CSL*, 22(1932)/6, 168–170.

[9] Szervezeti és szolgálati utasítás a Magyar Királyi Csendőrség számára, Pallas, Budapest, 1927, 387, 89. §, 512. pont. Tűzeset, vízáradás és elemi csapás esetén való eljárás, Szut. 312, 11–12. alpontja

[10] *CSL*, 17(1927)/22–24, 730. Szerkesztőségi közlemények: A győri csendőriskola újoncainak tűzoltásban való kiképzése.

[11] Bíró Kálmán: Mikor kell feljelentés helyett jelentést tenni? *CSL*, 1934/10, 290–293.

[12] Posszert Jakab: Tűzesetek nyomozása I. rész,. *CSL*, 20(1930)/14, 430–435.

Fire Protection Duties of the Royal Hungarian Gendarmerie between 1881 and 1945

VEDÓ ATTILA – KOMJÁTHY LÁSZLÓ

The Royal Hungarian Gendarmerie, which was founded in 1881 to ensure public safety in the countryside, was a militarily organised body with international recognition due to its exceptional effectiveness. As regards its services, it was subordinated to the Ministry of Interior but personnel-wise it belonged to the Ministry of Defence. The organisation was responsible for promoting safety of life and property in its area, maintaining peace and public order, preventing violation of laws and regulations, hazards and damages resulting from negligence or omission, restoring order and peace and handing over perpetrators to the competent court or the authorities. However, the body protected the rural population as well as the public and private properties in several other ways as well, including fire protection and enforcing its rules in the countryside,

which has not been studied yet. To grasp this area, it is necessary to be acquainted with the history of national fire legislation, the actual regulations on prevention, firefighting and fire inspection in that period.
Keywords: Gendarmerie, safety, fire, fire protection, countryside

Estók Sándor

Le defi logistique du 21e siecle: Transformation de la logistique horizontale en verticale

La logistique du 21e siècle adopte les principes, les méthodes et les applications acceptées par la science logistique. C'est la vision et la pensée de l'Humanité qui changent et qui dépassent les défis de l'industrie logistique horizontal terrestre. La tension coexistante autour de nous exige du changement et esquisse un nouvel espace et la vision rationnelle d'objectifs mieux définis. C'est ainsi que l'activité logistique se transforme d'horizontale en verticale ; parmi les objectifs de la logistique spatiale apparaissent la conquête de Mars et l'utilisation logistique de la Lune (Estók, 2015) y compris d'en extraire les ressources minérales et de fabriquer et faire fonctionner un réacteur nucléaire sur terre avec l'hélium extrait de la lune. Les possibilités futures du développement de la logistique sont l'apparition des applications logistiques intelligentes dans les chaînes d'approvisionnement, et l'assistance robotique sous surveillance humaine dans les opérations hybrides logistiques.
Mots clés: logistique intelligente, logistique verticale intégrée, infocommunication, espace interactif

Le developpement de la logistique apres le millenaire

Le développement qui a eu lieu après le millénaire a été décisif dans notre monde compétitif. Au niveau des processus logistiques, ainsi que les chaînes d'approvisionnement, l'information est devenue un composant intégré et à part entière avec ses systèmes et instruments dans la vie économique et professionnelle. (Estók 2009) Sa présence et son effet positif a apporté un nouvel élan et encore de meilleurs résultats ; un *environnement logistique intégré* s'est formé, puis *la logistique intelligente (Estók, 2007) et les systèmes des chaînes d'approvisionnement*, qui en sont une formulation plus complète, avec plus de contenu, basée sur *l'intégration et l'information*. Le développement logistique s'est intensifié d'avantage, en créant une nouvelle logistique inter-connectée dans les régions du monde, notamment *l'industrie logistique horizontale.* Cette nouvelle formation logistique a couvert tous les domaines des plus petites entreprises jusqu'à la logistique globale et a pu les orienter vers l'efficacité.

Grâce à la coopération (Pfohl, 2007–2008) et son effet positif sur l'organisation, les chaînes d'approvisionnement *s'organisent en réseaux* de plus en plus vite, qui ensuite se connectent entre eux (*la mise en réseau*). Il ne reste qu'une étape à franchir pour la logistique systématique réseaucentrique contrôlée par l'information.

A partir de 2007 j'ai élaboré en théorie le système logistique civil réseaucentrique, qui attend la continuation. A l'avenir, le plus haut niveau de la formation logistique peut évoluer en pratique; *la logistique réseaucentrique basée sur l'information.* Pendant le temps de ce développement il y a eu de nombreuses nouvelles solutions, mais tout n'est pas encore résolu, quelques questions restent sans réponse. Il faut donc finaliser la solution maintenant.

Le futur proche: *il faudra appliquer dans un environnement cosmique la logistique terrestre horizontale.* Avec l'expansion de l'espace, la dimension du temps n'est plus la même que sur Terre. Les activités de valeur ajoutée de la logistique terrestre se valorisent sans problème dans l'Espace en observant les régularités spéciales liées à la Lune. C'est une étape importante, quand la logistique horizontale devient verticale de façon indispensable et ainsi la logistique systématique réseaucentrique devient une force animatrice dynamique. (Estók, 2015)

La logistique reseaucentrique; le commencement de l'ere operationnelle integree

La première décennie du 21e siècle a apporté un changement important, notamment de nouveaux outils techniques et de nouvelles technologies dans l'environnement logistique, dont l'exploitation suppose des systèmes d'infocommunication développés. J'attache une grande importance au réseau d'infocommunication, qui organise à partir *de l'espace d'information virtuelle, l'acquisition*, l'adaptation, l'utilisation et la conservation de l'information sur l'environnement logistique et tout dépend de cela : la décision élaborée scientifiquement, l'avantage concurrentiel et le profit. (Estók, 2009) Une nouvelle *ère opérationnelle intégrée* est née dans l'environnement d'activités des réseaux logistiques intégrés.

Dans le système réseaucentrique les matières circulent aussi que l'information virtuelle. Pourtant, au niveau des réseaux, des tâches concrètes se réalisent (avec une circulation de matière réelle) sans contact personnel, mais sur la base des coopérations réelles.

Dans le réseau d'infocommunication il y a les gestions des réseaux, qui peuvent être n'importe où physiquement, mais doivent être connectées primairement au réseau d'infocommunication et les gestions d'autres réseaux.

Ce qui demande le plus d'expertise, est *la connexion des réseaux logistiques systématiques d'exécution*. Les systèmes logistiques (des entreprises, des réseaux, des chaînes d'approvisionnement, de petites entreprises, des parcs industriels, des centres de services

logistiques et d'autres organisations qui font partie d'une intégration ou réseau) sont liés à d'autres réseaux de système d'où, selon leurs autorisations de classification, ils peuvent tirer de l'information jusqu'à la mesure définie. Selon leurs compétences, ils peuvent prendre des décisions, organiser des tâches et réaliser leurs propres tâches.

Le réseau de système d'infocommunication a un rôle clé. Tous les systèmes se connectent ici, avec *l'information que chacun organise*, avec les procédés complets des entreprises membres. Je souligne les processus majeurs, les points de jonction, les gestions, qui apparaissent en leur réalité sur le réseau de système. Il est très important de faire voir le procès et les événements logistiques de chaque entreprise sur un réseau informatique clos et chiffré.

Les defis logistiques dans les decennies a venir

Parmi les chercheurs, les experts et les pratiquants de la logistique *la logistique réseaucentrique et centrée sur l'infocommunication* n'est pas largement connue. Le développement qui s'accélère rend indispensable l'amélioration de la qualité logistique, le maintien de la compétitivité et la formation interdisciplinaire des systèmes scientifiquement organisés. La nouvelle ère logistique est là ; la création et l'opération des systèmes logistiques réseaucentriques, scientifiques *intégrés, interactifs et intelligents sont en cours* pour la société à venir.

Pour former les systèmes énumérés il faut réfléchir et décider quelles sont les questions les plus importantes à poser. Le plus important (Estók, 2015) est l'approche d'où l'on peut partir vers le développement. Voilà un raisonnement logique pour formuler les points de départ d'une approche logistique verticale :

1. La logistique horizontale (l'industrie logistique) doit être transformée en logistique verticale,

2. La logistique intégrée et intelligente doit être transformée en logistique interactive,

3. La logistique et la chaîne d'approvisionnement (réseau) qui sont opérationnelles aujourd'hui peuvent être organisées dans une chaîne d'approvisionnement et un réseau verical.

4. A partir des réseaux logistiques on peut créer la logistique systématique réseaucentrique verticale. Cela veut dire cinq éléments de système réseaucentrique.

– Un système de logistique réseaucentrique,
– Un système d'infocommunication réseaucentrique,
– Un système réseaucentrique de capteurs, senseurs, satellites et fusées,
– Un système réseaucentrique des réseaux informatiques,
– Un espace virtuel interactif,

Parmi les cinq systèmes réseaucentriques ce ne sont pas tous les éléments de la logistique que l'on peut rendre vertical, car il y a des régularités relatives au temps qui ont

un effet dans l'environnement terrestre, ce qui, en même temps, peut être résolu dans le système d'information et de communication d'effet multidirectionnel en appliquant de nouvelles solutions ou technologies.

5. A partir d'un système d'information un système réseaucentrique d'infocommunication peut être formulé, organisé d'une façon verticale. Le système d'information existe déjà dans un espace virtuel pour la plupart, et fonctionne dans une direction verticale.

6. Quand au système d'infocommunication réseaucentrique un nouvel élément scientifique a été introduit: l'Information Just In Time, un point clé dans le système d'infocommunication, que je n'ai pas encore traité formellement. Au coeur et au centre du système d'information est ce qui peut avoir accès à l'Information JIT 0-24, et ce sont les partenaires eux-mêmes qui l'utilisent, qui rendent le système plus fort.

7. A partir du processus de synergie, il faut créer la gestion de la synergie, pour diriger tous les systèmes du réseau. Le flux de synergie verticale est viable dans tous les réseaux partenaires ainsi que dans la logistique systématique réseaucentrique.

8. La circulation de trois éléments parmi les plus importants des éléments de la logistique systématique réseaucentrique sont:

– la circulation de la matière,
– la circulation de l'information,
– la circulation des synergies

9. La formation d'un espace interactif se réalise: Quatre dimensions dans l'espace et le cyberespace (espace virtuel)

Sur Terre: Sous et sur l'eau, sur terre, dans l'air, sur les planètes du Système solaire, dans le proche avenir, sur la Lune, et probablement sur Mars à partir de la 4e décennie de notre siècle.

L'espace virtuel interactif fonctionne virtuellement au niveau des quatre dimensions. La réalisation des procès matériaux peut accélérer le flux des matières, les mouvements de nature matérielle, les processus de travail physique, l'expédition, le transport, la comptabilité et l'administration de nature matérielle.

10. Le système d'information et d'infocommunication dans l'espace interactif

– L'information, présente dans tous les réseaux, s'avance du début jusqu'à la fin d'une façon organisée
– L'information est JIT (just in time),
– Le flux d'information, (avec la circulation des matières et des synergies)
– Les informations de la logistique réseaucentrique traversent les réseaux d'infocommunication, et touchent tous les éléments.
– Un centre d'information, qui comprend toutes les informations.
– Les informations des réseaux informatiques, qui sont en temps réel et simultanées dans chacun des réseaux.

Les espaces d'information et les formes d'apparition différentes des réseaux et des sys-

tèmes de réseaux énumérés sont un élément clé dans le réseau logistique. L'espace virtuel se commence ici, ainsi que la transformation vers la direction verticale, dans ces six environnements d'apparition, où l'information est déjà verticale et où les solutions d'infocommunication raccourcissent (dans le temps et l'espace) les procédés relatifs aux matières.

Les correlations de la logistique verticale systematique

Ces 10 critères sont décisifs pour rendre la logistique de système vertical. Tout d'abord, il faut examiner les corrélations horizontales et verticales.

Pour la plupart, l'information circule dans un système vertical, qui a un effet sur le flux de matière ainsi que la gestion. Les gestions logistiques des réseaux sont présentes en tant que des organismes dans le centre d'infocommunication réseaucentrique, d'où elles peuvent suivre, diriger et intervenir dans le fonctionnement de leurs systèmes. C'est un point décisif, le premier domaine des réseaux logistiques, qui peut diriger les réseaux d'une façon verticale. Ainsi, l'environnement vertical est déjà donné (qui est décisif au niveau du système logistique) et des effets verticaux émanent de l'espace virtuel aux flux de matière physique horizontaux. Les informations créées au cours des flux logistiques entrent dans un espace vertical. Le centre d'information est aussi dans un espace virtuel, d'où tout est dirigé à l'aide de la logistique systématique.

L'information JIT est déjà verticale et virtuelle et assure la connexion constante aux partenaires de la logistique réseaucentrique dans l'espace horizontal physique. Chaque chaîne d'approvisionnement, chaque réseau, chaque élément et gestion présents dans le système logistique peut avoir accès à partir de l'espace vertical à 7-8 informations différentes n'importe quand et n'importe où dans le monde.

Dans une période donnée, on peut atteindre une efficacité exponentielle. Le temps est un facteur qui est rendu vertical, au niveau de la compétition, des tâches, de l'efficacité et des résultats, aussi comme une relation de partenariat, ou sous un intervalle beaucoup d'informations traversent les réseaux de partenariat.

Il est très important d'évaluer les informations reçues des quatres dimensions et de l'espace interactif; au niveau physique, l'utilisation de l'information sera de grande intensité, l'efficacité sera d'un grand élan, en augmentant l'intensité et l'opérabilité des systèmes logistiques. Le dialogue interactif et la coopération rendent les résultats exponentiels, l'augmentation et le développement sont détectables. Tout cela déplace l'activité logistique dans une direction verticale d'une façon organisée.

Interactivite, concentration de temps et exponentiation des resultats dans les proces logistiques

Chaque partenaire (et même son représentant) peut utiliser l'interactivité d'un droit subjectif. Chacun peut avoir accès aux informations nécessaires, grâce à l'*Information Just In Time*, et peut les utiliser à plusieurs niveaux, selon ses activités, d'une façon constructive, n'importe quand et à son propre intérêt et de ses partenaires.

Si l'on examine *les corrélations du temps et des activités* dans les procès logistiques, on va percevoir *l'augmentation des résultats*. Ces trois facteurs sont tous liés à l'interactivité et les possibilités de l'espace interactif. Ce qui se passe en réalité est que quand la multitude des tâches, des effets, des informations traversent la chaîne d'approvisionnement ou réseau logistique dans une unité de temps mesurable, le temps devient *concentré* et cette concentration rend le temps vertical, ce qui multiplie, exponentialise l'activité.

Sous un intervalle donné il y a plusieurs activités interactives entre les partenaires, il y a plusieurs tâches, plusieurs objets dans le système ramifié du réseau. En poursuivant cette idée, si le temps devient vertical, plus de tâches peuvent être réalisées et le résultat, donc le profit, augmente d'une façon exponentielle. C'est non seulement le temps qu'il faut rendre vertical, mais aussi la logistique. Il est peu probable, que le temps devienne vertical sans que la logistique le soit. Quand l'efficacité devient constante systématiquement, alors on peut dire que le *procédé logistique est devenu vertical*. Tout cela peut se réaliser si la circulation des matières, de l'information et les synergies sont bien organisées. Aussi, l'activité des gestions influence largement le résultat du procès logistique. Chaque membre du réseau doit bien organiser son activité majeur et diminuer, externaliser les activités superflues ou parallèles. Les sous-systèmes de l'organisation doivent être effectués pas-à-pas, jusqu'à l'étape finale. C'est ici que les possibilités de la synergie peuvent et doivent être effectuées. L'*organisation* relative à la logistique touche *toutes les activités*, ce qui n'est pas une sorte de contrôle, mais plutôt la création de l'harmonie du flux de l'information, des matières et des synergies, d'une façon supportable par des calculs, des capacités, des résultats, etc. Il faut chercher le plus d'harmonie possible des trois flux de la tâche, dans l'espace et le temps.

L'organisation ne peut pas devenir routinière, mais il faut des solutions spécialisées sur la compagnie, qui sont perfectionnées tous les jours et adaptées aux exigences. Il n'y a pas de solution ultime et il y a toujours une meilleure ; le procédé de la perfection continue toujours dans l'avenir.

Selon l'approche verticale, il faut transformer *l'information organisée* en *information Just in Time (JIT)*, et aussi transformer le procédé logistique en *logistique intelligente et interactive* et la placer dans un espace interactif. En même temps, notre 21e siècle force un nouveau *processus de compétition et de réorganisation constante,* où il faut réorganiser *la compagnie/l'entreprise et/ou la chaîne d'approvisionnement*. Ceux qui sont incapables

de remplir cette condition se laissent dépasser et se retrouveront en situation de désavantage concurrentiel. Cependant, ceux qui peuvent se réorganiser constamment, selon les besoins du marché des concurrents, seront compétitifs. Tout cela ne suffit pas encore pour former la logistique réseaucentrique systématique verticale, mais traverser cela requiert un changement qualitatif, qui porte en lui-même les nouvelles connaissances et les changements de contenu.

A chaque niveau, les partenaires doivent disposer des informations, constamment et quand ils en ont besoin, n'importe où ils sont dans le monde. Pour *l'information JIT* logistique sans barrières, il faut le plus haut niveau d'organisation des systèmes d'infocommunication et de logistique réseaucentriques, avec leurs opérations et capacités.

Synthese

Le procédé logistique systématique réseaucentrique peut être rendu vertical par la concentration des effets et variations différentes de l'information. Il est décisif, que les effets cardinaux arrivent d'un espace virtuel vertical dans un flux de matières horizontal. Pourtant, les informations qui apparaissent ici, sont verticales. L'information JIT transmet des informations verticales aux partenaires dans l'espace horizontal et vertical. L'information et l'infocommunication co-existent dans le temps, sous chaque forme. L'information qui vient des quatre dimensions et de l'espace interactif sera de grande intensité au niveau physique et elle augmentera l'opérabilité des systèmes logistiques, exponentialise ses résultats. Dans une unité de temps, il peut y avoir plusieurs activités interactives. Les partenaires sont en coopération au niveau des tâches, des objets, des réseaux dans les systèmes ramifiés. Le temps devient vertical ainsi que la logistique. L'organisation centrée sur la logistique touche toutes les activités dans les systèmes. L'information organisée devient information JIT, ainsi tous les partenaires y auront accès dans le réseau, ce qui améliore le fonctionnement des systèmes. L'Information Just In Time, un point clé dans le système d'infocommunication, que je n'ai pas encore traité formellement. Au coeur et au centre du système d'information est ce qui peut avoir accès à l'Information JIT 0-24, et ce sont les partenaires eux-mêmes qui l'utilisent, qui rendent le système plus fort.

Je pense que cette solution d'organiser la logistique verticale signifie une nouvelle qualité logistique, qui crée et fait fonctionner une logistique systématique scientifique, interdisciplinaire, intégrée, intelligente et interactive. La synergie apparaît également dans ce système, qui est élevée à un niveau stratégique, et a sa propre gestion à tous les niveaux dans les systèmes réseaucentriques.

Bibliographie

[1] Estók S.: Hálózatközpontú integrált interdiszciplináris logisztika (Logistique réseaucentrique interdisciplinaire intégrée),. *Bolyai Szemle*, 2009/3.
[2] Estók S.: Intelligens logisztika digitális környezetben (Logistique intelligente dans l'environnement digital),. *Tranzit*, novembre, 2007.
[3] Estók S.: Kozmikus ellátási lánc a Föld és a Hold között (La châine d'approvisionnement cosmique entre la Lune et la Terre),. *Hadtudományi Szemle (online)*, 1(2015)/1.
[4] Haig Zs.: *Hadviselés az információs hadszíntéren (Guerre sur le champ de bataille de l'information.)*, 2005.
[5] Estók S.: A XXI. század logisztikai kihívásai, trendjei és lehetőségei. *Logisztika. Trendek és legjobb gyakorlat*, 1(2015. ápr.)/1, 35–38. (HU ISSN 2416-0555)
[6] Pfohl, H. C.: *Hálózatok együttműködésének alapjai (Les bases de la coopération des réseaux)*,. Logisztikai Évkönyv 2007–2008, Magyar Logisztikai Egyesület.

The logistic challenge of the 21st century: transforming horizontal logistics to vertical

Estók Sándor

The logistics of the 21st century adapt the principles, methods and applications accepted by the science of logistics. It is the vision, the approach and thinking of Mankind that changes and surpasses the challenges of terrestrial horizontal logistics. The tension coexisting around us demands change and a rational vision of well-defined objectives. This is how logistic activity transforms horizontal logistics into vertical ; among the objectives of space logistics the conquest of Mars and the logistic use of the Moon appear (Estók, 2015), including the extraction of its mineral resources and the setting up and operation of a nuclear fusion reactor on Earth, with the Helium extracted on the Moon. The future possibilities of the development of logistics are the introduction of smart logistic applications to supply chains and the robotic assistance under human supervision in hybrid logistic operations.
Keywords: intelligent logistics, integrated, vertical logistics, infocommunication, interactive space

A XXI. század logisztikai kihívása: a horizontális logisztika vertikálissá alakítása

Estók Sándor

A 21. század logisztikája vallja a logisztikatudomány által elfogadott elveket, módszereket és alkalmazásokat. Az emberiség világlátása, szemlélete és gondolkodása változik, már túl van a földi horizontális logisztikai ipar kihívásain. A körülöttük és velük élő, változást követelő feszítő erő új teret és határozott célok racionális jövőképét rajzolta meg. Így érkezett el a logisztikai tevékenység a horizontális logisztika vertikálissá tételéhez, az

űrlogisztikai célok között a Mars meghódításához és a Hold logisztikai hasznosításához (Estók, 2015), ásványi kincsei kitermeléséhez, a nukleáris magfúziós reaktor elkészítéséhez és működtetéséhez a Földön a kibányászott héliumból. A logisztika fejlesztésének jövőbeli lehetősége az okos logisztikai alkalmazások megjelenése az ellátási láncokban, valamint a robotok közreműködése emberi felügyelet mellett a hibrid logisztikai műveletekben.

Kulcsszavak: intelligens logisztika, integrált, vertikális logisztika, infokommunikáció, interaktív tér