HADMÉRNÖK

Katonai műszaki tudományok
on-line

XII. évf. 4. szám – 2017. december

A szerkesztőség / Editorial office:

Nemzeti Közszolgálati Egyetem
1101. Budapest, Hungária krt. 9-11.
Postacím: 1581. Budapest Pf.:15.
„A." épület 9. emelet, 901. iroda
Telefon: +36-1-432-9000 /29-289/ Fax: +36-1-432-9025
e-mail: hadmernok@uni-nke.hu
web: http://hadmernok.hu

Kiadó / Publisher :

Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
National University of Public Service; Faculty of Military Science and Officer Training

ISSN 1788-1919

Jelen számban megjelent írások szerzői / Authors of the Current Issue:

Beke Éva – Óbudai Egyetem, KGK, ügyvivő szakértő
Csősz László – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Dobor József – Nemzeti Közszolgálati Egyetem, KI, adjunktus
Dr. habil. Endrődi István – Nemzeti Közszolgálati Egyetem, KI, egyetemi docens
Gémes Csaba – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. habil. Gyarmati József – Nemzeti Közszolgálati Egyetem, HHK, egyetemi docens
Dr. Gyulai Gábor
Hegedüs Ernő – Nemzeti Közszolgálati Egyetem, HHK, oktató
Kadëna Esmeralda – Óbudai Egyetem, BDI doktorandusz
Dr. Kaló József – Nemzeti Közszolgálati Egyetem, HHK, egyetemi docens
Dr. Kollár Csaba – Szent István Egyetem, GTK, adjunktus
Kossa György – Inter-Tan Ker Zrt.
Dr. habil. Kovács Tibor – Óbudai Egyetem, BGK egyetemi docens
Kui László – Nemzeti Közszolgálati Egyetem, RDI doktorandusz
Kuk Enikő Eszter – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Kuti Rajmund – Széchenyi István Egyetem, MÉK, adjunktus
Lakatos József – Óbudai Egyetem, BDI doktorandusz
Lányi Márton – Óbudai Egyetem, BDI doktorandusz
Menyhárt József – Óbudai Egyetem, BDI doktorandusz
Mies Gereald – Óbudai Egyetem, BDI doktorandusz
Nguyen Huu Phuoc Dai – Óbudai Egyetem, BDI doktorandusz
Nyikes Zoltán – Óbudai Egyetem, BDI doktorandusz
Dr. Pántya Péter – Nemzeti Közszolgálati Egyetem, KI, adjunktus
Prof. Dr. Pátzay György – Nemzeti Közszolgálati Egyetem, KI, egyetemi tanár
Plébán J. Kristóf – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Prof. Dr. Pokorádi László – Óbudai Egyetem, BGK egyetemi tanár
Prof. Dr. Rajnai Zoltán – Óbudai Egyetem, BGK egyetemi tanár
Somosi Vilmos – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Prof. Dr. Szabolcsi Róbert – Óbudai Egyetem, BGK egyetemi tanár
Szökrény Zoltán – Nemzeti Közszolgálati Egyetem, HHK, tanársegéd
Dr. Tóth András – Nemzeti Közszolgálati Egyetem, HHK, adjunktus
Dr. Tóth Bence – Nemzeti Közszolgálati Egyetem, HHK, adjunktus
Dr. Vég Róbert László – Nemzeti Közszolgálati Egyetem, HHK, egyetemi docens
Dr. Zentay Peter – Budapesti Műszaki Egyetem, GTK, egyetemi docens

TARTALOMJEGYZÉK

Védelmi elektronika, informatika, kommunikáció

Fórum

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

A 4. IPARI FORRADALOM VÁRHATÓ HATÁSA A BIZTONSÁGIRÁNYÍTÁSRA

THE EXPECTED EFFECT OF THE 4TH INDUSTRIAL REVOLUTION ON THE SAFETY MANAGEMENT

LAKATOS József

(ORCID: 0000-0001-7396-3295)

lakatosjozsef@outlook.com

Absztrakt

A vállalkozások által működtetett menedzsmentrendszereknek alapkövetelménye a folyamatos fejlesztés. Ilyen fejlesztési irány a 4. ipari forradalom zászlóshajójaként emlegetett Ipar 4.0. Ez a kutatási program vizsgálja, hogy milyen jövőbe mutató, innovatív technológiai megoldások állnak rendelkezésre ahhoz, hogy hatékonyan növelhető legyen a termelékenység, csökkenthető legyen a gyártások biztonsági kockázata, minimalizálható legyen a technológiákban használt gépek, berendezések meghibásodásából adódó termeléskiesés és veszélyhelyzet. Az Ipar 4.0-val együtt járó szemléletváltás hatással lesz a veszélyes technológiákat működtető vállalatok biztonságirányítási rendszerére is, egyúttal újabb fejlesztési irányokat indikál a vállalkozás szervezetének struktúrájában.

Kulcsszavak: *ipari forradalom, Ipar 4.0, biztonságirányítás, innovatív megoldások*

Abstract

The continuous development is a basic requirement for the management systems of the enterprises. The Industry 4.0 known as the flagship of the 4th industrial revolution is a kind of development direction. This research program examines what kind of future-oriented, innovative technological solutions are available to effectively increase the productivity, reduce the safety risks of the production, and minimize the production losses and emergency situations caused by machines and equipment failures. The change of approach associated with Industry 4.0 will also impact on the safety management system of the companies that operate dangerous technologies, while pointing to new development directions in the organization of the enterprise.

Keywords: *industrial revolution, Industry 4.0, safety management, innovative solutions*

A kézirat benyújtásának dátuma (Date of the submission): 2017.06.20.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.06.26.

BEVEZETÉS

Az egyre speciálisabb vevői elképzelések és elvárások teljesítéséhez a mai vállalkozásoknak fejlesztési irányokban kell gondolkodniuk. Fejleszteni szükséges az alkalmazott technológiai megoldásokat, optimalizálni kell az alapanyag és energiafelhasználásokat, ehhez új innovatív megoldásokra van szükség. Kérdés, hogy ezek az innovatív megoldások alkalmazhatók e minden ipari szektorban? Ha alkalmazhatók, akkor a szektor mely elemeiben és milyen hatékonysággal? A veszélyes anyagokat gyártó és felhasználó vállalkozások is ki tudják használni ennek előnyeit? Sok kérdés fogalmazódik meg amikor egy olyan, még nem bevezetett megoldás elvi alkalmazhatóságáról beszélünk, ami elindította a 4. ipari forradalmat.

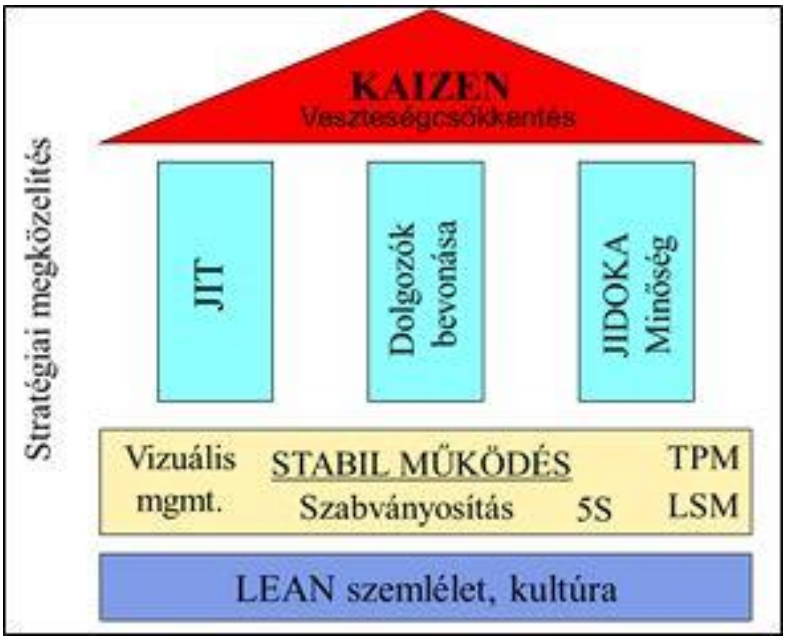
Az ipari tapasztalatok azt mutatják, hogy a továbbiakban egyre kevésbé lesz fenntartható az energiafogyasztás, általában az erőforrás-felhasználás eddigi gyakorlata, ami a termelésnek is korlátot szabhat. Ez a felismerés hívta életre az Ipar 4.0-t, amely jövőbe mutató kutatási projektként azt vizsgálja, hogy az információs technológiának milyen pozitív hatásai lehetnek az ipar működésére.

A versenyképesség növelésén kívül vizsgálni szükséges azt is, hogy az új megoldásoknak milyen hatása várható a biztonságos működés szempontjából, pontosan mi az ami szavatolja egy veszélyes tevékenységet folytató vállalkozás technológiai rendszereinek biztonságát, hogyan építhető ez be a vállalkozás folyamatszabályozási rendszerébe. [1]

MINŐSÉGMENEDZSMENT A BIZTONSÁGIRÁNYÍTÁSBAN

A különböző minőségügyi technikák már régóta alkalmazott hatékonyságnövelő eszközök akár egy veszélyes anyagokat gyártó és feldolgozó vállalkozás esetében is. Ezeket az eszközöket részben vagy egészben beépítették a vállalkozás menedzsment rendszereibe. A Lean filozófia megjelenése és alkalmazása a vegyiparban egyértelműen igazolta, hogy a társaságok milyen hatékonyan tudják alkalmazni ezeket a technikákat a biztonsági teljesítményük növelésére. Hogyan értelmezhető ez a filozófia a negyedik ipari forradalom kapujában?

A Lean menedzsment, mint a Toyota gyártási rendszerén alapuló menedzsmentrendszer középpontjában az ember, az emberek bevonása áll. Ennek a rendszernek a két fő pillére a JIT és a JIDOKA (1. ábra). A JIT filozófia azt jelenti, hogy a megfelelő anyag, a megfelelő helyen, minőségben és időben álljon rendelkezésre. A JIDOKA pedig japánul annyit jelent körülbelül, hogy automatizálás + ember. Azaz, hogy az automatizálás (IPAR 4.0) és az emberi munkavégzés nem alternatívái, hanem kiegészítői egymásnak. Azért automatizálunk, hogy az embereket tehermentesítsük az alacsonyabb hozzáadott értékű munkától, és felszabaduljanak, hogy nagyobb hozzáadott értékű munkát (felügyelet, karbantartás, beállítás, fejlesztés, problémamegoldás) végezzenek. [2]



1. ábra A Lean szemlélet kivetülése a vállalat működésében *[Forrás: Kvalikon]*

IPAR 4.0 – HATÉKONY, BIZTONSÁGOS TERMELÉS, DE HOGYAN?

Az Ipar 4.0-t a gyártás digitalizációjával, az automatizálás térhódításával is jellemzik. A Lean menedzsmenttel is összefüggésbe hozzák, ugyanis az Ipar 4.0 megoldásai összhangban vannak a Lean elvekkel, a folyamatos javítást pedig a digitalizáció, az előrejelző rendszerek kialakítása teszi lehetővé. Az Ipar 4.0-tól a termelési hatékonyság megnövekedését várják, ezzel:

- fokozódhat a termelés tervezés, -irányítás, logisztika automatizálása,
- szükségessé válik nagyobb fokú automatizálás előtt a folyamatok optimalizálása,
- fókuszba kerülnek a munkatársakkal szemben támasztott követelmények a képzést és a változásokra való képességet illetően. [3]

Az Ipar 4.0-val kapcsolatos lehetőségek feltárására, annak az egyes ipari szektorokban való használhatóságára, az elképzelések megvalósításának szektorspecifikussá tételére a Magyarország Kormányának támogatásával létrejött az Ipar 4.0 Nemzeti Technológiai Platform. A Platform 7 munkacsoportja dolgozik azon, hogy a magyar iparlehetőségeit felmérve célok fogalmazódhassanak meg a 4. ipari forradalommal együtt járó technológiai kihívásokhoz való felzárkózáshoz. [4]

Hogyan kapcsolódik mindez a biztonságos üzemmenethez, technológiai biztonsághoz? Vajon tényleg alkalmazhatók és testre szabhatók az Ipar 4.0 által kínált megoldások minden iparág számára? Amikor robottechnológiákról, gyártásszimulációs modellekről hallunk, elég nehéz például a vegyipari szektorra gondolni. Mégis, a már előzőekben előrevetített hasznok, mindenképp a biztonság irányába mutatnak a termelés hatékonyságának növelése mellett. A speciális ipari szektorokban működtett biztonságirányítási követelményeket a termelési hatékonyság növelésére megfogalmazott céloknál mindig figyelembe kell venni.

Nem lenne ez másképp az Ipar 4.0 által kínált megoldások bevezetésénél sem. Ugyanis a vállalkozás, például a veszélyes technológiák üzemeltetője figyelmet fordít a berendezésekben, a tárolóeszközökben és a gyártásban végrehajtott változtatásokra. E változtatásoknak a biztonságra vonatkozó vetületeit már a változtatások tervezése és kivitelezése során előzetesen figyelembe veszi. A termeléssel kapcsolatos biztonsági, illetve termelékenységi problémák megelőzésével kapcsolatosan kitűzött célok elérésének

folyamatos vizsgálata érdekében módszereket dolgoz ki. A feladatok végrehajtásának helyzetét folyamatosan értékeli, a hiányosságokat feltárja, és kialakítja az azok kiküszöböléséhez szükséges megoldásokat. [5]

Ha az Ipar 4.0 megoldásainak bevezetését egy folyamatban akarjuk elképzelni az alábbiakra gondolhatunk, előtérbe helyezve a biztonsági szempontokat (2. ábra).

2. ábra Az Ipar 4.0 megoldások bevezetése a termelési tevékenységbe (készítette: a szerző)

A különböző ipari szektorokban való Ipar 4.0 automatizálási megoldások kellő biztonsággal történő bevezetéséhez fel kell mérni az adott vállalkozás tevékenységének, technológiáinak jelenlegi állapotát és meg kell határozni azokat a lehetséges pontokat, ahol a digitalizáció, az automatizálás növelheti a biztonsági és termelékenységi színvonalat és csökkentheti a kockázatokat.

A fejleszthető technológiai pontok felmérése után megvalósíthatósági tanulmányt kell készíteni az automatizálási lehetőségekről. Ennek az előzetes felmérésnek tartalmaznia kell a megvalósításhoz szükséges költség- és erőforrásokat, pontos adatokat, információkat a megtérülést és hasznot illetően, valamint itt szükséges előrevetíteni a még ránk váró feladatokat a bevezetni kívánt megoldással kapcsolatban.

Az új megoldás bevezetése a termelése mindenképpen változást jelent, ezért ezt ennek megfelelően kell kezelni. Felül kell vizsgálni a fejleszteni kívánt technológiai pontok működési-, biztonsági kockázatait, bár egy fejlesztő megoldástól mindig a kockázatok csökkenését várjuk, azért nem árt részletesen átvizsgálni, a rendelkezésre álló módszerek alkalmazásával. Az így rendelkezésre álló információk birtokában, az új megoldás bevezetéséhez szükséges döntés meghozható.

Minden új megoldás bevezetése különösen, ha az egy veszélyes technológiát érint, a működtetett biztonságirányítási rendszer vonatkozó szintjein is leképeződik. A változásokat rendszerbe kell illeszteni, ehhez kell igazítani a vonatkozó utasításokat, előírásokat, meg kell

határozni a munkavállalók esetleges új szerepét az egyes technológiák működtetésében (mechanikus feladatok helyett, pl. figyelemmel kísérés) és a bevezetés előtt erről tájékoztatni, képezni kell az érintett munkavállalókat.

A megvalósítás során hatékony projektmenedzsment működtetésével kísérhető figyelemmel a folyamat, és a beruházás mértékétől függően folyamatos tervegyeztetés szükséges a tervező és kivitelező szakemberekkel.

A megoldások bevezetése, próbaüzeme előtt fontos meghatározni, hogy a technológiát működtető személyzet közül ki az a felelős, aki figyelemmel kíséri az új automatizált technológiai megoldás működésének hatékonyságát.

A működés tapasztalatait az előre meghatározott időperiódus után értékelni kell, majd végleges alkalmazásba vétele megtörténhet. Ha további fejlesztő automatizálási megoldásra adódik lehetőség, vagy válik szükségessé a folyamat elölről kezdődik.

Fenti folyamat annak szemléltetésére készült, hogy az Ipar 4.0 által kínált jövőbe mutató, fejlesztő megoldásoknak meg van a helye a vállalkozás biztonságirányítási rendszerében, hiszen minden fejlesztő megoldás bevezetésének van valamilyen hatékonyság növelő vagy kockázatcsökkentő hatása. Így teremthetünk értéket és strukturálhatjuk át a vállalkozás szervezeti egységeinek feladatait magasabb szintre a Lean filozófia alkalmazásával.

MÁR MEGVALÓSULT IPAR 4.0 MEGOLDÁSOK

A 4. ipari forradalom úttörői mertek nagyot álmodni, amikor olyan megoldásokat kezdtek alkalmazni, ami eddig a technikai színvonal hiánya miatt nem volt lehetséges, vagy túl kockázatos lett volna. Alábbiakban a teljesség igénye nélkül néhány példa szemlélteti az automatizált megoldások hatékonyságát.

Avatarok az olajiparban. Ilyen volt az olajiparban a Total E&P megoldása, amikor is virtuálisan, 3D-ben előre felépítette az angolai partokhoz tervezett Pazflor úszó platformját (FPSO, Floating Production, Storage and Offloading unit), s ezen képezte ki a személyzetet. Ezáltal a cég a tervezetthez képest két hónappal előre hozta a kitermelés megkezdését.

Prediktív alkatrészrendelés. A vizualizáció csak egy kiegészítő funkció ahhoz, hogy egy adott telephelyről begyűjtött információ minden érintett számára elérhető legyen, és ennek alapján a helyszíntől távol lehessen dönteni a szükséges beavatkozásról. Prediktív elemzéssel meg is lehet előzni a hibákat. A rendszer meghatározza a karbantartás idejét, és előre megrendeli az alkatrészeket is. A Wingas kombinált hő- és villamos (CHP) erőműve a németországi Lubminban már így tervezi meg a karbantartást. [3]

Előrejelző karbantartás. A Schaeffler 2016-ban mutatta be a lehetséges hibák szöveges kijelzésével működő, egyszerű beépítésre kész ellenőrző rendszer telepítésének és üzembe helyezésének rendszerét. A korai figyelmeztető rendszer egy érzékelő egységből, egy érintőképernyős kocka alakú házból valamint az áramellátáshoz és adatátvitelhez szükséges kábelből áll. Kifejezetten elektromotorok, szivattyúk, ventillátorok és azok gördülőcsapágyai rendellenességeinek felismerésére lett kifejlesztve és a gyár által készre konfigurálva. A monitoring rendszer összesen öt hibát tud azonosítani és a képernyőn megjeleníteni: csapágyhibát, kiegyensúlyozatlanságot, súrlódást/kavitációt (centrifugál szivattyúknál), hőmérsékletemelkedéseket valamint minden olyan általános elváltozást a rezgésmintákban, amelyek nem rendelhetőek egyértelműen hozzá valamelyik előbb említett hibához és további elemzések elvégzését teszik szükségessé. [6,7]

Jelen példák igazolják az Ipar 4.0 megoldásainak hatékonyságnövelő valamint biztonsági kockázatokat csökkentő hatásait, hiszen például az előrejelző karbantartás alkalmazásával szivattyúk, ventilátorok üzembiztonsága szavatolható, a meghibásodásokból adódó termeléskiesések, valamint a technológiai rendszerből való veszélyes anyag kijutások lehetőségét minimálisra csökkentve. A prediktív alkatrészrendeléssel a berendezések műszaki-biztonsági paramétereinek tudatában meghatározott karbantartási periódus

figyelembevételételével akár fölösleges üzemleállításoktól óvhatja meg magát az üzemeltető. Ezen megoldások hasznát nem szükséges bizonygatni, azonban a helyüket meg kell találni a vállalkozás menedzsment rendszereiben és hozzá kell rendelni a szükséges forrásokat.

KÖVETKEZTETÉSEK

Az Ipar 4.0 megoldásai egy új dimenziót nyitnak meg a termelés hatékonyságának növelésében, azonban jelen pillanatban biztonságtechnikai vonatkozásai, haszna még nincs kellőképpen hangsúlyozva. Alaposabban megvizsgálva az Ipar 4.0 célkitűzéseit és a már megvalósult megoldások biztonságtechnikai vonatkozásait is, egyértelművé válik, hogy az irányítási rendszerek, célkitűzéseit, tükrözi vissza. Az irányítási rendszerbe való illesztése, elkötelezettségként fogalmazható meg a folyamatos fejlesztés iránt, a Lean gondolkodásmód alkalmazásával. A biztonságirányításra való hatása általánosságban biztonsági kockázatokat csökkentő kell legyen, de ennek megállapítására a biztonsági kockázatok felülvizsgálata szükséges, hiszen a szervezet és személyzet feladat és hatáskörei is megváltozhatnak egy-egy új megoldás bevezetésénél.

Előbbiek figyelembevételével, az Ipar 4.0 által kínált megoldások kis léptékben való bevezetésével, biztonságirányítási rendszerünk egy folyamatosan fejlesztett, hatékonyan működő rendszer lesz, amire jellemző, hogy folyamatközpontú, mert folyamatokban gondolkodik, emberközpontú, mert a minden intézkedésnél a biztonságnak van prioritása a termelékenység mellett, hosszú távon gondolkodó, mert úgy építi ki a folyamatait, hogy az alkalmazott műszaki megoldásokkal, megelőző intézkedésekkel zavartalanul működhessen, mindenki részt vesz benne, mert számításba veszi a felelősségi és hatásköröket, valamint megfelelő kommunikációt folytat, folyamatosan, kis lépésekben javít, amely során felismeri problémákat és priorizál, amivel veszteséget csökkent és közelebb kerül a KAIZEN megvalósításához.

FELHASZNÁLT IRODALOM

[1] KIS E.: Ipar 4.0 – A jövő gyára, Gyártástrend, 2013. április 14. URL.: http://gyartastrend.hu/informatika/cikk/ipar_4_0__a_jovo_gyara (letöltés: 2017.06.06)

[2] Gyártástrend. Versenyképesség, de hogyan? URL.: http://gyartastrend.hu/esemenyek/cikk/versenykepesseg__de_hogyan (letöltve: 2017.06.06)

[3] Controlling portal. Ipar 4.0 megoldások. URL.: http://www.controllingportal.hu/ipar-4-0-megoldasok/ (letöltve: 2017.06.06)

[4] Ipar 4.0. https://www.i40platform.hu/ (letöltve: 2017.06.06)

[5] KÁTAI-URBÁN L., VASS G., SIBALINNÉ FEKETE K.: Establishment and Implementation of Hungarian system for critical infrastructure protection. In: Andrea Peterkova (szerk.). Riešenie krízových situácií v špecifickom prostredí: 19. medzinárodná vedecká konferencia, 21.-22.máj 2014, Žilina : zborník. 1. část. 264 p. Konferencia helye, ideje: Zilina, Szlovákia, 2014.05.21-2014.05.22. Zilina: Žilinská univerzita v Žiline, 2014. pp. 353-360. (ISBN:978-80-554-0872-9)

[6] Techstory. Előrejelző karbantartás 4-0. URL.: http://www.techstorym2m.hu/elorejelzo-karbantartas-4-0.html (letöltve: 2017.06.06)

[7] E., ANCZA, M., BAKOSNÉ DIÓSZEGI, M., HORVÁTH: Hydrodynamic Cavitation Device that Makes Straw Cuts Suitable for Efficient Biogas Production APPLIED MECHANICS AND MATERIALS 564: pp. 572-576. (2014)

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

ÁRUFUVAROZÓI VÁLLALATMÉRET HATÁSA AZ ÁRUBIZTONSÁGRA

INFLUENCE OF TRANSPORTER COMPANY SIZE ON CARGO SECURITY

LÁNYI Márton

(ORCID: 0000-0001-8867-0292)

mlanyi@freemail.hu

Absztrakt

A cikk célja felmérni a Magyarországon tevékenykedő közúti fuvarozók biztonságtudatossági szintjét. A téma minden eddiginél aktuálisabb, hiszen a magyar külkereskedelem jelentős része Európán belül zajlik. A közúti szállítások részaránya folyamatosan növekszik a vasúti szállításhoz képest. Ebből következik, hogy a legtöbb áru közúton jut el a célállomásra. Európában, az egy évben közúti szállítás közben árubiztonsági kérdéskörrel összefüggésbe hozható kár Euro milliós nagyságrendűre nőtt. A cikk rámutat a biztonságtudatosság kialakulásának alapvető összefüggéseire, legyen az vállalatméret, korábbi tapasztalat vagy egy megrendelő nagyvállalat rendszer szemléletű logisztikai stratégiája. Jelen cikk a kutatás második részének bemutatása.

Kulcsszavak: *biztonságtudatosság, felmérés, fuvarozás, logisztika*

Abstract

The purpose of the article is to measure the security awareness level of the road carriers acting in the Hungarian market. The topic is getting very actual as the largest portion of the Hungarian foreign trade is handled within Europe. The proportion of the road haulage in relation to the rail freight volumes is getting higher. Based on these facts it is obvious that most of the shipments in foreign trade are travelling on road. The claims caused by security incidents during road transportation in Europe rose to Euro millions per year. The article deals with basic questions and correspondences of the evolving security awareness that can be a result of an earlier experience, the size of the company or a customer with a systemized logistics approach strategy. This article is the next issue of a two-part publication.

Keywords: *security awareness, carrier, measurement, logistics*

A kézirat benyújtásának dátuma (Date of the submission): 2017.07.10.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.01.

BEVEZETÉS

A Magyarországon tevékenykedő közúti fuvarozók biztonságtudatossági szintjének felmérése minden eddiginél aktuálisabb, hiszen a magyar külkereskedelem jelentős része Európán belül zajlik. A közúti szállítások részaránya folyamatosan növekszik a vasúti szállításhoz képest. Ebből következik, hogy a legtöbb áru közúton jut el a célállomásra. Európában az egy évben közúti szállítás közben árubiztonsági kérdéskörrel összefüggésbe hozható kár Euro milliós nagyságrendűre nőtt [1]. Korábbi kutatási eredményeim [2] rámutattak, hogy a biztonságtudatosság nem egy homogén tényező, megjelenése és mélysége függ a vállalat méretétől. Ebben a cikkben ismertetem a vonatkozó szakirodalmat és az eddig elvégzett kutatási munka végeredményét. A biztonságtudatosság mérési kutatásom első részének eredményeit alapul véve további vizsgálatokat végeztem a hazai fuvarozók körében. A kutatás elmélyítése mellett azért döntöttem, mert az eredmények új megvilágításba helyezték a vizsgált vállalatok biztonsághoz, mint alapértékhez fűződő viszonyát. A felmérésem első része a megkötött biztosítások feltételeivel és az azokban tükröződő biztonságtudatosság kialakulásának viszonyrendszerével foglalkozott. Összefüggést találtam a vállalatméret és a biztonságtudatossági szint között. Ez alapján a kisebb járműparkot üzemeltetők (1-es és 2-es csoport) kevesebb tudatossággal rendelkeznek, mint nagyobb versenytársaik. Az interjúk megerősítették azt a feltevést, hogy e vállalkozások többnyire nem is feltételezik egy biztonsági esemény bekövetkeztét, vagy könnyelműen bíznak annak elmaradásában. Erre a tényre mutat rá, hogy nem rendelkeznek megfelelő biztosítással sem. [2]

Az 1-2 járművel rendelkezők esetében az egzisztencia vizsgálatok 47%-ban negatív eredményre jutottak, ennek magyarázata a kis vállalatméretben keresendő, működésük még nem vállalatszerű. Az interjúk során kialakult kép, hogy ebbe a csoportba tartozó vállalkozók jellemzően korábbi gépkocsivezetők, csekély menedzsment ismerettel rendelkeznek.[2]

További kutatásokat végzek a témában annak megállapítására, hogy a biztonságtudatosság kialakulásának vannak-e további feltételei. Feltételezem, hogy nő a tudatosság egy elszenvedett bűncselekmény hatására, illetve vevői nyomásra. Jelen cikknek továbbiakban része annak a tudástranszfernek a mérése melyet a megbízó vállalatok nyújtanak a fuvarozóknak.

Kutatásom tehát a fuvarozók biztonság tudatosságának a vizsgálata irányul. Pontosabban arra, hogy mennyire jelenik meg folyamataikban, illetve a biztonságtechnikai eszközök alkalmazásában a biztonság, mint alapérték. Célom, hogy több szempontból is igazoljam a hipotézist, miszerint a fuvarozók biztonsági szempontból nem képeznek homogén egységet, azok egyes ismérvek alapján jól profilozhatóak. A profilok alapján egyszerűsödik azok menedzsmentje a várható biztonsági kockázatok körülhatárolásának következtében. Tágabb értelemben véve az ellátási láncok megbízhatóságának egyik alapvető tényezője a fuvarozó által nyújtott biztonság. A kérdés tehát nem csak az árubiztonsági, hanem az annál szélesebb körű, ellátás biztonsági területet is érinti. Ebben a megközelítésben egy fuvarozó értékét nem az általa nyújtott alapszolgáltatások, hanem a megbízhatósága testesíti meg.

Szakirodalmi áttekintés

A hazai közúti fuvarozók biztonságtudatossági vizsgálatára mindeddig, tudomásom szerint, nem került sor. Kutatásom alapján, a fuvarozók viselkedésnormáit feltáró, tudományos szintű eredmények hiányoznak a szakirodalomból. Közúti fuvarozás témakörével is csak néhány hazai kutatás foglalkozik [3], ahol részletes elemzést találhatunk a fuvarozásra ható legújabb trendek eredményeként. A vizsgált területtel határos logisztikai alrendszerek kutatása széleskörűen megvalósult. Ezek közül a legfontosabbak az ellátási lánc menedzsment elméleti és gyakorlati kérdéseivel foglalkozó kutatások [4;5;6;7;8;9], melyek egyes, alvállalkozói kiválasztással és értékeléssel foglalkozó részei relevánsnak tekinthetőek a tárgyalt téma

tekintetében. Ványi 2012-ben publikált irodalmi áttekintése [10] és összefoglalója az ellátási láncon belüli kapcsolatokra összpontosít. Hasonlóképpen tett Karmazin 2014-ben a logisztikai szolgáltatók tekintetében 11]. További, kutatásom számára releváns terület a hazai vállalatok innovációs és fejlesztési kérdéseinek vizsgált aspektusai [12;13;14]. Bokor [15] a megbízhatóságot kiválasztási kritériumként definiálta, amely indirekt módon tartalmazza a biztonságot, mint alapvető értéket. Tanulmánya következtetéseket von le a közúti árufuvarozás tekintetében és rendszerezi a kiválasztási kritériumokat fuvarozási módonként. Alapvető következtetése, hogy a közúti fuvarozás részaránya tovább bővül a belátható időtávon belül. Bank [16] más megközelítést használt, mikor a várható trendekről előrejelzést készített, magyar fuvarozók profitabilitás-vizsgálatán keresztül. A fuvarozókon túl a logisztikai szolgáltatókról is készültek tanulmányok a közelmúltban [11;17].

Nemzetközi szinten, a téma szempontjából az egyes biztonsági kérdéseket érintő kutatások relevánsak. Legutóbbi vizsgálat a közlekedési ipar biztonsági kultúrájával foglalkozik [18]. Több tanulmány irányul az alvállalkozói kiválasztás és értékelés kritériumrendszerére, melyekben a biztonság, mint alapérték újból megjelenik [19]. A humán erőforrás rendszereken belüli toborzás és a szelekció során a (személyes) kompetenciák, személyiségjegyek így a biztonságra törekvés is óriási szerepet kapnak [20]. Az ellátási lánc biztonság keretein belül a tudatosság, mint a kockázat-menedzsment fontos eleme jelenik meg. Eljárásokat és rendszerezett méréseket alakítottak ki a megfelelő biztonsági terv kialakítására [21]. További kutatók foglalkoztak a biztonsági kultúra hatásával a biztonsági tevékenységek operatív teljesítményére [22].

A mélyebb biztonságtudatossági kutatások hiánya arra késztetett, hogy magam végezek el egy szekunder kutatást a magyar közúti fuvarozók körében. Eredeti hipotézisem alapja az előzőekben tárgyalt biztonságtudatossági heterogenitás megkérdőjelezése volt.

Vállalati bontás

A kutatás első szakaszában azt találtam, hogy a következő csoportosítás szignifikáns korrelációt mutat, ezért jelen cikkben a továbbiakban így alkalmazom:

- 1.csoport: 1-2 járművel rendelkező társaságok: jellemzően a tulajdonos, illetve annak közeli hozzátartozója a gépkocsivezető, az ügyintézést is ők végzik.
- 2.csoport: 3-14 járművel rendelkező társaságok: a tulajdonos már ritkán vezeti a járműveket, a társaság már elindult a vállalattá válás útján, megjelennek az irodai alkalmazottak, saját tulajdonú telephely jellemzően nincs.
- 3.csoport: 15-30 járművel rendelkező társaságok: jellemző, hogy már megjelenik a saját telephely, a vállalatnak már komoly referenciái vannak, a tulajdonos jó tárgyaló képességű, magasabb iskolai végzettségű menedzser.
- 4.csoport: 30 fölötti járművel rendelkező társaságok, nem ritkán pénzügyi befektetők is megjelennek, adott régióban fajsúllyal rendelkező vállalkozás. Nagyobb kereslet kielégítésére önmagában is képes.[2]

A KUTATÁS EREDMÉNYE

A megelőző kutatási szakaszhoz hasonlóan ez alkalommal is a Subco Vetting Form[1]-ok kielemzésének eredményét mutatom be 66 vállalat részvételével.

[1] Subco Vetting Form: Alvállalkozói kiértékelő lap

Alapvető biztonsági folyamatok

A kérdőív ezen része a transzparens biztonsági működés, valamint bizonyos biztonsági témákhoz kapcsolódó felelősségi körök deklarálási szükségességének a felismerését biztosító folyamatok meglétére kérdezett rá. A feltett 16 kérdés felöleli azon területek folyamatszabályozását is, amelyekkel kapcsolatos mulasztás a múltban biztonsági eseményhez vezetett. Ezen folyamatok hiánya kiemelt biztonsági kockázattal bír és az adott vállalat biztonságtudatossági szintjét is minősíti. Az alábbi táblázatban bemutatom a kiértékelt kérdéseket, valamint feltüntetem az válaszok összesített eredményét is.

KÉRDÉS	POZITÍV VÁLASZOK ARÁNYA
Van-e írott toborzási folyamat?	52%
A személyi felelősségek deklarálva vannak-e a toborzási folyamatban?	55%
Van-e ellenőrző lista a céges eszközök és hozzáférések átvételére az új alkalmazottak számára?	67%
A büntetlen előélet ellenőrizve van-e a teljes személyzet vonatkozásában?	76%
A büntetlen előéletet igazoló dokumentumok archiválva vannak-e és hozzáférhetőek-e a foglalkoztató irodájában?	45%
A személyi referenciák az előző munkahelyek vonatkozásában ellenőrizve vannak-e?	70%
Van-e titoktartási szerződés aláíratva minden alkalmazottal?	62%
Része-e a toborzási folyamatnak minden új alkalmazottnál a képzés az Általános Biztonsági Tudnivalókról?	67%
Része-e a toborzási folyamatnak minden új alkalmazottnál a képzés a Rablás Esetén Tudnivalókról?	62%
Van-e általános újraképzési program az Általános Biztonsági és Rablás Esetén Tudnivalókról?	53%
Személyi felelősségek deklarálva vannak-e az újraképzési folyamatleírásban?	50%

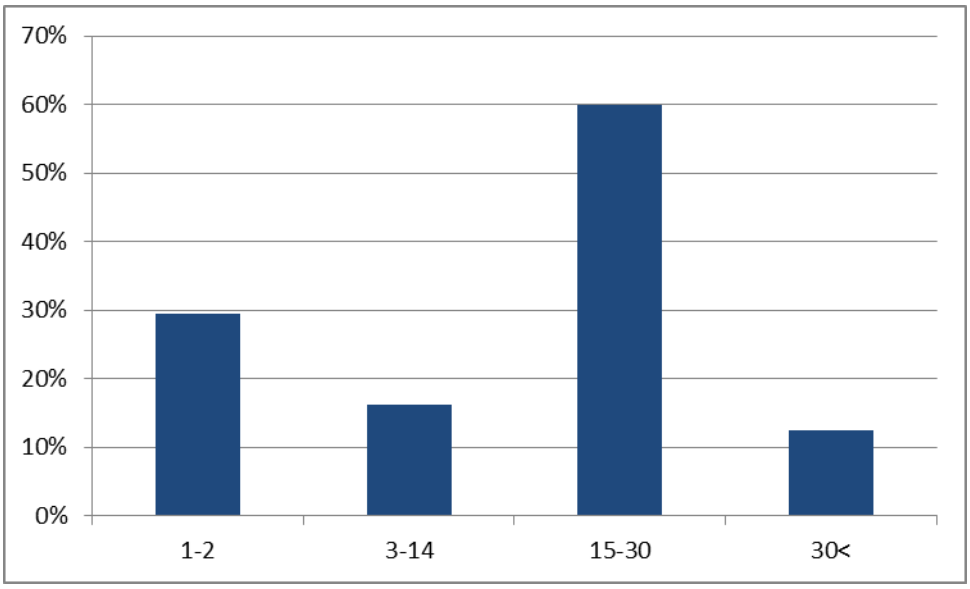
Van-e írott munkafolyamat munkaviszony megszüntetésére?	61%
Személyi felelősségek deklarálva vannak-e munkaviszony megszüntetésére vonatkozó folyamatban?	59%
Van-e ellenőrző lista a céges eszközök és jogosultságok visszavonására a cégtől távozó személyzet részére?	62%
Van-e információ védelmi szabályozás, a megfelelő információ kezelés érdekében?	53%
Van-e írott kulcskezelési szabályzat?	48%

1. táblázat Biztonsági folyamatok %-os alkalmazási aránya kérdésenként.

A leggyengébben teljesítő 20 vállalat 5 vagy annál kevesebb kérdésre adott pozitív választ. A legjobban teljesítő felső harmadban 32 vállalat található, mely kevesebb, mint az összes mintának a fele. Jellemző az önbevallás alapján, hogy a büntetlen előéletet és az előző munkahelyi referenciákat kiemelkedően sokan ellenőrzik, 76% illetve 70%. A büntetlen előéletet igazoló dokumentumokat ellenben csak 45% archiválja. Igazolva látszik az önbevallásos kérdőíves módszertan egyik hátránya, miszerint az alacsony érvényességgel rendelkezik. Ha feltételezzük, hogy a fuvarozók érdeke, hogy jobb eredményt mutassanak a valóságosnál, akkor a kapott válaszok magasabbra értékelik a vállalatukat, tehát a valóság a mutatni szándékozott összképnél csak rosszabb lehet.

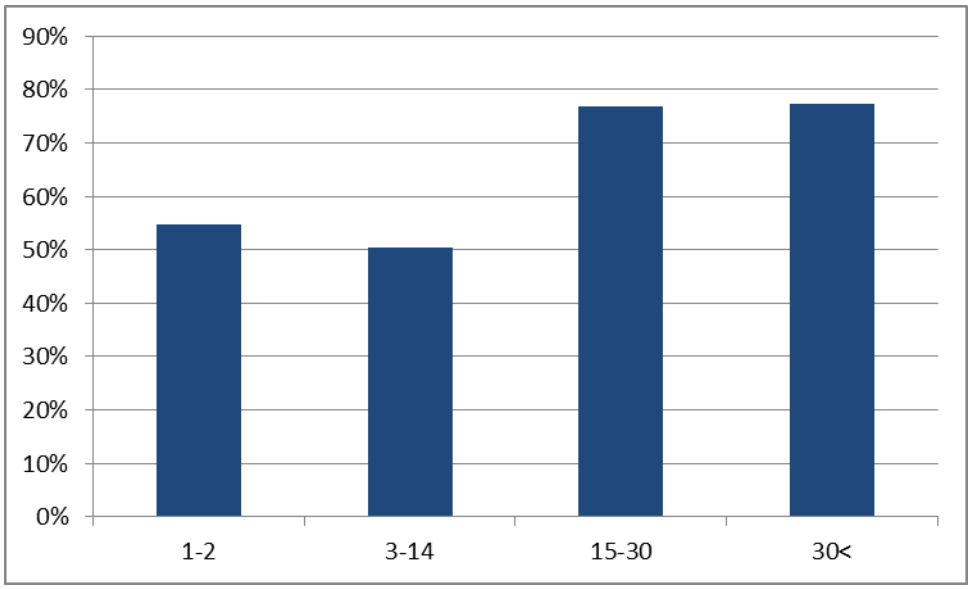
Az 1.ábra bemutatja, hogy az egyes csoportok milyen arányban feleltek meg a folyamatok felmérésén. Az ábra képe szerint legnagyobb arányban (60%) a 15-30 járművel rendelkezők végzik a napi rutinjukat a biztonsági kérdések szem előtt tartásával. Érdekes fejlemény, hogy a nagyobb vállalatoknál szignifikánsan (13%-ra) csökkent a szint. Továbbá megfigyelhető, hogy 1-2 járművel rendelkezők jobban teljesítenek, mint a 3-14 teherautóval rendelkező vállaltok. A vizsgált vállalatok 26%-ánál voltak elfogadhatóak a belső biztonsági folyamatok. Az eredmény ugyan nem reprezentatív a nagyobb vállalatok vizsgált kis mintanagysága miatt, viszont alkalmas további összefüggések megállapítására. Az összevetés figyelembe veszi az 1.táblázatban szereplő kérdések mellett, hogy melyik fuvarozó alkalmazza az úgynevezett DiDb[2] kártyákat. A DiDb kártyák ellenőrzését és a rendszer vállalati szintű bevezetését a biztonságtudatosság alapvető jelének tekintjük.

[2] DiDb kártya: gépjárművezetők szakmai előéletét igazoló, pozitív diszkrimináción alapuló adatbázisban regisztrált munkavállalók azonosítására szolgáló mágneskártya. Jelenleg a regisztráltak létszáma több, mint 24000 fő.[23]



1. ábra Biztonsági folyamatok és DiDb kártya átlagos alkalmazási aránya vizsgált csoportonként.

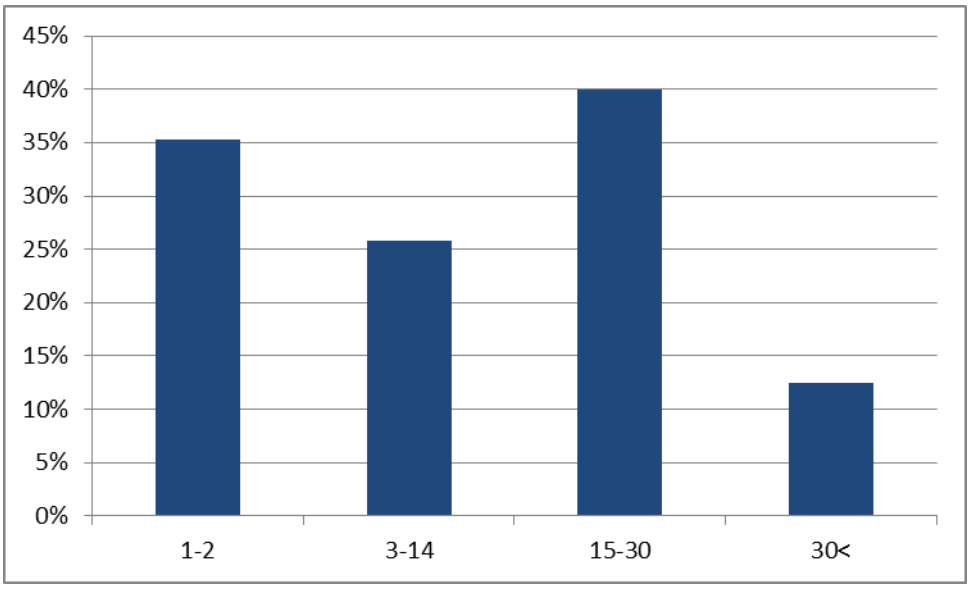
A 2.ábrán szemléltetem a DiDb kártyák birtoklásának figyelembe vétele nélkül készült összehasonlítást. A fuvarozókat ez a megközelítés két részre osztja - az 1-es 2-es csoportba tartozókra és a 3-as és 4-es csoportba tartozókra. A két rész között szignifikáns különbséget találtam. Míg a kisebb méretű vállalkozók 50-55%-ban feleltek meg, addig a nagyobb vállalatok rendre 77%-ban.



2. ábra Biztonsági folyamatok átlagos alkalmazási aránya vizsgált csoportonként.

Járművek biztonsági eszközei

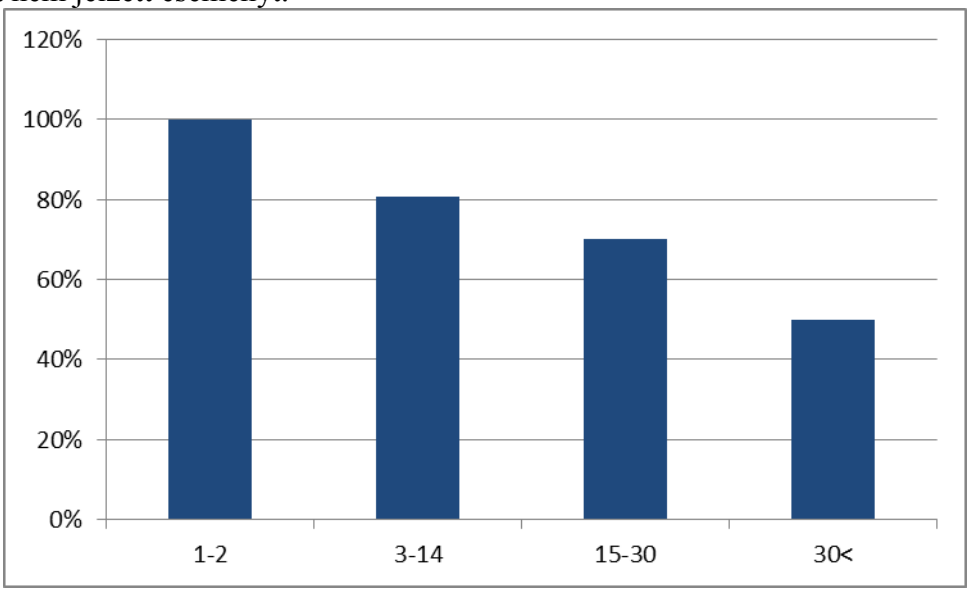
A kérdőív utolsó szekciója a járművekre felszerelt biztonsági berendezések fajtáját és számosságát vizsgálta. A kérdések között szerepelt ajtónyitás érzékelővel, pánik gombbal és riasztó rendszerrel kapcsolatos kérdés. A 3.ábrán bemutatott eredmény nagyon hasonlóan alakult a 1.ábrához, az abszolút összegek viszont alacsonyabbak. Itt is megfigyelhető a 15-30 járművel rendelkező vállalatok relatív felülteljesítése. Az összes vizsgált vállalatnak csupán 26%-ánál jelentek meg az említett biztonsági eszközök. A válaszadók járműveinek többségében (84%) GPS alapú nyomkövető rendszer van telepítve.



3. ábra Biztonsági berendezések %-os alkalmazási aránya vizsgált csoportonként.

Biztonsági események hatása

A felmérés rákérdez az elmúlt 3 évben tapasztalt biztonsági eseményekre, melyekre a válaszadók önbevallással válaszoltak. Ez az egyik olyan kérdéskör, melynek valóság tartalmát igen nehéz ellenőrizni. Egy árulopás esetén keletkező iratok csak véletlenszerűen lelhetőek fel, amennyiben a fuvarozó nem vezet külön nyilvántartást. A szerződött biztosítót titoktartás köti és ha referenciának is olyan megbízót ad meg, ahol nem volt eseménye, akkor nagyon alacsony a reveláció kockázata, ha hamisan állítja, hogy nem volt biztonsági eseménye. A következő ábrán (4.ábra) szemléltetett válaszok, azt mutatják, hogy az egyes csoportok hány százaléka nem jelzett eseményt.



4. ábra Biztonsági eseményt nem jelentettek aránya vizsgált csoportonként.

Az első csoportnak a válaszok szerint egyáltalán nem volt káreseménye, a második csoportból 81%, a harmadikból 70%, a negyedikből 50% nem jelentett eseményt. Matematikailag magyarázható és evidens, hogy a több járművel rendelkezők kitettsége vállalati szinten nagyobb, azaz egy esemény bekövetkezésének az esélye nagyobb 80 járműnél, mint 1-nél. Az összes vizsgált vállalat vonatkozásában 80%-nak nem volt

káreseménye. A kutatás nem vizsgálta, hány esemény történt vállalatonként, melyből levonható lenne egy relatív biztonsági szintet kifejező, következtetett mutatószám melynek alapját az események száma és az üzemeltetett jármű darabszámok hányadosa képeznék. Az viszont bizonyos, hogy az első csoport nem jelzett eseményt, tehát ennek a csoportnak a mutatószáma lenne a legjobb, éppen nulla. A mutatószám azért relatív, mert nem veszi figyelembe az elszállított áru értékét és piacképességét.

Arra a feltételezésre kerestem a továbbiakban illeszkedő adatsort, hogy egy bekövetkezett biztonsági esemény hatására nő-e a biztonságtudatossági szintje a közúti fuvarozóknak. Megvizsgáltam van-e szignifikáns eltérés azok között, akik az elmúlt 3 évre vonatkozólag jelentettek biztonsági eseményt és azok között, akik nem. Összefüggést találtam az esemény bekövetkezte és a biztosítási kondíciók megfelelősége között. Az eseményt jelző vállalatok 62%-ának van minden szempontból kielégítő biztosítása, míg azoknak, akik nem jeleztek incidenst, csak 28%-ban volt a biztosítása elfogadható. A többi vizsgált paraméter tekintetében nem találtam szignifikáns eltérést. Azt a feltételezésemet nem tudtam igazolni, hogy egy káresemény hatására megnőne a beruházási hajlandóság a biztonsági berendezésekbe. A járművekbe beszerelt eszközök tekintetében még visszaesést is mértem 26%-ról 18%-ra, ez az adat azonban nem korrelál az események bekövetkeztével. A beruházási hajlandóságot véleményem szerint az egyes üzleti megállapodásokban meghatározott elvárások mozgatják.

Tudástranszfer és reflexió mérése ismételt auditok elemzésével

"A reflektív gondolkodás tudatos, összekapcsolja az elméleti tudást a korábbi gyakorlati tapasztalatokkal egy fejlődési cél elérése érdekében. A reflektív gondolkodáshoz nyitott, a fejlődés iránt elkötelezett és azért felelősséget vállaló attitűd szükséges. A mélysége alapján a gyakorlatban megkülönböztethetjük az azonnali és az előzetesen átgondolt reflexiót. A reflexiót körforgás jellegű folyamatként ábrázolhatjuk, a tevékenység közbeni módosításból következik a tevékenység utáni elemzés, értékelés. Ezután az újabb tevékenység előtt a korábbi tervek felülvizsgálata, módosítása következik."[24]

Az átvilágítási eljárás megismétlésére jelentős hiányok feltárása esetén, illetve már foglalkoztatott fuvarozók időszakos újraellenőrzésekor kerül sor. A vizsgált 66 vállalat közül 22 lett legalább 2-szer eljárás alá vonva, ebből 4 vállalat háromszor és 1 vállalkozás négyszer. A 22 eset elemzése lehetőséget nyújt a megbízó által képviselt normák, biztonsági színvonal, folyamatszabályozási eljárások megismerésének a hatásvizsgálatára. Az első ellenőrzést megelőző kérdőívben feltett kérdésekből a válaszoló következtethet az auditáló vállalat által elvárt normákra. Feltételezem, a kevésbé ellenőrizhető állításokra, a valóságot torzítva nagyobb arányban érkezik pozitív válasz. A válaszoló már az első felmérés alkalmával is tájékoztatást kap az információk későbbi helyszíni visszaellenőrzéséről.

A megismételt eljárás során az auditált vállalat már felkészültebben tölti ki a kérdőívet és egy tanulási folyamat reflexiójaként megjelennek az elvárt folyamatok. A folyamatot felfoghatjuk úgy is, mint egy adott területen szaktudással rendelkező vállalat tudástranszfere a saját hálózatában tevékenykedő kisebb, elemi résztvevők felé. Kialakul egyfajta rendszer központú gondolkodás, mely átlépi a vállalatok által eddig saját maguk által lehatárolt területek határait. A management eszközök és tudás kiterjesztése alapvető fontosságú egy logisztikai hálózat értelmezésében. A haladó infokommunikációs eszközök forradalmaként az információ ma már nagy mennyiségben áll rendelkezésre, és nem az információk elérhetősége, hanem megszervezése a jelenkor legnagyobb kérdése, kihívása. Az okos megoldások éppen ettől okosak. Az információ azonnali, megszervezett elérhetősége felgyorsítja a döntéshozatali és válaszadási folyamatokat. A logisztikai biztonságot éppen ilyen okos, hálózati megoldásokkal képzelem el. Kutatásaim célja ezen hálózatok és eszközök definiálása, azonban e cikk keretein ez túlmutat.

Az ismételt eljárások eredménye a reflexió mérése is egyben. A vizsgált esetekben kimutatható javulást találtam a vállalatok egzisztencia vizsgálatánál, az első felméréskor 68%-os volt a pozitív eredmény, a másodiknál 91%. A biztosítások vizsgálata 23% helyett 45%-ban hozott elfogadható eredményt. A biztonsági folyamataikat a korábbi 23%-os megfelelés, az ismételt auditkor 32% jellemezte. A biztonsági berendezések alkalmazási szintje csökkent 26%-ról 21%-ra növekvő összesített jármű darabszám mellet (518 db-ról 521 db-ra). Az eredmények az összes vizsgált kérdőív átlagát tükrözik. Megállapíthatjuk, hogy a reflexió tisztán kimutatható, területenként eltérő hatékonysággal. A 22 vállalatból 6 jelzett biztonsági eseményt a két audit közötti időszakban. Annak érdekében, hogy a bekövetkezett biztonsági események hatását különválasszam a reflexiótól a két vállalatcsoportot külön is elemeztem. Az új eseménnyel rendelkező vállalatok az átlag fölött növelték megfelelőségüket biztosítás (17%-ról 50%-ra) és a biztonsági folyamatok (17%-ról 33%-ra) területén, de a 6 darabos minta túl kicsi, hogy további érdemi következtetéseket vonhassunk le. A biztonsági események hatásánál tapasztalt eredmény szerint a fuvarozók jellemzően a biztosításuk felülvizsgálatával reagálnak. A biztosítások újrakötése miatt 28% helyett 62% volt a pozitívan elbírált biztosítások aránya ebben a csoportban, de a biztonsági folyamataikon nem változtattak. A biztonsági események torzítását teljesen kizárva, a biztosítások területén mért reflexió 45%-os megfelelésről 39%-osra változik, amely még így is szignifikáns javulás az elsőre elfogadott 23%-hoz képest.

Mélyinterjú eredménye

A statisztikai elemzést kvalitatív módszer segítségével tovább értelmeztem. A számok mögött rejlő okok, folyamatok és fuvarozói gondolkodás jobb megértéséhez mélyinterjút készítettem. Az interjúban részt vett az auditáló vállalat biztonsági vezetője, Horváth Miklós és minőségügyi vezetője, Tóth Dániel. Mindketten több mint tíz évet töltöttek el szakterületükön különböző vezető logisztikai vállalatoknál. Az interjúk során megkértem a válaszadókat, hogy értelmezzék a kapott eredményt és egészítsék ki saját tapasztalataikkal. Alábbiakban összegzem a megállapításaikat.

- Az interjúk alatt megerősítést nyert, hogy a fuvarozók egy kár elszenvedése kapcsán szembesülnek a CMR Egyezményből[3] adódó kötelezettségekkel és a biztosítás térítési szintjével vagy annak térítési hajlandóságával. A biztosítás kikötéseit és kizárásait jellemzően ekkor olvassák és értelmezik először.
- A fuvarozó biztonsági eszközökbe, a GPS-en kívül ügyfél nyomására hajlandó beruházni, nem látja annak pénzügyi megtérülését.
- Jellemzően a biztosítások feltételrendszereinek és térítési szintjének javítását választják a fuvarozók, nem a biztonsági esemény megelőzésére költenek. Alább néhány az említett okok közül:
    - *"A CMR biztosítás kötelezettség, a biztonsági eszköz lehetőség."*
    - *"Ha mind a kettőre költene, úgy érezné, többszörös pénzügyi teher nehezedik rá ugyanazért."*
    - *"Rájön, hogy a berendezés nem önjáró, foglalkozni kell vele!"*
    - *"100%-os védelmet nem nyújtanak az elérhető eszközök."*
- Az első személyes audit során az auditáló logisztikai vállalat sablon folyamatokat mutat be és oktat le, valamint biztosítások témakörét is részletesen átveszik.

[3] CMR: Nemzetközi közúti árufuvarozási szerződésekről szóló egyezmény. Az Egyezmény 1961.07.02-án lépett hatályba, ma már szinte minden európai ország csatlakozott hozzá. Magyarország 1970.07.28-i hatállyal, az 1971.évi 3. számú törvényerejű rendelet hirdette ki.[25]

- Az fuvarozó által egyik legkevésbé szabályozott terület a kulcskezelés folyamata. Ennek oka, hogy vélhetően nem ismerik fel a jelenlegi vagy korábbi alkalmazottak által elkövethető bűncselekmények bekövetkezésének lehetőségét, veszélyét.
- Az ismételt audit kapcsán javuló egzisztencia vizsgálati eredmények egyrészt a referenciák jobb és elégséges definiálásával, másrészt a 24 órás rendelkezésre állás és cégekhez köthető telephelyi elérhetőségek megadásán keresztül valósulnak meg.
- Az összes vizsgált vállalat vonatkozásában 80%-nak nem volt káreseménye. Az egyes csoporté ezen belül nulla biztonsági eseménnyel áll az élen. A kérdéskörben több választ rögzítettem.
    - *"Mivel többnyire a tulajdonos vezet, ezért relatív magas az 1-es csoportban a biztonságtudatosság egy elemi, atavisztikus fajtája. A tulajdonos jobban ügyel a gépjármű és a rakomány biztonságára, mint egy alkalmazott."*
    - *"Az esetek egy részében a személyes audit kapcsán kerülnek elő események, melyeket elfelejtettek jelenteni, vagy a kérdőívben nem tartottak említésre méltónak, vagy azért nem említettek, mert hátrányos megkülönböztetéstől tartottak."*
- Az interjú alanyok megfigyelései szerint a járműpark átlagéletkorának növekedésével fordítottan arányos a vállalat biztonság színvonala. A tulajdonos figyelmét leköti a járművek folyamatos üzemben tartása, illetve javítása.
- Az interjú alanyok megfigyelései szerint hátrányos a fuvarozó cég biztonsági felkészültségét tekintve, amennyiben alulméretezett adminisztratív emberi erőforrással, esetleg a management és adminisztrációs, szerviz feladatok a tulajdonos által egy személyben kerülnek megoldásra a mindennapi működésben, ugyanis a feladatkörök sokrétűsége, alkalomszerűen időigényenyessége, valamint a korlátozott ráfordítási lehetőségek miatt nem megfelelő alapossággal kerülnek kivitelezésre olyan feladatok, amelyek később növelik a cég kitettségét egy esetleges incidens bekövetkezésének vonatkozásában.
- További biztonsági tényező amennyiben a vállalkozás mindig ugyanazon az útvonalon jár, a gépjárművezetők és vezénylők kiismerik magukat a környéken, ismerik a szokásokat, tisztában vannak a nyitva tartásokkal, kommunikációs sémákkal. Ezzel szemben egy mindig változó útvonal kihívások elé állítja a személyzetet, amely fokozott biztonsági kockázattal jár. (Az állandó útvonal kifigyelhetőségéből kockázat is jelentkezik, azonban ez csökkenthető több állandó útvonal definiálásával és azok véletlenszerű kiválasztásával egy konkrét szállítási feladat teljesítése során.)
- Jellemző, hogy egy generáció váltás révén management ismeretekkel bővül a cégvezetés és a cég elindul a vállalattá válás útján.
- A 30 autónál kisebb vállalatok vezetői még ismerik személyesen a gépjárművezetőket, nagyobb bizalmuk van a folyamataikban, a tevékenységet egymaguk átlátják és ellenőrzik.
- Sajnálatos észrevétel, hogy a vállalkozók mérettől függetlenül nem érzik át a jelentőségét az új belépők előzetes ellenőrzésnek. Jellemzően nem kérnek sem erkölcsi bizonyítványt, sem DiDb kártyát. A legtöbb új alkalmazott régi ismeretség által vagy „ismerős ismerőseként" kerül a vállalthoz. Ebben az összefüggésben az a személy akinek az ajánlására bekerül az illető a vállalathoz mintegy személyi garanciát vállal az ismerőséért és az ő elmondása lesz a az új munkavállaló kapcsán a megítélés alapja a munkavégzés minőségét és előélet feddhetetlenségét illetően. Az előző munkahely ellenőrzése referenciaként nem jellemző.
- A reflexió egy tudatos folyamat, mely során nem csak az auditált vállalatok fejlődnek és válik egyre átgondoltabbá a belső működésük, hanem az auditorok is

beépítik a megszerzett tapasztalatokat az oktatási-számonkérési rendszerükbe. Ezáltal a helyszíni ellenőrzések módja és a súlypontok időben változnak.

KÖVETKEZTETÉSEK

A biztonságtudatossági szint mérésének az eredménye, hogy a magyar közúti fuvarozók negyede képes a mai kor biztonsági kihívásainak megfelelni. A biztonsági berendezések alkalmazása többnyire nem öncélú, belülről jövő kezdeményezés, hanem ezek egy adott üzlet által megkövetelt norma alapján kerülnek beépítésre. A vizsgálat eredményeit összefüggéseiben értelmezve megállapítom, hogy az érzékeny, több odafigyelést, magasabb biztonsági szintet megkövetelő küldemények szállítására a legalkalmasabbak a 15-30 járművel rendelkező fuvarozók, az ő biztonságtudatossági szintjük jellemzően magasabb a többi csoportban mért szinttől, bár a biztonsági berendezések területén náluk is nagy a hiányosságok tapasztalhatók. A 30 járműnél nagyobb kategóriában kimutathatóan esik a színvonal, ez egyrészt betudható lehet az alacsony mintaszámnak, de további magyarázat, hogy a nagyobb vállalatok már kerülik a kockázatos termékek szállítását. Az 1-2 járművel rendelkezők esetében egyes vizsgálatok negatív eredményre jutottak, ennek magyarázata a kis vállalatméretben keresendő, működésük még nem vállalatszerű. A kategóriáról ellenben bebizonyosodott, hogy magasabb biztonságtudatossági szinttel rendelkezik, mint az azt követő 3-14 járműs csoport. Az interjúk során bebizonyosodott, hogy az új munkavállaló előélet ellenőrzése alatt lényeges értelmezésbeli különbség van. A fuvarozók szóbeszédre hagyatkoznak, míg az elvárt viselkedés az erkölcsi háttér bizonyítható ellenőrzése lenne. Ez utóbbi eltérés miatt a fuvarozók magasra teszik a saját bevallásukban a folyamatokra adott értékelésüket, holott az éppen ellenkezőleg nagyon alacsony. Összegezve megállapítható, hogy a hazai közúti fuvarozók átlagos biztonságtudatossági szintje csekély, ezért további kutatásra van szükség a megfogalmazott tudományos probléma megoldására. A tudástranszfer egy központi vállalat felől lehet egy jövőbeli megoldás, hiszen e cikkben mért eredmény alapján a reflexió mérhetően jelen van, ugyanakkor annak hatékonysága még ismételt auditok esetén is szerény. A tanulási folyamat részeként oktatások és időszakos felülvizsgálatok szükségesek, de nem várható, hogy a fuvarozók felismerjék saját érdeküket az áruvédelem és biztonság területén és ezáltal maguk álljanak az innováció élére. Az innovációt szükségképpen a fuvaroztatók (központi vállalatok) irányítása mellett képzelem el, rendszerlogisztikai infokommunikációs eszközökkel. Kutatásom a jövőben erre a területre koncentrálom. Új eredményként vonom le azt a következtetést, hogy a közúti fuvarozók méret szerinti csoportosítása alapján, előre jól behatárolható kockázatokkal kell számolnia a fuvaroztatónak.

FELHASZNÁLT IRODALOM

[1] Lloyd's Loading List,(2016) *Reported cargo crime doubles in Europe*, online, 17.05.2016, News, http://www.lloydsloadinglist.com/freight-directory/news/Reported-cargo-crime-doubles-in-Europe/66428.htm#.V_ZhtXoRpNg, (17.10.2016)

[2] LÁNYI, M.(2017): *A fuvarozói kiválasztás egyes biztonsági kérdései*, Hadmérnök, XII Évfolyam 2.szám pp.14-21, Budapest, 2017.június, ISSN:1788-1919

[3] OLÁH J.(2016): *21. századi fuvarozáshoz szükséges, működést támogató technikai eszközök bemutatása (Introduction of operation support technical devices needed for the transportation in the 21st century)*, 2016, Logisztika Menedzsment Tanszék, Alkalmazott Informatika és Logisztika Intézet, Gazdaságtudományi Kar, Debreceni Egyetem, Magyarország, Gradus Vol 3, No 1 (2016) pp. 454-460.

[4] DYER, J. H.(1996): *Specialized Supplier Networks as a Source of Competitive Advantage: Evidence from the Auto Industry*, Strategic Management Journal, Vol. 17., 271-291

[5] DYER, J. H.- CHO, D. S.- CHU, W.(1998): *Strategic Supplier Segmentation: The Next „Best Practice" in Supply Chain Management*, California Management Review, Vol. 40 No 2,Winter, pp 57-77

[6] MENTZER, J. T.- DEWITT, W.- KEEBLER, J. S.- MIN, S.- NIX, N. W.- SMITH, C. D.- ZACHARIA, Z. D.(2001): *Defining supply chain management*, Journal of Business Logistics, 22, 1-25.

[7] GELEI A.- DOBOS I.- KOVÁCS E.(2010): *Ellátási lánc kapcsolatok modellezése (Modelling Supply Chain relationships),* number 124. Műhelytanulmány, Budapesti Corvinus Egyetem,Vállalatgazdaságtan Intézet

[8] NAGY J.(2008): *Ellátási lánc menedzsment technikák (Supply Chain management techniques)*, number 100. Műhelytanulmány (Study), Budapesti Corvinus Egyetem

[9] ESTÓK S.(2011): *A katonai és civil ellátási lánc fejlődésének lehetőségei nemzetközi környezetben (Development possibilities of the military and civil supply chain in international environment)*, PhD work, Zrinyi Miklós Nemzetvédelmi Egyetem, Kossuth Lajos Hadtudományi kar, Hadtudományi Doktori Iskola

[10] VÁNYI N.(2012): *Members of a supply chain and their relationships*, Applied Studies in Agribusiness and Commerce, 6(5), pp. 131-134

[11] KARMAZIN GY.(2014): RESEARCH RESULTS ON THE KEY SUCCESS FACTORS OF HUNGARIAN *Logistics Service Providers*, Periodica Polytechnica, 42(2), pp. 91-95

[12] BÁNFI T.- BOROS Á.- LOVAS A.(2012): *Vállalati vezetők innovációs érzékenysége, szemlélete és szándékaik – egy felmérés tapasztalatai (Managers' innovation sensitivity, approach, and purposes – experience of a survey),* Vezetéstudomány / Budapest Management Review, 43 (3). pp. 2-18.

[13] CSAPÓ, K.(2010): *A gyorsan növekvő kis- és középvállalkozások jellemzői és fejlesztési lehetőségei Magyarországon (The characteristics and development possibilities of fast-growing small and medium-sized companies in Hungary)*, Doktori értekezés (PhD work), Budapesti Corvinus Egyetem, Gazdálkodástani Doktori Iskola.

[14] KISS K.(2014): *A hazai kis-és középvállalkozások növekedését befolyásoló egyéni és vállalati tényezők (Impact of individual and company factors on the growth of inland small- and middle sized enterprises)*, PhD work, University of Pécs, Természettudományi Kar Földrajzi Intézet, Földtudományok Doktori Iskola

[15] BOKOR Z.(2005): *Evaluating the intermodal logistics services and exploring their development possibilities (Az Intermodális logisztikai szolgáltatások helyzetének értékelése, fejlesztési lehetőségeinek feltárása)*, BME OMIKK Logisztika, 10 (3), pp. 22-65.

[16] BANK D.(2010): *Analyzing the Hungarian freight, forwarding and logistics market (A magyarországi szállítási, szállítmányozási és logisztikai piac elemzése)*, GKI Economic Research Co. (2010/October), pp. 1-5.

[17] BOKOR Z.(2012): *Cost Calculation Model for Logistics Service Providers*, Promet - Traffic - Traffico, 24 (6), pp. 515-524

[18] ARBOLEDAA, A.- C. MORROW, P.- R. CRUMC, M.- C. SHELLEY IID, M.(2003): *Management practices as antecedents of safety culture within the trucking industry: similarities and differences by hierarchical level*, Journal of Safety Research, Volume 34, Issue 2, April 2003, Pages 189–197

[19] MEIXELL, M.- NORBIS, M.(2008):*A review of the transportation mode choice and carrier selection literature*, The International Journal of Logistics Management, Vol. 19 Iss: 2, pp.183 – 211

[20] VARGA E , HAJÓS L , SZIRA Z..(2016) *The examination of the relevant competencies in the labour market from the point of view of employers*, Annals of faculty of engineering Hunedoara – Inernational Journal of engineering 14:(2) pp. 155-159.

[21] LAM,J. - DAI ,J.(2015): *Developing supply chain security design of logistics service providers: An analytical network process-quality function deployment approach*, International Journal of Physical Distribution & Logistics Management, Vol. 45

[22] ZAILANI, S.H. - SUBARAMANIAM, K.S. - IRANMANESH, M. - SHAHARUDIN, M.R.(2015): *The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy: Security culture as moderator*, International Journal of Physical Distribution & Logistics Management, Vol. 45 Iss: 7, pp.652 – 673

[23] DiDb system, DiDb.eu, online, http://www.didb.eu/en/didb_system, (17.11.2016)

[24] Online:http://www.oktatas.hu/kozneveles/projektek/tamop_315_pedkepzes_fejl/projekhirek/reflexio_pedagoguskomptenciak_ertekeleseben (10.11.2016)

[25] Online: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=97100003.TVR (31.06.2017)

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

A KUTATÁS FEJLESZTÉS SZEREPE ÉS HATÁSA AZ OKTATÁSRA AZ NKE HHK HADITECHNIKAI TANSZÉKÉN

THE ROLE AND IMPACT OF RESEARCH AND DEVELOPMENT ON EDUCATION AT THE NUPS MSOT DEPARTMENT OF MILITARY TECHNOLOGY

GÁVAY György; GYARMATI József; HEGEDÜS Ernő; VÉG Róbert László

(0000-0003-0632-5650); (0000-0001-7594-2383); (0000-0001-8457-5044); (0000-0002-9786-6702)

gavay.gyorgy@uni-nke.hu; gyarmati.jozsef@uni-nke.hu; hegedus.erno@hm.gov.hu; vegh.robert@uni-nke.hu

Absztrakt

A cikk bemutatja a kutatás-fejlesztés helyét szerepét a katonai felsőoktatás egy kiválasztott szegmensében. A eddigi tapasztalatok feldolgozásán keresztül megmutatja, hogy a K+F tevékenység milyen mértékben befolyásolja az intézmény működését és az oktatási tevékenységének a színvonalát. Ismertetésre kerülnek az elmúlt évtized kutatásainak fő irányai, valamint azok eredményei, és vázolja, hogy az elkövetkező néhány évben milyen kutatások beindítása lenne célszerű, figyelembe véve a technikai fejlődést és a felhasználói igények folyamatos változását.

Kulcsszavak: *kutatás-fejlesztés, oktatás, haditechnika*

Abstract

The article describes the position and role of research and development in a chosen segment of the military higher education. It introduces – through the experiences gained so far – how the R&D activities impact the opration of the institution and the quality of its educational activities. The main directions and results of research performed in the last decade will be presented and and the article will also outline the research activities that would be worth to start in the next few years, taking into consideration the development of technology as well as the continous change of the user requirements.

Keywords: *research and development, education, military technology*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.10.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.22.

BEVEZETÉS

A felsőoktatási intézmény 2011. évi CCIV. törvény (felsőoktatási törvény) 2.§ szerint oktatáson kívül tudományos kutatás céljából létrehozott szervezet. A tudományos kutatást a vonatkozó törvény az oktatási intézmény egyik alaptevékenységének tekinti. A szervezetnek tehát nem csak az ismeretek, legyenek, azok bár a legkorszerűbben átadásával kell foglalkozniuk, hanem bizonyos ismeretek előállításával, amelyet kutatás-fejlesztési tevékenységen keresztül lehet csak megvalósítani. A felsőoktatási intézménynek a kutatási tevékenység tehát egy olyan alaptevékenysége, amely hozzájárul a működésének alapfeltételeihez.

A kutatás céljait az NKE Kutatás Fejlesztési és Innovációs Stratégiája (KFIS) három fő területre csoportosítja:

- a művelt tudományterület és az azon belüli tudományág szerinti gyakorlati tevékenység támogatása;
- oktatási tevékenység támogatása;
- a tudományos ismeretek és a módszertan bővítése.

A kutatási tevékenység megléte egy felsőoktatási intézményben tehát az előbb felsorolt törvény, illetve belső szabályozó szerint a szervezettől egy nem csak elvárható tevékenység, hanem mint alaptevékenység a működés egyik alapfeltételének tekinthető. Melyek lesznek azok a gyakorlati okok, amelyek a jogszabályi kötöttség mellett szintén olyan közvetlenül vagy közvetetten elkerülhetetlenné teszik egy felsőoktatási intézmény számára a kutatási fejlesztési tevékenység folytatását?

A továbbiakban a cikk ezen gyakorlatból származó okokat sorolja fel, valamint bemutatja, hogy az elmúlt mintegy nyolc évben milyen gyakorlati megvalósítása vált láthatóvá a Nemzeti Közszolgálati Egyetem Haditechnikai Tanszékén. A cikk bemutatja a tanszék oktatási és kutatási kapacitásait azok változását, és azt, hogy a saját kapacitások kihasználása mellett, együttműködve más szervezetekkel, legyen az felsőoktatási intézmény illetve honvédségi szervezet, milyen kutatási célokat tudott kitűzni és milyen eredményeket volt képes elérni.

A KUTATÁSI TEVÉKENYSÉG HELYE, SZEREPE

Ahogy az előző fejezetben megemlítésre került a kutatási tevékenység a felsőoktatási intézmény és ezzel együtt az NKE HHK részére törvényi kötelezettség. A vonatkozó jogszabály a felsőoktatási törvény elő is írja, hogy az felsőoktatásban dolgozó oktatók a munkaidejük legalább 20%-át kötelesek kutatásra fordítani. A törvényi előírásokon felül viszont attól lényegesen nyomósabb gyakorlati okok is léteznek, amelyek a kutatást lényegében nem elkerülhetővé teszik. A kutatások folytatását előidéző gyakorlati okok:

- publikációs kényszer;
- pályázatokon való sikeres szereplés;
- lehetséges bevételi forrás;
- képesség fenntartása (például kutatások megrendelésére vonatkozó képesség).

Az oktatók kutatási tevékenységének a jelenleg használt legjobb mérési lehetősége a publikációs tevékenység nyomon követése. Ezt teljesen nyilvánosan, mindenki számára

hozzáférhetően az Magyar Tudományos Művek Tára (MTMT)[1] lehetővé teszi. Az oktatók teljesítménye a MTMT adatlapon a publikációikra és azok minőségére jellemző adat segítségével jól mérhető. Ilyen például a publikációk száma, a hivatkozások száma, vagy a Hirsch index.

A publikációk száma mellett a Magyar Tudományos Akadémia illetékes bizottságai a folyóiratokat szakmai tartalmaik alapján rangsorolják, vagyis nem csak a publikációk darabszáma számít, hanem a tartalma, amit a folyóirat szakmai súlya jelez vissza. A hazai besorolás mellett léteznek olyan nemzetközi adatbázisok, amelyekben alapvetően a cikkekre való hivatkozások száma segítségével rangsorolnak (Web of Science, SciVal Experts). A publikációk súlyának és adott tudományterületre gyakorolt hatásának a megállapításában szerepet játszik az azt közzétevő folyóirat tudományterületi besorolása és rangsora, valamint az adott publikációra történő hivatkozások száma és a hivatkozást tartalmazó publikációt megjelenítő folyóirat tudományterületi rangsora.

Az oktatók publikációs tevékenységének a mértéke és színvonala a különböző pályázatok során, legyen az magasabb oktatói fokozatba történő jelentkezés, vagy tudományos mű elkészítése (PhD, habilitáció) az adott tudományterületre jellemző tudománymetria szerint kerülnek értékelésre. Az MTA Hadtudományi Bizottsága az ide tartozó folyóiratokat „A”, „B”, „C” kategóriába sorolja. A magasabb szintű pályázatok esetében fontos az oktató nemzetközi hatásának a mérése, amit a külföldi publikációk mennyisége és minősége segítségével állapítanak meg. Több olyan doktori iskola létezik különböző tudományterületeken, ahol már a PhD értekezések sikeres védésének előfeltétele a külföldi illetve az Impact Faktoros (IF) publikáció.

Ilyen háttér mellett az oktatók saját érdeke a minél több, színvonalas folyóiratban megjelenő publikáció elkészítése.

A kutatási tevékenység tartalmilag szoros összefüggésben áll a kutató oktatási tevékenységével. Ezt egyrészről a vonatkozó szabályozók is ösztönzik, például az NKE KFIS, amely szerint a kutatási tevékenység egyik célja a tananyag előállítása. Ezen felül teljesen egyszerű gyakorlati ok kényszeríti az oktató-kutatót, hogy a kutatási tevékenysége az általa oktatott tudományágon belül legyen, vagy még szűkebben közelítse az általa oktatott tantárgyak által határolt tudományterületet. Így ugyanis közvetlenül oldható meg a tantárgyak folyamatos korszerűsítése. A kutatás egy jelentős része az irodalom feldolgozása, amely segítségével a legfrissebb kutatási eredmények válnak elérhetővé az oktatásban.

A pályázatokon való sikeres szereplés fontos része az oktató habitusának, egyszersmind fontos bevételi forrás is. A felsőoktatási intézmények fejlesztésében a központi költségvetési forrásokon kívül a sikeres intézmények egyéb bevételi forrásokkal is rendelkeznek, amelyek fontos, sőt meghatározó hányadát is adhatják a költségvetésnek. Ezek a források a következők lehetnek:

- közvetlen vállalati támogatás (pl. szakfejlesztési támogatás);
- pályázat.

A pályázati forma a pályáztatótól függetlenül gyakran használt eljárás a rendelkezésre álló összegek elosztására. A pályázatokon való sikeres szereplésnek sokszor alapfeltétele a pályázó korábbi tevékenysége és annak a minősége. A pályáztató ugyanis az általa felügyelt összegek hasznosulásában érdekelt és ezt általában úgy tudja elérni, ha azokat a pályázókat támogatja, akik már értek el eredményeket az adott területen. Speciális helyzetet állít elő ez a gyakorlat azokon a területeken, ahol az oktatás és a kutatás jelentős eszközigénnyel bír ennek

[1] https://vm.mtmt.hu

megfelelően magasak a költségek. Ilyen terület a műszaki tudomány és azon belül a katonai-műszaki tudomány. A kutatások költségesek a jelentős eszközigény miatt és azok a szervezetek lesznek sikeresek, ahol ezt a tevékenységet folytonosan megszakítás nélkül tudják folytatni. A folytonos kutatás tudja biztosítani a korszerűsítést, a folyamatos eredményességet és az oktató-kutató utánpótlást is. Ebből viszont következik, hogy a kezdés vagy az újrakezdés esetében kevésbé lehet számolni a pályázati forrásokkal, ezekben az esetekben megnő a központi költségvetési források jelentősége.

A folyamatos és eredményes kutatási tevékenység eredményeképpen olyan képesség jöhet létre, amely olyan értéket képviselhet, amelyeket megrendelések formájában külső szervezetek (vállalati vagy kormányzati szféra) is igénybe vehetnek. Erre jó példát jelent a hazai autóipar és a műszaki felsőoktatás kapcsolatrendszere, de jó példa az NKE HHK KLI Haditechnikai Tanszék és a HM VGH KFTO közös kutatása. [1]

A KUTATÁSI TEVÉKENYSÉG AZ ELMÚLT ÉVTIZEDBEN

Ahogy az az előző pontban tisztázva lett a kutatási területnek szoros összefüggésben kell lennie az oktatási területtel. Így a kutatás tartalmilag az oktatás kiterjesztett, meghosszabbított részeként fogható fel. A Haditechnikai Tanszék fő oktatási feladata a katonai logisztikai szakszolgálatok számára fegyverzeti, valamint páncélos- és gépjárműtechnikai szaktisztek képzése. A képzés bár jelentős műszaki tartalommal történik, nem a műszaki képzési területen van akkreditálva. A jelenlegi képzés és a korábbi (hadmérnök) képzések és azok szakmai tartalmának összehasonlításával foglalkoznak a [2], [3], [4] irodalmak.

A tanszék oktatási tevékenysége tehát műszaki területen belül történik. A kutatási tevékenység négy főcsoportba sorolható:

a. többszempontú döntési problémák műszaki adaptációja [5];
b. gépjárművezető képzés műszaki tartalma [6];
c. aknavetők műszaki megoldásai [7], [8];
d. lövedék páncéllemezen való áthatolása [9], [10];

A kutatási témákat áttekintve megállapítható, hogy valamennyi katonai-műszaki tudományági kutatásokat tartalmaz. A kutatások közül az a. a b. és a c. bekezdésekben lévőkről elmondható, hogy viszonylag kis berendezés igényű alacsony költségű kutatások. A d. pontban említett kutatás viszont kísérleteket igényel, amelyekhez lőtér, mérőműszerek és sok egyéb költséges anyagok és kiegészítő berendezések szükségesek. Általánosságban és a korábban leírtak alapján viszont elmondható, hogy az ilyen kutatásoknak lesznek olyan eredményei, amelyeket színvonalas (Scopus, IF) nemzetközi folyóiratokban is meg lehet jelentetni.

Az elmúlt évtized kutatásainak eredményességét legjobban az ebben az időszakban megjelent publikációkkal lehet jellemezni, amelyet az 1. táblázat mutat.

	Folyóiratcikk			Könyv	Konferenciaközlemény	
	Nemzetközi	Idegennyelvű	Hazai		Idegen	Magyar
Pulikációk száma:	**3**	**11**	**66**	**3**	**6**	**4**

1. táblázat A haditechnikai tanszék publikációinak a száma az elmúlt évtizedben (saját szerkesztés)

A KUTATÁSI CÉLOK

Lövedék páncéllemezen való áthatolása

A ballisztikai vizsgálatok során az elsődleges kutatási cél a lövedék áthatolása során az anyagszerkezetben bekövetkező szerkezeti változások nyomon követése volt. A kutatás során együttműködő partner volt a Szent István Egyetem Gépészmérnöki Kar Gépipari Technológiai Intézete. A kísérletet az NKE saját belső pályázatán keresztül saját forrásból támogatta. A pályázati forrás lehetővé tette a lőtér bérletének a fedezését. Ezen felül a kísérleti minták feldolgozásához szükséges anyagok, valamint azon szolgáltatások megvétele is lehetségessé vált, amelyek elvégzését a résztvevő felek saját gépparkja nem tett lehetővé. Ilyen volt például a minták alacsony hőmérsékleten történő elővágása, ami vizes technológiával lett végrehajtva. A kutatás elvégzését a rendelkezésre álló pályázatból származó fedezet rendkívüli mértékben megkönnyítette. Ennek felhasználásával, lehetett azon szolgáltatásokat megvásárolni, amelyek a kísérlet elvégzéséhez szükségesek voltak, de szervezetileg nem álltak rendelkezésre. A rendelkezésre álló költségvetés másik előnye, hogy az előre nem látott műszaki természetű problémák menet közben anyag vagy szolgáltatás vásárlásával könnyen megoldható volt.

A kutatási célok az anyagszerkezeti változások azonosítása volt, amely csiszolatok gyártásával lett kivitelezve. A kísérlet és annak eredményei hazai és nemzetközi konferencián, valamint folyóiratokban lettek publikálva.

A kísérlet lefolytatásáról összegezhető tapasztalat az volt, hogy a kutatási cél elérése alapvetően magas költségű kísérletet és feldolgozást eredményezett. A publikációk viszont nemzetközi szinten is megjelentek, tehát a költségek megtérültnek tekinthetők.

A kutatási terület másik fázisa abban tért el lényegesen, hogy ebben az esetben semmilyen forrás nem állt rendelkezésre. A kísérleteket úgy kellett megtervezni, hogy mind a kísérleti lövészet végrehajtása, mind pedig az eredmények feldolgozása saját erőforrások felhasználásával elvégezhető legyen. A lövészet végrehajtásához ennek megfelelően partnert kellett keresni, aki bérmentesen rendelkezésre bocsátja a lőterét. A HM VGH ebben a NKE törvény, valamint a NKE és a Honvédelmi Minisztérium közötti Együttműködési Megállapodás alapján partner volt. Ennek megfelelően a lövészet elvégezhetővé vált. A saját berendezések amortizációja viszont nem tette lehetővé az anyagszerkezeti változások további vizsgálatát, ezért másik kutatási célt kellett választani, ez a páncéllemezről leváló repeszek geometriájának a meghatározása lett. A kutatás sikeresen el lett végezve, viszont megállapítható, hogy a forráshiány a kutatási célok meghatározását megnehezítette, a kitűzhető célok körét jelentős mértékben szűkítette. A mérések során csak a legegyszerűbb mérőeszközök lettek felhasználva. A komolyabb műszerek használatát igénylő mérések például a repeszek sebessége nem lett elvégezve.

A forráshiány ellenére a második lövészet során is meg lehetett határozni, olyan új kutatási célokat, amely alapján tervezhető egy harmadik kísérleti lövészet. A kutatási célok pontos meghatározása viszont akkor rendelkezésre álló összeg függvényében történhet meg.

Vezetéstechnikai jellegű kutatások és előzményeik

A Nemzeti Közszolgálati Egyetem létrejötte előtt a Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Karán a Haditechnikai Tanszék oktatói által működtetetten a Bolyai autósiskola keretén belül folyt a honvéd tisztjelöltek „B” és „C” kategóriás közúti járművezető képzése. Az autósiskola vezetése, az elméleti, valamint a biztonsági ellenőrzés és üzemeltetés tantárgyak oktatása is a meglevő oktatói állománnyal valósult meg. A képzés érdekében az autósiskola saját biztonsági ellenőrzés és üzemeltetés szaktantermet hozott létre a Haditechnikai Tanszék oktatási bázisán, amelyben a közlekedési hatóság a honvéd tisztjelöltek vizsgáztatását is végre tudta hajtani. A saját képzés számos előnnyel rendelkezett,

egy hagyományos, úgymond „civil” autósiskolával szemben. A hallgatók szocializációja nem szakadt meg, végig katonai környezetben folyt a képzés, nagyrészt katona oktatók által, ezáltal megőrizve a megfelelő fegyelmezett légkört, ami elősegítette a tananyag feldolgozását, és mivel az oktatás helyben a saját bázisunkon történt, így kimaradt a kiutazással járó holt időtartam. A biztonsági ellenőrzés és üzemeltetés tantárgy, mint gyakorlati tárgy oktatása egy a Magyar Honvédségben rendszeresített gépjárművön történt, így már a hallgatók kellően korán megismerkedhettek az adott típusú gépjárművel, ezáltal nemcsak a közlekedési hatóság követelményei teljesültek, hanem a Magyar Honvédség technikai eszközét is jobban megismerték a gépjárművezető képzés során. Már az autósiskola működése alatt is több tudományos cikk készült a gépjárművezető képzés témakörében, feltárva az aktuális problémákat és megoldásokat keresve azokra. Ezek a cikkek többnyire az autósiskola működésével és feltételrendszerével voltak összefüggésben.

Az autósiskola megszűnte után tovább folytatódott a megkezdett szakmai munka, immár szakmai-tudományos vonalon. A képzés során, a több év alatt megszerzett tudást kamatoztatva számos tudományos cikk született mind a „B” és „C” kategóriás képzés vizsgálatában, mind pedig a Magyar Honvédség gépjármű technikai eszközeinek alkalmazási lehetőségeinek vonatkozásában, és több tudományos pályázatot is megalapozott. Az évek során elvégzett kutató- és tudományos munka eredményeképpen 2013-ben doktori (PhD) értekezés született „A műszaki oktatás szerepe a közúti gépjárművezető képzésben” címmel. Az értekezés tudományos kutatómódszerek alkalmazásával dolgozta fel a felmerült problémát, és az elvégzett kutatómunka által új tudományos eredmények születtek. 2014-ben az ÁROP 2.2.21. Tudásalapú közszolgálati előmenetel projekt keretében megalkotásra került „A „B” járműkategóriás gépjárművezető-képzés műszaki oktatása” című egyetemi jegyzet, amely nagymértékben segíti a honvéd tisztjelöltek oktatását. A jegyzetben kidolgozásra kerültek azon műszaki ismeretek, amelyek szükségesek a meglevő tankönyvek mellett a sikeres és hatékony első tiszti beosztás betöltéséhez. Jelenleg a honvéd tisztjelöltek „B” kategóriás járművezető képzése közbeszerzés által, külső autósiskola keretein belül valósul meg. A képzőszerv minden a közlekedési hatóság által előírt feltételt biztosít a képzéshez, ami a sikeres vizsga letételéhez szükséges. A fennálló feltételek mellett, jelen kutatási területtel foglalkozó oktatók, mégis fontosnak tartják, hogy a megszerzett tudás és a tudományos kutatómunka hasznosításaként kiegészítő tananyagot biztosítsanak a honvéd tisztjelölteknek, a mind mélyebb és korszerűbb ismeretek megszerzésének érdekében.

Jelenleg a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosító számú, ”A jó kormányzást megalapozó közszolgálat-fejlesztés” című kiemelt projekt keretében, az Egyed István Posztdoktori Program megvalósításaként folyik kutatás melynek címe „A műszaki oktatás szerepe a közszolgálatban”. A kutatási tevékenység elvégzésére 18 hónap áll rendelkezésre, amelynek eredménytermékei hat tudományos cikk és egy kismonográfia. Jelen kutatás a közszolgálatban széleskörűen alkalmazott speciális gépjárművek vezetéséről és kezeléséről szól, ezek a gépjárművek teljesen más működési feltételek között üzemelnek és szerkezetileg is lényegesen különböznek a közúti áruszállító társaiktól. A kutatás során meghatározásra kerülnek a közszolgálati járművek használatára vonatkozó járművezetési és műszaki ismeretek, korszerűsítésre kerül a tan- és vizsgaanyag. [11] A kutatás kivetítéseként felvázolásra kerülnek a műszaki oktatásnak a lehetséges fejlődési irányvonalai a várható technikai fejlődés figyelembe vételével, a közszolgálatban alkalmazott gépjárműtechnikai eszközök biztonságosabb és hatékonyabb kezelésének érdekében. A kutatási eredmények által, a magasabb és korszerűbb szintű ismeretek elsajátításával a gépjárművezetők biztonságosabban tudnak részt venni a közúti közlekedésben.

A Haditechnikai Tanszék több tanműhellyel és laborral is rendelkezik, ahol a honvéd tisztjelöltek, ezen belül jellemzően a haditechnika specializáción tanulók folytatják tanulmányaikat. A haditechnikai képzés kiemelkedően technika orientált, és a magas szintű

szakmai képzéshez rendelkezni kell a megfelelő tárgyi eszközökkel. A tanszék gépjármű diagnosztika laborja biztosítja a képzéshez elengedhetetlenül szükséges technikai hátteret. A diagnosztika labor segítségével végre lehet hajtani a gépjárművek műszaki állapotának felméréséhez és a hibák megállapításához szükséges legfontosabb diagnosztikai vizsgálatokat. A diagnosztikai labor segítségével el lehet végezni a futómű műszeres vizsgálatát, megbontás nélküli motordiagnosztikai vizsgálatokat, lengéscsillapító és próbapadi fékvizsgálatot, a motorok kipufogógázának elemzését, stb. Mivel a járműdiagnosztika rohamos fejlődésben van, így szükséges az állandó szinten tartáson (meglevő műszerek karbantartása, kalibrálása, szoftver frissítése) kívül a fejlesztés is, amely a mind újabb és korszerűbb diagnosztika eszközök beszerzését jelenti. A diagnosztika labor az adott korszerűsítések figyelembe vételével alkalmas lehet kutatási feladatok végrehajtására is, a meglevő diagnosztikai eszközök felhasználásával. A tanszék igyekszik felhasználni a megjelenő új oktatástechnikai eszközöket, amellyel elő lehet segíteni a honvéd tisztjelöltek hatékonyabb tananyag elsajátítását. [11] Új és korszerűbb tananyagok (jegyzetek, könyv) elkészítése által a tanulók megfelelő és jól tanulható ismeretekhez jutnak hozzá. A diagnosztika területén egy lehetséges kutatási irány a rezgésdiagnosztikai eljárások alkalmazási lehetőségeinek vizsgálata a Magyar Honvédség gépjármű-technikai eszközeinél, és a rezgésdiagnosztika, mint vizsgálati módszer beépítése a gépjárművek egységes technikai kiszolgálási rendszerébe. A kutatás időigényes (jellemzően hosszú időtartamú vizsgálatokra van szükség a megfelelő következtetések levonásához) eszközigényes, és érdemben csak akkor lehet foglalkozni vele, ha a mérőműszer közvetlenül rendelkezésre áll. Jelenleg a kutatási terület alapozása folyik eszköz hiányában, ennek eredményeként született meg egy a műszaki diagnosztika szerepét a technikai kiszolgálás és járműjavítás tevékenységében feldolgozó tudományos cikk. [12]

Egy lehetséges további kutatási területet képezhetnek a szemkamerával végrehajtandó vizsgálatok. A szemkamera alkalmas a gépjárművezető szemmozgásának vizsgálatára, vagyis, hogy a vezető a jármű kezelése közben mire figyel, mely külső hatások vonják el a figyelmét a vezetéstől. A vezetés során mennyi ideig kell figyelnie a kezelőszervek működtetésére, vagy pedig a visszajelzők üzem közbeni jelzéseire. A kutatás alkalmas lehet annak a megállapítására, hogy a járművezetők tevékenységét mely tényezők befolyásolják negatív irányban, akadályozva a biztonságos járművezetési tevékenységét.

ÖSSZEFOGLALÁS

A haditechnikai K+F hosszú és jelentős forrásigényű folyamat. A katonai felsőoktatáson belül ennek a tudományágnak a művelése a költséges berendezések miatt komoly nehézségekbe ütközik. A felsőoktatásban, ezen belül a katonai felsőoktatásban folytatott K+F tevékenység egyik fontos kimenete és mérhető mennyisége a kutatási eredményekről megjelenő publikációk mennyisége és minősége. A minőségi mutatók, vagyis a hazai és a nemzetközi besorolás szerinti színvonalas folyóiratokban történő megjelenés feltétele a színvonalas kutatás és a kutatási eredmények ugyancsak színvonalas feldolgozása. Ezen kettő együttese viszont feltételezi a források meglétét.

Célként megfogalmazható, hogy célszerű megcélozni azon folyóiratokat, amelyeknek van nemzetközi besorolása (WoS, Scopus), amit alátámaszt a tudománymetria napjainkban látható alakulása is.

A katonai-műszaki területek további sikeres művelésének feltétele a sikeres együttműködés mellett a források megléte. A pályázati források mellett viszont itt jelentős szerepe marad a központi költségvetési forrásoknak is.

FELHASZNÁLT IRODALOM

[1] GYARMATI J., GÁVAY GY., HAJDÚ F., BIMBÓ I.: *Védelmi célú kutatások a Hadtudományi és Honvédtisztképző Kar Haditechnikai Tanszékén, együttműködésben a HM Védelemgazdasági Hivatallal;* Hadtudomány: A Magyar Hadtudományi Társaság folyóirata 26: (3-4) (2016) (DOI 10.17047/HADTUD.2016.26.3-4.89) 89-99. o.

[2] POHL Á.: *A logisztikai tisztképzés - múlt, jelen, jövő*; In: Horváth L Attila (szerk.) 52 év a katonai logisztika szolgálatában. 2014 p. Budapest: Dialóg Campus Kiadó, 2017. (ISBN: 978-615-5680-53-3) 25-50. o.

[3] PAP A., TAKSÁS B.: *A gazdálkodási és módszertani ismeretek oktatásának összehasonlítása a (katonai) gazdálkodási és a katonai logisztika alapképzésekben;* Hadtudományi szemle 9:(2). (2016) 211-224. o.

[4] SEBŐK I., TAR CS.: *A katonai alapképzési szak fegyverzettechnikai moduljának felépítése a korábbi képzések tükrében, a szakmai tantárgyakra fordított óramennyiség szemszögéből;* Bolyai szemle 2016:(3) (2016) 11-19. o.

[5] GYARMATI J.: *Military Application of Multi-Criteria Decision Making;* Academic And Applied Research in Military and Public Management Science 14:(4) (2015) pp. 291-297.

[6] VÉG R. L.: *Az elméleti műszaki oktatás szerepe a "C" kategóriás járművezető képzésben;* Műszaki katonai közlöny 27:(1) (2017) 59-74. o.

[7] SEBŐK I.: *Az MH Haditechnikai Intézetnél utolsóként kifejlesztett 81 mm-es DE-81 SP típusú önjáró automata aknavető;* Haditechnika 49:(1) (2015) 27-31. o.

[8] SEBŐK I.: *A Haditechnikai Intézet által kifejlesztett 82 mm-es 2B9M MTLB-U alvázú önjáró autonóm automata aknavető* Haditechnika XLIX:(július-augusztus) (2015) 44-49. o.

[9] GÁVAY GY, GYARMATI J, KALÁCSKA G, SEBŐK I, SZAKÁL Z.: *Lövedék páncéllemezen történő áthaladás metallográfiai vizsgálata;* Hadmérnök 9:(3). (2014) 21-31. o.

[10] SEBŐK I.: *Különböző lövedéktípusok repeszhatása a célban;* Katonai logisztika 2016:(3) (2016) A katonai logisztika időszerű kérdései. Budapest, Magyarország: 2016.11.29 (Nemzeti Közszolgálati Egyetem) 452-461. o.

[11] VÉG R.: *Új oktatástechnikai eszközök alkalmazása a gépjárműtechnikai képzésben*; Bolyai Szemle különszám (Haditechnika 2006 szimpózium). Budapest: ZMNE nyomda, 2006. 7. o.

[12] VÉG R.L.: *A műszaki diagnosztika szerepe a technikai kiszolgálási és járműjavítási tevékenységben;* Hadmérnök 2016. XI. évfolyam 2. szám. Budapest: NKE Online kiadvány, ISSN: 1788-1919 (2016) 1-9. o.

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

A KUTATÁS-FEJLESZTÉS SZEREPE A HADITECHNIKAI ESZKÖZÖK ÉLETÚTJA SORÁN

ROLE OF R&D IN THE LIFECYCLE OF MILITARY EQUIPMENT

GYULAI GÁBOR

(ORCID ID: 0000-0001-9598-1187)

gabor.gy12@gmail.com

Absztrakt

A haditechnikai eszközök életútja során meghatározó szerepet tölt be a kutatás-fejlesztés (K+F). A folyamat sok szállal kapcsolódik az oktatáshoz, az iparhoz, a gazdasági élet számos területéhez, az alkalmazói szintekhez, illetve a logisztika egyéb területeihez. A szerző ebben a cikkben a haditechnikai eszközök életútjának mérnöki szemléletű összefüggésekre világít rá.

Kulcsszavak: *Kutatás-fejlesztés (K+F); haditechnikai eszközök; életút*

Abstract

Research & Development (R&D) plays determining role in the lifecycle of military equipment. It has bearing on the industry and a lot of fields of economy, the troops and the other fields of logistics. The author, as an engineer highlights the relationship of lifecycle of military equipment in this paper.

Keywords: *Research & Development (R&D); lifecycle; military technology*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.13.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.03.

BEVEZETÉS

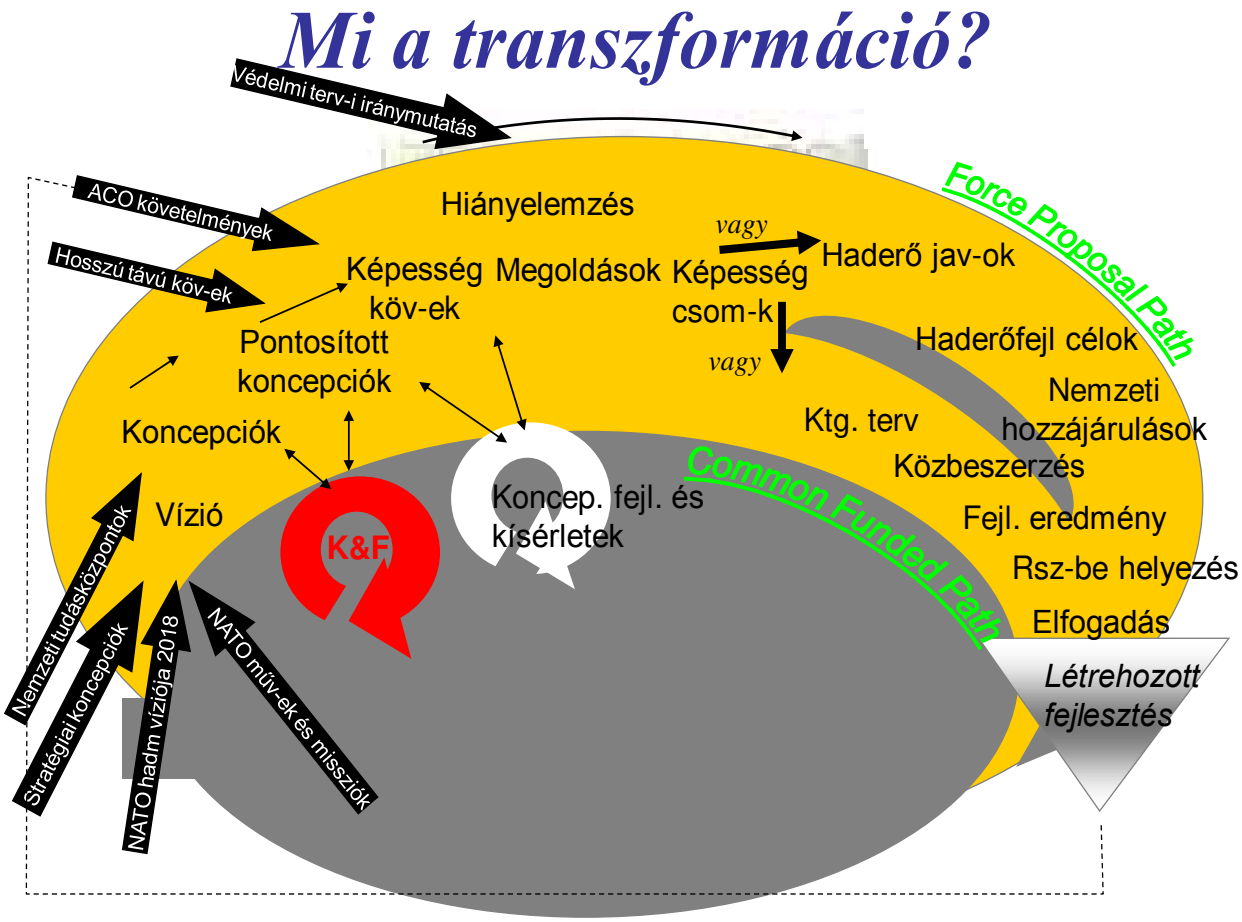
Egy ország haderejének hadrafoghatósága, alkalmazhatósága alapvetően a szervezet felépítésétől – természetesen beleértve az ott szolgálatot teljesítő személyi állomány létszámát és kiképzettségét, – a haditechnikai eszközök minőségétől és mennyiségétől, valamint ez előbbieket is figyelembe vevő (harc)eljárások kidolgozottságától függ. Ebben a cikkben a haditechnikai oldallal kívánok foglalkozni. Konkrétan: a haditechnikai kutatás-fejlesztés (továbbiakban: K+F) területével, annak is azzal a szerepével, melyet az eszközök életútjában betölt. Be fogom mutatni, hogy egy haditechnikai eszköz rendszerbeállítását milyen lépéseknek kell feltétlenül megelőznie ahhoz, hogy az megfeleljen az alkalmazói-, hatósági-, és a szabványosítási követelményeknek.

Itt, rögtön a cikkem bevezető részében egy, a témához szorosan hozzátartozó – általam fontosnak tartott – szóhasználati területtel is foglalkozni szeretnék. Ez pedig nem más, mint az „életút”, illetve az „életciklus”. A hadfelszerelési eszközökkel kapcsolatban – meggyőződésem szerint sajnos - elterjedt az "életciklus" szó használata. Ezzel nem értek egyet, és már évek óta próbálok küzdeni ellene. Nagyon valószínű, hogy ez a kifejezés az angol "lifecycle" szóból származik. Szerintem a szótárakban, – mivel ezeket sokkal inkább nyelvészek készítik, mintsem a szakterületek alapos ismerői – sem helytálló a fordítás. A lényeg, szerintem: A "ciklus" szó olyan folyamatokat, jelenségeket takar, amelyek esetében az ismétlődés fontos kritérium. Tehát, ciklusa van a periodikusan ismétlődő jelenségeknek például a forgó mozgásnak, a föld keringésének, illetve forgásának, az évszakok változásának... A hadfelszerelési eszközök megtervezéséhez, kifejlesztéséhez, gyártásához, alkalmazásának, illetve kivonásának folyamatához nem rendelhető periódusidő, így tehát – szerintem – ciklusuk sem lehet. (A rendszeres karbantartás, illetve az időszakos javítás tekintetében lehet létjogosultsága a ciklus kifejezésnek, ez azonban az eszköz életútjának csak egy meghatározott szakaszához köthető.) Tehát a technikai eszközök vonatkozásában sokkal pontosabb meghatározás az "életút", ezért használom ezt.

A HADITECHNIKAI ESZKÖZÖK ÉLETÚTJA

Annak szemléltetésére, hogy a haditechnikai eszközök, illetve rendszerek életútja során hol és milyen módon játszik szerepet a bevezetőben meghatározott K+F tevékenység összeállítottam egy folyamatábrát, melynek alapjául a [1-3] hivatkozási számú dokumentumok mellett saját tapasztalataim szolgáltak. Ez utóbbiak jelentős részéhez, – mint a NATO K+F szervezete (akkor RTO, most STO) szakmai munkájában 10 évig résztvevő tag – a partnerországok képviselőivel folytatott konzultációk révén jutottam. (Helyenként – a fentiekre alapozva – saját elképzeléseim is megjelennek a folyamatábrán, illetve az annak működését taglaló magyarázatokban, illetve javaslatokban.)

Annak szemléltetésére, hogy a NATO Transzformációs Parancsnoksága (Allied Command Transformation = ACT) hogyan képzeli el az átalakítás folyamatát, és ebben a folyamatban hol helyezkedik el a haditechnikai K+F az 1. számú ábrát hívom segítségül.



1. ábra A haditechnikai K+F helye a NATO-átalakításban
(forrás: „NATO Erőforrás- menedzsment” című előadás, melyet Dr. Szenes Zoltán ny. vezds. CSc 2011. 02. 16-án a Vezérkari Tanfolyam résztvevői számára tartott)

Az ábrából számomra az olvasható ki, hogy a K+F tevékenység egy örökösen megújuló folyamatba ágyazva, a koncepciókkal és követelményekkel folyamatos kölcsönhatásban funkcionáló részfolyamat. (Természetesen az itt vázolt ciklikus folyamat nem keverendő össze a technikai eszközök – bevezetésben említett – életútjával!) Most azonban a folyamat azon részeire kívánok koncentrálni, melyek fókuszában egy új, illetve felújított technikai eszköz kialakítása áll. Ebben a fent említett (az írás végén található 2. számú ábra) folyamatábrát veszem alapul.

1. A folyamat ismertetését a „*hadműveleti követelmények megfogalmazása*” blokkal kezdem. Ebben a fázisban történik meg a konkrét igény megfogalmazása, melynek alapját a stratégiai célok, valamint a gyakorlati tapasztalatokon nyugvó alkalmazói igények képezik. Ez az első olyan platform, ahol meg kellene jelennie – a biztonságpolitikai-, stratégiai és egyéb hazai-, és nemzetközi kutatási eredmények mellett – a műszaki tudományok, illetve a technikai-technológiai kutatási eredmények „kínálatának” is. Ezt azért tartom fontosnak, hogy a hadműveleti követelmények megfogalmazásában már ne lehessenek irreális, a fizika, a matematika vagy egyéb természettudományok törvényeit figyelmen kívül hagyó, „álomszerű” igények. Tehát ebben a fázisban a politikusok, az alkalmazók és szinte valamennyi szakterületet képviselő kutatók konszenzusára van szükség ahhoz, hogy az egy bizonyos tervidőszakra vonatkozó valamennyi igényt pontosan meg lehessen fogalmazni. Ez azért is nagyon fontos, mert, ennek alapján egy előzetes

prioritási sorrend felállítására is szükség van a későbbi döntés optimalizálása érdekében.

2. A következő fázis, az „*elemzés*” során fokozott szerephez jutnának a mérnökök, akinek a termelői logisztika egyéb területeivel összhangban kell javaslatot kidolgozni arra vonatkozólag, hogy az igényelt eszköz egy meglévő modernizálása révén vagy új eszköz vásárlása, illetve kifejlesztése útján valósuljon meg. Ez az a fázis, ahol – véleményem szerint – az eddigieknél sokkal távolabbra látóan, komplexebben gondolkodva kellene a döntési javaslatokat kidolgozni. A komplex szemlélettel rendelkező szakemberek véleménye és saját tapasztalataim alapján állítom, hogy a külföldről beszerzett eszközök jelentős része csak „első ránézésre” tűnik olcsóbbnak és jobb választásnak a hazaiaknál. Természetesen tisztában vagyok azzal, hogy egy ilyen „nem kellően körültekintő” tervezésnek egyik fő oka, hogy a kalkulációban nagyon sok olyan paramétert, illetve szempontot kellene figyelembe venni, melyeket nem lehet, illetve csak nagyon nehezen lehet számszerűsíteni. Ilyenek lehetnek például az alábbiak:
    - Egy itthon fejlesztett, illetve gyártott eszköz esetében annak javítása általában sokkal gyorsabban, rugalmasabban megoldható, mint a külföldi esetében, – különösen, ha nem európai országról van szó, vagy nincs a cégnek állandó magyarországi szervizképviselete.
    - Könnyű belátni, hogy az itthon fejlesztett, illetve gyártott eszköz esetében annak későbbi modernizálása vagy – szoftverek esetén – frissítése is sokkal egyszerűbben megoldható.
    - A külföldi fejlesztések, illetve beszerzések esetén gyakran találkozunk fordítási pontatlanságokból adódó problémával, amely a hazai termék beszerzése esetén nem jelentkezik.

A másik fő ok a – mérnökök számára nem is igen követhető és érthető - gazdasági-pénzügyi szabályozásokra vezethető vissza, illetve az ezekre a szabályozásokra épülő sajátos szemlélet merevnek tűnő alkalmazásaira. Ilyenek lehetnek például az alábbiak:

- Egy bizonyos terület „gazdája” csak a számára, illetve a tevékenységi területre „megcímzett”, jóváhagyott forrásokkal tud számolni. Az átcsoportosítás például az „intézményi” rovatból a „felhalmozási” oszlopba szinte kilátástalan próbálkozás. A szükségletek gyors, hatékony kielégítése egy költségvetési szervnél sosem lehet olyan rugalmas, mint a mindennapi életben. Amikor tízezer forinttal a zsebemben és elsőszülött fiammal a kezemben annak idején elindultam moziba, de menet közben a játszótéren – máig is rejtélyes és érthetetlen körülmények között – a gyermekem cipőjének levált a talpa és a nadrágjának térde környékén a szövet folytonosságában erőteljes hiányosságok keletkeztek gyors és célravezető elhatározásra kellett jutnom: a mozi elmaradt és helyette új lábbeli és nadrág soron kívüli beszerzésére került sor. Szerintem a döntés logikus és minden tekintetben indokoltnak értékelhető. Hasonló jellegű szituációk a napi életben is előállhatnak: Amikor például egy „zónázási” mérés végrehajtása közben egy speciális mérőkábel meghibásodik – és a mérési sorozatból még két-három napra való feladat hátra van és az egésszel a hét végéig végezni kellene (!) – a szabályok értelmében az életnek meg kell állnia. A Magyar Honvédség főtisztjének nincsen joga a fent említett családi példa algoritmusa szerint megoldani a problémát. Szolgálati jegy → beszerzési eljárás legalább három árajánlattal… → legalább fél év mire lesz új kábel… (!) → a feladat végrehajtása a legjobb indulattal sem kaphatna „real-time” jelzőt.

- Az éves költségvetés tervezése általában az előző év augusztusában szokott kezdődni. Az ezzel foglalkozó kollégák ekkor szokták megkérdezni, hogy mennyi pénzt tervezzenek K+F-re. Természetesen ilyenkor még közelítőleg sem lehetne összeget mondani, hiszen a következő évre vonatkozó K+F tervkötet – hivatalosan – leghamarabb december közepén kerülhet jóváhagyásra. (A gyakorlatban – az egyeztetések elhúzódása miatt – mindig legalább 2-3 hónap késéssel tudott csak elkészülni a tervkötet. Az átmeneti, átszervezési időszakokban ez még tovább húzódik. (Meglátásom szerint az elmúlt évtizedben az átszervezések szinte egymást érik…) A másik ok, ami miatt augusztusban még nem lehet „megcímkézve" betervezni a K+F költségeket a folyamatábrából is kiolvasható: A felmerülő igénynek, – amelyik már hadműveleti követelményekkel is rendelkezik – már túl kellene lennie azon a döntésen, amely meghatározza az igény kielégítésének módját (modernizálás, fejlesztés, beszerzés). A leírtakból következik az a javaslatom miszerint a fejlesztési pénzek felhasználásának lehetőségeit sokkal rugalmasabbá kellene tenni.

3. A folyamatábrán – „*K+F*", illetve „*korszerűsítés*" vonalán – továbbhaladva a K+F szűkebb értelembe vett algoritmusa alapján működő szakaszba érünk:
   - A "*megvalósíthatósági értékelés*" elkészítése a HTI, illetve utódszervezeteibe tartozó témafelelősnek a feladata. Ennek lényege a feladat megvalósíthatósági lehetőségeinek számbavétele, illetve a lehetőségek elemzése. Az értékelés kimeneteként egy (esetleg több) javaslat születik a feladat műszaki megoldásra, illetve arra vonatkozólag, hogy a folyamat a kísérleti fázissal, vagy az eszközfejlesztési fázissal folytatódjon. A javaslat elfogadásáról a Tudományos Műszaki Tanácsülés (TMT) dönt. A TMT-n hivatalos résztvevője valamennyi a fejlesztésben érintett szakember, valamint az alkalmazó képviselője. A TMT határozati javaslatának jóváhagyása az FHH főigazgatójának, illetve fegyverzettechnikai igazgatójának volt a hatásköre néhány évvel ezelőtt. Azóta – a folyamatos átszervezések miatt – többször is változás volt. Jelenleg nem TMT, hanem egyeztetések zajlanak, melyekről emlékeztetők készülnek.
   - A kísérleti szakasz első lépéseként a *Harcászati Műszaki Feladat (HMF)* kidolgozására kerül sor. Ebben olyan eszköz kifejlesztése a cél, amelyet „teljesen az elejéről" kell kezdeni. Ilyen esetben, a folyamatnak ebben a fázisában még nem lehet pontosan megfogalmazni a fejlesztendő eszközzel szemben támasztott követelményeket, csak körvonalazni azokat. Tehát a HMF-ben gyakoriak a következő jellegű megfogalmazások: „az eszköz legyen képes a tervezett hőmérséklettartományban az alábbi funkciók végrehajtására:…"; „Lehetőleg rendelkezzen még az alábbi funkciókkal:…". Nagyon sok fontos paraméter általában ekkor még csak megközelítőleg (maximálva vagy minimálva) határozható meg. Például: „Az eszköz maximális tömege legyen 20kg" vagy „Az eszköz legyen képes saját akkumulátoráról – újabb feltöltés nélkül – legalább 12 órát üzemelni; HMF műszaki tartalmának kidolgozása komplex mérnöki feladat – nagyon sok egyeztetéssel és kompromisszummal.
   - A HMF alapján készül el a „*kísérleti minta*" (régebbi, polgári kifejezéssel „deszkamodell"). Ez utóbbi kifejezés nagyon találó, ugyanis – az esetek többségében – egy hevenyészetten összetákoltnak tűnő, de – alapfunkcióit tekintve – működőképes szerkezetet értünk alatta. Ennek a fázisnak a végeredménye tehát egy funkcionálisan működő olyan eszköz, amely

produkálja (optimális esetben) valamennyi tőle előzetesen elvárt üzemmódot és funkciót. Külalakját tekintve azonban – és többek között ennek köszönhetően is – klimatikai-, mechanikai ellenállósági követelményeknek való megfelelése szempontjából még nem rendelkezik a megkívánt végső paraméterekkel, azonban elegendő információkkal szolgálhatnak ezek meghatározására.

- A következő lépés a *kísérleti minta vizsgálatait* valamint az eredmények értékelését foglalja magában. Ennek lényege, hogy a HMF-ben leírt elvárásokkal össze kell hasonlítani az elkészült kísérleti mintát, illetve mag kell állapítani, hogy ezeken kívül mire képes még az eszköz. A vizsgálatok eredményeképpen egy „*Vizsgálati jegyzőkönyv*" készül az eredmények rögzítése céljából. A vizsgálati jegyzőkönyv alapján kerül összeállításra a „*Beszámoló jelentés*", amely arra hivatott, hogy a tervezett funkciók tekintetében is összevesse az eredményeket az elvárásokkal, értékelje azokat és javaslatot tegyen a TMT számára. A kísérleti szakasz lezárását a TMT határozata jelenti, amely alapvetően kétféle lehet: pozitív eredmények esetén a következő, eszközfejlesztési fázisba lép tovább a folyamat; részsikerek esetén a kísérleti minta módosítására (újabb kísérletek és vizsgálatok…), illetve – az alkalmazókkal folytatott egyeztetések nyomán akár – a HMF módosítására is sor kerülhet. A gyakorlat azt mutatja, hogy egy harmadik, reális kimenetel is lehet: a téma felfüggesztése (pl.: átmeneti forráshiány miatt), illetve (az eredmények elégtelenek voltak, illetve forráshiány vagy koncepcióváltás miatt) a témának ebben a fázisban történő lezárása, törlése. Ez utóbbi lehetőséget a folyamatábrán nem tüntettem föl ugyan, de gyakorlatilag a döntéshozó bármikor, a folyamat bármely pontján élhet a fenti opciók (felfüggesztés, lezárás) bármelyikével.
- A következő, eszközfejlesztési fázis „sarokköve" a *Harcászati Műszaki Követelmények (HMK)* elnevezésű dokumentum, melynek nemcsak itt, hanem a rendszeresítéshez vezető valamennyi úton kulcsszerepe van. Ebben minden olyan követelményt pontosan meg kell határozni, melyet az eszköznek életútja során (az előállítástól a megsemmisítésig, illetve újrahasznosításig) ki kell, hogy elégítsen. A HMK elkészítésének alapja fejlesztés esetén a HMF valamint a kísérleti minta vizsgálatai nyomán meghatározott adatok. Új eszköz vásárlása esetén a helyzet egy kicsit könnyebb, hiszen kész gyártmányok, termékek paramétereinek szakszerű összerendezéséről, illetve az alkalmazói igényekkel, követelményekkel való összefésüléséről van szó.
- Fejlesztés esetén a HMK alapján elkészült eszköz a „*minta*". Ennek a fázisnak a belső algoritmusában ugyanazokra a lépésekre kerül sor, mint a kísérleti szakaszban. A különbség az, hogy a minta már egy használható, kész eszköz, amely – ideális esetben – rendelkezik valamennyi a HMK-ban megfogalmazott funkcióval, illetve kielégíti a HMK-ban megfogalmazott valamennyi követelményt. Annak ellenőrzése, hogy ez valóban így van-e két lépcsőben zajlik: *laboratóriumi vizsgálatok* és a *katonai alkalmazhatósági vizsgálatok (KAV)* szakasza. (Ez utóbbi további két részre osztható, de erről később, a *d)* pontban fogok írni.) A laboratóriumi vizsgálatok során valamennyi olyan ellenőrzésre sor kerül, melyeket laboratóriumi körülmények között el lehet végezni például az eszköz szélső értékekig történő lehűtése, illetve felmelegítése a peremfeltételekként megadott páratartalom mellett, vagy az úgynevezett „rázópados"

vizsgálatok… A laboratóriumi vizsgálatok eredményeiről jegyzőkönyv készül, amely alapján TMT határozatban dönt az eszköz haditechnikai ellenőrző vizsgálatokra bocsáthatóságáról, illetve a további módosításokról – indokolt esetben a HMK egyes részei is módosításra kerülhetnek.

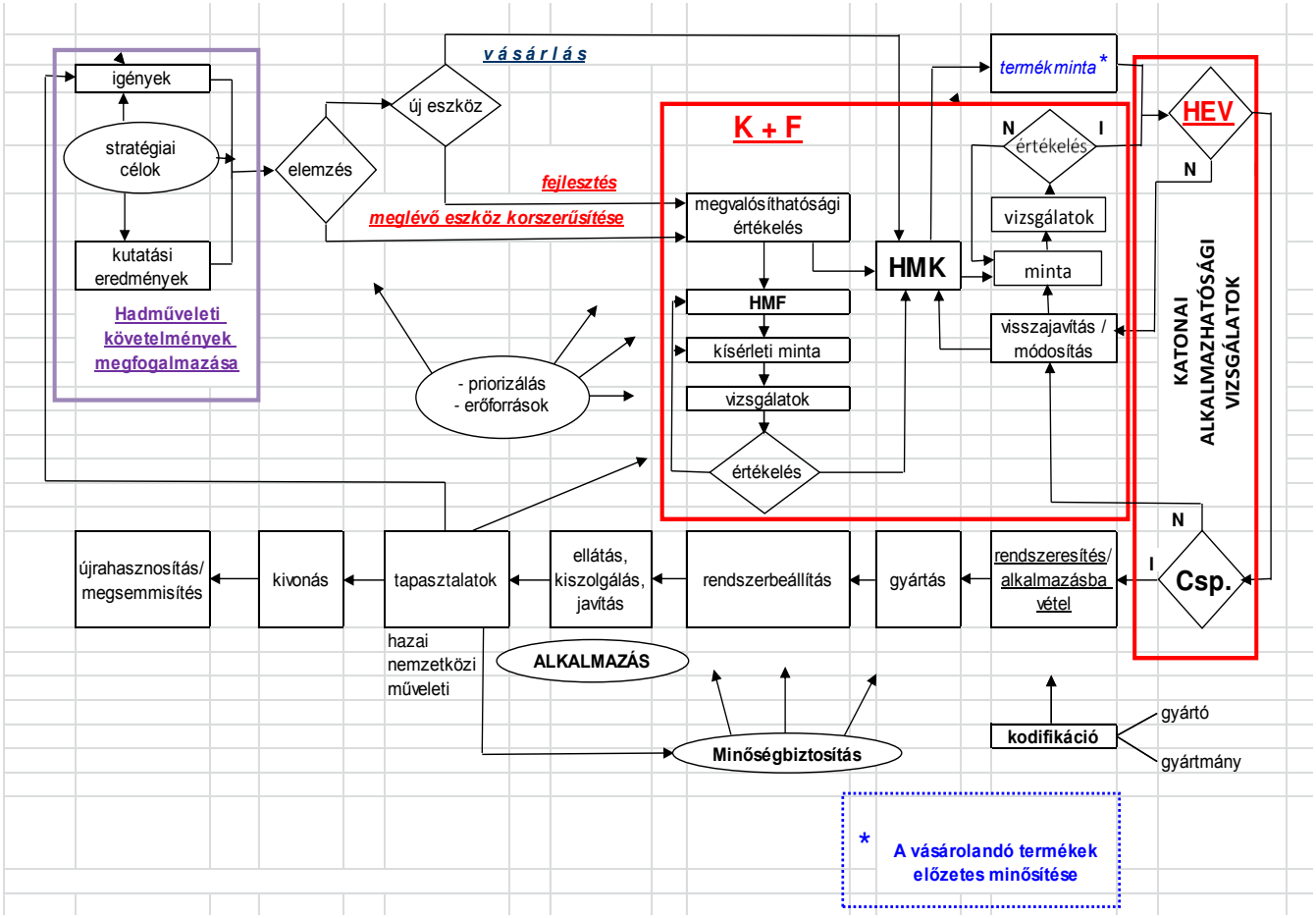
4. A folyamat következő fázisa a *KAV*, amely két jogilag is elkülönülő szakaszból áll: a *haditechnikai ellenőrző vizsgálatokból (HEV) és a csapatpróbából (Csp.*).
   - A HEV során kell valamennyi olyan vizsgálatot, tesztelést végrehajtani, melyet laboratóriumi körülmények között nem lehet végrehajtani, valamint ennek részét képezik a különféle hatósági (tűz-, és munkavédelem, közlekedésfelügyeleti, érintésvédelmi…) vizsgálatok is. Ennek azért van nagy jelentősége, mert nem csak azt kell megállapítani, hogy az eszköz funkcionálisan rendelkezik valamennyi elvárt képességgel, hanem azt is, hogy alkalmazása során sem veszélyes-e használójára, illetve annak környezetére. Ennek a fázisnak az eredményes lezárásáig az alkalmazók – az ellenőrzött körülmények között folytatott kísérletek, illetve vizsgálatok kivételével – jogszerűen nem használhatják az eszközt. Ezért van az, hogy a beszerzési eljárás eredményeként megjelenő „termékminta" esetében is szükséges a HEV végrehajtása. Fontos megjegyezni, hogy ebben az esetben sokkal egyszerűbb szokott lenni a folyamat mivel ezek a termékek nagy része rendelkezik akkreditált laboratórium által kiállított vizsgálati eredményekkel, különféle hatósági bizonyítványokkal, esetleg NATO nyilvántartási számmal (NSN) is. Optimális esetben – ha rendelkezésre áll valamennyi szükséges dokumentum és a HMK(!), – ilyenkor a HEV mindössze néhány nap alatt végrehajtható, mivel ekkor elegendő a termékhez benyújtott dokumentációk tartalmának összehasonlítása a HMK-ban leírtakkal. A HEV eredménytelensége esetén a K+F útján ide került eszköz a „visszajavítás", illetve módosítási fázisba kerül vissza, a termékminta esetében általában a gyártótól további dokumentumok bekérésére szokott sor kerülni. Indokolt esetben a HMK is módosításra kerülhet.
   - A *csapatpróba* az eszköz rendszeresítéséhez vezető úton, az utolsó ellenőrzési fázis, melynek általános célja, hogy valamennyi a HMK-ban deklarált alkalmazási feltétel között kipróbálják az alkalmazók, hogy az eszköz képes-e valamennyi HMK-ban megfogalmazott funkcióját ellátni. Ekkor kell ellenőrizni olyan fontos képességeket is, mint például az interoperabilitás, kezelhetőség… A csapatpróbát, melyek vezetője az alkalmazó szervezet valamely vezető beosztású főtisztje annál az alakulatnál kell végrehajtani ahol az eszközt rendszeresítésre tervezik. A csapatpróba végrehajtását követően a bizottság javaslatot tesz az eszköz módosítások nélküli rendszeresítésére, vagy rendszeresítésére utólagos módosításokkal (ebben az esetben arra is javaslatot kell tenni, hogy ennek megtörténtét követően a csapatpróbát meg kell-e ismételni teljesen vagy csak részlegesen, illetve nincs szükség újabb csapatpróbára). Természetesen még ekkor is születhet akár olyan döntés is, hogy nincs szükség a kifejlesztett, modernizált vagy éppenséggel beszerzett eszközre.
5. A következő lépés (inkább a „nagy ugrás") az eszköz *rendszeresítése*, illetve *alkalmazásba vétele*. A rendszeresítés a MH egészére, vagy több szervezetére vonatkozó döntést takar, míg az alkalmazásba vétel csak egy speciális részére. Ahhoz, hogy a rendszeresítési bizottság elé kerülhessen egy eszköz – elméletileg – arra van szükség, hogy a KAV-on megfelelő minősítést kapjon. Mivel ezeknek a

vizsgálatoknak a lényegét a HMK-ban megfogalmazott követelményeknek való megfelelőség ellenőrzése jelenti, állítottam azt néhány bekezdéssel feljebb, hogy a HMK a folyamatnak olyan „sarokköve", melynek „a rendszeresítéshez vezető valamennyi úton kulcsszerepe van". HMK híján nem lenne minek alapján vizsgálni, illetve mivel összevetni a vizsgálati eredményeket… A rendszeresítés egy következményekkel járó aktus, egy döntés, amely a Honvédségi Közlönyben is megjelenik. A rendszeresítés folyamatához kapcsolatosan említem meg a kodifikációt, melynek röviden annyi a lényege, hogy egységes jelölési rendszer alapján besorolja a gyártót és a gyártmányt is egyaránt.

6. Ezt követően kezdődhet el a *gyártás*, illetve az eszközök *beszerzés*e. Itt említem meg, hogy a K+F folyamat valamennyi mozzanata során valamilyen formában jelen van a minőségbiztosítás. A katonai minőségbiztosítási feladatok a beszerzések minőségbiztosítását, a szállítók minőségirányítási rendszereinek tanúsítását, és a NATO kölcsönös minőségbiztosítási feladatait (Állami minőségbiztosítás) foglalják magukban. Az Intézet jelenleg is az ISO 9001-es minőségbiztosítási rendszernek megfelelő algoritmussal dolgozik, melyből a „gyártásközi ellenőrzés", valamint a „végátvétel" jelentkezik ebben a szakaszban. (A HM TH rendelkezett ISO 9001-es tanúsítvánnyal, azonban ennek megújítása 2008-ban, az önálló szervezet megszűnését követően már elmaradt. Fennállása alatt az FLÜ, illetve az FHH vezetése is tervezte a tanúsítvány ismételt megszerzését, de erre nem kerülhetett sor.)
7. Az eszközök beszerzése nyomán kezdődhet meg a *rendszerbeállítás* folyamata, amely a csapatok eszközökkel való feltöltéséből, illetve a kapcsolódó logisztikai feladatokból, a kiképzésből, szakutasítások elkészítéséből, stb. áll.
8. A (hadi)technikai eszközök alkalmazása is több részfolyamatból tevődik össze, mint például: üzemeltetés, fenntartás, használat, tárolás, szállítás, illetve az ezekhez kapcsolható egyéb kiszolgálási feladatok, melyek közül az ábrán csak az alábbi kettőt emeltem ki:
    - Az ellátás, valamint a kiszolgálás és szükség szerinti javítás folyamatában látszólag kizárólag az alkalmazónak és a logisztikai rendszernek van szerepe. Azonban nem szabad figyelmen kívül hagyni, hogy ekkor keletkezik azoknak az információknak a nagy része, melyeket az „a)" pontban említettem, mint a hadműveleti követelmények összeállításához szükséges bemeneti információk egyike. Amennyiben a rendszer jól működik, akkor a folyamatban résztvevő valamennyi szereplő megérti ennek – a folyamat hatékonysága szempontjából lényeges visszacsatolás – fontosságát.
    - A legtágabb értelemben vett alkalmazói – tehát a hazai-, nemzetközi-, illetve műveleti területekről származó valamennyi közvetett és közvetlen – tapasztalatok összegyűjtése és rendezése, majd továbbítása jelenti a folyamat „zárását". Azért tettem idézőjelbe a zárás szót, mert – mint azt az „a)", illetve „b)" pontban írtam – egy következő folyamat egyik bemenetét is jelenti egyben. Ez különösen igaz abban az esetben, ha a felhasználói igény kielégítése a meglévő eszköz korszerűsítése révén valósul meg.
9. Egy (hadi)technikai eszköz „szolgálati idejének" végét a rendszerből történő kivonás jelenti, amely egy – a rendszeresítési bizottság által hozott – határozattal történik.
10. Az életút vége – ezeknek az eszközök esetében is – a megsemmisítés, illetve az újrahasznosítás. Annak, hogy az eszköz esetleg további értékesítésre kerül-e, vagy

nem csak abban van jelentősége, hogy ennek végrehajtásáért a Tárca vagy a vevő a felelős.

Megítélésem szerint a NATO Logisztikai Kézikönyvének 17. fejezetében [4] megfogalmazottak elvileg ugyanazokat a fázisokat takarják, melyeket a fentiekben leírtam – természetesen korántsem azzal a részletességgel. A dokumentum nagy erényének tartom az előkészítő jellegű fázisok (követelmények meghatározása, megvalósíthatóság, stb.) hangsúlyozottságát.



2. ábra A haditechnikai eszközök, rendszerek életútja (saját szerkesztés)

KÖVETKEZTETÉSEK

Ebben a cikkben arra kívántam rámutatni, hogy egy (hadi)technikai eszköz életútjában milyen sokrétű folyamatként jelentkezik annak megtervezése, illetve kivitelezése. A mindenoldalú tervezési-, és döntési pontok bármelyikének indokolatlan kihagyása előreláthatatlan idő-, anyagi-, illetve legsúlyosabb esetben személyi veszteségekhez vezethet. Világosan látszik, hogy a követelmények, elvárások gyakori változtatása teljesen ellehetetleníti a csapatok (hadi)technikai eszközökkel történő ellátását. Több vezető beosztású személytől hallottam már a „ciklusokon átívelő” tervezésről is, azonban ennek maradéktalan megvalósulása – véleményem szerint – eddig még váratott magára. Mint a haditechnikai K+F területén 20 évig dolgozó hadmérnök a *Harcászati Műszaki Követelmények* meglétének, illetve annak pontos összeállításának fontosságát kívánom hangsúlyozni. Ennek logikája nagyon egyszerű: Addig nem kerülhet (hadi)technikai eszköz rendszeresítésre, amíg nem vett rész a csapatpróbán → addig nem kerülhet (hadi)technikai eszköz csapatpróbára, amíg nem vett rész haditechnikai

ellenőrző vizsgálatokon → csak akkor mondhatja ki a HEV, majd a csapatpróba, hogy „*megfelelt*", ha létezik pontosan megfogalmazott HMK, melyben megfogalmazott követelményekkel a vizsgálatok során össze lehet hasonlítani az eszközt. Tehát a HMK nemcsak a K+F tevékenység alapját képező kulcsfontosságú dokumentuma, hanem a kész termék beszerzésén alapuló eljárási rendnek is.

A folyamat fenti, részletes ismertetésével arra is rá kívántam világítani, hogy ez a folyamat mennyire összetett, és érzékeltetni, hogy abban minden lépésnek meg van a maga nélkülözhetetlen szerepe. Nem az a lényeg, hogy egyes dolgok időközben átnevezésre kerültek (például: a TMT-t már nem annak hívják, hanem „egyeztetésnek"), hanem a folyamat logikai menete! Cikkemmel azt is el szeretném érni, hogy azok, akik „alkalmazói szemmel nézik a világot" is lássák, megértsék a folyamatot, – abból a remélhetőleg nem túl naiv elképzeléssel, – hogy ezáltal annak türelmesebb, sőt aktívabb közreműködőjévé válnak.

A K+F tevékenység is egy olyan folyamat, melynek logikai felépítése évszázadok alatt fejlődött ki, és jelentéktelennek mondható eltérésekkel a világon mindenütt hasonlóan működik. Tehát erre is igaznak tartom azt a mondást, miszerint: *„Azért mert időközben feltalálták a teflonbevonatot, még nem kell a nagymama bevált receptjeit válogatatlanul kidobni!"*

Reményeim szerint az ebben a cikkben leírtak alapján – kiegészítve a Hadtudomány 2016. évi különszámában megjelent írásomat [5] – az is könnyebben elképzelhető, hogy egy ilyen összetett folyamat mennyivel egyszerűbb, rugalmasabb lehet abban az esetben, ha az eszközök fejlesztése, illetve gyártása, szervizelése, stb. hazai bázison zajlik.

FELHASZNÁLT IRODALOM

[1] 17/2006. (HK6.) *HM utasítás a hadfelszerelési anyagok rendszeresítéséről és rendszerből történő kivonásáról, Honvédelmi közlöny CXXXIII. évfolyam 6. szám, 2006. március 1.*

[2] A haditechnikai K+F egységes metodikája (1141/1983 HM MN Haditechnikai Fejlesztési Főnöki intézkedés - hatályba léptetve a 72/1989 MN fegyverzeti és technikai főcsoportfőnöki intézkedéssel)

[3] http://www.nato.int/docu/logi-en/1997/lo-924.htm (A letöltés ideje: 2011. 04. 02.)

[4] NATO LOGISTICS HANDBOOK http://www.nato.int/docu/logi-en/logistics_hndbk_2012-en.pdf (A letöltés ideje: 2017. 08. 31.) pp. 177-186

[5] GYULAI G.: *A hazai haditechnikai kutatás-fejlesztés komplex megközelítése;* Hadtudomány XXVI. évfolyam, 2016. évi különszám; 103-117. o. (DOI-azonosító: 10.17047/HADTUD.2016.26.K.103)

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

AUTONÓM FELSZÍNI JÁRMŰVEK AKKUMULÁTORAI ÜZEMÁLLAPOTÁNAK VIZSGÁLATA SZIGMOID FÜGGVÉNNYEL

ANALYSIS OF THE BATTERIES OF THE AUTONOMOUS GROUND VEHICLES USING SIGMOID FUNCTION

MENYHÁRT József; SZABOLCSI Róbert

(ORCID: 0000-0001-5541-7565); (ORCID: 0000-0002-2494-3746)

jozsef.menyhart@eng.unideb.hu; szabolcsi.robert@bgk.uni-obuda.hu

Absztrakt

Az autonóm felszíni járművek fedélzetén a leggyakrabban villamos energiát használnak a hajtástechnika, a szenzorrendszerek, a fedélzeti informatikai-, és telekommunikációs rendszerek működtetésére. Az autonóm felszíni járművek fedélzetén a villamosenergia tárolás egyik széles körben alkalmazott eszköze az akkumulátor. Az akkumulátorok helyes üzemeltetésének, töltésének és kisütésének, az akkumulátor műszaki állapotának egyik régről ismert, klasszikus módszere a feszültségmérés. Ez a módszer a feszültségmérés elvét, és azt a módszert használja, hogy a mért feszültségértékeket előre megadott minimum, vagy maximum értékekkel hasonlítjuk össze. A szerzők által javasolt lágyszámítási módszer segítségével az akkumulátorok megfelelő szintű biztonság mellett mélyebben kisüthetőek, és nagyobb feszültségre tölthetőek, tehát számottevően növekszik az akkumulátorok hatásfoka. A javasolt műszaki állapotbecslés Fuzzy-elvű megközelítésre épül, hiszen egy akkumulátor kicsit mélyebb kisütése, és egy esetleges kicsit nagyobb feszültségre történő feltöltése rendszerint nem eredményezi annak tönkremenetelét.

Kulcsszavak: *Autonóm felszíni jármű, MATLAB, Fuzzy logika, szigmoid függvény.*

Abstract

Autonomous ground vehicles use mostly electrical energy to activate drive systems, and to supply vehicle sensor systems, onboard electronics and telemetry systems. The electrical energy used is stored into batteries. The batteries technical status, discharging and charging processes are monitored via voltage measurement and control. This maintenance strategy is based on voltage measurement and comparing measured voltages with those voltage levels preliminary defined both for discharging and charging processes. Basic idea of the authors based upon using soft computing methods outlined in the paper allowing to extend possible domain of the lower and upper voltage levels of the batteries simultaneously guaranteeing safety level at the same or at the better level. The proposed method will allow to improve efficiency of the battery maintenance. The method introduced is based on Fuzzy logic, namely sigmoid functions are applied to estimate technical status of the batteries allowing to take into consideration both deep discharging, or, overcharging a bit the batteries with no serious consequences.

Keywords: *Autonomous ground vehicle, MATLAB, Fuzzy logic, Sigmoid function*

A kézirat benyújtásának dátuma (Date of the submission): 2017.08.30.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.23.

BEVEZETÉS

A modern járműgyártók egyre inkább az alternatív járműhajtásokat kezdik előnyben részesíteni. A gyárak energiaforrásként a villamos áramot jelölték meg, amelynek felhasználása, és a hozzá kapcsolódós energiatárolók és hajtásrendszerek robbanásszerű fejlődésen mennek keresztül, elég itt csak a Tesla cég járműveire gondolni. A technikai fejlődés mellett fontos megjegyezni, hogy a járművek karbantartásához és üzemeltetéséhez elengedhetetlen a megfelelő infrastruktúra és karbantartási folyamatok fejlesztése is.

Az új hajtásláncok használata szigorú előírásokhoz kötöttek, amelyek megszegése komoly műszaki károkat képes okozni. Fontos megjegyezni, hogy a karbantartást végző személyeknek megfelelő tapasztalattal is rendelkezniük kell. Bizonyos üzemeltetési körülmények között a felhalmozott emberi tapasztalat felülírhatja a gépkönyvekben lévő utasításokat, szabályokat.

A jelenleg nagy népszerűségnek örvendő „Lean” elvek érvényesülése miatt a fentebb írt tapasztalati adatokra való támaszkodás kiemelkedően fontos egy gyár mindennapjaiban. A gyakorlatban léteznek olyan esetek, amikor a vevők igényeinek kiszolgálása felülbírálja a karbantartási és üzemeltetési szabályokat és folyamatokat, tehát a robotok és járművek karbantartása később történik meg, mint az az előírások szerint elvárható lenne. Gondoljunk csak a saját autónkra, amikor a járművet az előírt szerviz intervallumon túl használjuk.

Fontos elvárás, és alapvető követelmény, hogy a járművek fedélzetén alkalmazott villamos energiatároló (akkumulátor) a lehető legnagyobb kapacitással rendelkezzen, hogy a jármű mozgását a lehető leghosszabb ideig biztosítani tudja. Az akkumulátorok optimális kihasználásához egyre összetettebb üzem menedzsment rendszereket fejlesztenek és használnak. Ezek a rendszerek az akkumulátorok paramétereit figyelik, töltés vezérlést végeznek, valamint naplózzák a jármű üzemeltetési adatait. A modern előremutató fejlesztések alapján ezek a rendszerek már különböző, a mesterséges intelligenciához kapcsolódó algoritmust használnak.

A karbantartási stratégiák tervezése során a tapasztalati adatokat fontos figyelembe venni. Ezen tapasztalatok minden esetben az emberi hozzáértésen és szakértelmen alapulnak. A cikk a következő fejezetekből áll: az első fejezetben bemutatjuk az AGV és UGV rendszerek, majd a második fejezetben a Fuzzy logika kerül ismertetésre. A harmadik fejezet a szigmoid függvényeket mutatja be, míg a negyedik fejezet a szigmoid függvények lehetséges alkalmazását vázolja a gyakorlatban, végül következtetéssel és irodalomjegyzékkel zárul a cikk.

AGV ÉS UGV RENDSZEREK

A legtöbb gyárban egyre népszerűbbek a különböző automata anyagmozgató berendezések, amelyek főleg robotokra és önvezető járművekre épülnek. Iyen robotok például az AGV-k (Automated Guided Vehicle). Hasonló robotok nem csak zárt környezetben fordulhatnak elő, hanem a gyárak kapuin kívül is, ahol úgynevezett UGV-ket (Unmanned Ground Vehicle) alkalmaznak. Az AGV és UGV rendszereket külön kell kezelni a gyakorlatban. Felépítésük hasonló, mégsem ugyanazokról az eszközökről van szó [1, 2].

Az ’Unmanned’ szó személyzet nélkülit jelent magyarra fordítva, tehát az Unmanned Ground Vehicle-t személyzetnélküli szárazföldi járműnek lehet fordítani. Ezek a járművek olyan elektro-mechanikus berendezések, amelyek képesek különféle összetett mozgásokra. Mozgásuk előzetes tervezését fejlett szenzorrendszerek segítik, valamint speciális számítógépes hardware-rel és szoftveres formában megjelenő logikai feltételekkel képesek végrehajtani navigációs feladataikat, és elviselni a környezeti behatásokat és változásokat.

A személyzet nélküli rendszerek képesek az előírt feladatot teljesen, vagy annak egy részét önállóan, autonóm módon elvégezni.

Az ilyen jellegű járműveknek több változatát ismerjük, ezeket széles körben alkalmazzák katonai és polgári vonatkozásban egyaránt. (U**x**V):

- levegő (air): UAV
- vízi: UUV (Unmanned Underwater Vehicles), USV (Unmanned Surface Vehicles)

A fent említett járművek mindegyike tartalmazza a következő részeket:

- mechanikai elemek (hajtás, energiaellátás, alváz, felépítmény stb.)
- elektronika
- rakomány/hasznos teher
- kommunikációs rendszer
- vezérlő
- felhasználói interfész

A felsorolás alapján látható, hogy a járművek vagy robotok közel ugyanazokból az elemekből épülnek fel, érdemi különbséget a feladatuk és azok ellátásának módja között lehet felfedezni.

Az Automatic/Automated Guided Vehicle (AGV) felépítésében és működésében hasonló jeleket mutat, mint UGV-k. Számítógép vezéreltek, kezelő nélküliek, elektromos meghajtásúak és többnyire anyagmozgatásra és logisztikai feladatokra használják őket termelő üzemekben, mint például Milk Run körjáratok. Ezek a robotok valamilyen jelölést vagy felfestést követnek a padlón, vagy optikai navigációt alkalmaznak, esetleg valamilyen mágneses anyagot használnak, hogy a megfelelő pályán végig tudjanak haladni. A viszonylag kötött pálya miatt többnyire ipari környezetben használják őket. Az első AGV-t 1953-ban készítette a Barrett Electronics of Northbrook Illinois-ban az Amerikai Egyesült Államokban. 1973-ban a Volvo a svédországi Kalmar üzemében több mint 280 AGV-t kezdett el használni különböző anyagmozgatási és logisztikai célokra. 1976-ban megjelent az első egységrakomány szállítására alkalmas AGV.

Használatuk elterjedésének számos okát ismerjük. Monoton, ismétlődő munkákat végeznek, valamint nehéz anyagokat mozgatnak sokkal nagyobb pontossággal, mintha azt gépkezelők vagy logisztikusok végeznék. Fontos megjegyezni, hogy több műszakban is üzemeltethetők, pihenőidő nélkül.

A rendszer felépítését tekintve az könnyen bővíthető, illetve a robotok útvonala könnyen módosítható. Az UGV-kel ellentétben nem távirányítással működnek, hanem előre meghatározott úgynevezett körjáratokon végeznek feladatokat. Ezáltal működésük kiszámíthatóbb, karbantartásuk könnyebben tervezhető. Termelő vállalatoknak ez nagyon fontos, és a napjainkban népszerű Lean termelési filozófia keretein belül kiemelten fontos a kiszámíthatóság, amíg egy ember adott esetben eléggé bizonytalan tud lenni.

AGV-nek több típusát különböztetjük meg:

- Villás
- Vontató
- Egységrakományos
- Egyéb

Az előre meghatározott útvonaluk számítógép segítségével készül el. Négy különböző módon közlekedhetnek üzemen belül:

- Optikai: színes jelölők
- Huzal: beágyazva a padlóba
- Inercia: giroszkóp, mágnesek segítségével
- Lézer

A termelőüzemek nagy része zárt vagy részben nyitott, ebből kifolyólag az AGV-k meghajtására nem lehet belső égésű motort vagy hibrid rendszereket használni. Az AGV működtetéséhez villamos energiára van szükség, amelyet akkumulátoraiban tárol. AGV-ket manapság már nemcsak az autóipar használ, hanem egyéb más területeken is megfigyelhetők, mint kutatásfejlesztés, egészségügy vagy a repülőterek.

Az 1. ábrán látható AGV egy egységrakományt szállít. Megfigyelhetők a padlón lévő jelölések, amelyeket mozgása során követ.

1. ábra Automated Guided Vehicle

A FUZZY LOGIKA

A Fuzzy egy angol eredetű szó, amelyet *életlennek*, vagy *homályosnak* lehet fordítani. A Fuzzy logikát a pontatlanság egy fajtájaként is meglehet közelíteni, amelynek a célja, hogy a túlságosan összetett problémákat, feladatokat egyszerűen lehessen kezelni. Mérnöki vagy műszaki szempontból a Fuzzy logika hatalmas jelentőséggel bír [3, 4].

Sok szakirodalomban a Fuzzy logikát úgynevezett elmosódott halmazok logikájaként lehet megtalálni, ami valójában számos elméletet takar. Számos szakirodalom hivatkozik különböző példára, hogy egyszerűen érthetővé váljon a Fuzzy logika lényege. A leggyakrabban használt példa az úgynevezett Szóritész paradoxon.

A paradoxon egy homok vagy kavics kupacról szól. Ha egy kavicskupacból elveszünk egy kavicsot, attól még az a kupac, kavicskupac marad. Tehát akárhány kavicsot veszünk el, a kavicskupacnak, kavicskupacnak kell lennie. A valóságban viszont ez nem lehetséges, egy bizonyos mennyiség elvétele után már nem beszélhetünk kavicskupacról. Hasonló példa még az úgynevezett kopasz ember paradoxonja is. Egy dús hajú ember nyilvánvalóan nem kopasz. Ha egyenként kihúzzuk a hajszálait, hol lenne az a pont, ahol már kopasz emberről beszélünk? Mindkét paradoxon esetében a lényeg az, hogy a jellegzetességek fokozatosan, apránként változnak vagy tűnnek el. Ebből kifolyólag lesz olyan állítás, amely nem nevezhető igaznak, de ugyanakkor hamisnak sem, mert csak részben igazak. A Fuzzy logika az az eszköz, amely megengedi a részben igaz állításokat.

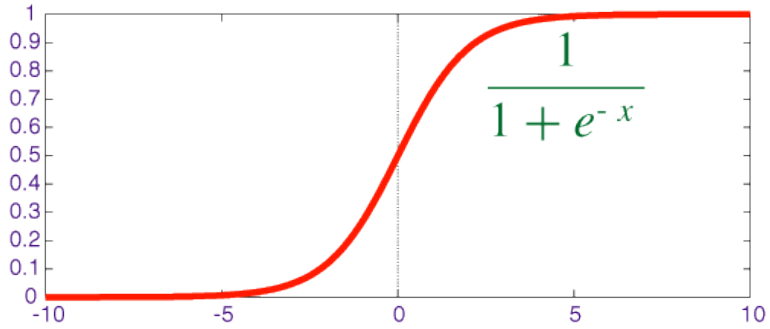
SZIGMOID FÜGGVÉNYEK

A Fuzzy tagsági függvények egy leképezést, vagy leképezéseket valósítanak meg. Ez a leképezés a vizsgált terület alaphalmazbeli (vagy univerzum béli) értékei és a [0, 1] intervallum között történik. A tagsági függvény (μ) feladata, hogy kifejezze, hogy az univerzum béli elem milyen mértékben tartozik egy úgynevezett nyelvi értékkel leírt csoportba. Ilyen vizsgálatra és leírásra alkalmazzák az úgynevezett szigmoid függvényeket.

A szigmoid függvény nem más, mint egy gyűjtőnév, amely az ’S’ alakú függvényképpel rendelkező valósértékű, folytonos függvényeket foglalja össze. Az ilyen függvények

jellegzetessége, hogy szimmetriát mutatnak az induló és a megállapodó tartományban, rendelkeznek egy monoton felfutási szakasszal, egy középső lassan változó szakasszal, valamint egy a növekedést megközelítő konstans szakasszal [5, 6].

A felsorolt 3 szakasz egy 'S' betűre hasonlít, mint ahogyan azt 2. ábra szemlélteti.



2. ábra Szigmoid függvény

Bizonyos folyamatokról hiányozhat részletes leírás és információ, ezeket a szigmoid függvény pótolhatja és ábrázolhatja az adott függvényt vagy folyamatot. Nagyon gyakran a szigmoid függvény az úgynevezett logisztikai függvényre utal.

A logisztikus függvények a XX. század folyamán kezdtek el egyre nagyobb népszerűségnek örvendeni, amikor a statisztikai számítások fontos fejlődésen mentek keresztül. Manapság a logisztikus függvényeket inkább neveznénk determinisztikus trendmodell alapfüggvényének. A folyamatokra jellemző, hogy egy bizonyos pontig vagy ideig növekedést mutatnak, majd elérnek egy olyan szakaszt, amikor a növekedés korlátjai érzékeltetik hatásukat, ennek hatására e növekedés csökkenni kezd, és végezetül, egy idő után pedig megközelíti a nullát.

A logisztikus függvény általános alakja [3, 4, 5, 6]:

$$y_t = \frac{k}{1+ae^{-bt}}, \tag{1}$$

$k, a, b > 0$ paraméter eloszlásokkal. Később ettől eltérő paraméterezést is használtak. A különböző paraméterek az (1) függvény más és más tulajdonságait befolyásolják.

A szigmoid függvény általános alakja, amely könnyen alkalmazható Fuzzy függvényekhez [3, 4, 5, 6]:

$$\mu_i(x) = \frac{1}{1+e^{a_i(b_i-x)}} \tag{2}$$

EREDMÉNYEK ÁBRÁZOLÁSA SZIGMOID FÜGGVÉNNYEL

Korábbról ismeretes, hogy az akkumulátorok műszaki paramétereinek gyakorlati értékei mást mutathatnak, mint a katalógusokban és a gyártói weboldalakon megadottak. A 1. táblázatban egy tetszőleges lítium polymer akkumulátor adatai láthatók.

Kapacitás	90 Ah
OV	2,8-4V
Tömeg	3 kg
Méretek	143X61X218

1. táblázat A felső szinthez tartozó igazságértékek értékei (saját szerkesztés)

A feszültségszintek szabályzását minden esetben az úgynevezett BMS (Battery Management System) egység látja el. Gyártói előírások alapján ismert az akkumulátorok működési feszültségtartománya, annak alsó, és felső értéke, amelyek megfelelően hosszú élettartamot és kiváló üzembiztonságot adnak az akkumulátoroknak.

Az akkumulátorok gyakorlati üzemeltetési tapasztalatai azt mutatják, hogy az akkumulátor-üzemeltetés az előírtaktól eltérhet, tehát az akkumulátor akár többlettöltést is felvehet, vagy adott esetben, előfordulhat bizonyos határok között az akkumulátorok mély kisütése is.

A fent vázolt lágyszámítási módszer alkalmazásának szemléltetésére méréseket végeztünk, melynek adatait a 2. táblázat foglalja össze [3, 4, 5, 6]. A táblázat értelemszerűen tartalmazza a mért alsó-, és felső feszültségértékeket, valamint a gyártó által megadott maximális és minimális feszültségértékeket is.

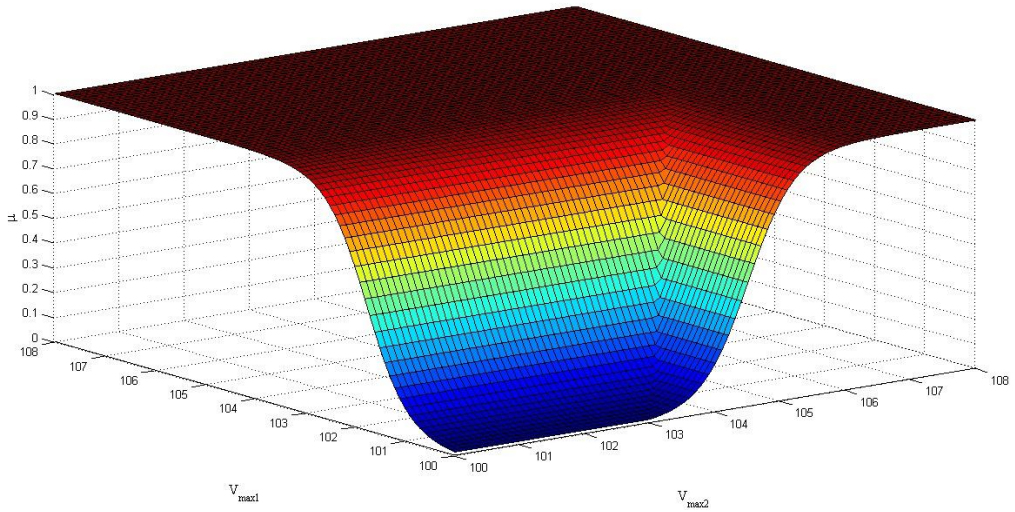
Mérések száma [db]	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.
Felső feszültség értékek [V]	3,6	3,68	3,69	3,7	3,74	3,75	3,781	3,82	3,83	3,833
Gyártó által előírt maximális feszültség [V]	3,55									
Alsó feszültségérték [V]	2,2	2,25	2,283	2,293	2,456	2,534	2,574	2,697	2,713	2,965
Gyártó által előírt minimum feszültségérték [V]	3									

2. táblázat Az előírt és a mért feszültségparaméterek (saját szerkesztés)

Az előző fejezetben ismertetett szigmoid függvény segítségével az akkumulátorok feszültség paraméterei ábrázolhatók MATLAB program segítségével. A 3D-s felületen egyértelműen látszanak a töltési stratégiák közötti különbségek, amelyeket eltérő színek jelölnek. Az ábrázoláshoz alkalmazott képlet a következők:

$$\mu(V_{max1}; V_{max2}) = \mathrm{MAX}\left(\frac{1}{1+e^{a_{V_{max1}}\left(b_{V_{max1}}-x\right)}}; \frac{1}{1+e^{a_{V_{max2}}\left(b_{V_{max2}}-x\right)}}\right) \quad (2)$$

A 3. ábrán 3 tengely látható, x, y és z. A μ értéke a függőleges tengelyen, míg a két vízszintes tengelyen a feszültségértékek olvashatók százalékos értékben. A jobb oldalán az SVM-mel is megvizsgált, míg a baloldalon a csak Fuzzy logikával vizsgált. Az ábrázolt 3D-s grafikonon, ahol a függvények felülete látszik színek is segítik a könnyebb megértést. Üzemeltetési szempontból a piros színnel jelölt területek jelentenek nagy kockázatot, míg a kék színnel jelölt részek nagyfokú megbízhatóságot mutatnak.



3. ábra V_{max1} és V_{max2} igazságértékeinek felülete

A 3D-s grafikonok segítségével az akkumulátorok feszültségértékei ábrázolhatók és a színekkel ellátott grafikon a lehető legjobban tükrözi két töltési stratégia közötti különbséget. Ennek segítségével a szemléltetés egyszerűbb és átláthatóbb, a tapasztalati adatok és becslések könnyebben elhelyezhetők a színes 3D-s felületeken és könnyebb őket értelmezni, mint puszta számokat.

KÖVETKEZTETÉSEK

A cikk összefoglalja az AGV és UGV rendszerek közötti fontosabb hasonlóságokat és ismerteti az UGV-k felhasználási lehetőségeit különböző helyszíneken, legyen az levegő vagy víz. A harmadik fejezet a Fuzzy logikát ismerteti és annak felhasználását, majd a következő fejezet a szigmoid függvényekkel foglalkozik. A Következtetések fejezet előtt pedig a szigmoid függvények segítségével megvizsgáltunk két elméleti akkumulátortöltési stratégiát.

A kapott 3D függvényképen jól látható a két töltés között az eltérés, melynek ábrázolására a szigmoid függvények kiválóan alkalmasak. Gyakorlati szempontból láthatóvá válnak azok a pontok és tartományok, ahol az akkumulátorok még megfelelő szintű biztonsággal üzemeltethetőek.

Összességében kijelenthető, hogy a szigmoid függvények segítségével az akkumulátorüzemeltetési paraméterek jól modellezhetők és kiválóan megjeleníthetők. Az így végzett vizsgálatokból több információ nyerhető hosszú távon úgynevezett Big Data elemzésekkel, amelyek akár több ezer mérési eredményt foglalnak magukba. A nagyszámú mérés eredményeinek köszönhetően a kitolt üzemeltetési határok pontosabbak lesznek, így maximalizálva az akkumulátorok teljesítményét és élettartamát.

FELHASZNÁLT IRODALOM

[1] SZABOLCSI R., MENYHÁRT J.: *Loads Affecting UGVs'*. Review of the Air Force Academy, No. 3. (30) 2015, pp(15-20).

[2] Szabolcsi, R., Menyhárt, J.: *The Importance of Maintenance During UGV Use*. Land Forces Academy Review, No4:(80/2015), pp(486-492).

[3] POKORÁDI, L., MENYHÁRT, J.: *Electric Vehicles' Battery Parameter Tolerances Analysis by Fuzzy Logic*, Proceedings of the 11th IEEE International Symposium on

Applied Computational Intelligence and Informatics, May 12-14, 2016. Timisoara, Romania. ISBN 978-1-5090-2380-6, pp(361-364). DOI: 10.1109/SACI.2016.7507402.

[4] POKORÁDI L., MENYHÁRT J.: *Elektromos jármű akkumulátorok paraméter-eltéréseinek Fuzzy elemzése*. IFFK 2016, Budapest, 2016. augusztus 29-31., ISBN: 978-88875-3-5, pp(1-6).

[5] MENYHÁRT J., SZABOLCSI R.: *Support Vector Machine and Fuzzy Logic*. Acta Polytechnica Hungarica, ISSN 1785-8860, Vol 13: (No5), pp. 205-220. (2016). DOI: 10.12700/APH.13.5.2016.5.12.

[6] SZABOLCSI, R., MENYHÁRT, J.: *Battery Voltage Limit Analysis with Support Vector Machine and Fuzzy Logic*. Advances in Military Technology, ISSN 1802-2308, Vol12: (No1), pp(21-32), 2017.

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

ÁLLOMÁSOK ÉS ÁLLOMÁSKÖZÖK ZAVARÁNAK GRÁFELMÉLETI ALAPÚ VIZSGÁLATA A MAGYARORSZÁGI VASÚTHÁLÓZATON

GRAPH THEORY-BASED ANALYSIS OF THE EFFECT OF BREAKDOWNS OF STATIONS AND LINE SECTIONS ON THE RAILWAY NETWORK OF HUNGARY

TÓTH Bence

(ORCID: 0000-0003-3958-187X)

toth.bence@uni-nke.hu

Absztrakt

A cikkben bemutatok egy, a magyarországi vasúthálózatot modellező súlyozott irányított gráfot. Ennek segítségével kiszámítom az egyes állomáspárok közötti minimális menetidőket és menetvonalhosszokat, valamint hogy ezek mekkora része érinti az egyes állomásokat és állomásközöket. Vizsgálom továbbá az egyes hálózati elemek zavarának hatását a teljes vasúthálózatra.

Kulcsszavak: *kritikus infrastruktúra, vasúthálózat, gráfelmélet, legrövidebbút-probléma*

Abstract

A weighted directed graph modelling the railway network of Hungary is presented. Using this graph, the minimal running times and lengths of paths are calculated for every pair of stations. The ratio of these paths passing through each station and line section is determined. The effect of the damage of each station and line section on the whole system is also examined.

Keywords: *critical infrastructure, railway network, graph theory, shortest path problem*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.06.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.12.05.

BEVEZETÉS

A vasút mindig is alapvető szerepet töltött be a szállításban, közlekedésben. Infrastruktúrájának a közúthoz képesti drága kiépítését és fenntartását [1; 28-29. o.] ugyanis ellensúlyozza, hogy nagyobb távolságokra a közúti fuvarozáshoz képest „viszonylag olcsón egyszerre nagy tömegű árut és utastömeget képes szállítani" [1; 35. o.] (bár hogy mekkora az a távolság, amelynél ez már megéri, az egyes publikációk erős szórást mutatnak: 150-300 km [2], kb. 200 km [3], 200-350 km [4], 500-750 km [5]).

A vonatkozó kormányhatározat alapján „kritikus infrastruktúrának minősülnek azon hálózatok (...) melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére." [6],[7] Ezen definíció alapján a vasúthálózat is kritikus infrastruktúra, és mivel „Magyarország felszíni közlekedési hálózata erősen sugaras szerkezetű, és alapvetően egy (Budapest) központú, egy-egy kritikus műtárgynál bekövetkező »folyamatossági hiány« (pl. rombolás, baleset, hóakadály, sztrájk) komoly forgalomkiesést eredményezhet" [8]. Zavarérzékenysége és nehéz védhetősége miatt terrorfenyegetettség szempontjából az ún. puha célpontok közé tartozik [9], hiszen a teljes magyarországi „vasúthálózat vágányainak és műtárgyainak álladó őrzése és technikai megfigyelése megoldhatatlan feladatot jelent", a jelenlegi erőforrások „csak a fontosabb műtárgyak és néhány vonalszakasz időleges védelmét teszik lehetővé." [10]

De általánosan is elmondható, hogy a vasúti közlekedés a hálózat neuralgikus pontjain [11] fellépő bármilyen eredetű zavarra rendkívül érzékeny. A hálózat egy pontjának sérülése esetén ugyanakkor elvárt lenne, hogy legyen „viszonylag rövid időn belül (a sérülés nagyságától függően 1-3 nap) helyreállítható a vasúti közlekedési rendszer működőképessége, vagy aktiválhatók a szükséges helyettesítő kapacitások." [12]

Annak összehasonlításához, hogy az egyes hálózati elemek zavara mekkora hatást gyakorol a hálózatra, célszerű ezen hatásokat számszerűsíteni. Jelen cikknek ez a fő célja egy egyszerű modell keretein belül.

MAGYARORSZÁG VASÚTHÁLÓZATÁNAK GRÁFMODELLJE

Magyarország vasúthálózata a 2016-os adatok alapján 7 438 kilométernyi építési hosszú normál nyomtávú vasúttal rendelkezik [13], ez 8,00 km/100 km^2 vonalsűrűséget jelent. Ennek a hálózatnak a leírására kell keresni egy jól illeszkedő matematikai modellt, melyen a konkrét számolások elvégezhetők. Erre egy élsúlyozott gráfot [14; 36. o.] használtam, azaz egy olyan gráfot, melynek élein adott egy ún. távolságfüggvény, mely azonban nem csak fizikai távolságot jelenthet, hanem egy általánosabb távolságfogalmat takar, ami lehet például az út költsége vagy (ahogy esetünkben is) az időszükséglete. Az élsúlyozott modellgráfban – értelemszerűen – az egyes állomások voltak a gráf csúcsai, a köztük levő vasútvonal-szakaszok pedig az élek [14; 3. o.].

Alapfogalmak

Gyakran használt fogalmak lesznek a menetvonal, annak hossza és a hozzá tartozó menetidő. A vonatkozó törvény alapján [15] „menetvonal: a vasúti pályahálózat kapacitásnak az a része, amely egy adott időszakban egy vonat két pont között történő közlekedtetéséhez szükséges". A menetvonal hosszát annak két végpontja között a hozzá tartozó útvonal hosszaként értelmezzük és kilométerben mérjük. A két végpont között sok menetvonal lehetséges különböző állomások érintésével, melyeknek így a hossza különböző. A definícióban szereplő „adott időszak", melyben a vonat közlekedik, a menetidő, azaz az érkezési és az indulási

időpontok különbsége (melyet percben mérünk). Az egyes állomáspárok közti menetvonalaknak ez a két tulajdonsága az a két paraméter, melyekre a számolásokat elvégzem. Más lehet ugyanis egy menetvonal konkrét útvonala és így az időtartama és a hossza is, ha a menetidőre vagy magára a megtett útra, annak hosszára, a menetvonalhosszra optimalizálunk.

Állomások

A megállóhelyek, ahol a vonatfordulás nem lehetséges, nem voltak a gráfban csúccsal reprezentálva, de az olyan állomások sem, melyek egy vonalszakasz közbenső állomásai. Csak az elágazó- és csatlakozó állomások [16; 23. o.] szerepeltek tehát csúcsként a gráfban, ez alól kivételt csak a zsákvonalak végpontjai és a határátmenetek, valamint az ez utóbbiakat közvetlenül megelőző állomások, a határállomások jelentettek.

Állomásközök

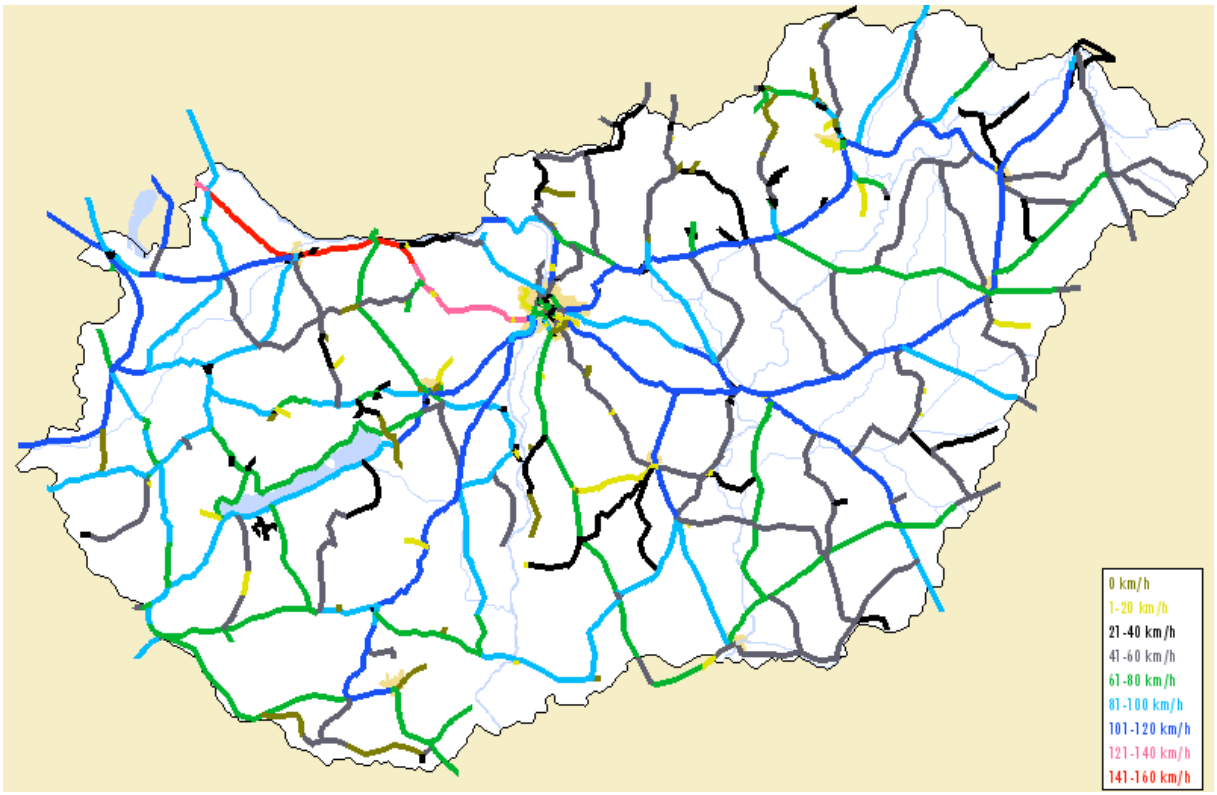
Állomásköz alatt a két szomszédos állomás közötti nyílt pályát értjük. Mivel jelen modellben nem szerepel minden magyarországi állomás, itt az „állomásköz” fogalmat a gráfelméleti „él” értelemben fogom használni, azaz a magyarországi vasúthálózatot leíró gráf egyes éleit fogom így nevezni, melyek a csúcsokkal reprezentált állomásokat összekötik.

A súlyozás, azaz az egyes élekhez hozzárendelt távolságfüggvény-érték, vagy az adott állomásköz hossza volt kilométerben vagy az adott állomásközre érvényes maximális engedélyezett sebesség alapján számított menetidő percben. A vontatási nem, a tengelyterhelés, a vágányok száma nem szerepel a modellben.

Az egyes állomások egymástól mért távolságainak fő forrása a VPE Kft. weblapján [17] elérhető értékek voltak. Néhány, itt nem szereplő iparvágány hosszadata a vonatkozó kormányrendelet [18] alapján lett a modellbe beépítve, az ebben sem szereplőké pedig a Google Maps-en [19] végzett saját távolságmérések alapján.

Az egyes állomások közötti menetidők ezen távolságadatok és az engedélyezettsebesség-értékek [17],[20],[21] alapján lettek meghatározva. Ez természetesen azt is jelenti, hogy ezek a menetidő-értékek egy alsó korlátot képviselnek, melyek még a tiszta menetidőnél [22; 65. o.] is alacsonyabbak, mivel pl. az indítási és a fékezési idők, az ívekben engedélyezett alacsonyabb sebességértékek, az esetleges lassújelek (állomásiak is), a terepviszonyokból adódó sebességcsökkentések, melyek mind növelik a menetidőt, nem lettek figyelembe véve. De általánosságban is elmondható, hogy jelenleg a magyarországi vasúti pályáknak csak kevesebb mint kétharmadán közlekedhetnek a vonatok a kiépítési sebességgel [23],[24].

Itt jegyezném meg azt is, hogy bár a TEN-T hálózat részét képező vonalszakaszokon (lásd pl. [25]) elvárt lenne a legalább 160 km/h-s engedélyezett sebesség [26],[27], a MÁV-Start Zrt. tájékoztatása szerint [28] jelenleg csak az 1-es számú vasútvonal Tata és Hegyeshalom közti szakaszára van ez a sebesség engedélyezve, ott is csak legfeljebb 18,0 tonna tengelyterhelésű szerelvényeknek. Bár a pálya alkalmas 22,5 tonna tengelyterhelésű vonatok közlekedésére is, ezek csak 120 km/h-s korlátozott sebességgel közlekedhetnek [29]. Az egyes vonalakra engedélyezett maximális sebességeket lásd az 1. ábrán.



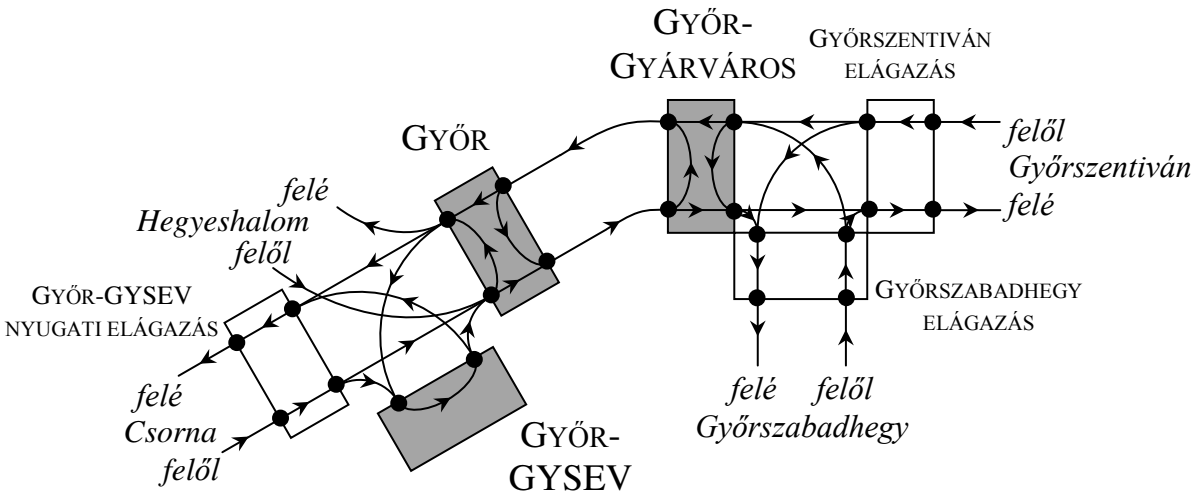
1. ábra Az egyes magyarországi vasútvonalakra engedélyezett maximális sebesség. [17]

Emiatt a számolásaimhoz, lévén célom a vasúti szállítás modellezése, a nagyobb tengelyterheléshez tartozó kisebb engedélyezett sebességet vettem figyelembe. Hasonlóan, amelyik pályaszakaszokon a motorkocsikra nagyobb sebesség engedélyezett, mint mozdonnyal továbbított szerelvényekre [30] ott is a kisebb, mozdonyos szerelvényre vonatkozó engedélyezettsebesség-értéket vettem alapul.

Irányváltás

Figyelembe vettem ugyanakkor az egyes állomásokon esetlegesen szükséges irányváltás idejét, mégpedig úgy, hogy egy ilyen fordulás egy előre meghatározott értéket, 15 percet [22; 234. o.],[31] adjon hozzá a teljes menetidőhöz. Ennek érdekében minden állomást (pontosabban minden elágazást, a deltavágányok egyes kitérőit is) négy csúcsként reprezentáltam a gráfban (ezt csúcsszéthúzásnak nevezzük, lásd [32]). Például Győr állomás esetében annak keleti és nyugati oldalán is definiáltam egy bemeneti és egy kimeneti pontot, melybe, illetve melyből a szomszédos állomásokat reprezentáló csúcsokba, illetve csúcsokból a gráf élei be- és kifutnak. Az állomásokon való fordulás időigényét egy, az azonos oldali bemeneti és kimeneti csúcsok közötti 15 perc súlyú éllel lehet reprezentálni. Emellett szükséges még a gráf egyes éleinek irányítása [14; 21-22. o.], hogy a kimeneti pontok biztosan kimeneti pontokként, a bemenetiek pedig bemenetiekként funkcionáljanak és ne legyen lehetséges irányváltás a 15 perc súlyú élek elkerülésével (lásd példának a 2. ábrán a Győr-GYSEV → Győr → Hegyeshalom útvonalat, melyben irányítás nélkül a Győr → Hegyeshalom útvonal indulhatna Győr állomás nyugati bemeneti pontjából is, figyelmen kívül hagyva az irányváltás időszükségletét. Az állomásokon való áthaladásnak a modellben nincs extra időszükséglete, ezen élek súlya 0 perc. Mivel deltavágányon fordulás nem lehetséges, csak áthaladás, ezért bár szintén négy ponttal reprezentáltak a gráfban, csak 0 perc súlyú áthaladó élek tartoznak hozzájuk. Minden, állomást leíró él távolság-súlya 0 km volt.

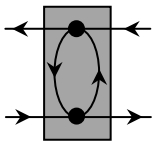
Fejállomások esetében, ahol csak egy bemeneti és egy kimeneti irány van (és ez a kettő megegyezik), az állomás reprezentálásához elég két csúcs köztük egy 15 perc súlyú éllel.



2. ábra Magyarország vasúthálózata gráfmodelljének felépítési elvei Győr és néhány környező állomás (szürke) és deltavágány (fehér) példáján szemléltetve (saját szerkesztés)

Egy kimeneti pontot természetesen akármennyi, másik állomáshoz tartozó bemeneti ponttal összeköthet egy-egy irányított él (állomásköz).

Az állomások megvalósíthatóak lennének egyszerűbben is, két csúcs és a két irányváltást leíró él segítségével (3. ábra), azonban mint később látni fogjuk, ez nagyban elbonyolítaná egy állomás zavarának leprogramozását.



3. ábra Alternatív megoldás állomás reprezentálására (saját szerkesztés)

A számításokhoz használt gráf

A számolások alapjául szolgáló gráfban 291 állomás szerepel. Az ezeket leíró csúcsokon felül szerepel még benne 26 csúcs, melyek deltavágányokat írnak le. A gráf összesen 1808 élt tartalmaz, melyből 730 él (365 él-pár) szomszédos állomások közti viszonylatot, a többi az állomások „belső szerkezetét” és a deltavágányok kapcsolatát írja le. Mindegyik élhez tartozik két súly, egy hosszúságérték km-ben és egy menetidőérték percben. A számítások során természetesen egyszerre csak az egyiket rendelhetjük hozzá az élekhez. Az azonos viszonylathoz tartozó két ellentétesen irányított él súlya megegyezik. A későbbiekben az erre a két súlyozott gráfra való hivatkozás egyszerűsítése érdekében jelöljük a menetidőkkel súlyozott gráfot G_t^{00}-vel, a távolságokkal súlyozottat pedig G_ℓ^{00}-lel.

A gráfokat leíró éllista a súlyokkal együtt letölthető a http://www.octans8.hu/railway01/ weblapról a később bemutatandó térképek nagyfelbontású változataival és az összes, állomásokra és állomásközökre vonatkozó numerikus eredménnyel együtt.

A SZÁMÍTÁSI MÓDSZEREK

Az alábbiakban röviden bemutatom a számolásokhoz használt programot, módszereket, eljárásokat.

A legrövidebb út számolása

A két állomás közötti, menetidő vagy menetvonalhossz szempontjából legrövidebb út számítása az `R` programozási nyelv és környezetben [33] történt a Csárdi Gábor és Nepusz Tamás által kifejlesztett `igraph` csomag [34] `distances()` függvénye segítségével. Ez a függvény olyan élsúlyozott gráfok esetében, melyek csak nemnegatív súlyú éleket tartalmaznak (mint a mi esetünkben is), a Dijkstra-algoritmust [35],[14; 37. o.] használja a legrövidebb út meghatározásához.

Lefuttatva a legrövidebbút-keresést minden $\langle a,b \rangle$ állomáspárra (ahol $1 \le a \le 291$ és $1 \le b \le 291$) a menetidő- és a távolságsúlyokkal is és a kapott értékeket egy mátrixba rendezve úgy, hogy a sorok a kiinduló, az oszlopok az érkező állomást jelentik (azaz egy klasszikus szállítási feladat költségmátrixához hasonlóan), egy-egy 291×291-es mátrixot kapunk, melyeket jelöljünk $\mathbf{T}^{00}$-lal, illetve $\mathbf{L}^{00}$-lal. Ezek a jelenlegi magyarországi vasúthálózaton az adott két állomás közötti legrövidebb eljutási idők és távolságok – amelyekhez tartozó menetvonalak útvonalai nem feltétlenül esnek egybe.

A főátlóban az $a = b$ esetekhez tartozó zérus értékek szerepelnek. Mind a $\mathbf{T}^{00}$, mind az $\mathbf{L}^{00}$ mátrix szimmetrikus, mivel adott a és b állomásokhoz tartozó minimális menetidőre és a minimális menetvonalhosszra is igaz, hogy $\mathbf{T}^{00}_{a,b} = \mathbf{T}^{00}_{b,a}$ és $\mathbf{L}^{00}_{a,b} = \mathbf{L}^{00}_{b,a}$. Az egyes mátrixok tehát $N^{00} = 42\,195$ darab független menetidő-, illetve menetvonalhossz-értéket tartalmaznak.

Állomások és állomásközök zavarának számítása

Zavar alatt egy állomás vagy állomásköz hálózatból való teljes kiesését fogom érteni: a zavart állomáson nem haladhat át menetvonal és annak végpontja sem lehet. Hasonlóan, zavart állomásközön nem lehet végighaladni. Egyszerre a hálózatnak csak pontosan egy elemének zavarát vizsgáltam, mégpedig úgy, hogy az adott állomást vagy állomásközt leíró éleket töröltem a gráfból. Az így keletkezett új gráfon elvégeztem a menetidők és a menetvonalhosszak kiszámítását minden lehetséges állomáspárra, ugyanúgy, mint a zavarmentes esetben.

Állomások zavara

Az `igraph` csomag a gráfot élek halmazaként kezeli: egy élt az a két csúcs definiál, amelyek között az él található. Egy gráfból tehát csak az egyes éleket lehet eltávolítani, csúcsokat önmagukban nem. Egy csúcs csak akkor szűnik meg, ha az összes oda vezető és onnan kiinduló élt töröljük. A 3. ábra szerinti állomásreprezentáció esetében tehát meg kellene keresni az adott csúcshoz tartozó összes élt törölni őket.

Ebből a szempontból tehát egyszerűbb az alkalmazott reprezentáció, mivel egy állomás kiiktatásához négy (fejállomás esetében egy), pontosan ismert élt kell törölni a gráfból. Ezek az állomásokat leíró élek ezért az egyszerűbb kezelhetőség érdekében egymás után, az állomások közötti viszonylatokat leíró élektől elkülönítve kerültek bele a gráfot leíró éllistába.

Ekkor azonban még lehetséges a b állomás zavara esetén is az $a \to b$ menetvonal számítása. Ennek kiküszöbölésére először mindig az került megvizsgálásra, hogy a számítandó menetvonal valamelyik végpontja a zavart állomás volt-e, és ha igen, akkor a legrövidebbút-keresés nem lett elvégezve, hanem annak értéke automatikusan nullává lett téve. Később látni fogjuk, hogy ez a fajta definíció miért célszerű a zavarok vizsgálatához.

Több olyan állomás található a magyarországi vasúthálózaton, melyek elhagyásával még legalább egy állomás elérhetetlen lesz, azaz a G^{00}_t és a G^{00}_ℓ gráf is egyszeresen összefüggő

[14; 34. o.] Az így elérhetetlenné vált állomásokat, mint végpontot tartalmazó menetvonalak hossza és menetideje is nulla értékkel szerepel a számolásokban.

Jelöljük $G_t^{\mathbf{i0}}$-vel és $G_\ell^{\mathbf{i0}}$-lel az *i*-edik állomást leíró élek törlésével létrehozott, menetidők, illetve távolságok szerint súlyozott gráfot ($1 \le i \le 291$). A zavarmentes hálózatot leíró gráfokhoz hasonlóan minden állomáspárra lefuttatva a legrövidebbút-keresést az *i* paraméter minden lehetséges értékére, kétszer 291 darab 291×291-es mátrixot kapunk. Jelöljük $\mathbf{T}^{\mathbf{i0}}$-lal és $\mathbf{L}^{\mathbf{i0}}$-lal az *i*-edik állomás zavara esetén az állomáspárok közötti legrövidebb menetidőket, illetve menetvonalhosszakat tartalmazó mátrixot.

Állomásközök zavara

Az állomásközök zavara egyszerűbben kezelhető: az ezeket leíró 730 irányított él közül az azonos viszonylatot leíró (és az éllistában is egymás mellett szerepeltetett) két élt kell egyszerre törölni a gráfból.

Ha azonban az adott állomásköz nem része egy körvonalnak [14; 16. o.], akkor megszüntetésével lesz olyan állomás, ami elérhetetlenné válik. A $G_t^{\mathbf{00}}$ és a $G_\ell^{\mathbf{00}}$ gráf is ilyen, ún. egyszeresen élösszefüggő [14; 34. o.] gráf. Az így elérhetetlenné vált állomásokat végpontként tartalmazó menetvonalak menetideje és hossza is nulla értékkel van szerepeltetve.

Jelöljük $G_t^{\mathbf{0j}}$-vel és $G_\ell^{\mathbf{0j}}$-lel a *j*-edik állomásközt leíró két irányított él törlésével előállított, menetidők, illetve távolságok szerint súlyozott gráfot, ahol $1 \le j \le 365$.

A *j* paraméter minden lehetséges értékére lefuttatva a legrövidebbút-keresést kétszer 365 darab 291×291-es mátrixot kapunk a menetidőre és a menetvonalhosszra, melyeket az állomások zavaránál használt jelöléshez hasonlóan jelöljünk $\mathbf{T}^{\mathbf{0j}}$-vel, illetve $\mathbf{L}^{\mathbf{0j}}$-vel.

A ZAVAROK HATÁSA A MENETIDŐKRE ÉS A MENETVONALHOSSZAKRA

A legrövidebbút-keresések lefuttatása után összesen 1314 darab, 291×291-es mátrixot kapunk, melyek analízise több, a vasúthálózatra vonatkozó információt is szolgáltat.

Az egyes állomásokon és állomásközökön áthaladó menetvonalak

Az első kérdés, ami felmerül, hogy az egyes állomásokat és állomásközöket az összes menetvonal hány százaléka érinti.

A legkisebb menetidejű átmenő menetvonalak aránya

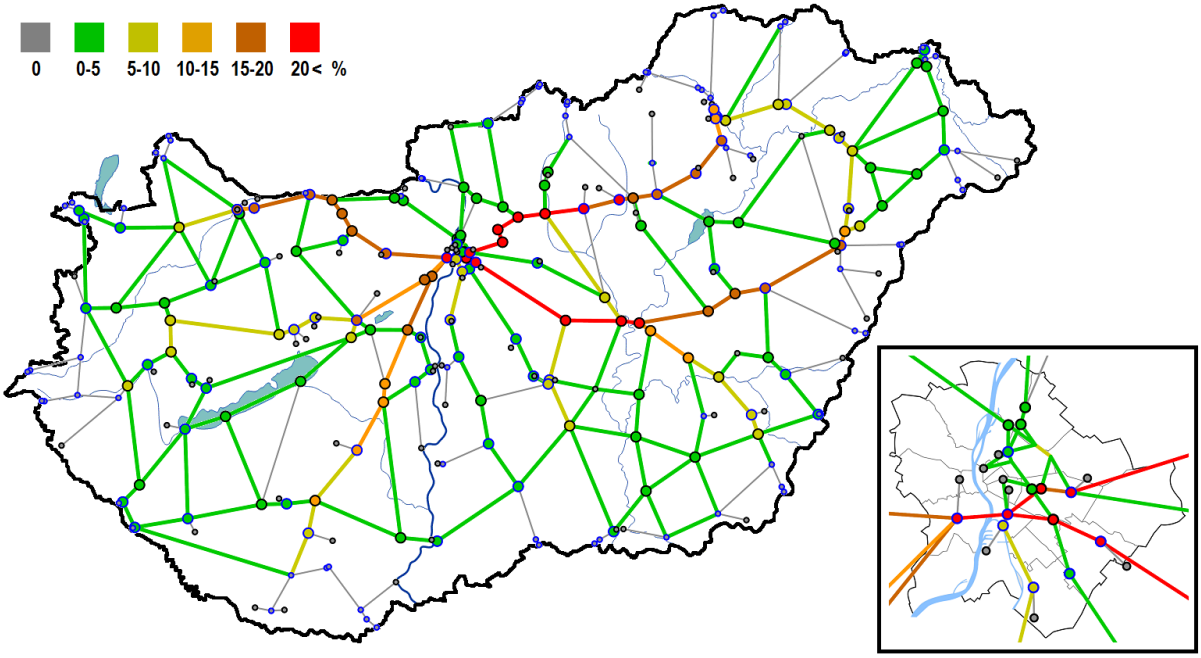
Az *i*-edik állomást érintő minimális menetidejű menetvonalak darabszámának meghatározásához vizsgáljuk meg a $\mathbf{\Delta T^{i0} = T^{i0} - T^{00}}$ mátrixot. Ennek egyes elemei lehetnek pozitívak, negatívak vagy nullák. A $\mathbf{\Delta T}_{a,b}^{\mathbf{i0}}$ elem csak akkor lehet pozitív, ha a zavarmentes és a zavart hálózatban is létezik menetvonal az *a* és a *b* állomások között, hiszen $\mathbf{T}_{a,b}^{\mathbf{00}}$ definíció szerint a lehető legkisebb menetidő a két állomás között a $G_t^{\mathbf{00}}$ gráfban. A kevesebb élt tartalmazó $G_t^{\mathbf{i0}}$ gráfban nem lehetséges ennél rövidebb időtartamú menetvonal. Azaz $\mathbf{T}_{a,b}^{\mathbf{i0}} \ge \mathbf{T}_{a,b}^{\mathbf{00}} \ \forall i.$

A $\mathbf{T}_{a,b}^{\mathbf{i0}} = \mathbf{T}_{a,b}^{\mathbf{00}}$ egyenlőség két esetben lehetséges. Lehet, hogy a minimális menetidejű menetvonal nem érintette az adott állomást sem a $G_t^{\mathbf{00}}$, sem a $G_t^{\mathbf{i0}}$ gráfban, így az *i*-edik állomás megszüntetésével a legrövidebb menetidejű menetvonal nem változott: $\mathbf{T}_{a,b}^{\mathbf{00}} = \mathbf{T}_{a,b}^{\mathbf{i0}} \neq 0$ és $\mathbf{\Delta T}_{a,b}^{\mathbf{i0}} = 0$. Azonban az is lehet, hogy az *a* és a *b* állomások elérhetetlenek egymás számára mind a $G_t^{\mathbf{00}}$, mind a $G_t^{\mathbf{i0}}$ gráfban, azaz $\mathbf{T}_{a,b}^{\mathbf{00}} = \mathbf{T}_{a,b}^{\mathbf{i0}} = 0$ és így $\mathbf{\Delta T}_{a,b}^{\mathbf{i0}} = 0$.

A $\Delta \mathbf{T}^{i0}_{a,b}$ elem negatív akkor lesz, ha a G_t^{00} gráfban létezik menetvonal az a és a b állomások között ($\mathbf{T}^{00}_{a,b} > 0$), azonban az i-edik állomás megszüntetésével a két állomás elérhetetlenné válik egymás számára ($\mathbf{T}^{i0}_{a,b} = 0$). Ez azonban azt is jelenti, hogy a G_t^{00} gráfbeli menetvonal áthalad az i-edik állomáson.

Megszámolva tehát a $\Delta \mathbf{T}^{i0}$ mátrix pozitív és negatív elemeit, és ezt leosztva az összes menetvonal darabszámával, N^{00}-lal, megkapjuk zavarmentes hálózatban az i-edik állomást érintő minimális menetidejű menetvonalak arányát az összes menetvonalhoz képest.

Hasonlóan, a $\Delta \mathbf{T}^{0j} = \mathbf{T}^{0j} - \mathbf{T}^{00}$ mátrix negatív és a pozitív elemeit összeszámolva és leosztva N^{00}-lal megkapjuk a zavarmentes hálózatban a j-edik állomásközön áthaladó minimális menetidejű menetvonalak arányát. A számolások eredménye a 4. ábrán látható.



4. ábra Az egyes állomásokat és állomásközöket érintő minimális menetidejű menetvonalak aránya (a zsákvonalak kivételével). A kék szegélyű állomások bármelyikének elhagyásával a gráf két részgráfra esik szét. (saját szerkesztés)

Látható, hogy még ebben az egyszerű modellben is, pusztán a menetidők figyelembe vételével és országon belüli menetvonalakra (azaz a szomszédos országokon keresztül történő kerülést figyelmen kívül hagyva) is a TEN-T hálózat Mediterrán és Orient folyosóihoz [25] tartozó hálózati elemek adódtak a legfrekventáltabb vonalszakaszoknak. Ez persze nem véletlen: éppen a többinél magasabb kiépítési sebességük miatt ezek az állomásközök „vonzzák” a minimális menetidejű menetvonalakat.

Azonban a rendszernek vannak szűk keresztmetszetei. Az Összekötő vasúti hídon tizenkétszer több minimális menetidejű menetvonal halad át, mint az Újpesti vasúti hídon és a bajai Türr István hídon összesen (az összes menetvonal majdnem fele) vagyis „az ország keleti és nyugati fele közötti tranzitforgalom lényegében egy műtárgyon, a Déli Vasúti Duna-hídon bonyolódik le” [36]. Az átkelő forgalmának pedig csak egy részét lehet annak zavara esetén átcsatornázni, azt is csak jelentős kerülővel és kisebb kapacitással [37]. A két leginkább érintett állomás is ennek az állomásköznek a két végpontja.

A második legtöbb menetvonal a Szolnok–Szajol állomásközön, vagyis a szolnoki vasúti Tisza-hídon halad át, mely „a legterheltebb tiszai vasúti átkelési lehetőség” [27]: a rajta áthaladó minimális menetidejű menetvonalak darabszáma ötszöröse a második legterheltebb átkelőnek, a

Tokaj–rakamazi vasúti Tisza-hídnak és 3,5-szerese az összes többi Tisza-hídon átmenők együttes darabszámának. A harmadik és a negyedik legérintettebb állomás is ennek az állomásköznek a két végpontja.

Erre a két műtárgyra azonban nem teljesül az az elvárás, hogy legalább egy helyettesítő létesítmény azonnal rendelkezésre álljon [38].

A 100a számú, Budapest–Cegléd–Szolnok és a 80a Budapest–Hatvan vasútvonal az ország legforgalmasabb vasútvonalai közé tartozik.

Kilenc viszonylatra hívnám még fel a figyelmet (1. táblázat), melyek a 4. ábrán szürke színnel jelennek meg úgy, hogy létezik a két állomás között alternatív útvonal. Ezek az állomásközök ugyanis nem részei egyetlen ideális útvonalnak sem, így a rendszerből való kivételük egy állomáspár közti legrövidebb útvonalra sem gyakorol befolyást.

A 4. ábra alapján ilyennek tűnhet a 22-es számú Körmend–Zalalövő vonal is, de az ezen engedélyezett legnagyobb sebesség jelenleg 0 km/h. Ez az állomásköz azért szerepel mégis a gráfban, mert a Mediterrán TEN-T folyosó zavara esetén annak Boba és a szlovén határ közti szakaszán kerülőútirányaként szóba jöhető vasútvonal [40], illetőleg a tervezett RFC11 korridor egyik lehetséges útirányának is része [41].

viszonylat	ℓ (km)	t (min)	kerülő állomás(ok)	ℓ (km)	t (min)	$\Delta\ell$ (%)	Δt (%)
Kaposvár–Siófok	100	200	Fonyód (↔)	94	79	–6	–61
Rákospalota-Újpest–Vácrátót (↯)	31	47	Vác (↯ ↔)	35	35	+13	–26
Vámosgyörk–Újszász	61	61	Hatvan (↯)	73	42	+20	–31
Tócóvölgy–Tiszalök	62	93	Debrecen, Nyíregyháza	87	54	+40	–42
Fülöpszállás–Kecskemét	42	120	Kiskunhalas, (↯) Kiskunfélegyháza	120	78	+186	–35
Szerencs–Hidasnémeti	51	77	Felsőzsolca (↯ ↔)	90	66	+76	–14
Sárbogárd–Börgönd	29	44	Pusztaszabolcs (↔)	50	42	+72	–5
Kisterenye–Kál-Kápolna	54	81	Hatvan (↔)	92	79	+70	–2
Mezőhegyes–Kétegyháza	39	79	Békéscsaba, Orosháza	87	79	+123	–0

1. táblázat Az állomásközök, melyeken a menetidő nagyobb, mint a két végpont közötti menetidő egy (alkalmasan megválasztott) kerülő állomáson át. ↯: villamosított vonalszakasz, ↔: irányváltás szükséges (saját szerkesztés)

A 35-ös Kaposvár–Siófok vonal 100 km-ét 200 perc alatt lehet megtenni, míg a 30-as és 36-os vonalakon, fonyódi irányváltással is csak 39 percig tart a 94 km-es út. A Somogyi-dombságon át vezető vonal tehát nem csak menetidőben, de kilométerben is hosszabb úton köti össze a két várost.

A 71-es vonal Rákospalota-Újpest és Vácrátót közti, a 86-os vonal Vámosgyörk és Újszász közti és a 109-es vonal Tócóvölgy és Tiszalök közötti szakasza helyett kerülőutat választani a kilométerben hosszabb út ellenére a jelentős megtakarított menetidő miatt lehet figyelemre méltó.

A 152-es számú Fülöpszállás–Kecskemét vonal és a 98-as Szerencs–Hidasnémeti vonal esetében már kétséges a menetidőben rövidebb kerülőirány választásának előnyös volta hosszabb út árán. Mégis, a 152-es vonal (az azóta meghiúsult) V0 vonal részeként, a 98-as vonal pedig a 90-es Miskolc–Hidasnémeti TEN-T vonal alternatív útvonalaként jöhet(ett) számításba [40].

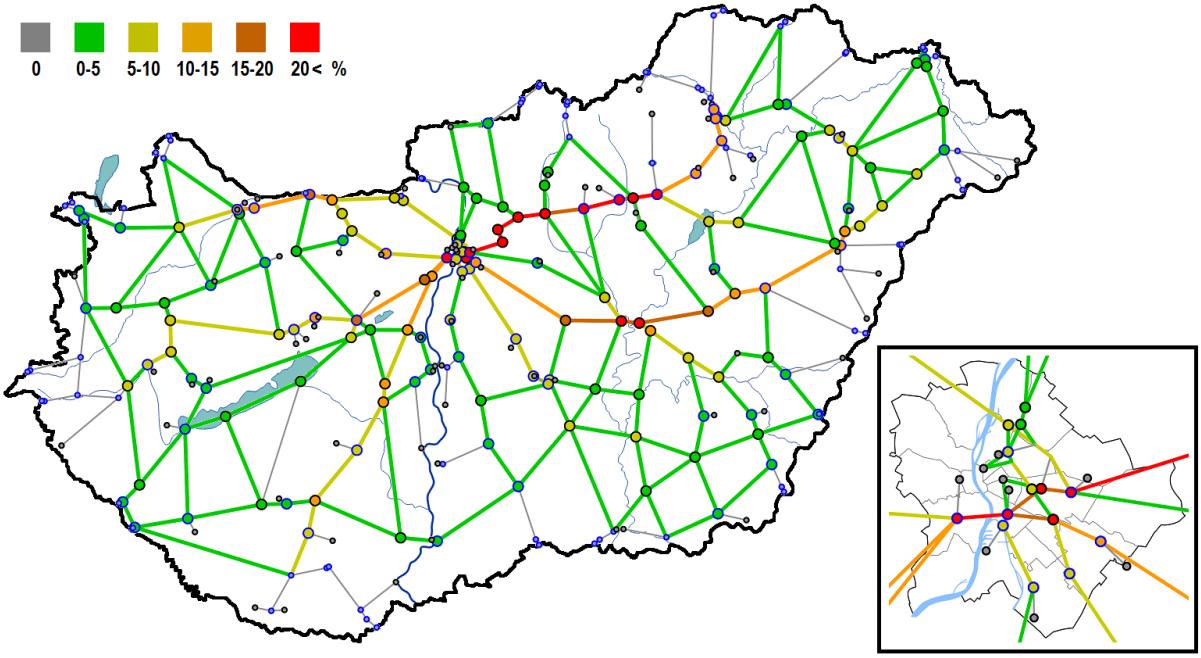
A 45-ös vonal Sárbogárd és Börgönd közti szakasza, a 84-es Kisterenye–Kál-Kápolna vonal és a 121-es vonal Mezőhegyes és Kétegyháza közti szakaszának kerülőútja már csak

hibahatáron belül rövidebb időben, ugyanakkor kilométerben jelentősen hosszabb. Ennek ellenére a 84-es vonal az MH ARB (mára már kiürített, de scvp. vágánykapcsolattal továbbra is rendelkező [18]) káli bázisa miatt bírhat még jelentőséggel [39].

A határállomások és a zsákvonalak állomásai mellett több másik csomópont is szürke színű a 4. ábrán. Ez azt jelenti, hogy az adott állomást csak olyan minimális menetidejű menetvonalak érintik, melyeknek az adott állomás az egyik végpontja.

A legkisebb hosszúságú átmenő menetvonalak aránya

Az előző alpontban leírtakhoz hasonlóan definiálhatjuk a $\Delta L^{i0} = L^{i0} - L^{00}$ és a $\Delta L^{0j} = L^{0j} - L^{00}$ mátrixokat és segítségükkel az ott leírt módon meghatározhatjuk azon minimális hosszúságú menetvonalak arányát, melyek érintik az adott állomást, illetve állomásközt a zavarmentes hálózatban. A kapott eredményeket az 5. ábrán láthatjuk.



5. ábra Az egyes állomásokat és állomásközöket érintő minimális hosszúságú menetvonalak aránya (a zsákvonalak kivételével). A kék szegélyű állomások bármelyikének elhagyásával a gráf két részgráfra esik szét. (saját szerkesztés)

A menetidőkhöz hasonlóan itt is az átlagnál terheltebbek a Mediterrán és Orient TEN-T folyosók. Ezek a vonalak tehát nem csak az átlagosnál nagyobb engedélyezett sebességük miatt, hanem földrajzi elhelyezkedésükből fakadóan is az állomások közötti legrövidebb úton fekvő szakaszok.

Ez tehát a magyarországi vasúthálózat inherens tulajdonsága. A fővonalak nem csak az engedélyezett sebesség, a villamosítottság, esetleg a két vágány miatt fővonalak, hanem elhelyezkedésük, vonalvezetésük miatt is. Ez már csak a magyarországi vasúthálózat története miatt is így van: egy, a mellékvonali hálózat kiépülése előtti térképet megnézve (például 1885-ből [42]), azon gyakorlatilag csak ezek a vonalak szerepelnek. Azt láthatjuk tehát, hogy a mellékvonalak vonalvezetésük alapján is ráhordó, illetve lokális jelentőségű vasutak. Ennek ellenére, vagy inkább épp ezért, a mellékvonalak fontos részei a magyarországi vasúthálózatnak, hiszen annak a „legkisebb elemére is szükség van a ráhordó szerepe miatt” és „ha a mellékvonalakat felszámolják, akkor közvetve a fővonalak forgalmát is csökkentik” [43]. A (megfelelően kiválasztott) mellékvonalak ezért semmiképp sem elhanyagolandók, hogy a fővonalak zavara esetében reális idő- és úthossz-paraméterekkel rendelkező alternatív útvonalat tudjanak nyújtani.

A minimális hosszúságú menetvonalakról is elmondható az Összekötő vasúti híddal kapcsolatban, mint ami a minimális menetidejűekről: az összes menetvonal több mint harmada érinti a hidat. Mivel ez az egyetlen Duna-híd, mely a TEN-T folyosók része, ezért evidens, hogy „a páneurópai folyosó tehervonati forgalma (...) 100%-ban Budapesten keresztül (...) a Déli vasúti összekötő hídon vezet át” [24].

A minimális menetidejűekhez hasonlóan a Tiszán áthaladó minimális hosszúságú menetvonalak fele a szolnoki Tisza-hídon halad át, és „a szolnoki Tisza-híd és a Zagyva-híd stratégiai jelentőségét tovább növeli az a sajnálatos tény, hogy jelentős kapacitású tiszai átkelő a közelben nem található” [27].

A menetvonalhossz szerinti minimalizálás során a 80 és a 80a számú vonalak Budapest és Füzesabony közti szakasza adódott a legtöbb menetvonal által érintettnek mind az állomások mind az állomásközök szempontjából.

Zavar hatása a hálózat egészére

Akár egyetlen állomásnak vagy állomásköznek is országos jelentőségű hatása lehet. Elég csak Kelenföld és Ferencváros állomásokra és a köztük levő hídra gondolnunk: mivel a Dunán áthaladó menetvonalak nagy része itt lép át a folyón, ennek a hálózati elemeknek a zavara a lokális környezeténél jóval nagyobb területre terjedhet ki.

Zavar országos hatása a menetidőkre

Ennek meghatározásához azokat az $\langle a,b \rangle$ állomáspárokat kell figyelembe venni, melyekre $\mathbf{T}^{\mathbf{i0}}_{a,b} > 0$, illetve $\mathbf{T}^{\mathbf{0j}}_{a,b} > 0$, azaz az összes, a zavart hálózatban létező menetvonalat. A

$$T_{\mathrm{i0}} = 100 \frac{\sum\limits_{\langle a,b \rangle} \mathbf{T}^{\mathbf{i0}}_{a,b}}{\sum\limits_{\langle a,b \rangle} \mathbf{T}^{\mathbf{00}}_{a,b}} - 100 \tag{1}$$

kifejezés azt mutatja meg, hogy az *i*-edik állomás zavarának hatására a hálózat összes minimális menetidejű menetvonalának összmenetideje hány százalékkal nő meg a zavarmentes hálózat összmenetidejéhez képest. Hasonlóan, a *j*-edik állomásköz zavarának esetében:

$$T_{\mathrm{0j}} = 100 \frac{\sum\limits_{\langle a,b \rangle} \mathbf{T}^{\mathbf{0j}}_{a,b}}{\sum\limits_{\langle a,b \rangle} \mathbf{T}^{\mathbf{00}}_{a,b}} - 100 . \tag{2}$$

Ezen számítások eredményeként azt kapjuk, hogy Ferencváros és Kelenföld állomások és a köztük levő állomásköz okoz a teljes vasúthálózaton 20 %-nál nagyobb menetidőnövekedést, azaz mindössze ezek miatt a hálózati elemek miatt nem felel meg a magyarországi hálózat a robusztusság követelményének [40]. A következő két állomás Hatvan és Szajol, állomásköz pedig a Szajol–Szolnok viszonylat. Ezek zavara kb. 10%-kal kisebb, de még messze nem elhanyagolható hatást gyakorol a teljes hálózatra.

Mint az előző pontban is láttuk, éppen ez az a két állomásköz, melyet a legtöbb menetvonal érint, azaz nem pusztán az átmenő menetvonalak darabszáma szempontjából kiemelt jelentőségű állomásközök (hidak) ezek, hanem zavaruknak a hálózat egészére kiterjedő hatása miatt is.

Természetesen a fellépett zavar áthidalásaként felmerülhet a „megkerülés a szomszédos országok vasúthálózatának igénybevételével” vagy „a jelenleg rendelkezésre álló vasúti hidak

kerülő úton történő igénybe vétele", de „ezek a megoldások csak részben tudják átvenni a kieső hídon átmenő forgalmat" [36].

Zavar országos hatása a menetvonalhosszakra

Hasonlóan az előző alpontban leírtakhoz, azokat az $\langle a,b \rangle$ állomáspárokat figyelembe véve, melyekre $\mathbf{L}^{\mathbf{i0}}_{a,b} > 0$, illetve $\mathbf{L}^{\mathbf{0j}}_{a,b} > 0$, meghatározhatjuk, hogy az adott állomás vagy állomásköz zavarának hatására a teljes hálózat menetvonalhosszainak összege hány százalékkal nő meg:

$$L_{\mathrm{i0}} = 100 \frac{\sum\limits_{\langle a,b \rangle} \mathbf{L}^{\mathbf{i0}}_{a,b}}{\sum\limits_{\langle a,b \rangle} \mathbf{L}^{\mathbf{00}}_{a,b}} - 100, \tag{3}$$

$$L_{\mathrm{0j}} = 100 \frac{\sum\limits_{\langle a,b \rangle} \mathbf{L}^{\mathbf{0j}}_{a,b}}{\sum\limits_{\langle a,b \rangle} \mathbf{L}^{\mathbf{00}}_{a,b}} - 100. \tag{4}$$

Az eredmények azt mutatják, hogy egy állomás sem növeli meg a hálózat összes menetvonalának összhosszát több mint 20%-kal: a legnagyobb növekedést Ferencváros állomás zavara okozza, 12%-ot. A Kelenföld–Ferencváros állomásköz zavara 10%-kal növeli az összmenetvonalhossz értékét.

Azonban az az eredmény, hogy nem csak a menetvonalak jelentős hányada halad át az Összekötő vasúti hídon, hanem hogy kiesése országos hatású zavart eredményez, újra felhívja a figyelmet arra, hogy „a Dunán az egyik legégetőbb probléma a megfelelő számú és területi eloszlású híd biztosítása" [12] és ezért egy alternatív útvonal kialakítása mielőbb szükséges lenne. De nem csak zavar esetén válik kritikussá egy alternatív dunai átkelő hiánya, hanem mivel nem kielégítő a nagy folyókon levő hidak mennyisége és területi eloszlása, „a kedvezőtlen hídhelyzetből adódó kényszerkerülők miatt évente több milliárd forint nagyságrendű közlekedésüzemi többletköltségek jelentkeznek." [44]

Az átjárhatóság az Összekötő vasúti híd és az Újpesti vasúti híd között közvetve ugyan megoldott [38], azonban az eltérő vontatási nem és sok esetben a vonatfordulás is megnehezítheti kerülő irány használatát.

A fentiek miatt időről időre előkerül a Déli (vagy a Kelenföldi) és a Nyugati pályaudvar összekötése egy Duna alatti vasúti alagúttal [45],[46].

ÖSSZEFOGLALÁS

A magyarországi vasúthálózat modelljeként egy élsúlyozott irányított gráfot használtam. Az egyes állomások és állomásközök zavarát a megfelelő élek gráfból való törlésével modelleztem. A zavarmentes és a zavart hálózatokban is kiszámítottam az összes állomáspár közötti minimális menetidő- és menetvonalhosszakat.

Ezek alapján meghatároztam az egyes hálózati elemeken áthaladó menetvonalak arányát. Az országos fővonalak mind az idő, mind a távolság szerinti optimalizálás esetében a legforgalmasabb vonalszakaszoknak adódtak, azaz ez a tulajdonságuk a rendszer felépítéséből ered. Kiemelkedik ezek közül is az Összekötő vasúti híd és a szolnoki Tisza-híd.

Kiszámítottam, hogy egy hálózati elem zavarának következtében módosuló minimális menetidejű, illetve hosszú menetvonalak mekkora átlagos hatást gyakorolnak a hálózat menetvonalainak összességére. Az Összekötő vasúti híd menetidő szempontjából abszolút

kritikusnak bizonyult országosan 20% fölötti átlagos menetidőnövelő hatásával, de a menetvonalhosszakban is országosan 10% fölötti növekedést eredményez a zavara. A második legkritikusabb műtárgy a szolnoki vasúti Tisza-híd.

FELHASZNÁLT IRODALOM

[1] ERDŐSI, F.: *Európa közlekedése és a regionális fejlődés*, Dialóg Campus Kiadó, Budapest; Pécs, 2004.

[2] SHORT, H.: *Pipes, Trains, and Trucks: How to move biomass cost effectively*; https://snrecmitigation.wordpress.com/2009/04/24/pipes-trains-and-trucks-how-to-move-biomass-cost-effectively/ (letöltve: 2017.08.23.)

[3] MARINOV, M.; GIUBILEI, F.; GERHARDT, M.; ÖZKAN, T.; STERGIOU, E.; PAPADOPOL, M.; CABECINHA, L.: *Urban freight movement by rail*; J. Transp. Lit. **7** (3), pp. 87-116 (2013) (DOI 10.1590/S2238-10312013000300005)

[4] GONZALES, D.; SEARCY, E.M.; EKŞIOĞLU, S.D.: *Cost analysis for high-volume and long-haul transportation of densified biomass feedstock*; Transportation Research Part A **49**, pp. 48-61 (2013) (DOI 10.1016/j.tra.2013.01.005)

[5] RODRIGUE, J. P.; COMTOIS, C.; SLACK, B.: *The geography of transport systems*; Routledge, London and New York, 2013., p. 107. (ISBN 978–0–415–82253–4)

[6] 2080/2008 (VI. 30.) *Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról*

[7] 2012. évi CLXVI. *törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*

[8] TÓTH, A.; TÓTH, B.: *A nagyvárosok felszíni közlekedési rendszereinek vizsgálata a terrorfenyegetettség tükrében*; Hadmérnök IV. 4. (2009) 108-122. o.

[9] HORVÁTH, A.: *A vasúti közlekedés terrorfenyegetettségének jellemzői a városokban*; Hadmérnök IV. 3. (2009) 180-189. o.

[10] HORVÁTH, A.: *A közúti, vasúti és vízi közlekedés terrorfenyegetettségének jellemzői* In: TÁLAS P. (szerk.): *Válaszok a terrorizmusra II.*; Mágustúdió, Budapest, 2006., 321-336. o.

[11] HORVÁTH, A.: *A kritikus infrasrtuktúra védelem komplex értelmezésének szükségessége* In: HORVÁTH, A. (szerk.): *Fejezetek a kritikus infrastruktúra védelemből*; Magyar Hadtudományi Társaság, Budapest, 2013., 18-37. o. (ISBN 978-963-08-6926-3)

[12] SZÁSZI, G.: *A vasúti közlekedési alágazat, mint kritikus infrastruktúra* In: HORVÁTH, A. (szerk.): *Fejezetek a kritikus infrastruktúra védelemből*; Magyar Hadtudományi Társaság, Budapest, 2013., 167-190. o. (ISBN 978-963-08-6926-3)

[13] Vasútvonalak hossza (2007–) http://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_odmv004.html (letöltve: 2017.08.23.)

[14] HAJNAL, P.: *Gráfelmélet*; Szegedi Egyetemi Kiadó Polygon, Szeged, 2017. (ISSN 1417-0590)

[15] 2005. évi CLXXXIII. *törvény a vasúti közlekedésről*

[16] *F. 2. sz. Forgalmi Utasítás*; MÁV ZRt. Pályavasúti Üzletág Forgalmi Főosztály; 22-23. o.

[17] Vasútvonalak http://www.vpe.hu/takt/vonal_lista.php (letöltve: 2017.08.23.)

[18] 277/2014. (XI. 14.) *Kormányrendelet a vasúti közlekedési hatóság által kiszabható bírság mértékéről és megfizetésének részletes szabályairól*

[19] Google Maps https://www.google.hu/maps/

[20] SZÁSZI, G.: *A védelmi szempontból meghatározó repülőterek vasúti kapcsolatának helyzete Magyarországon*, Repüléstudományi Közlemények (1997-től) XXI. Különszám (2009) 1-22. o.

[21] SZÁSZI, G.: *Katonai vasúti szállítások a Magyar Honvédség missziós feladatainak rendszerében*; Szolnoki Tudományos Közlemények XIV. (2010) 101-118. o.

[22] SZILY, I.; SZABÓ, L.: *Vasúti üzemtan II.*; Széchenyi István Egyetem - Universitas-Győr Kht. (Győr), 2006.

[23] SZÁSZI, G.: *Magyarország közlekedési infrastruktúrájának fejlesztése napjainkban: Közút vagy vasút?* – Katonai Logisztika 15. 2. (2007) 32-59. o.

[24] KÁLMÁN, L.: *Budapest vasúti közlekedésének fejlesztése - Vasút a Duna alatt (1. rész)*; Sínek Világa 2011/4, 16-20. o.

[25] SZÁSZI, G.: *Transz Európai Közlekedési Hálózat (TEN-T) tervezett fejlesztési iránya, várható hatása Magyarország vasúthálózatának fejlesztésére*; Szolnoki Tudományos Közlemények XVI. (2012) 402-425. o.

[26] *Trans-European transport network - TEN-T priority axes and projects 2005*; European Commission, Office for Official Publications of the European Communities, Luxembourg, 2005., 72. o. (ISBN 92-894-9837-4)

[27] SZÁSZI, G.: *Jász-Nagykun-Szolnok megye vasúthálózatának védelmi szempontú elemzése*; Szolnoki Tudományos Közlemények XIII. (2009) 101-125. o.

[28] TENCZER, G.: *Mikor fogunk itthon százhatvannal vonatozni?*; http://index.hu/belfold/2017/01/31/mikor_fogunk_itthon_szazhatvannal_vonatozni/ (letöltve: 2017.08.23.)

[29] *2016/2017. menetrendi időszakra vonatkozó Hálózati Üzletszabályzat a MÁV Zrt. és a GYSEV Zrt. nyílt hozzáférésű vasúti pályahálózata igénybevételének feltételeiről, 3.3.1.1 melléklet*; https://www2.vpe.hu/hu/hatalyos-husz-2016-2017 (letöltve: 2017.08.23.)

[30] *F. 2. sz. Forgalmi Utasítás függelékei, 15. sz. függelék*; MÁV ZRt. Pályavasúti Üzletág Forgalmi Főosztály, 101. o.

[31] ERCSEY, Z.; KISTELEKI, M.; VINCZE, T.: *Lassújelek hatásai a vasúti közlekedés költségeire 2. rész*; Vasútgépészet 2012/3. 16-19. o.

[32] ZENTAI, D.: *Gráfelméleti módszerek a kritikus infrastruktúra védelemben*; Hadmérnök XII. 2. (2017) 341-347. o.

[33] *R Core Team (2012). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. ISBN 3-900051-07-0, URL http://www.R-project.org/*

[34] CSARDI, G., NEPUSZ, T.: *The igraph software package for complex network research*, InterJournal, Complex Systems 1695. 2006. http://igraph.org

[35] DIJKSTRA, E. W.: *A Note on Two Problems in Connexion with Graphs*; Numerische Mathematik I. (1959) 269-271. o. (DOI 10.1007/BF01386390)

[36] SZÁSZI, G.: *Nagyfolyami vasúti hidak, mint közlekedési létfontosságú rendszerelemek* In: HORVÁTH, A.; BÁNYÁSZ, P.; ORBÓK, Á. (szerk.): *Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről*; Nemzeti Közszolgálati Egyetem, Budapest, 2014. 27-46. o. (ISBN 978-615-5305-30-6)

[37] SZÁSZI, G.: *Long-span railway bridges in the transport system of Hungary*; Hadmérnök VIII. 2. (2013) 98-107. o.

[38] ENDRŐDI, I.: *A közlekedési ágazat kritikus infrastruktúra elemei, kapcsolatuk a katasztrófavédelemmel, figyelemmel az Európai Unió Kritikus Infrastruktúrák Azonosításáról és Kijelöléséről szóló 2008. évi 2008/114/EK Tanácsi Irányelvében megfogalmazottakra* In: HORVÁTH, A. (szerk.): *Fejezetek a kritikus infrastruktúra védelemből*; Magyar Hadtudományi Társaság, Budapest, 2013., 238-267. o. (ISBN 978-963-08-6926-3)

[39] SZÁSZI, G.: *A vasúti hálózati infrastruktúrával szemben támasztott újszerű védelmi követelmények kutatása, a továbbfejlesztés feltételrendszerének vizsgálata (Doktori értekezés)*; Nemzeti Közszolgálati Egyetem, katonai Műszaki Doktori Iskola, Budapest, 2013. (DOI: 10.17625/NKE.2014.028)

[40] FELLER, T; HÍDVÉGi, G.; KÖLLER, L.: *A nemzetgazdaság és nemzetbiztonság által igényelt „kritikus infrastruktúra" hálózatok komplex szemléletű vizsgálata (tanulmány)*; Budapest, 2010.

[41] KÖLLER, L.: *Hatékonyság, versenyképesség a vasúti hálózatokon (A különböző vasúti hálózatok vonali és hálózati hatékonysága, illetve a versenyképesség értelmezése a vasútnál hazai tapasztalatok és nemzetközi példák alapján)*; http://www.vki.hu/~tfleisch/~haver/indulo.html (leöltve: 2017.08.23.)

[42] PÉTERI, L.: Környezetbarát vasúti közlekedés (vissza)fejlesztési tendenciái Németországban és Magyarországon; http://realzoldek.hu/modules.php?name=Content&pa=showpage&pid=242 (letöltve: 2017.08.23.)

[43] KOVÁCS, Gy. A.: *A regionális vasutak helye vasúti közlekedésünkben*; Földrajzi értesítő XLVIII. 3-4. (1999) 303-312. o.

[44] TÓTH, B.; HELMECZI, G.: *Védelmi követelmények a gazdasági és közlekedési minisztérium közlekedési szakterületén*; Katonai Logisztika XIV. 2. (2006) 37-55. o.

[45] SZAMOS, A.: *Budapest vasúti és elővárosi közlekedésének fejlesztése*; Sínek Világa Különszám (2006) 24-29. o.

[46] *A Budapesti Regionális Gyorsvasúti Rendszer koncepciója*; Főmterv-Közlekedés konzorcium, 2007.

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

A HATÁRŐRIZETI CÉLÚ IDEIGLENES BIZTONSÁGI HATÁRZÁR TOVÁBBFEJLŐDÉSE, AVAGY A MÁSODIK KERÍTÉS MINDENT MEGOLD?

DEVELOPMENT OF THE TEMPORARY TECHNICAL BARRIER AT THE BORDER, OR THE SECOND FENCE IS SOLVE EVERYTHING?

KUI László

(ORCID: 0000-0001-6411-4179)

kui.laszlo@uni-nke.hu

Absztrakt

Magyarország déli határszakaszán tovább folytatódik a határőrizeti célú ideiglenes biztonsági határzár fejlesztése. A történelemben több példát találhatunk az államhatárok fizikai akadállyal való lezárására, azonban ezek nem jelentettek sikeres megoldást. A tömeges méretű illegális migrációs nyomás miatt a magyar–szerb határszakasz műszaki megerősítése 2015-ben kezdődött el és jelenleg is folyamatban van. A fejlesztés során a műszaki tartalom egyre bővült, a rendszer egyre összetettebbé és intelligensebbé vált. Vajon mindez valóban áthatolhatatlanná teszi az államhatárt?

Kulcsszavak: *határrendészet, határőrizet, államhatár műszaki megerősítése, illegális migráció, határőrizet technikai támogatása*

Abstract

Continuing the development of the temporary technical barrier at the southern border of Hungary. In the history we can found more example for the close with physical barrier of the state borders, but these examples not were successful solutions. For the massive illegal migration in 2015 started the technical fortification of the Hungarian–Serbian border section and its nowadays is in progress. During the development the technical content has expanded, and the system became more and more complex and intelligent. Whether all this really make the border unpenetrable?

Keywords: *border policing, border surveillance, technical fortification of the state border, illegal migration, technical support of the border surveillance*

A kézirat benyújtásának dátuma (Date of the submission): 2017.07.27.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.06.

BEVEZETÉS

Ez év tavaszán különböző médiumok tudósításaiból értesülhettünk arról a hírről, amely szerint a magyar–szerb államhatáron büntetésvégrehajtási fogvatartotti munkaerő alkalmazásával elkészült a határőrizeti célú ideiglenes biztonsági határzár (rövidítve IBH, de maradjunk az általánosan használt „kerítés" megnevezésnél) második vonala. A második vonal kiépítésének indoka az volt, hogy a nyárra várhatóan fokozódó illegális migrációs[1] nyomás továbbra is feltartóztatható legyen a magyar–szerb viszonylatban, mivel a nyugat-balkáni migrációs útvonalon zajló illegális migrációs folyamatok újbóli felerősödése esetén továbbra is elsődlegesen e viszonylatban kell számolni tömeges jellegű tiltott határátlépési szándékkal. A híradásokból nem ismert, hogy az a feltételezés, amely szerint az illegális migrációs folyamatok nyárra felerősödének, milyen konkrét, elemzett-értékelt adatokon alapul. Jelen írás tárgyát nem képezi ilyen jellegű mélyebb elemzés, azonban saját tapasztalataim alapján megerősíthetem, hogy a zöldhatárral összefüggő illegális migrációs folyamatok az időjárási tényezők miatt a tavasztól őszig tartó időszakban általában nagyobb aktivitást mutatnak, viszont ennek mértékét egzaktan nem lehet előre meghatározni. Kormányzati nyilatkozatok alapján a második kerítés kiépítésére irányuló beruházás 4,8 milliárd forintba került, viszont a magyar határvédelem minden eddiginél erősebbé vált, a biztonságot pedig sikerült tovább növelni, mivel a továbbfejlesztett kerítésrendszer gyakorlatilag áthatolhatatlan, és képes bármekkora embertömeget feltartóztatni. [2]

HATÁRVÉDELEM VAGY HATÁRRENDÉSZET?

A hírekkel, tudósításokkal kapcsolatban gyakran mondjuk, hogy minden csoda három napig tart, én azonban a közmondásos három nap elteltével is szeretnék egy kicsit részletesebben és szakmai-tudományos szemszögből foglalkozni az immár kettős kerítés kérdéskörével és az illegális migrációra, valamint a határőrizeti rendszerre gyakorolt várható hatásaival.

Rögtön az első szempont, amelyre „szakmabeliként" és a rendészet tudományát tanulmányozóként ráirányul a figyelmem, a határvédelem megfogalmazás. Nemcsak a fentebb hivatkozott hírben, hanem a tömeges méretű illegális migrációval kapcsolatos szinte minden sajtómegnyilvánulásban, illetve különböző nyilatkozatokban rendszeresen a határvédelem megnevezést alkalmazzák a Magyarország déli határai mentén végrehajtott rendőrségi tevékenységek összefoglaló megnevezéseként. Véleményem szerint a határvédelem-határrendészet kifejezések megközelítése és alkalmazása hasonló problémákat vet fel, mint a rendvédelem-rendészet kérdése, még akkor is, ha az Alaptörvény a rendőrség alapvető feladatai között az államhatár rendjének védelmét nevesíti és nem pl. az államhatárral kapcsolatos rendészeti feladatok ellátását.

A határvédelemnek, mint fogalomnak a Rendészettudományi Szószedetben az alábbi két meghatározása található meg:

„1) Az ország elleni katonai támadás esetén határterületen megvalósított katonai védelmi tevékenység.

(2) Alapvetően a Magyar Honvédség csapatainak a korábban létezett Határőrség, továbbá a Rendőrség, valamint a katasztrófavédelmi szervezet kijelölt erői - eszközei bevonásával végrehajtott olyan védelmi harctevékenysége, mely egységes elgondolás és irányítás alapján

[1] Az illegális/irreguláris migráció fogalmának elhatárolását lásd: Hautzinger Zoltán–Hegedüs Judit–Klenner Zoltán: A migráció elmélete, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2014., [1, 17-18. o.]

az agresszor támadásának megállítására, megsemmisítésére majd az eredeti helyzet visszaállítására irányul."

Bár kétségtelen, hogy a második fogalommeghatározásban szereplő Határőrség ma már nem létező szervezet, azt hiszem, hogy mindkét definícióból jól látható, hogy a határvédelem valamilyen külső fegyveres fenyegetés fegyveres (katonai) eszközökkel történő elhárítására irányul, tehát egyfajta katonai tevékenységként értelmezhető. Ezzel szemben a határrendészet, vagy az államhatár rendészete a Rendészettudományi Szószedetben rendészeti eszközökkel és módszerekkel megvalósított hatósági tevékenységként került definiálásra.

A fenti definíciók tartalmi elemei alapján úgy gondolom, hogy – különösen annak fényében, hogy Magyarország az Európai Unió és a Schengeni Térség teljes jogú tagállama – a magyar terminológiában a magyar–szerb viszonylatban az államhatár őrizetével[2] összefüggő rendőrségi intézkedések összességére a határrendészet kifejezés tekinthető helytállóbbnak.

KERÍTÉS ÉS ÁTHATOLHATATLANSÁG

Az államhatárok „áthatolhatatlan" vagy legalább az áthatolást nagymértékben megnehezítő fizikai akadályokkal való megerősítésével az emberiség már az ókori államok létrejöttekor kísérletezett. A városállamok területét a kezdeti időktől igyekeztek falakkal körülvenni, de az államhatár műszaki megerősítésére a legközismertebb példa a Kína északi határán kiépült, Nagy Falként ismert erődrendszer, amelynek célja az ország lakosságának megvédése volt az északi nomád törzsek támadásaitól. Megemlíthetjük még az Európa területén épült ún. „limes" néven ismert, sáncokkal és árkokkal, őrtornyokkal megerősített határzárat, amely a Római Birodalom területét volt hivatott védeni a barbár támadásokkal szemben. [4]

Amint történelmi tanulmányainkból ismerjük, egyik határvédelmi megoldás sem vált be, a Nagy Falon át a nomádoknak sikerült bejutni Kína területére, a Római Birodalom pedig – többek között a barbár támadások miatt – elbukott.

A modern kori Magyarországon a határőrség a háború utáni megalakulásától kezdve törekedett az államhatár különböző jellegű megerősítésére[3]. A legközismertebb példa azonban a „vasfüggöny", amelynek kiépítésével és alkalmazásával próbálták elérni az államhatár százszázalékos „sérthetetlenségét". Bár a vasfüggöny esetében a cél nem a befelé, hanem a kifelé irányuló tiltott határátlépések megakadályozása volt, a változó politikai és társadalmi viszonyok közepette ez a rendszer sem tudta beváltani a hozzá fűzött reményeket. A rendszer üzemeltetési és fenntartási költségei aránytalanul magasak voltak[4], rendkívül nagy volt a hamis riasztások száma, amely feleslegesen terhelte az állományt, illetve annak ellenére sem tudta az elvárt százszázalékos eredményességet és megfelelő visszatartó erőt produkálni, hogy mindenki tisztában volt a határőrök éles lőfegyverhasználati jogával. [7]

---

[2] A határőrizet meghatározását és tartalmi elemeit részletesen elemzi Balla József a 2017-es tanulmányában. Balla József: A Magyar Honvédség helye és szerepe a határőrizeti rendszerben, Hadtudományi Szemle, 2017. X. évfolyam 1. szám, 2017., [3, 354-364. o.]

[3] Lásd Fórizs Sándor: A határőrség megalakulása, valamint tevékenysége az első években (1945-1950). Magyar Rendészet XV. évfolyam, 2015/6. szám, 2016.[5, 89-102. o]

[4] Az államhatár műszaki megerősítése sosem eredményezte anyagi és humán erők megtakarítását. A műszaki jellegű biztosítást mindig fokozott mértékű plusz igénybevételt eredményezett. Lásd Fórizs Sándor: Az államhatár műszaki megerősítésének kezdete 1948-ban. Hadtudomány, XXV. évfolyam 2015. 1. elektronikus szám [6, 101-110. o.]

IBH, A MAGYAR KERÍTÉS

Ritecz György és Sallai János korábban részletesen, nemzetközi és hazai statisztikai adatok elemzésével vizsgálta a kerítés alkalmazásainak eddigi tapasztalatait, valamint az illegális migrációra gyakorolt hatását. Végkövetkeztetésük, hogy az ISIS visszaszorulása, a macedón-görög határ lezárása és a hatékonyabb török migrációkezelés mellett 2016-ig a kerítés önmagában nem volt képes megakadályozni az illegális migrációt, magyar részről szükséges volt a kerítéshez kapcsolódóan új jogszabályok és joggyakorlat kidolgozása és bevezetése. [8]

A 2015. évi kezdettel épült kerítéssel, illetve az illegális migrációra és a határőrizeti tevékenységre gyakorolt hatásaival [9] összefüggésben én a későbbiekben csak néhány adatot szeretnék felvillantani.

A magyar kormány a 1401/2015. (VI. 17.) számú kormányhatározatban döntött arról, hogy – a különböző nemzetközi (és európai!) példákhoz hasonlóan – fizikai akadállyal zárja le a zöldhatárt a szerb viszonylatban. Első lépésként a rendkívüli bevándorlási nyomás[5] kezelése érdekében szükséges egyes intézkedésekről szóló kormányhatározat értelmében körülbelül 175 km hosszúságban 4 méter magas határőrizeti célú ideiglenes kerítés létesítésének előkészítése került elrendelésre, amely 2015. augusztus végére készült el. A műszaki tartalom nem került egységesítésre, mivel a határszakaszon eltérő terepviszonyok többfajta műszaki megoldást igényeltek. Mindezzel a határőrizeti rendszerben új technikai elemként jelent meg és döntő változást eredményezett a szerb és a horvát viszonylatban az IBH telepítése és a határőrizeti rendszerbe történő integrálása.

A szerb viszonylat 2015. szeptember 15-én történt teljes lezárását[6] követően az illegális migráció iránya azonnal a horvát viszonylat felé fordult, majd 2015. október 16-án a horvát viszonylatban is befejeződött az IBH kiépítése, amellyel megvalósult a zöldhatár fizikai akadállyal történő lezárása a teljes déli határszakaszon. [11]

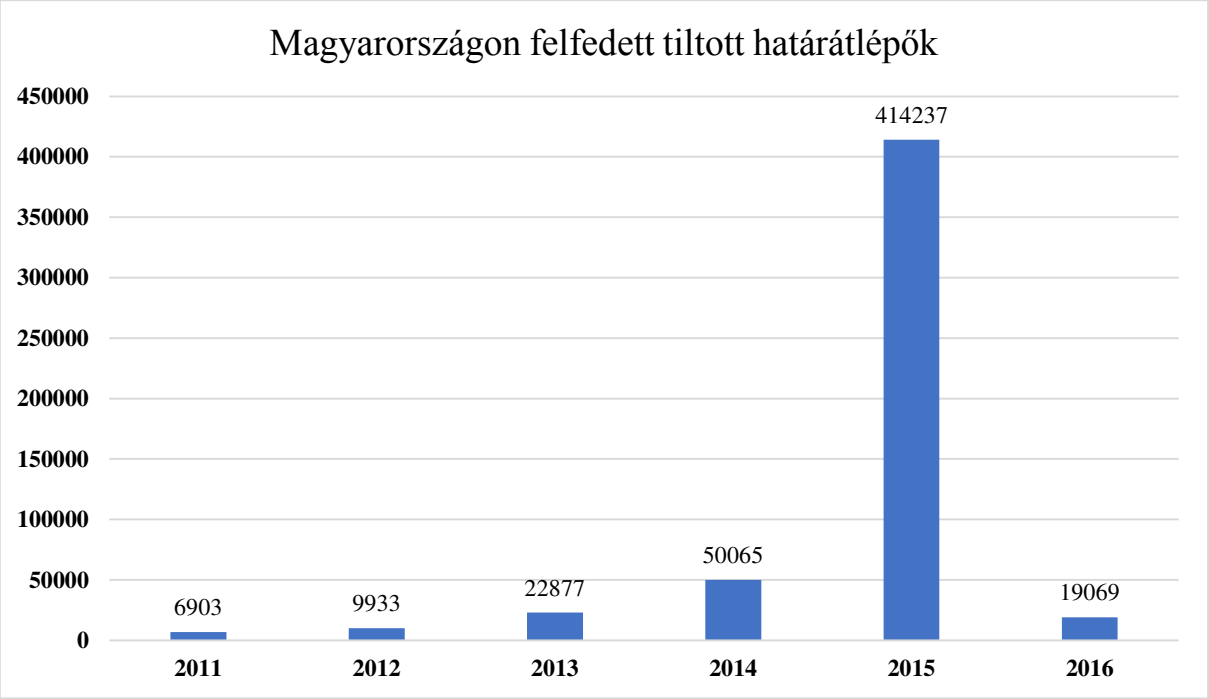
A határőrizet szempontjából a változást az jelentette, hogy a kerítés, mint fizikai akadály tulajdonképpen egy óriási kiterjedésű műszaki berendezés, amely azonban statikus jellege miatt önmagában nem jelentett leküzdhetetlen akadályt, hiszen köznapi eszközökkel (drótvágó, emelőrúd, ásó) azt át lehetett vágni, alá lehetett ásni, szét lehetett feszíteni, stb. Mindezek miatt a már korábban is meglévő technikai eszközök alkalmazását mintegy a kerítés védelmére kellett alapozni. A rendelkezésre álló (stabil, mobil, kézi) hőképfelderítő eszközökkel a veszélyeztett szakaszokat kellett megfigyelés alatt tartani, a határzár tiltott átlépésének hathatós megakadályozása érdekében pedig a kerítés közvetlen közelében nagy létszámú, megfelelő mobilitási képességgel és különböző egyéb megfigyelő eszközökkel rendelkező élőerőt, valamint szolgálati kutyákat kellett koncentrálni. A rendőrség határbiztonsági szerepvállalásának megnövekedését Kovács Gábor dolgozta fel tanulmányaiban. [12] [13] [14] Természetesen a rendszerben beállt változásokra az irreguláris migránsok és az embercsempészek is reagáltak. Először is már a kerítés építésének hírére a határ illegális átlépését tervező személyek még nagyobb számban vágtak neki a határnak, hogy még a kerítés befejezése előtt eljuthassanak Nyugat-Európába, majd a kerítés kiépülését követően változatos eszközökkel és módszerekkel próbáltak azon átjutni.

Ugyanakkor kétségtelen, hogy a kerítéssel és a hozzá kapcsolt jogi eszközökkel [15] sikerült jelentős mértékben csökkenteni a Magyarország felé irányuló illegális migrációt, amelyet az alábbi ábra (1. ábra) is jól szemléltet.

---

[5] A jogszabály címe a rendkívüli bevándorlási nyomás kezelése érdekében szükséges egyes intézkedésekről szóló 1401/2015. (VI. 17.) számú kormányhatározat. Talán helytállóbb lett volna az „illegális migrációs nyomás” kifejezést használni [10, 1. o.]

[6] Ekkor történt meg a Röszkei Közúti és Autópálya határátkelőhelyek lezárása.



1.ábra Magyarországon felfedett tiltott határátlépők (a szerző szerkesztése a [16] alapján)

Meg kell említeni, hogy a 2016-os tiltott határátlépési számadat mellett (2017-ben is) jelentős azoknak a személyeknek a száma is, akik esetében megakadályozásra került a határzár tiltott átlépése.[7] Szintén jelentős azoknak a száma, akik a határon lefolytatott menekültügyi eljárás széles körben való alkalmazhatóságának megvalósításához szükséges törvények módosításáról szóló 2016. évi XCIV. törvény rendelkezései alapján[8] az államhatártól számított 8 km-en belül kerültek feltartóztatásra és a kerítés túloldalára visszakísérésre.

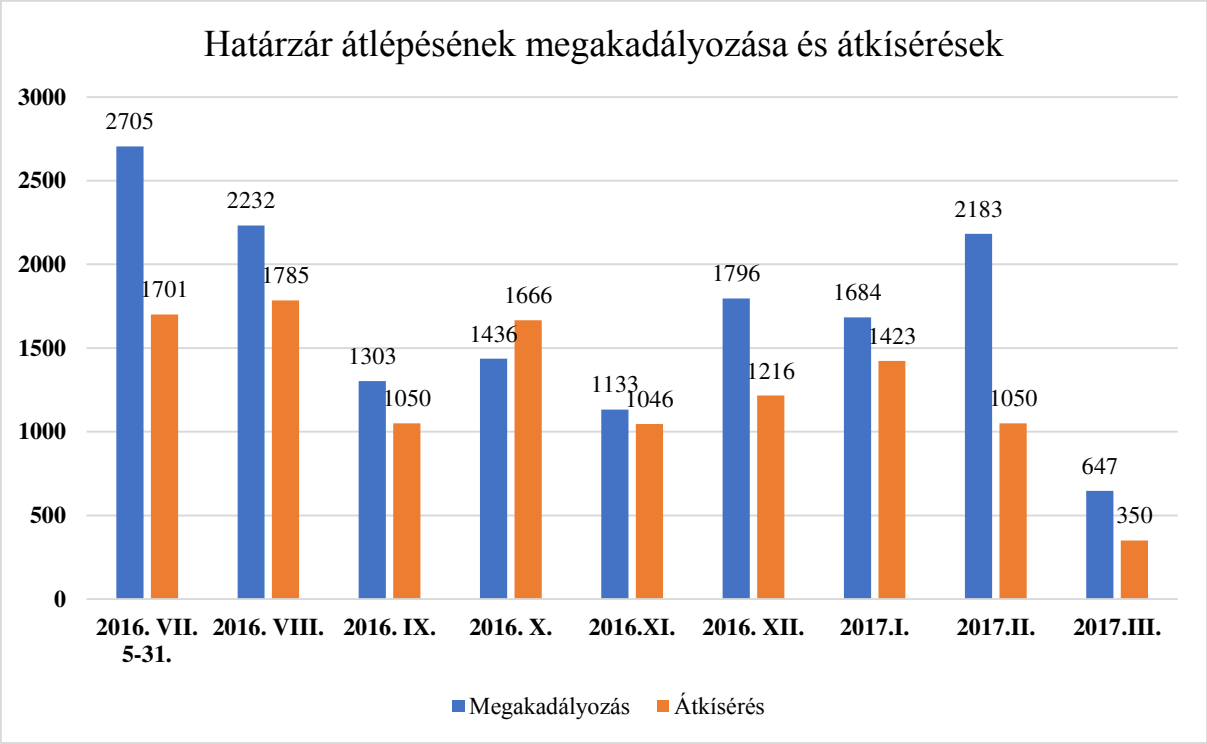
A következő ábra adatai alapján látható, hogy kerítésen 2016. évben végrehajtott további technikai fejlesztések (manőverút kiépítése, magasfigyelők, mozgásérzékeny kábel, nappali és hőkamerák beépítése, illetve a hozzájuk kapcsolódó jelzéskezelő központok rendszerbe állítása) ellenére továbbra is magas volt azoknak a száma (2. ábra), akik esetében sikerült megakadályozni a kerítésen való átjutást, vagy átjutottak azon és visszakísérésre kerültek a kerítés túloldalára.[9] Jelentős csökkenés e tekintetben 2017. márciusában következett be, amikor a kerítéshez kapcsolódó újabb jogszabály módosítás (2017. évi XX. törvény) már olyan jelentős visszatartó erőt képviselt, hogy az irreguláris migránsok részére szinte

[7] A Büntető Törvénykönyvről szóló 2012. évi C. törvény 352/A. §-a határozza meg a határzár tiltott átlépésének törvényi tényállását.

[8] 2017. július 5-től a törvény 3. § (1a) pontja alapján „a rendőr Magyarország területének a Közösségi Kódex 2. cikk 2. pontjának megfelelő külső határ szerinti határvonaltól, illetve a határjeltől számított 8 km-es sávon belül feltartóztathatja a Magyarország területén jogellenesen tartózkodó külföldit, és az (1) bekezdés szerinti létesítmény legközelebbi kapuján átkísérheti, kivéve, ha bűncselekmény elkövetésének gyanúja merül fel.” 2017. márciustól a 2017. évi XX. törvény 11. § (1b) pontja eltörölte a 8 km-es sávhatárt.

[9] 2017. évben március 31-ig összesen 633 fő követett el tiltott határátlépést, vagy kísérletét, amelyhez képest továbbra is magas a megakadályozások és átkísérések száma.

kilátástalanná vált az az alternatíva, hogy a magyar–szerb viszonylaton keresztül jussanak magyar területre. [10]



2.ábra Határzár átlépésének megakadályozása és átkísérések (a szerző szerkesztése a [17] alapján)

2017. áprilisra került kiépítésre a kerítés második, belső vonala, amely szintén acél oszlopokra rögzített dróthálóból áll, helyenként gyorstelepítésű drótakadállyal megerősítve, illetve a kerítésre 8 mm-es átmérőjű hegesztett acél síkháló került rögzítésre, amely egyszerű kézi drótvágó eszközökkel már nem átvágható, valamint a háló sűrűsége olyan kicsi, hogy abba nem lehet a lábat bedugni és a kerítésre felmászni. A kerítésrendszer felépítése az államhatár felől az újabb fejlesztés után így alakul:

1. a határvonal közelében első ütemben telepített alapkerítés, amelynek határvonal felőli oldala gyorstelepítésű drótakadállyal is biztosított. Ezen a kerítésvonalon kerültek elhelyezésre a nappali és éjszakai kamerák, valamint a kerítéshálóba fűzött mozgásérzékeny optikai kábel, amelyek képi információi és jelzései a Mórahalmon és Bácsalmáson elhelyezett ún. command centerekbe futnak be
2. manőverút és a mellette kiépített vízelvezető árok, magasfigyelők

[10] A határőrizeti területen lefolytatott eljárás szigorításával kapcsolatos egyes törvények módosításáról szóló 2017. évi XX. törvény eltörölte a 8 km-es sávhatárt és szigorította a menekültügyi eljárás szabályait.
11. § Tömeges bevándorlás okozta válsághelyzet idején a rendőr Magyarország területén feltartóztathatja a Magyarország területén jogellenesen tartózkodó külföldit, és az (1) bekezdés szerinti létesítmény legközelebbi kapuján átkísérheti, kivéve, ha bűncselekmény elkövetésének gyanúja merül fel.
7.§ A menekültügyi hatóság az elismerését kérő részére a jogorvoslattal tovább nem támadható döntés vagy a dublini átadásáról hozott végzés végrehajthatóvá válásáig tartózkodási helyként a tranzitzóna területét jelöli ki. Az elismerését kérő a tranzitzóna területét a kiléptető kapun keresztül hagyhatja el.

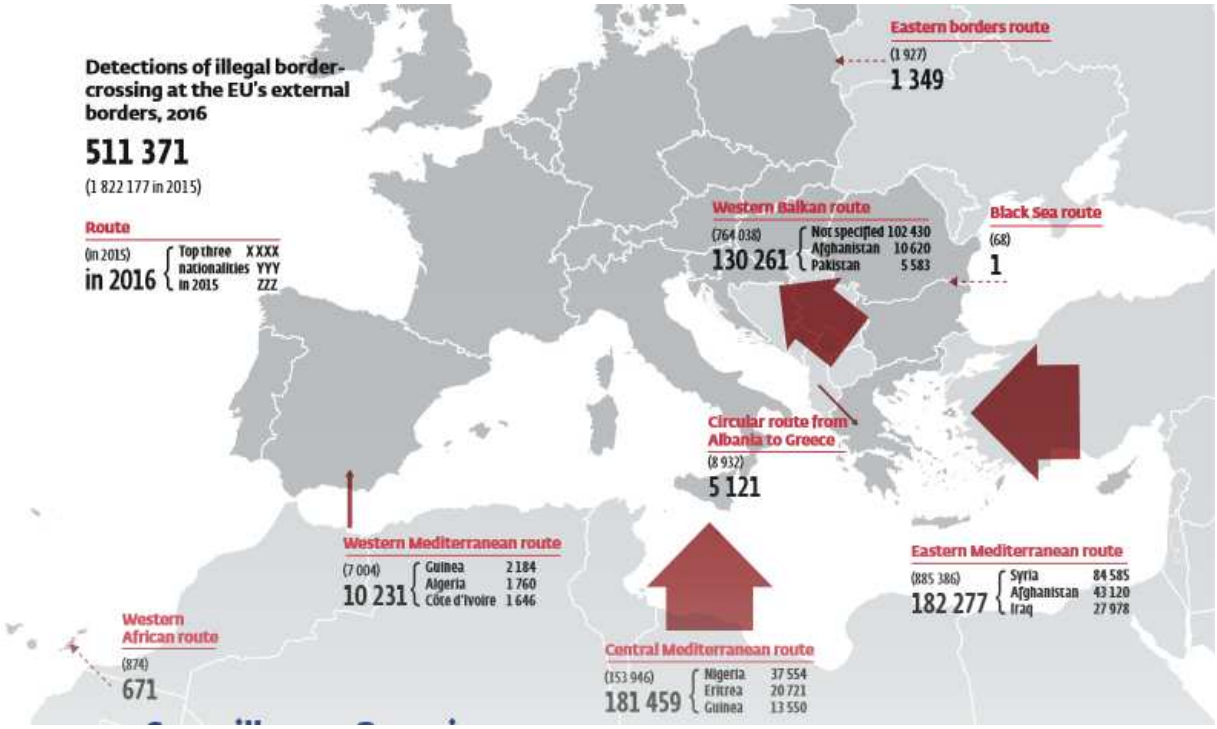
3. második kerítésvonal.

Az így kiépített, és elektromos feszültség alá helyezett[11] kétsoros kerítésrendszer lényegesen komolyabb fizikai akadályt képez, illetve főleg a második vonal kézi eszközökkel egyszerűen és gyorsan nem vágható át, amely azt eredményezi, hogy a felderítő és jelző berendezések jelzését követően az irreguláris migránsok nagyobb valószínűséggel tartóztathatóak fel már a két vonal között.

JÖVŐKÉP ÉS KÖVETKEZTETÉSEK

Ha a fenti kérdést az illegális migráció szempontjából közelítem meg, egyértelműen arra a következtetésre jutok, hogy a kerítés, a határőrizeti célú ideiglenes határzár már csak nevében tekinthető ideiglenesnek, hiszen nem várható, hogy azok a globális problémák, amelyek a jelenlegi illegális migrációs folyamatokat kiváltották, a közeljövőben megoldódnak és ezáltal az illegális migráció is megszűnik. Változások csak az illegális migráció mértékében és az útvonalakban következhetnek be, hiszen az irreguláris migránsok nyilván azokon az útvonalakon igyekeznek majd úti céljukhoz eljutni, amelyeken a legkisebb ellenállásba ütköznek.

Ezt támasztja alá a Frontex aktuális éves kockázatelemzése (3. ábra), amelynek adatai alapján 2016-ban a nyugat-balkáni útvonalon jelentős csökkenés állt be az illegális migrációs folyamatokban, ugyanakkor a nyugat- és közép-mediterrán térségben növekedés kezdődött el.



3.ábra Frontex kockázatelemzési adatai [18]

[11] A magyar-szerb határon kiépítésre kerülő intelligens jelzőrendszer működéséről szóló 1401/2017. (VI. 28.) Korm. határozatban a Kormány elrendelte a magyar-szerb határon kiépítésre kerülő intelligens jelzőrendszer 900 V névleges feszültségű alapesetben történő üzemelését.

Határőrizeti szempontból vizsgálva a kérdést, úgy gondolom, hogy a jövőben is indokolt lesz a kerítés folyamatos technikai fejlesztése/kiegészítése, mivel a fentebb említettek alapján az irreguláris migránsok és az embercsempész szervezetek is folyamatosan keresni fogják az új lehetőségeket és módszereket. Kétségtelennek tartom, hogy a kerítésre alapozott technikai fejlesztések hozzájárulnak a határőrizeti feladatok ellátásához szükséges élőerő létszámának csökkentéséhez. A jelenlegi tapasztalatok alapján a tiltott határátlépők már csak nagyon nehezen tudják átlépni a kerítés második, belső vonalát, ezért a megfelelő szintű reagáló képesség modellezésével és a kockázatelemzés alapján helyesen megválasztott szolgálati módokkal kialakítható az a minimális járőrlétszám, amellyel a kerítés elektrooptikai felderítő- és jelzőrendszereinek jelzései és képi információi alapján még a két kerítésvonal között biztonsággal végre lehet hajtani a feltartóztatásukat. Ugyanakkor az is kétségtelen, hogy a különböző technikai eszközök, felderítő és jelző berendezések észlelései alapján továbbra is élőerővel kell intézkedni, meg kell akadályozni a kerítés átlépését, vissza kell kísérni a feltartóztatott személyeket, amelyet a technika nem fog tudni megoldani az állomány helyett. Mindezeken kívül rendkívül nehéz pl. a határőrizet meglepetésszerűségének elvét [19] érvényesíteni, hiszen nem lehet meglepetésszerűségről beszélni akkor, amikor valamennyi irreguláris migráns tisztában van azzal, hogy Magyarország déli határai kettős kerítéssel összefüggően védettek. Megjegyzendő, hogy a kockázatelemzéssel, elektronikai eszközök alkalmazásával és határőrizeti elvekkel összefüggő gondolatmenetnek csak addig van létjogosultsága, amíg az illegális migráció úgymond „normál” keretek között jelenik meg a zöldhatáron. Abban az esetben, ha jelenleg nem prognosztizálható tényezők miatt olyan helyzetekre kerülne sor, mint a ceutai és melillai kerítés kapcsán, ahol többszáz fős tömegek rohamozzák meg egy adott ponton a kerítést, a kerítés masszivitásának fokozása és a csapatszolgálati tevékenység kerülne előtérbe.

Az illegális migráció továbbra is olyan európai szintű problémát jelent, amely kerítésekkel és pusztán rendészeti eszközökkel nem megoldható. A lehetséges megoldásoknak nem csak az államhatár vonalán kell megjelennie, hanem az Integrált Határbiztonsági Modell [20] egyes lépcsőinek megfelelően már a migrációt kibocsátó országokban, a harmadik és szomszédos országokban, valamint a szabad mozgás térségében, egységes, komplex rendszert alkotva. Mindez különösen azért fontos, mert hosszabb távon az illegális migrációs folyamatok további erősödését okozhatják pl. a klímaváltozás hatásai, vagy az afrikai kontinens nagymértékű népességgyarapodása, amelyhez nem párosulnak megfelelő megélhetési körülmények és ellátó rendszerek. Emellett az Európai Uniót tekintve az uniós politikának egységes álláspontot kellene képviselnie a külső határok őrizetével és a menekültüggyel kapcsolatban.

FELHASZNÁLT IRODALOM

[1] HAUTZINGER, Z.; HEGEDÜS, J.; KLENNER, Z.: *A migráció elmélete*, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar 2014.

[2] *Elkészült a második kerítés is,* origo.hu, http://www.origo.hu/itthon/20170428-elkeszult-a-ketsoros-keritesrendszer-masodik-keritese-a-magyar-szerb-hatarszakaszon.html (Letöltés: 2017. 05. 02., nem szó szerint idézve)

[3] BALLA J.: *A Magyar Honvédség helye és szerepe a határőrizeti rendszerben,* Hadtudományi Szemle, 2017. X. évfolyam 1. szám, Nemzeti Közszolgálati Egyetem 2017.

[4] BALLA, J.; KUI, L.: *A határőrizeti célú ideiglenes biztonsági határzár és határőrizetre gyakorolt hatásai.* Hadtudományi Szemle, 2017. X. évfolyam 1. szám, Nemzeti Közszolgálati Egyetem (2017) 223-225. o.

[5] FÓRIZS S.: *A határőrség megalakulása, valamint tevékenysége az első években (1945-1950)*. Magyar Rendészet XV. évfolyam, 2015/6. szám, 2015.

[6] FÓRIZS S.: *Az államhatár műszaki megerősítésének kezdete 1948-ban.* Hadtudomány, XXV. évfolyam 2015. 1. elektronikus szám 2015.

[7] SALLAI J: *Egy idejét múlt korszak lenyomata. A vasfüggöny története*. Hanns Seidel Alapítvány (2012) 70-73. o.

[8] RITECZ, GY.; SALLAI J.: *A migráció trendjei, okai és kezelésének lehetőségei 2.0.* Hanns Seidel Alapítvány, Budapest, (2016) 74-80. o.

[9] BALLA J.: *Határőrizeti intézkedések a migrációs válság kezelésére és megszüntetésére*, In.: Tálas Péter (szerk.), Magyarország és a 2015-ös migrációs válság, Dialóg Campus Kiadó (2017) 83-100. o.

[10] 1401/2015. (VI. 17.) számú kormányhatározat

[11] KUI L.: *A magyar határőrizet technikai támogatásának aktuális helyzete.* Határrendészeti Tanulmányok 2016/2. szám (2016) 122-123. o.

[12] KOVÁCS G.: *A Magyar Rendőrség szerepvállalása hazánk határbiztonságában és a schengeni külső határok ellenőrzésében*. Hautzinger Zoltán (szerk.) Migráció és rendészet. Magyar Rendészettudományi Társaság Migrációs Tagozat (2015) 69-84. o.

[13] KOVÁCS G.: *A migráció bűnügyi hatásai a magyar határrendészet kockázatelemzési rendszerére.* Hautzinger Zoltán (szerk.): A migráció bűnügyi hatásai. Magyar Rendészettudományi Társaság Migrációs Tagozat (2016) 141-150. o.

[14] KOVÁCS G.: *A rendőrség vezetésirányítási rendszerének sajátosságai a migrációs válsághelyzet kezelése során.* Tálas Péter (szerk.): Magyarország és a 2015-ös európai migrációs válság. Dialóg Campus Kiadó (2017) 148. o.

[15] HAUTZINGER Z.: *Büntetőjogi válaszok a tömeges bevándorlás okozta válsághelyzetre Magyarországon*. Tálas Péter (szerk.) Magyarország és a 2015-ös európai migrációs válság. Dialóg Campus Kiadó (2017) 72-74. o.

[16] http://www.police.hu/hu/a-rendorsegrol/statisztikak/hatarrendeszet (Letöltve: 2017. 05. 03.)

[17] http://www.police.hu/hu/a-rendorsegrol/statisztikak/hatarrendeszet (Letöltve: 2017. 05. 03.)

[18] http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2017.pdf (Letöltve: 2017. 05. 09.)

[19] KOVÁCS G.: *A határrendészetben ható törvényszerűségek és elvek érvényesülése az illegális migráció elleni küzdelemben. Modernkori veszélyek rendészeti aspektusai,* Pécsi Határőr Tudományos Közlemények XVI. kötet 2015.

[20] RITECZ, GY.; SALLAI J.: *A migráció trendjei, okai és kezelésének lehetőségei 2.0.* Hanns Seidel Alapítvány 2016.

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

A FELSZÍNI VIZEK CIANID ÉS NEHÉZFÉM SZENNYEZÉSEIVEL KAPCSOLATOS KÁRESEMÉNYEK TANULSÁGAI KATASZTRÓFAVÉDELMI SZEMPONTOK ALAPJÁN

LESSONS OF DAMAGE EVENTS RELATED TO CYANIDE AND HEAVY METAL CONTAMINATION OF SURFACE WATERS BASED ON DISASTER MANAGEMENT ASPECTS

CSŐSZ László

(ORCID: 0000-0003-1662-5139)

csosz.laszlo@uni-nke.hu

Absztrakt

A víz kémiai, fizikai, illetve biológiai sajátosságai alapján az élővilág és a társadalom számára a legfigyelemreméltóbb, legalapvetőbb és leginkább nélkülözhetetlen vegyület. Felszín alatti és felszíni vizeink egyaránt egyre nagyobb terhelésnek vannak kitéve. A felszíni vizek minősége a földtani felépítés, a talaj, de legfőképpen a társadalmi tevékenységek függvénye. A felszíni vizek szennyezőit három nagy csoportra oszthatjuk az iparra, a mezőgazdaságra és a különböző kommunális eredetű szennyezésekre. Ezek a negatív tendenciák kedvezőtlen hatással vannak vizeink minőségére és mennyiségére egyaránt. A szerző egy konkrét esettel prezentálja az ipari eredetű szennyezések csoportjába tartozó nehézfémszennyezések hatását, illetve elhárítási lehetőségeit.

Kulcsszavak: *ipari balesetek, nehézfém szennyezések, a Cher folyó szennyezése*

Abstract

Based on its chemical, physical and biological characteristics of water it is the most considerable, most basic and most indispensable compound for biosphere and society. Both our subsurface and surface waters are exposed to always bigger pollution. The quality of surface waters depends on geologic set-up, the soil, but mostly social activities. The pollutants of surface waters can be divided in three big groups: industry, agriculture and different contaminations of communal origin. These negative tendencies have an adverse effect onto the quality and quantity of our waters. The author presents the effect of heavy metal contaminations belonging to the group of contaminations of industrial origin and the elimination possibilities thereof respectively through a factual example.

Keywords: *industry disaster, heavy metal contamination, Cher river pollution*

A kézirat benyújtásának dátuma (Date of the submission): 2017.08.29.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.08.31.

BEVEZETÉS

Az iparban a különböző balesetek, robbanás, tűz és veszélyes anyag kibocsájtás formájában realizálódhatnak. A folyamatosan szigorodó szabályozás ellenére, mind hazánkban mind a szomszédos, illetve távoli országokban számos ipari baleset következett be az elmúlt évtizedekben, melyek során veszélyes anyagok kerültek ki a környezetbe, súlyosan károsítva azt. [1] A veszélyes anyagok nem csak az előállításuk során a gyárakból, a különböző ipari területekről kerülhetnek a környezetbe, hanem a szállításuk, illetve a tárolásuk során is. Az utakon kiemelten, a vasúthálózaton és egyre inkább a hajózható vizeken, illetve légi úton is jelentős mennyiségű veszélyes áru szállítása történik. [2] Jelenlegi életszínvonalunk fenntartásához elengedhetetlen az ipar működése, amely magában hordozza a veszélyes anyagok jelenlétét. [3] Hazánkban a katasztrófavédelemmel kapcsolatos jogszabályok előírják, hogy a veszélyes üzemek üzemeltetői a biztonsági dokumentációik mellékleteként belső védelmi tervet készítsenek, melyben bemutatják egy lehetséges ipari baleset elleni védekezést szolgáló intézkedéseket és a felhasználható erőforrásokat. Olyan üzemeknél, melyeknél számolni kell valamely veszélyes anyag kijutásával, és ez által az emberek egészségének károsításával, illetve a természetes és mesterséges környezet szennyeződésével vegyi felderítési és mentesítési feladatokat is kell tervezni és meg kell határozni az ezekhez szükséges erőforrás igényt is. [4] A szabályozások szigorításával jelentősen csökkenthetőek a veszélyes anyagokkal kapcsolatos balesetek bekövetkezései, azonban az emberi tényező szerepe miatt teljesen nem szüntethetőek meg, éppen ezért fontos, hogy a bekövetkezett ipari eredetű baleseteket kellőképpen megvizsgáljuk és levonjuk a következtetéseket. Ezen információk birtokában lehetőség van a továbbiakban az esetlegesen bekövetkező balesetek megakadályozására, a szennyezések gyors és szakszerű kezelésére, valamint a káros hatások felszámolására.

CIANID ÉS NEHÉZFÉM SZENNYEZÉSEK

A különböző nehézfémek természetbe jutásásának veszélyessége mérgező hatásukból ered, amely már kismértékű légköri, élővízi, valamint a talajban történő felhalmozódás esetén is rendkívül jelentős károsodást idézhetnek elő az élővilág táplálékláncában, illetve az ember egészségében egyaránt. A nehézfémek ugyanis erősen kötődnek a szerves anyagokhoz, illetve kelátvegyületek formájában abba be is beépülhetnek. [5]

Az elmúlt évtizedekben több ipari eredetű szennyezés történt, melyek súlyosan károsították a környezetet. 2000 januárjában gátszakadás következett be a romániai Aurul nagybányai üzemében, melynek következtében közel 100 ezer m3 cianid [6] tartalmú zagy szennyezte el a folyókat, főként a Tiszát. A cianid-szennyezés egészen a Duna-Tisza találkozásáig (Titel) fejtette ki káros hatását, sőt még a Duna-deltában is észlelték a szennyezést. 2000 márciusában a máramarosi Borsabányánál következett be cián szennyezés. 2004-ben a Szeret folyóba jutott ki közel 10 tonna cianid. Hosszasan lehetne még sorolni a különféle ipari eredetű szennyezéseket, azonban ezek csak azok a szennyezések, amelyek hazánkat is érintették, de számos cianid-szennyezés történt az Amerikai Egyesült Állomoktól Anglián át Kínáig. [7] A cianid, illetve a nehézfém szennyezések forrása elsősorban az ipar, azon belül a bányászat, de származhat a mezőgazdaságból is (intenzív műtrágyázás – ammónium, nitrát, foszfát, kálium).

1. ábra A Szennyezés területei és adatai [8]

A CHER FOLYÓ ELSZENNYEZÉSE

A baleset helyszíne egy 1994-ben épült telephely Allier régió területén, Saint Victor városában található Franciaországban. [9] A telephely fémrészek felületkezelési műveleteinek végrehajtása céljából, különösen autóalkatrészek horganyozásának céljából épült. A telephely 3,530 m^2 fedett épületből áll, ami 2 felületkezelő sornak, egy szárítórendszernek és kirakórendszernek ad otthont. A két rendszer hossza összesen 196 m. A telephely minősített létesítmény, amelynek működését a 2005. április 7-én a területileg illetékes hatóság engedélyezte. Az érintett fémkezelő sort autóipari alkatrészek ömlesztett kezelésére használják. Ez a következőket foglalja magába: horganyozás (fém felületkezelése), nikkelbevonat és lúgos cianid rézbevonat. A balesetet szivárgás okozta, ami a kezelősor iszapnyelő aknájában végzett szivattyúzási művelet közben keletkezett. Ez érintette a veszélyes komponensek eltávolítására szakosodott üzemrészt is.

2005. szeptember 14-én az egyik technikus szivárgást észlelt a kezelősorokon. A szűrőrendszerből kilépő csővezeték a lúgos rézcianidot tartalmazó tartályon szétkapcsolt, ezzel előidézve, hogy az iszapelnyelőbe folyjon. A technikus azonnal tájékoztatta a cég környezetvédelmi felügyelőjét. A felügyelő elrendelte, hogy a felületkezelő sort le kell állítani (a fűtőrendszer lekapcsolásával együtt) és hogy a folyadék maradjon az iszapnyelőben. Az incidenst az erre a célra szolgáló naplóban rögzítették.

2. ábra A telephely szivárgó csöve, amely a szennyezést okozta [10]

Másnap szeptember 15-én egy másik technikus észlelte, hogy a többszörös felületkezelő sor iszapnyelő aknája tele van folyadékkal és látta a naplóba beírt előző napi incidenst. Úgy döntött, hogy mobil szivattyút használ, hogy átemelje a terméket a koncentrált lúgos cianid szennyvizet tartalmazó tartályba. Normál üzemelés közben egy belső rendszer visszakeringeti ezt, ami semlegesíti a cianidokat, mielőtt azokat kibocsátják a környezetbe. Ekkor, ahogy azt minden reggel 9 óra körül megteszi, leolvasta a szennyezőanyag-koncentráció szintjét a telephely végső hulladék-kibocsátási pontján (kolorimetriás elemzéssel). Megjegyezte, hogy a cianidtartalom szokatlanul magas volt: 2mg/l fölött, 0.1 mg/l beállított határérték mellett. Haladéktalanul úgy döntött, hogy elzárja a végső szennyvízszelepet és elzárja a felületkezelő sorok vízellátását. A végső szennyvizet az erre a célra tervezett biztonsági tartályba irányította. Miután konzultált a technikussal, a környezetvédelmi felügyelő észlelte, hogy az iszapnyelő aknában lévő folyadékot, tévedésből a koncentrált lúgos cianid tartalmú szennyvizek számára fenntartott tartály helyett a króm öblítő (gyűjtő) tartályba szivattyúzták. A felügyelő nátrium-hipoklorittal semlegesítette a szennyezett reaktorokat és átszivattyúztatta a vizet a biztonsági tartályba. A krómeltávolító rendszer tisztítási műveletei szeptember 15-én egész nap folytatódtak. Szeptember 16-án 8 órakor a laboratórium/környezetvédelmi felügyelő végrehajtott egy cianid elemzést a dekromatizáló és neutralizáló rendszer kimenetén: nem figyelt meg szokatlan mérési adatot. A belső kezelőállomást így ismét üzembe helyezték. Ezt követően óránként teszteket hajtottak végre, hogy megbizonyosodjanak, hogy a cianid nincs jelen. Szeptember 17-én éjfélkor az iszap visszanyeréshez használt szűrőprést ismét üzembe helyezték. Szeptember 17-én körülbelül 15:30-kor a Cher mentén élő lakók a folyóban lévő tömeges halpusztulásról tájékoztatták a csendőrséget, továbbá tájékoztatták a Nemzeti Halászati Bizottságot, ami körülbelül 16:30-kor érkezett ki a helyszínre. A halpusztulás eredetének meghatározására vonatkozó vizsgálat gyorsan a felületkezelő cég szennyvizét a Cher folyóba engedő csőre irányult. 17:00 órakor értesítették a környezetvédelmi felügyelőt és tájékoztatták a mért adatokról. Miután visszatért a helyszínre és elemezte az ipari szennyvíz végső kibocsátási pontját, ismét feljegyezte cianid jelenlétét. Azonnal lekapcsolta a detoxikáló állomás és a végső szennyvízkibocsátási pont vízellátását. Az új szennyeződési incidens elemzése után a környezetvédelmi felügyelő meghatározta, hogy az iszapkezelő művelet okozta a szűrőprésekben lévő cianid kiszabadulását. 18:00 órára minden termelési műveletet felfüggesztettek azonnali hatállyal.

Szeptember 19-én a környezetvédelmi felügyelő megtisztította az „iszapvisszanyerő” rendszert, a semlegesítő rendszert, a pelyhesítő kamrát és az ülepítő tartályt, mivel a cianid ezeket a reaktorokat szennyezte, miután pénteken, 2005. szeptember 16-án visszanyerték a szűrőprésekbe az iszapot. Kedden, 2005. szeptember 20-án a detoxikáló állomást ismét üzembe helyezték és ellenőrzéseket hajtottak végre a nap folyamán: nem észleltek szennyeződésre utaló jelet. A kibocsátott szennyvíz minden paramétere az engedélyezett határérték alatt volt, a 2005. április 7-én kelt prefektusi rendeletnek megfelelően.

A telephely üzemeltetőjének becslése szerint a 3-5 g/l koncentrátumban cianidot tartalmazó szennyvízből megközelítőleg 320 m^3 került kibocsátásra a Cher folyóba, a Nemzeti Halászati Bizottság ügynökei halpusztulást jelentettek (közel 2,5 tonna), a telephely közelében vagy a Cher folyóba történő kibocsátáshoz közel élő lakosok nem jelentettek egészségügyi problémákat.

3. ábra A szennyezés következménye [10]

A baleset oka és körülményei

A baleset során lefolytatott vizsgálatok a termékeken, illetve a folyamaton, segítettek a baleset okainak gyors meghatározásában. A szennyezőanyagoknak a folyóba történő kibocsátása szervezeti és emberi hibáknak tulajdonítható. Egy technikus veszélyes termékeket tartalmazó (alkáli rézcianid) folyadékot engedett át egy öblítőtartályba, amelynek tartalma nem volt egyértelműen és olvashatóan feltüntetve. Mivel ez az öblítőtartály egy króm detoxikáló kezelőrendszerhez csatlakozott, a cianidot nem különítették el és így a Cher folyóba bocsátották jóval az engedélyezett szint feletti koncentrációban. A felületkezelő sor hibájának esetére teendő intézkedésekre vonatkozó írásos utasítások hiányában a technikusnak saját ítélőképességében kellett megbíznia, ami nem bizonyult szerencsésnek. Miután észlelték a nem megfelelő szennyvíz-kibocsátást, a kezelő leállította a műveleteket és megtisztította a kezelő létesítményt. A tisztítási műveletek valójában hiányosak voltak és a cianidok, amelyek az ipari szennyvízkezelő létesítmény (szűrőprés) részében maradtak feleltek a szennyezett víz két nappal később történő második kibocsátásáért.

Tanulságként megállapítható, hogy bizonyos folyamatok, még ha azt rendszeresen is hajtják végre, még mindig kockázatot hordozhatnak magukban. A balesetet követően végrehajtott vizsgálatok eredményeképpen feljegyezték, hogy a felületkezelő sor üzemeltetése igényli, hogy legalább az alábbi feltételek ellenőrzésre kerüljenek: atipikus helyzetben teendő

intézkedéseket rögzítő dokumentumok megszövegezése, a technikusok tájékoztatása és oktatása e dokumentumok használatáról rendszeres helyzetgyakorlatokkal.

NEHÉZFÉMMEL SZENNYEZETT FELSZÍNI VIZEK KEZELÉSI LEHETŐSÉGEI

A különböző természetes vizek természetes forrásból is tartalmaznak egészségre káros anyagokat, azonban a vizek szennyeződésének legfőbb oka a különböző emberi tevékenységek következményeivel azonosíthatók. A városok, az ipar, a közlekedés fejlődése, valamint a különböző foszforműtrágyák alkalmazása a fémek természetes biogeokémiai körforgásban megjelenő mennyiségének sokszorosát termelik ki és juttatják a környezetbe, illetve a vizekbe. A különböző vízminőségi problémák egyik legfontosabb kérdése a toxikus fémtartalom mennyisége és minősége. [11]

A 2000-ben bekövetkezett, a Tiszát és a Szamost érő romániai eredetű cianid- és nehézfém súlyosan károsította a folyók élővilágát. Az okozott közvetlen gazdasági kár mértékét, mintegy ötmilliárd forintra, az élővilágot ért kárt és a helyreállítás összegét, közel huszonöt milliárd forintra becsülték. [12] A cianid szennyezés levonulását követően a Tiszán és a Szamoson vett üledékmintákban több esetben a szennyezett talajokra vonatkozó beavatkozási határértékeket meghaladó koncentrációban észleltek kadmiumot, cinket, rezet, illetve arzént.

A különböző nehézfémek elsődleges negatív hatásai alapvetően a táplálékhálózatok alsó és felső szintjein jelentkeznek. Az oxigéntartalmú vizekben a nehézfémek vegyületei többnyire rosszul oldódnak, továbbá kicsapódva leülepednek az iszappal. A nehézfémek felhalmozódnak az üledék felszíni rétegeiben, ahol hatással vannak az ott gyökerező növényekre. Mint nem lebomló szennyezőanyagok a táplálékláncban feldúsulnak (biomagnifikáció), fokozottan veszélyeztetve a harmadlagos fogyasztókat, például a halakat fogyasztó madarakat, valamint az embert.

A fémes eredetű szennyezések eltávolítása a felszíni vizekből több megoldással is lehetséges. Ezek közül kiemelném a fitoremediációt. A fitoremediáció (fito = növény, remedium = orvoslás) [13] során növényekkel és a velük társult mikrobákkal távolíthatóak el, illetve bonthatóak le a szennyezőanyagok, köztük a nehézfémek a szennyezett talajból, valamint vízből. A fitoremediáción belül több eljárás is alkalmazható, például a fitoextrakció, a fitostabilizáció, valamint a fitodegradáció és a rizofiltráció. Gyorsan fejlődő környezetvédelmi technológiáról van szó, amelyet egyelőre még nem alkalmaznak üzemszerűen. A fitoremediációt vizsgáló kutatások a kilencvenes években gyorsultak fel igazán. A fitoremediáció legfőbb előnye, hogy környezetbarát technológia, amely viszonylag olcsó, kevesebb másodlagos szennyeződés keletkezik, továbbá az eljárás nagy felületen alkalmazható, így igen hatékony. Ennek a technológiának az alkalmazása azonban igen időigényes folyamat. További hátránya, hogy a növények nem képesek minden szennyezőanyagot lebontani, így ez az eljárás elsősorban a mérsékelten szennyezett talajoknál, illetve vizeknél alkalmazható.

KÖVETKEZTETÉSEK

Az Európai Unió mellett hazánk is komoly figyelmet fordít, illetve energiát fektet a jelentős felszín alatti, továbbá a felszíni vizeinek megóvására. Ezt jól szemlélteti, hogy vizeink zöme kevés kezeléssel megfeleltethető az ivóvízszabványban előírt követelményeknek. Földünk édesvíz készletei azonban veszélyben vannak és végesek is. Ezt nemzetközi tudományos kutatások eredményei és hazai tapasztalatok egyaránt alátámasztják. Ennek, az emberiség létét fenyegető globális környezeti problémának a kezelése összefogást és együttműködést igényel minden szinten. Hogy a jövőben is mindenki számára hozzáférhető legyen a tiszta ivóvíz, hogy megmaradhassanak a folyók és tavak, komoly erőfeszítéseket kell tennünk vizeink megóvásáért, illetve állapotuk javításáért az elkövetkezendő évtizedekben is. Fontos,

hogy megőrizzük vizeink jó minőségét, leginkább úgy, hogy megóvjuk azokat a különböző szennyezésektől. Hogy a cikkben részletezett balesethez hasonló súlyos szennyezésekkel járó balesetek bekövetkezését megelőzzük, fontos a szabályozás még szigorúbbá tétele. Mivel az iparban az emberi tényező szerepe óriási veszélyforrás, elengedhetetlen például, hogy a veszélyes anyagokkal munkájuk során kapcsolatba kerülő személyek megfelelő oktatásban részesüljenek, hogy egy esetleges baleset bekövetkezésekor, ha módjukban áll meg tudják hozni a megfelelő időben a megfelelő döntést, hogy megelőzzék azt vagy hogy a következmények káros hatását a minimálisra csökkentsék. A cikk az ipari eredetű fémes szennyezéseket, illetve a vízbázisok mentesítésére alkalmazott műszaki megoldásokat célozta prezentálni, különös hangsúlyt fektetve az egyre inkább teret nyerő biológiai, „zöld" módszerekre.

FELHASZNÁLT IRODALOM

[1] PÁTZAY GY.; DOBOR J.: Ipari tevékenységekből eredő veszélyforrások és elhárításuk. Egyetemi jegyzet. Nemzeti Közszolgálati Egyetem. Katasztrófavédelmi Intézet. Budapest, 2016. ISBN 978-615-5527-91-3

[2] KÁTAI-URBÁN L.; KOZMA S.; VASS GY.: Veszélyes szállítmányok felügyeletével kapcsolatos hatósági tapasztalatok értékelése; Hadmérnök. X. Évfolyam 4. szám. Budapest, 2015.

[3] DOBOR J.: The importance of the teaching of case studies of industrial accidents in the disaster management education, ECOTERRA - Journal of Environmental Research and Protection, 2017, Volume 14, Issue 1, nyomtatott kiadvány ISSN 1584-7071, online ISSN 2248-3128; http://www.ecoterra-online.ro/files/496321269.pdf (letöltve: 2017. 06. 24.)

[4] SZENDI R.; DOBOR J.: Veszélyes üzemek azonosítása és a kapcsolódó hatósági tevékenység(ek); HADMÉRNÖK 8:(3) pp. 125-131. (2013), ISSN 1788-1919

[5] E-MISSZIÓ TERMÉSZET ÉS KÖRNYEZETVÉDELMI EGYESÜLET: Kelet-magyarországi Biomonitoring Hálózat; Békéscsaba, 2014. http://tiktvf.zoldhatosag.hu/egyeb/tiktvf/life/hu/document/tanari_felkeszito_fuzet.pdf (letöltve: 2017.06.21.)

[6] MAGYAR HIDROLÓGIAI TÁRSASÁG: Hidrológiai tájékoztató; Budapest, 2005. ISSN 0439-0954

[7] MAGYAR TÁVIRATI IRODA: Tiszai ciánszennyezés; MTVA Sajtó- és Fotóarchívum; http://static.origos.hu/s/img/i/1501/20150130tiszai-cianszennyezes-infografika1.jpg?w=666&h=632 (letöltve: 2017.06.26.)

[8] FRIDRICH R.: A nagybányai gátszakadástól a ciánmentes Európáig; http://lmv.hu/files/ciankonf_100201_Fidrich_Robert.pdf (letöltve: 2017.06.27.)

[9] FRENCH MINISTRY OF ENVIRONMENT: Polluted effluents released into the Cher River; http://www.aria.developpement-durable.gouv.fr/wp-content/files_mf/FD_31236_StVictor_2005_ang.pdf (letöltve: 2017.06.27.)

[10] ARIA: Lessons learnt from industrial accident; http://www.aria.developpement-durable.gouv.fr/accident/31236_en/?lang=en (letöltve: 2017.06.27.)

[11] MUCZA N.: Fémekkel szennyezett felszíni víz kezelése bioszénnel; Budapesti Műszaki Egyetem, Budapest, 2015. http://enfo.agt.bme.hu/drupal/sites/default/files/Mucza_Fémekkel%20szennyezet%20felsz%C3%ADni%20v%C3%ADz%20kezelése%20bioszénnel_tervezés.pdf (letöltve: 2017.06.29.)

[12] TERRA ALAPÍTVÁNY: Cián és nehézfémszennyezések a Tiszán; http://www.terra.hu/cian/index.html (letöltve: 2017.06.29.)

[13] SIMON L.: Fitoremediáció; Környezetvédelmi füzetek; Budapest, 2004. http://zeus.nyf.hu/~tkgt/konyvek/fitoremediacio_simon2004.pdf (letöltve: 2017.06.30.)

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

ATOMERŐMŰVI BALESETEK ÉS ÜZEMZAVAROK TANULSÁGAI 2.

NUCLEAR POWER PLANT ACCIDENTS AND MALFUNCTIONS, LESSONS LEARNED 2.

DOBOR József; KOSSA György; PÁTZAY György

(ORCID: 0000-0003-0191-4261) (ORCID: 0000-0002-4404-2929)
(ORCID: 0000-0002-5541-8012)

patzay.gyorgy@uni-nke.hu; dobor.jozsef@uni-nke.hu; info@intertanker.hu

Absztrakt

A nukleáris energia jelentősége hazánkban számottevő, Magyarország energiastratégiájának egyik pillére. Nemzetközi értékelések alapján kevésbé veszélyes, mint a fosszilis energiahordozók használatát kísérő veszélyek. A jelentős társadalmi előítélet az elmúlt évtizedekben bekövetkezett káreseményeknek tulajdonítható. A cikk ismerteti az elmúlt évtizedek legjelentősebb nukleáris baleseteit, okait és tanulságait. A publikáció két részben kerül közlésre. Az ismertetett balesetek minden esetben műszaki-tervezési hiányosságok következményei és emberi hibákkal/tényezőkkel képeznek direkt kapcsolatot. Az írás kitér arra, hogy minden káresemény több – sokszor egymástól független – hiba okozataként következik be.

Kulcsszavak: *atomerőművi balesetek, Windscale, Three Mile Island, Chernobil, Fukushima, okok, következmények*

Abstract

Nuclear energy plays an important role in Hungarian energy production. According to frequency-consequence curves for severe accidents in various energy chains fatality rates are lowest for western hydropower and nuclear power plants. On contrary the large nuclear disasters (Chernobyl, Fukushima) caused a negative publicity to nuclear energy. In this paper the four significant nuclear energy disaster in last decades is discussed, including reasons and consequences. Paper has two parts. In these disasters technical, construction errors and deficiences are the main reasons and human errors are only consequence of existing danger.

Keywords: *Nuclear energy disasters, Windscale, Three Mile Island, Chernobyl, Fukushima, reasons, consequencest*

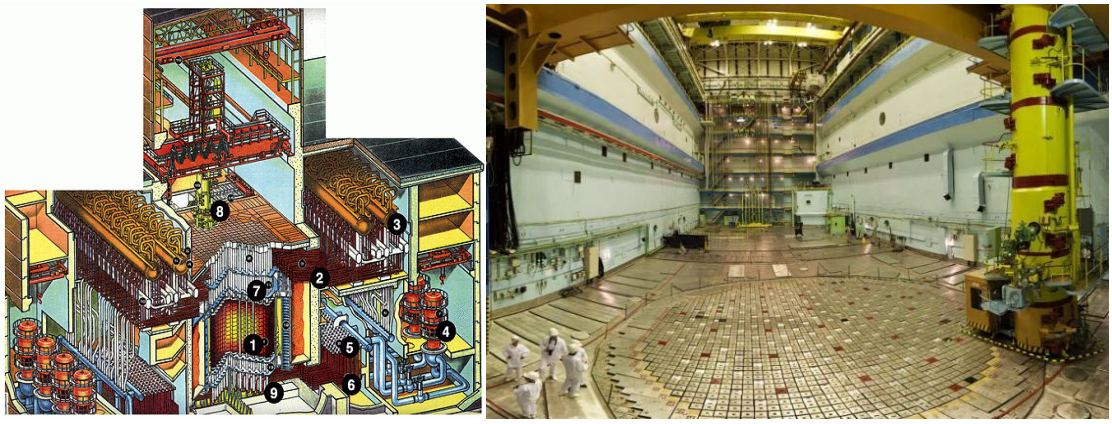
A kézirat benyújtásának dátuma (Date of the submission): 2017.08.29.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.09.02.

BEVEZETÉS

Az atomenergetika elmúlt évtizedeiben négy komoly atomerőművi baleset és számos üzemzavar következett be. Ezen nem kívánatos események részleges tanulságait és a levonható következtetéseket kívánjuk tárgyalni. Az a tény közismert, hogy az atomerőművek üzemi biztonságával szemben kezdettől fogva maximális követelményeket írtak elő és igyekeztek a biztonsági követelményeket betartani és betartatni. Mégis az elmúlt évtizedekben az egész világra, a közvéleményre, a politikára, az iparbiztonságra jelentősen kiható balesetek és üzemzavarok következtek be, melyeknek tanulságait a mai napig elemzik, értékelik és az atomerőművek biztonságát befolyásoló technikai és szervezési eljárásokat, előírásokat újra és újra átdolgozzák. Cikkünkben röviden összefoglaljuk az eddig bekövetkezett négy legsúlyosabb atomerőművi baleset eseményeit, tanulságait és a levonható következtetéseket. A cikksorozat 1. részében az általános alapelvek után tárgyaltuk a windscale-i (Nagy Britannia) és a Three Mile Island-i (USA) atomerőművi baleseteit [1] azok következményeit és a levonható tanulságokat. Jelen 2. részben a Csernobili (SZU) és a Fukushimai (Japán) baleseteket tárgyaljuk.

A CSERNOBILI ATOMERŐMŰ BALESET (SZOVJETUNIÓ, 1986 INES 7)

Az RBMK-1000 típusú forralócsöves reaktor felépítését mutatja a 1. ábra.



1. ábra A csernobili RBMK-1000 reaktor felépítés (1. aktív zóna, 2. forralócsövek, 3. gőzszeparátor, 4. fő keringtető szivattyú, 5. csoport osztófejek, 6. vízcsövek fejei, 7. felső biológiai védelem, 8. fűtőelem rakodógép, 9. alsó biológiai védelem, a szerzők szerkesztése a [2, 3] alapján)

A reaktor forralóvizes, csatornatípusú, grafittal moderált, könnyűvíz hűtésű, 3140 MW termikus, 1000 MW elektromos teljesítményű volt. A 4. Blokkot 1983 decemberében helyezték üzembe. A reaktorban 2000 db fűtőelem volt, melyben 180 t 1,8 %-os dúsítású UO_2 hasadóanyag található, 180 szabályozó rúddal. A reaktorban egy hengeres 21,6 m átmérőjű 25,5 m magas fedett betontartályban négyszögletes keresztmetszetű grafitoszlopok képezik az aktív zónát, melyek tengelye mentén hengeres csatornákat képeztek ki. A grafit moderátort gáztömör acélkonténerrel vették körül, melyet a grafit oxidációjának megakadályozására és jobb hűtése érdekében hélium-nitrogén gázkeverékkel töltöttek meg. A szovjetek kedvelték ezt a reaktortípust, mert katonailag felhasználható plutóniumot szolgáltatott, csak 1,8 %-ra dúsított fűtőelemmel működött, hosszabb kampányidővel dolgozhatott, mert átrakáshoz nem kellett a reaktort leállítani. Ugyanakkor jelentős hátrányokkal rendelkezett, több éghető anyagot tartalmazott a többi reaktortípusnál, 1661 db nyomás alatti forralócsöve közül bármelyik meghibásodhatott, a víz kifolyása esetén a forró grafit hidrogént fejleszthetett, és ami a legfontosabb "pozitív visszacsatolása" miatt könnyebben megszaladhat a teljesítménye,

mint a többi reaktor esetén. A technológiai csatornák a fűtőelemek elhelyezését szolgálják és itt áramlott a hűtővíz is. A csatornák központi része a 88 mm átmérőjű és 4 mm falvastagságú cirkónium cső volt, amely rozsdamentes acélban végződött. Egy csatornában két-két egyenként 18 fűtőelemet tartalmazó köteg volt. Egy fűtőelem UO_2 tablettáktól töltött, hermetikusan lezárt 13,5 mm átmérőjű és 3 500 mm hosszú cirkónium csövekből állt. A hűtőközeg víz-gőz keverék, tömegárama 36 500 t/h, a gőztermelés 5400 t/h, a telített gőz hőmérséklete 284 °C volt. A víz a technológiai csatornákban forrásig hevült és részlegesen (14 tömeg %) gőzzé alakul. A két-két gőzszeparátorban a két fázis elvált, a száraz gőz a két 500 MW-os turbinára áramlott, a vizet pedig a fő keringtető szivattyúk (körönként 4 db, összesen 8 db) visszatáplálták a reaktorba.

1986. április 26-án az ukrán csernobili forralócsöves (RBMK-1000) atomerőmű új, 4. blokkjában bekövetkezett az atomerőművek történetének addigi legsúlyosabb balesete. Az erőmű Kijevtől 100 km-re, északra Pripjaty és Csernobil városok közelében helyezkedett el. Az RBMK-1000 reaktor vízhűtésű, víz és grafit moderátorú forralócsöves reaktortípus volt. Mint minden akkori szovjet reaktor, a csernobili reaktor sem rendelkezett biztonsági védőtartály épülettel, konténmenttel. A reaktortípus alapvetően konstrukciós hibával rendelkezett: a víz és a grafit jelenléte miatt alacsony teljesítményen az ún. pozitív üregtényezői hatás következtében labilis volt. Itt a teljesítmény megszaladása könnyen bekövetkezhetett, ezért a reaktort tilos volt alacsony teljesítményen üzemeltetni. Ezen felül a grafit moderátor jelenléte fokozott tűzveszélyt is jelentett. A nagyon súlyos baleset fő oka az említett konstrukciós hiba volt mely rendkívül súlyos és felelőtlen emberi hibával párosult. A baleset időrendi eseményeit röviden az alábbiakban foglalhatjuk össze:

1986. április 25-én a reaktor karbantartási szünetének kezdete előtt nem nukleáris képzettségű, külső szakemberek egy ún. turbina kifutási kísérletet kívántak megismételni. A lecsökkentett teljesítményen végzett kísérletben arra kerestek választ, hogy turbina lekapcsolást eredményező kisebb üzemzavar esetén a generátor saját tehetetlenségénél fogva még mennyi ideig forog olyan sebességgel, melyhez tartozó generált elektromos energia még meghajtja a fő keringtető szivattyúkat, a tartalék áramforrást biztosító dízel generátorok beindulása előtt. A kísérlet megkezdésére késő estig várniuk kellet, de már addig is szabálytalanul kikapcsolták a zóna vészhűtő rendszert beindító automatikát.

Éjjel 11 óra körül hozzákezdtek a kísérlethez, melynek első lépése keretében megkezdték a teljesítmény csökkentését. Sajnos azonban a teljesítmény csökkentést nem jól vezérelték, ezért a csökkentett, de még biztonságos teljesítmény alá került a reaktor teljesítménye. Ekkor a reaktort azonnal le kellett volna állítani, de az automatikát itt is kikapcsolták és megpróbálták a szabályozó rudak fölhúzásával a teljesítményt feljebb tornázni. Ez azonban a közismert „jódgödör” effektus (a reaktorban felhalmozódott jód és egyéb izotópok neutron elnyelése miatt kezdetben nehéz a teljesítményt növelni) miatt nem sikerült. Ezért az összes szabályozó rudat teljesen kihúzták a reaktorból és még a hűtővíz átáramlási sebességét is lecsökkentették.

1 óra 23 perckor elkezdték a kifutási kísérletet és az egyik turbinát lekapcsolták, ennek eredményeként lassan csökkent az átáramoltatott hűtővíz mennyisége és a reaktor – mivel a labilis állapotban üzemelt – néhány másodperc alatt megszaladt. Az operátor észlelve a veszélyt vészleállítást kísérelt meg, de a lefelé haladó szabályozó rudak már nem tudtak belépni a zónába a megolvadt elgörbült szerkezetek következtében. Igen rövid idő alatt 3000 MW hőteljesítmény helyett 100-szor akkora, vagyis 300 000 MW hőteljesítmény szabadult föl, mely hatalmas hőimpulzus pillanatok alatt elforralta a hűtővizet és a gőzrobbanás szétvetette a reaktort. Az izzó cirkónium, acél, beton és grafit a vízből hidrogént és szén-monoxidot fejlesztett és a második, gázrobbanás tovább rombolta a reaktort és a grafit meggyulladását okozta. A robbanások letépték a reaktor fedelét, elvitték az épület sarkát és a kiszabaduló radioaktív gázok, gőzök, valamint a grafit égésével levegőbe porlasztott illékony

szilárd radioaktív anyagok közvetlenül a környezetbe kerültek. Egy részük a közelbe hullott ki, de a finomabb radioaktív por és a légnemű anyagok nagy távolságba és magasságba is eljutottak.

Óriási emberáldozat és hősiesség árán a kisebb tüzeket hamar, a grafit tüzet kb. 1 hét alatt oltották el. Ezután a reaktor alaplemezén lévő izzó összeolvadt „láva" alá egy második vastagabb és hűthető vasbeton lemezt építettek, hogy az ún. „Kína szindróma" esetleges bekövetkezését megakadályozzák. Ezt követően egy vasbeton szerkezettel (szarkofággal) borították be a sérült reaktort. Ennek jelentős kockázati tényezője, hogy a megépített szarkofág a még épen maradt, de jelentős hő- és sugárdózist szenvedett épületszerkezetekre támaszkodik. A 2. a, b ábrákon a sérült reaktor, a reaktor épület épen maradt részére támaszkodó megépített szarkofág látható.

a)

b)

2. ábra a) A sérült reaktor, b) az épület épen maradt részére támaszkodó megépített szarkofág (a szerzők összeállítása a [4, 5] irodalom alapján)

A reaktort övező 30 kilométeres körzet a kihullás következtében jelentősen elszennyeződött, ebből a zónából 135 000 embert kellett kiköltöztetni. A radioaktív porfelhő Európa majd minden országába eljutott és több-kevesebb kihullás, vagy kimosódás révén jelentős területeket szennyezett el. A kezdeti nagyobb aktivitásokban a rövidebb élettartamú jód, tellúr izotópok, néhány év elteltével a hosszabb élettartamú cézium és stroncium izotópok domináltak.

A zónaösszetételt és a kikerült radioaktív izotópok mennyiségét, a 10 nap alatti napi jódkibocsátásokat és a csernobili baleset bekövetkeztéig a környezetbe kikerült radioaktivitás mennyiségét mutatják a következő 1. és 2. táblázatok [6]. Az 3. táblázatban pedig a környezetbe került becsült radioaktív kibocsátások mennyiségi összehasonlítását mutatjuk be.

Zónaösszetétel 1986 április 26-án			teljes kibocsátás a baleset során	
Radionuklid	felezési idő	aktivitás (PBq)	a kikerült izotóp (%)	aktivitás (PBq)
^{33}Xe	5.3 d	6 500	100	6500
^{131}I	8.0 d	3 200	50 - 60	~1760
^{134}Cs	2.0 y	180	20 - 40	~54
^{137}Cs	30.0 y	280	20 - 40	~85
^{132}Te	78.0 h	2 700	25 - 60	~1150
^{89}Sr	52.0 d	2 300	4 - 6	~115
^{90}Sr	28.0 y	200	4 - 6	~10
^{140}Ba	12.8 d	4 800	4 - 6	~240
^{95}Zr	1.4 h	5 600	3.5	196
^{99}Mo	67.0 h	4 800	>3.5	>168
^{103}Ru	39.6 d	4 800	>3.5	>168
^{106}Ru	1.0 y	2 100	>3.5	>73
^{141}Ce	33.0 d	5 600	3.5	196
^{144}Ce	285.0 d	3 300	3.5	~116
^{239}Np	2.4 d	27 000	3.5	~95
^{238}Pu	86.0 y	1	3.5	0.035
^{239}Pu	24 400.0 y	0.85	3.5	0.03
^{240}Pu	6 580.0 y	1.2	3.5	0.042
^{241}Pu	13.2 y	170	3.5	~6
^{242}Cm	163.0 d	26	3.5	~0.9

1.táblázat A zónaösszetétel és a csernobili baleset során és a környezetbe került radioaktivitás (PBq és a készlet %-a) (a szerzők készítették a [6] irodalom alapján)

^{131}I izotóp napi kibocsátása

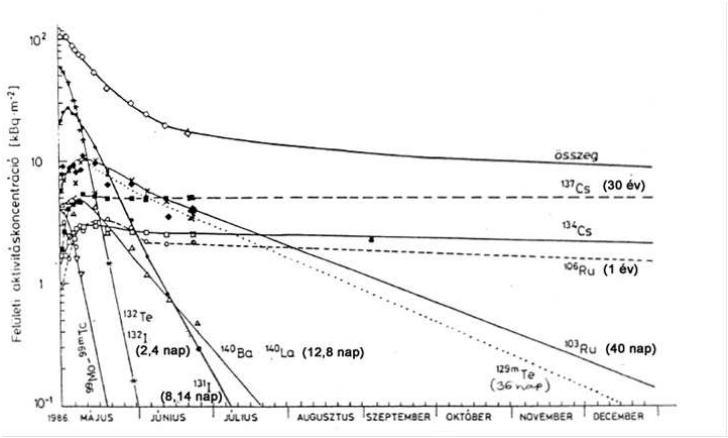
kibocsátás napja	napi kibocsátás (PBq)
április 26	704
április 27	204
április 28	150
április 29	102
április 30	69
május 1	62
május 2	102
május 3	107
május 4	130
május 5	130
összesen	1760

2.táblázat A környezetbe került jód 131-es izotóp kibocsátások időfüggése (PBq) (a szerzők készítették a [6] irodalom alapján)

Forrás	Ország	időpont	radioaktivitás (Bq)	fontos izotópok
Hiroshima-Nagaszaki	Japán	1945	$4x10^{16}$	hasadási termékek, aktinidák
Légköri atomrobbantások	USA-SzU	1963	$2x10^{20}$	hasadási termékek, aktinidák
Windscale	UK	1957	$1x10^{15}$	^{131}I
Cseljabinszk-Kisztim	SzU	1957	$8x10^{16}$	hasadási termékek, ^{90}Sr, ^{137}Cs
Three Mile Island	USA	1979	$1x10^{12}$	nemesgázok, ^{131}I
Csernobil	SzU	1986	$2x10^{18}$	^{131}I, ^{131}Cs

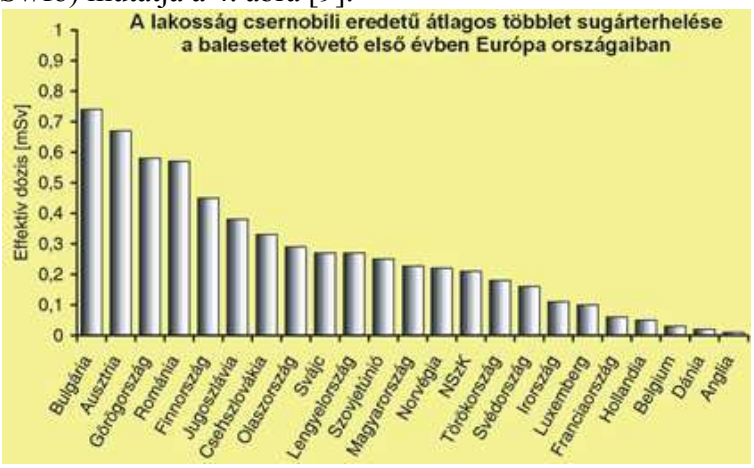
3.táblázat A környezetbe került radioaktív kibocsátások mennyiségi összehasonlítása (Bq)

A csernobili atomerőművi baleset kibocsátása hatással volt hazánkra is. A következő, 3. ábrán a baleset idején egy budapesti füves futballpálya talajfelszíni radioaktív szennyezettségét mutatja, az egyes komponensekre 1986. december 31-ig extrapolált értékekkel [7].



3. ábra A baleset idején budapesti füves futballpálya talajfelszíni radioaktív szennyezettsége, az egyes komponensekre 1986. december 31-ig, extrapolált értékekkel (kBq/m^2) [7]

Az ország lakossága által elszenvedett effektív többlet dózis 1986-ban az éves dózis mintegy 10-30%-a volt. Az európai országok lakosságát a baleset következtében ért többlet effektív dózist (mSv/fő) mutatja a 4. ábra [9].



4. ábra Európa lakosságának többlet sugárterhelése [9]

Azóta a sérült szarkofágot 2016-ban egy új biztonságosabb szarkofággal fedték be (5. ábra).

5. ábra Az új csernobili szarkofág [16]

A baleset következményei

- 50 tűzoltó és mentőszemélyzet, akit rövid időn belül sugárbetegségben haltak meg, 135 000 embert kitelepítettek az erőmű 30 km-es körzetéből
- A későbbiek során 9 gyermek pajzsmirigyrákban halt meg

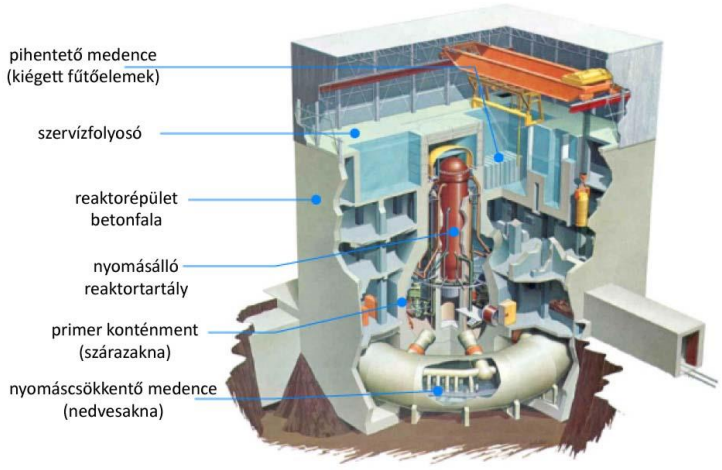
- 3940 ember halálát tételezik fel a jövőben a legszennyezettebb területeken a lineáris küszöbdózis hiányát feltételező elmélet szerint
- Összesen így megközelítőleg 4000 halálesettel számolnak

Összességében elmondható, hogy a baleset nem következett volna be abban az esetben, ha:

- tervezési hiba miatt nem építenek pozitív üregtényezővel rendelkező éghető grafitot tartalmazó vízhűtésű nagy erőművi reaktort;
- tervezési hiba miatt nem alkalmaznak a szabályozó rudak alján moderátort;
- ha emberi hiba következtében nem sértik meg többszörösen az alapvető biztonsági szabályokat

A FUKUSHIMA- ATOMERŐMŰVI BALESET (2011, JAPÁN)

A Fukushima Daiichi-ben (Japán) üzemelő reaktorok General Electric típusú forralóvizes reaktorok (BWR) voltak [5] és a 60-as években a Toshiba és a Hitachi cégek létesítették Mark I típusú konténmentekkel. Az 1.-3. blokkokat 1971-75 között üzemelték be, az 1. blokk 460 MW, a 2.-5. blokkok 784 MW, a 6. blokk pedig 1100 MW elektromos teljesítményű volt. Leállás esetén 40 perc múlva a maradékhő éréke a termikus teljesítmény ~1,5 %-a, azaz az 1. blokk esetén ez 22 MW, a 2.-3. blokkoknál 133 MW hőteljesítményt jelentett. Hűtés nélkül ez a nyomás alatti térben többlet elgőzölést okozhatott, melyet a szárazaknának nevezett primer konténmentbe (PCV) engednek át ilyenkor biztonsági szelepek segítségével. A reaktor sémája a 6. ábrán látható.



6. ábra A Fukushima Daiichi BWR reaktorok sémája [10]

A Daiichi telephelyen a 60-as évek elején épült forralóvizes reaktorokhoz tervezett cunami hullám védmű magassága először 3,1m volt, így a blokkokat 10m-rel a tengerszint fölé építették és a vízkivételi szivattyúk 4 méterrel a tengerszint alatt szívták a vizet. 2002-ben a tervező hullám magasságot 5,7 méterrel tervezték és ilyen gát épült. 1993-as szakértések már számoltak 14 m fölötti hullámmal is, de ennek tudatában sem tettek megelőző intézkedéseket, a diesel generátorok magasabbra helyezését és az épületek alsó részeinek vízszigetelését.

A baleset [10] lefolyása:

2011. március 11-én 2 óra 46 perckor a Japán Honshu sziget keleti oldalán a Richter skála szerinti 9-es erősségű földrengés keletkezett, melynek epicentruma 130 km-re volt Sendai városától 11 km-es mélységben. Ez volt Japán eddigi legerősebb és a világ ötödik legerősebb földrengése. A földrengés 3 percig tartott és a ritka dupla rengések csoportjába tartozott. A rengés során a tengerfenék egy része megközelítőleg 10-20 métert mozdult függőleges

irányban, Japán e szigete néhány méterre kelet felé mozdult el és a helyi tengerpart 0,5 métert süllyedt. A rengés után keletkező tengerár (cunami) 560 km^2 szárazföldet árasztott el és 19 000 ember halálát okozta. Több mint 1 millió épület sérült, vagy semmisült meg.

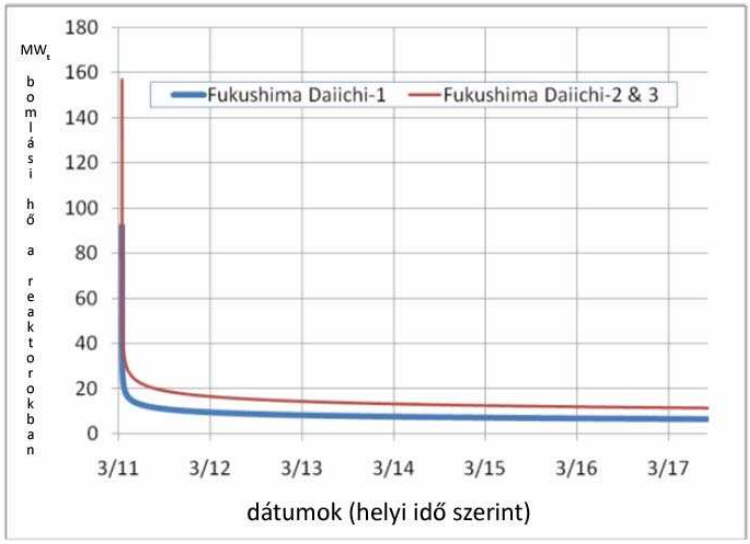
A térségben található 11 atomerőművi blokk közül az éppen üzemben lévők (Fukushima Daiichi 1,2,3, Fukushima Daini 1,2,3,4, Tohoku Onagawa 1,2,3, Japco Tokai 1) mindegyike a földrengés észlelésekor azonnal automatikusan leállt. A földrengés egyik reaktorban sem okozott észlelhető károsodást. A reaktorok mindegyike földrengésálló volt de cunamival szemben sérülékenyek voltak. A 11 blokkból az események után 8 esetén külső hálózatról, vagy tartalék dízelgenerátorokról üzemeltethető maradékhő elvonó rendszer állt rendelkezésre és lehűtve a reaktorokat megakadályozta a zónaolvadást.

A maradék 3 korábban üzemelt és azonnal leállt blokk a Daiichi telephelyen lévő 1,2,3 blokkok a földrengést 1 óra múlva követő 15 méter magas cunami következtében 3 óra 42 perckor elvesztették a maradékhő elvonó rendszerüket, mert a 13 tartalék generátor közül 12 tönkrement és a tengervizes hűtésű hőcserélő rendszerek is megsemmisültek (7-8. ábrák).

7. ábra A 6 m magas védőfalon átbukó cunami hullám 5m magasan mindent elpusztított [11]

8. ábra A Fukushima Daiichi 1.- 4. blokkjai a cunami előtt és után [11]

Ennek következtében az 1,2,3 blokkok és a hideg 4 blokkban lévő a reaktorból frissen kiemelt fűtőelemeket tároló lévő medence maradékhő elvonás nélkül maradt. A maradékhő számított értékeit mutatja a reaktorblokkokra a következő 9. ábra [8].



9. ábra A Fukushima Daiichi 1.-3. blokkok számított maradékhő értékei 2011. március 11.-17. között [12]

A földrengés és a cunami következtében 3 erőművi alkalmazott halt meg, de a radioaktív sugárzás következtében senki.

A földrengést több száz utórengés követte, köztük egy 7,1-es erősségű is, de további károk nem keletkeztek. A földrengés után, a blokkok leálltak és a teljes telepre megszűnt a külső áramellátás, így bekapcsoltak a turbina épületek alagsoraiban elhelyezett tartalék dízelgenerátorok.

41 perc múlva 3 óra 42 perckor megérkezett az első, majd 8 perc múlva a második cunami hullám. A 15 méteres cunami hullám következtében a turbina csarnokok, ahol a dízel generátorok is elhelyezkedtek 5 méteres víz alá kerültek, a teljes maradékhő elvonó rendszerük megsemmisült, egyedül egy léghűtésű generátor maradt üzemképes, mely az 5. és 6. blokkokat látta el árammal. Az 1. és 2. blokkot ellátó akkumulátorok is tönkrementek, a 3. blokk akkumulátorai pedig 30 óráig adtak áramot. Este 7 óra 3 perckor nukleáris veszélyhelyzetet hirdettek, 8 óra 50 perckor elrendelték a 2 km sugarú körön belüli lakosság kitelepítését, melyet 9 óra 23 perckor 3km-re, hajnali 5 óra 44 perckor pedig 10km-re terjesztettek ki. Még aznap a zónát 20 km-re bővítették.

A baleset során a növekvő nyomású gőzt a reaktorok alatti elnyelető térbe, a nedves aknába (wetwell) engedték és később bekapcsoltak a zóna vészhűtő (ECCS) rendszerek is. Áramellátás hiányában ezek a hűtő rendszerek 3 nap alatt folyamatosan megszűntek üzemelni és szombat után külső tűzoltó fecskendőkkel, tengervízzel hűtötték a nyomásálló teret, de ehhez le kellett csökkenteni a bennük lévő nyomást, a gőznek az elnyeletőbe történő lefúvatásával. Az elfolyó hűtővizet hűtötték és recirkuláltatták.

Az 1. blokkban már a nyomásnövekedés után 4,5 órával a fűtőelem kötegek szárazra kerültek, hőmérsékletük elérte a 2800 ^{0}C értéket és a központi mag kezdett megolvadni és később a kötegek felső része az alul lévő vízbe zuhant. Ezután a hőmérséklet csökkent. A nyomásnövekedés miatt a konténmentet igyekeztek lefúvatni, főleg kézi vezérléssel, ennek sikertelensége miatt a reaktor épülete károsodott. A távozó gőz radioaktív nemesgázokat, jódot és aeroszolokat tartalmazott, hidrogén gázzal keverve és szombaton délután 3 óra 36 perckor a reaktor konténment feletti szervizfolyosón hidrogénrobbanás történt letépve az

épület fedelét és megrongálva a reaktor felső részét. A hidrogén a fűtőelemek cirkónium burkolatának a magas hőmérsékletű vízgőzzel történő reakciójában keletkezett. A sérült aktív zóna feltételezések szerint a nyomásálló tér aljára került, de később kiderült, hogy átolvasztva a reaktortartály fenekét 65 cm mélyen behatolt az alatta levő 2,6 m vastag beton lemezbe, majd hűlés közben megszilárdult és a szárazakna nem sérült.

A 2. blokkban 2011. március 14-én megszűnt a gőzinjektoros vízhűtés és csak 6 óra múlva kezdték hűteni tűzoltó fecskendőkkel a reaktort. Így a töltet szárazra került, felső része megolvadt és az alul lévő vízbe zuhant. A növekvő nyomás miatt lefúvatást végeztek többször is a hidrogénrobbanás elkerülésére. 15-én mégis, valószínűleg hidrogénrobbanás következtében a nedvesakna elnyeletű valószínűleg felhasadt és lecsökkent a másodlagos konténmentben (szárazakna, drywell) a nyomás. Valószínűleg a sérült három blokk közül innen juthatott ki a környezetbe a radioaktivitás döntő része.

A 3. blokkban 2011. március 12-én megszűnt a maradékhő elvonás és a zóna vészhűtő rendszer nagynyomású egysége sem működött, a fűtőelemek körül csökkent a vízszint. A megnövekedett gőznyomást az elnyeletű térbe (nedves akna) fúvatták és tűzoltó fecskendőkkel, tengervízzel hűtötték a reaktort. Az előző blokkokhoz hasonlóan itt is megolvadt a fűtőelem kötegek egy része, olvadt felső részük az alul lévő vízbe zuhant és részben átégethették a tartály falát, elérve az alatta lévő betont. 14-én a lefúvatott illékony elegy egy része visszajuthatott a felül lévő szervizfolyosóba és hatalmas hidrogéngáz robbanás következett be és a 2 blokkhoz hasonlóan roncsolta a reaktorépület felső részét, radioaktív részecskéket szórva szét a telephelyen.

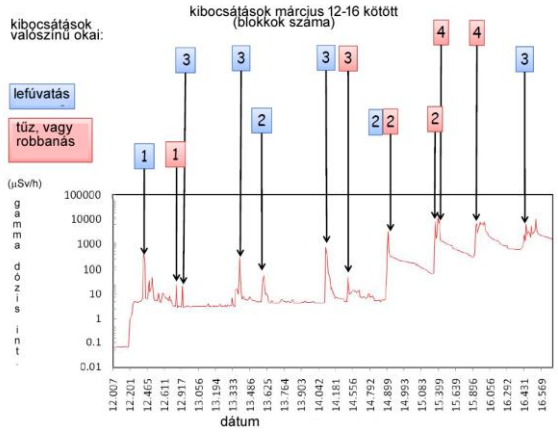
A 4. blokkban 2011. március 15-én hidrogénrobbanás következett be, valószínűleg a 3. blokkban keletkezett és a lefúvatás során a szellőzőn keresztül az épületbe jutott hidrogéngáz robbant fel.

2012-es év elejére a reaktorterekben a hőmérséklet 27-54 ^{0}C értékekre csökkent le. Az összes blokk külső áramforrásból történő energiaellátását 2012. március végére oldották meg. 2016 márciusára a három blokk maradékhő teljesítményének összege 1 MW-ra esett.

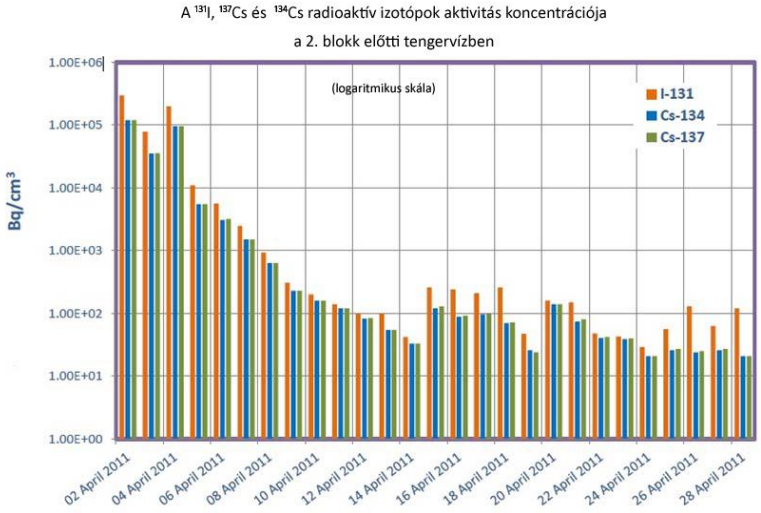
A sérült három blokk mellett komoly problémát jelentett a 4. blokk frissen kirakott (548 db), és a blokk tetején elhelyezett pihentető medencében lévő hőtermelő fűtőelem kötegek hűtése. A folyamatos hűtés megszűnése után a medence vizének egy része elpárolgott, de a kötegek még így is víz alatt maradtak. A blokkban történt hidrogén robbanás után is sikerült elkerülni a kötegek megolvadását.

Az 1.-3. blokkok tengervízzel történő hűtése során a hűtővíz mintegy 40 %-a elpárolgott. A reaktorokból kifolyt radioaktív hűtővíz egy része a tengerbe jutott. A radioakivitás kibocsátási csúcsa 15-én volt, döntően a 2. blokkból. A kibocsátott radioaktív nuklidok zöme ^{131}I és ^{137}Cs, ^{134}Cs volt. A^{131}I-ekvivalens értékben ($A_{I\text{-}131}+A_{Cs\text{-}137}*40$) kibocsátott aktivitás becsült értéke 570 PBq volt, ez~10%-a volt a csernobili baleset során kibocsátott 5200 PBq ^{131}I-ekvivalens kibocsátott radioaktivitásnak. A blokkonkénti levegőbe történő kibocsátást és a tengervíz, valamint a prefektúrában[1] lévő talaj radioaktivitását mutatja a következő három 10., 11., 12. ábra.

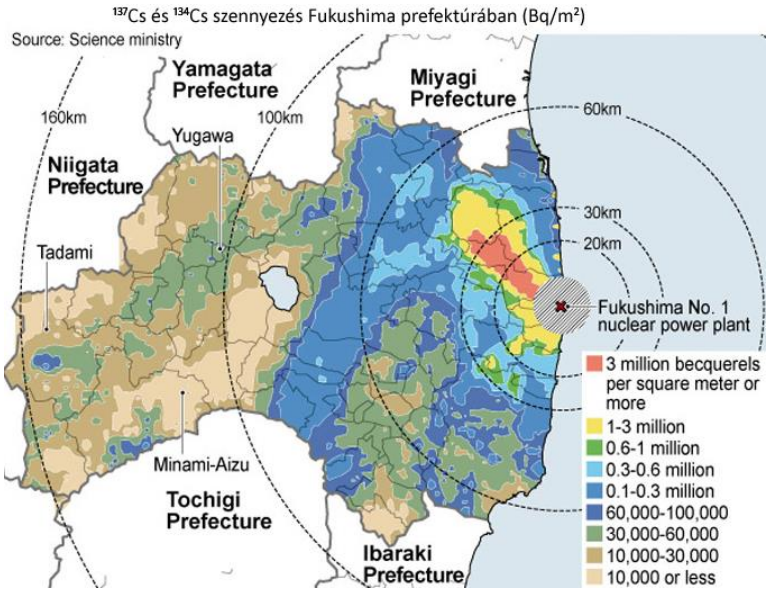
[1] prefektúra: közigazgatási egység



10. ábra Radioaktivitás kibocsátások következtében mért dózisintenzitások az 1.-4. blokkokból 2011. március 12.-16. között (μSv/h) [12]

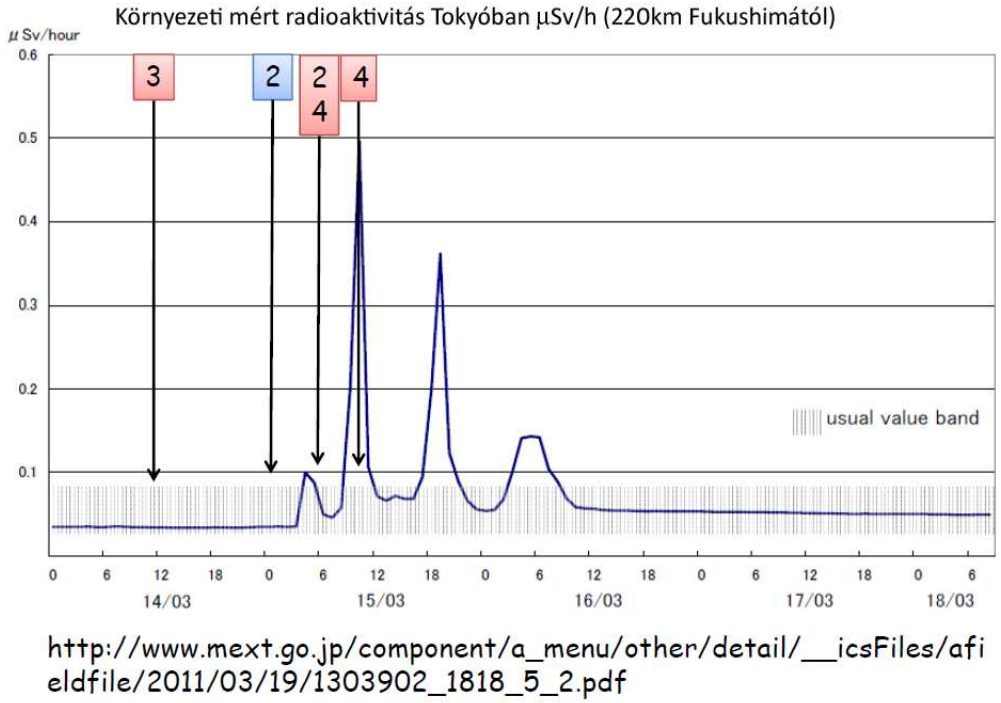


11. ábra Radioaktív jód és cézium aktivitás koncentrációk (Bq/cm3) a tengervízben a 2. blokk előtt [13]



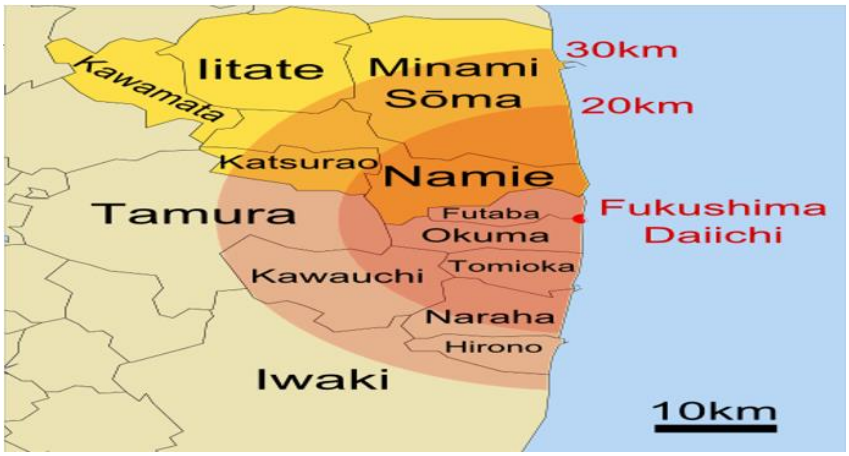
12. ábra A talaj radioaktív cézium szennyezettsége Fukushima prefektúrában [14]

A Fukushima Daiichi teleptől 220 km-re fekvő fővárosban, Tokióban mért környezeti dózisintenzitásokat mutatja a következő 13. ábra.



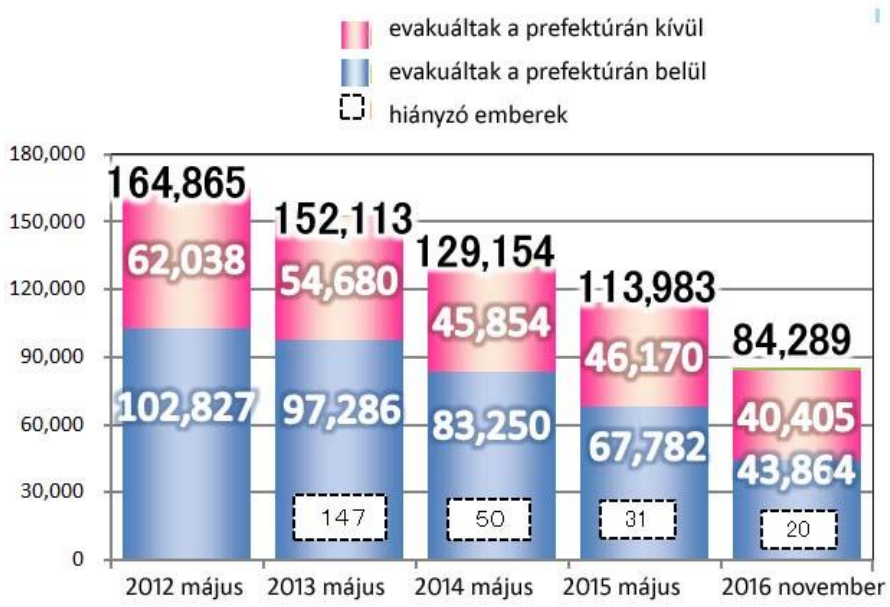
13. ábra A 2, 3 és 4. blokkok kibocsátásai alapján mért környezeti mért dózisintenzitások Tokióban [12]

A reaktor környezetéből a lakosság kitelepítését több lépcsőben végezték. A baleset napján 134 000 embert telepítettek ki az erőmű 3-20 km-es körzetéből, majd 4 nappal később a 20-30 km közötti lakosokat, további 354 000 embert is kitelepítettek. A zónákat mutatja a következő 14. ábra.



14. ábra A kitelepítési zónák [14]

A 20 km és 30 km zónák közti területre egy 20 mSv/év dózisintenztási korlátot állítottak fel és ez az érték volt a visszaköltöztetés küszöbértéke is. A 20-50 mSv/év dózisintenzitású területekre tilos volt visszaköltözni és dekontaminálási tevékenységekkel, igyekeztek csökkenteni a szennyezettséget. A cunami a területen működő 24 mérőállomásból 23-at tönkretett. A kitelepítettek arányát és visszaköltöztetését foglalja össze a következő 15. ábra.



15. ábra A kitelepítettek száma 2012. május – 2016. november között [14]

A baleset következményei:

- erős földrengés után 15 méteres cunami szökőár tönkretette a maradékhő hűtést 3 reaktornál
- 3 BWR reaktor és 4 pihentető medence sérült, 4 reaktor végleg kiesett az energiatermelésből
- 3 reaktor 30-70 %-os zónasérülést szenvedett (fűtőelemek, reaktortartály primer konténment)
- legalább 4 hidrogénrobbanás következett be, valószínűleg tűz volt több pihentető medencénél is
- a 3 reaktort július végére lehűtötték és december közepére hideg leállítás helyzetbe hozták
- a tengerbe hosszabb ideig szivárgott radioaktív hűtővíz
- az erőmű területe radioaktív hasadási termékekkel szennyeződött
- 20 km sugarú szennyezett zóna keletkezett
- a baleset INES minősítése 7, mert a 4.-5. napok között jelentős radioaktív izotóp kibocsátás történt, melynek becsült értéke 570 PBq 131I-ekvivalens aktivitás volt
- az erőművi balesetnek nem volt sugárzás okozta halottja, 165 000 embert telepítettek ki, ezek közül 84 000 már visszatérhetett
- a kitelepítések következtében több mint 1000 (főként idős) ember halt meg.

Összességében megállapítható, hogy a baleset nem következett volna be, ha az 1993-as szakértői jelentések alapján magasabb cunami gátat emeltek volna és a diesel generátorok magasabbra helyezésével és az épületek alsó részeinek vízszigetelésével megelőzték volna a cunami romboló hatását.

KÖVETKEZTETÉSEK

Az elmúlt évek négy legsúlyosabb atomerőművi baleseteinek rövid értékelése alapján a következő általános következtetéseket vontuk le:

- Négy komoly atomerőmű balesetet tekintettünk át, mind a négy esetben tűz és három esetben robbanás is bekövetkezett az atomerőművi blokkokban és zónasérülés, valamint reaktor szerkezeti sérülés lépett fel.
- A két legsúlyosabb balesetet (Csernobil és Fukushima) az INES skálán 7-es, a TMI balesetet 5-ös kategóriába sorolták. Mindegyik baleset során radioaktív anyagok kerültek ki a reaktorokból a környezetbe és szennyeztek el kisebb nagyobb területeket.
- A legsúlyosabb radioaktív kibocsátással és következménnyel a csernobili baleset járt, a baleset következtében bekövetkezett közvetlen halálesetek száma 50-100 közé tehető, a baleset késői hatásaként várható halálesetek becsült száma 4000 fő.
- A két, komoly lakossági kitelepítéssel járó baleset stressz hatások következtében bekövetkezett haláleseteit Csernobil és Fukushima esetén is 1000-2000-re becsülik.
- Ugyanakkor a nukleáris baleset következtében nem volt haláleset sem a windscale-i, sem a Three Mile Island-i, sem a fukushimai események során.
- Megállapítható, hogy a TMI és a fuksuhimai atomerőművi baleset elkerülhető, illetve enyhíthető lett volna, ha a jelenlévő személyzet időben pontos információhoz jutott volna a reaktorokban lévő hűtővíz pontos mennyiségéről és a zónaolvadások következtében létrejött olvadt aktív zóna pontos térbeli elhelyezkedéséről. Erre amerikai kutatók [15] a gyors neutronok és a gammasugárzás mérésén alapuló roncsolásmentes, ún. „hodoszkópos” szintmérést illetve anyageloszlás mérést javasoltak. Sajnos ez a hiányosság már a TMI baleset értékelésénél kiderült, de nem került be a reaktorbiztonsági műszaki követelmények közé, így Fukushimában is a személyzet „sötétben tapogatózott”.
- Az utóbbi három súlyos atomerőművi baleset elsődleges oka konstrukciós hibaként jelölhető meg, azaz a TMI esetben a fennakadásra hajlamos lefúvató szelep hibáját már a Davis-Besse eset után ki kellett volna küszöbölni, Csernobilban nem lett volna szabad egy alapvetően kis teljesítményen labilis nagy erőművi reaktort megépíteni és Fukushimában a tengerparti erőművek esetén a vészhűtő rendszerek összes elemét tengerár számára elérhetetlen helyen kellett volna elhelyezni.
- Az utóbbi három baleset során természetesen operátori és más emberi hibák is közrejátszottak, de a konstrukciós hibák hiányában nem következtek volna be még ekkor sem súlyos balesetek.
- A balesetet szenvedett 2. generációs atomerőműveket felváltó 3. és 3+ generációk esetén az említett tanulságokat beépítették a tervezésbe és megvalósításba, figyelembe véve a mélységi védelem, a védelmi gátak rendszere, a kis valószínűségű többszörös hibák halmozott hatása és a rendszerekben természeténél fogva jelenlévő (inherens) tulajdonságok elveinek felhasználását.

FELHASZNÁLT IRODALOM

[1] DOBOR J.; KOSSA GY.; PÁTZAY GY., Atomerőművi balesetek és üzemzavarok tanulságai 1. (Nuclear Power Plant Accidents and Malfunctions, Lessons Learned 1.), Hadmérnök, XII. Évfolyam 1. szám, 2017. március, 58-71

[2] http://ncbj.edu.pl/rbmk-reaktor-z-czarnobyla/budowa-reaktora-rbmk (letöltve: 2016.06.29.)

[3] http://insp.pnnl.gov/-reports-status-2001status_rpt-statrpt2001_appa.node.htm (letöltve: 2016.06.29.)

[4] https://www.nbcnews.com/news/world/chernobyl-anniversary-ukraine-holds-fast-nuclear-energy-despite-disaster-n554036 (letöltve: 2016.06.29.)

[5] http://m.futurist.ru/articles/930-zapovednaya-zona-otchuzhdeniya-kak-zhivet-pripyaty-cherez-30-let-posle-katastrofi (letöltve: 2016.06.29.)

[6] https://www.oecd-nea.org/rp/chernobyl/c02.html (letöltve: 2016.06.29.)

[7] BÍRÓ T., FEHÉR I., SZTANYIK B. L.Ó: *A csernobili atomerőmű baleset sugárzási következménye Magyarországon,* Energia és Atomtechnika, XI. évf. 4. szám,145-155

[8] *William D'haeseleer Nuclear Safety*, 9a. safety_BNEN intro_2012-13.ppt (letöltve: 2016.06.29.)

[9] *Sugárözönben élünk, a környezeti radioaktivitás összetevői*, https://www.google.hu/search?client=opera&q=sug%C3%A1r%C3%B6z%C3%B6nben+%C3%A9l%C3%BCnk+a+k%C3%B6rnyezeti&sourceid=opera&ie=UTF-8&oe=UTF-8 (letöltve: 2017. 01. 06.)

[10] *Fukushima Accident World Nuclear Association.pdf,* (Updated November 2016), (letöltve: 2017. 01. 06.)

[11] M. RAGHEB, FUKUSHIMA EARTHQUAKE AND TSUNAMI STATION BLACKOUT ACCIDENT, http://mragheb.com/NPRE%20402%20ME%20405%20Nuclear%20Power%20Engineering/Fukushima%20Earthquake%20and%20Tsunami%20Station%20Blackout%20Accident.pdf (letöltve: 2017. 01. 06.)

[12] JOSEPH E SHEPHERD, *The Crisis at Fukushima Dai-ichi Nuclear Power Plant* Aerospace and Mechanical Engineering California Institute of Technology Pasadena, CA, (letöltve: 2017. 01. 06.)

[13] FEHÉR Á. *Mi történt Fukushimában* http://www.sugarvedelem.hu/sugarvedelem/docs/kulonsz/2011sv/szekcio5/fukushima_helyzet.pdf, (letöltve: 2017. 01. 06.)

[14] *Transition of evacuation instruction zones*, http://www.pref.fukushima.lg.jp/site/portal-english/en03-08.html http://www.pref.fukushima.lg.jp/site/portal-english/(letöltve: 2017. 01. 06.)

[15] A.DEVOLPI, *Nuclear Reactor Safety: Lessons from Three mile Island and Fukushima*, Federation of American Scientists Public Interest Report, 2012 summer edition, Summer2012_NuclearPowerSafety-deVolpi.pdf, (letöltve: 2014. november 05.)

[16] http://chnpp.gov.ua/uk/ (letöltve: 2017. 01. 06.)

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

LES TACHES DES ORGANISATIONS BENEVOLES DE DÉFENSE CIVILE EN COURS D'ÉVACUATION ET DE RÉCEPTION

TASKS OF VOLUNTARY CIVIL DEFENSE ORGANIZATIONS IN THE IMPLEMENTATION OF DEPORTATION AND RECEPTION

ENDRŐDI ISTVÁN; PLÉBÁN J. KRISTÓF

(ORCID: 0000-0002-3376-1389); (ORCID: 0000-0003-3194-3565)

Endrodi.Istvan@uni-nke.hu; kristofjp@gmail.com

Absztrakt

Dans le domaine des dommages, les organisations de sauvetage disposent d'équipements spéciaux, de ressources humaines qualifiées et de capacités logistiques dans la répartition des responsabilités entre les organisations coopérantes et contributives, les unités administratives, les forces professionnelles et volontaires de l'État.
Le libellé de la réponse efficace aux défis de la création de la sécurité et de la mise en œuvre des tâches de protection civile dans un environnement social en constante évolution exige que les organisations bénévoles continuent de maintenir et de développer les qualifications, ce qui devrait se traduire par la formation, la formation continue, les pratiques de coopération et dans la conception du concept d'utilisation d'appareils techniques.
Dans cette publication, l'auteur examine les domaines possibles du rôle des organisations bénévoles de sauvetage dans le système d'évacuation et d'inclusion, les antécédents réglementaires juridiques qui les soutiennent et la structure de la préparation à l'exécution des tâches et les possibilités de financement durable.

Mots de clé: *protection civile volontaire, formation, exercices, délocalisation*

Abstract

In the field of damage, the rescue organizations have their special equipment, skilled human resources and logistics capabilities in the division of duties between the cooperating and contributing organizations, the administrative units, the state professional and voluntary forces.
The formulation of effective remedial response to the challenges of security creation, the implementation of civil protection tasks in a constantly changing social environment, the need for continuous capacity upgrading and qualification of volunteer organizations, which should be reflected in the training, further training, cooperation practices and in the design of the concept of using technical devices.
In this publication, the author examines the possible areas of the role of volunteer rescue organizations in the evacuation and inclusion system, the legal regulatory background supporting them, and the structure of the preparation for the task execution and the possibilities for sustainable financing.

Keywords: *voluntary civil protection, training, exercises, relocation-reception*

A kézirat benyújtásának dátuma (Date of the submission): 2017.08.31.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.09.04.

CONTEXTE JURIDIQUE REGLEMENTAIRE

Contexte législatif de la protection de la population

La protection de la population est la tâche fondamentale de la protection civile, dont le but est de protéger la vie des citoyens et d'assurer les conditions de survie. Le cadre juridique pour la mise en œuvre de cette tâche est assuré par les lois et les règlements d'application. À l'article 52 de la Loi CXXVIII de 2011 sur la protection contre les catastrophes et les activités connexes [1] (ci-après dénommée la « Loi sur la réponse aux catastrophes »), elle définit les tâches de la protection civile liées à la prévention des catastrophes, et l'évacuation, l'enlèvement et la réception de la population, dont le règlement d'application apparaît dans le chapitre VII de 234/2011 (XI.10) Décret Gouvernemental (ci-après : décret gouvernemental) [2]. Le décret gouvernemental exige l'application de la méthode de protection de la population locale et longitudinale, les règles d'alerte et les informations d'urgence, les tâches connexes et les responsabilités des responsables de l'évacuation, de l'expulsion, de l'accueil et de la réintroduction.

Le Ministère de l'Intérieur Décret 62/2011 sur certaines règles en matière de protection contre les catastrophes (XII.29.) [3] définit dans la chapitre IX la préparation aux catastrophes pour la population, les formes d'information active et passive. Le règlement juridique connexe réglemente la fourniture des tâches de protection civile nécessaires au conflit armé conformément au CXIII de 2011 sur la défense des forces de défense hongroises et les mesures à prendre dans l'ordre juridique [4], la section 11, selon laquelle la tâche d'alerte, d'évacuation et d'accueil requise par les conditions de guerre est affichée conformément aux tâches prescrites dans la Loi sur la protection contre les catastrophes en temps de paix. Le chapitre IV de décret de 290 / 2011(XII.22.) [5] sur la protection des forces de défense hongroises et l'ordre spécial des forces de défense hongroises définit les circonstances et les responsabilités de la population en préparation et remplit les dispositions statutaires de la protection de la population.

Contexte législatif de la performance des organismes bénévoles de sauvetage

La possibilité d'une intervention directe des citoyens en matière d'action corrective est garantie par la loi uniquement dans un cadre coordonné et organisationnel. L'attitude des citoyens actifs envers la sécurité de votre propre et de votre environnement est régie par la portée des organisations de protection civile volontaires, dont le statut juridique, la définition de leurs fonctions et le niveau d'organisation sont régis par la Loi sur la protection contre les catastrophes et son règlement d'application. Conformément à la section 3, point 19 de la Loi sur la protection contre les catastrophes, le rôle des organisations de sauvetage en tant que « personnel civil spécial équipé de moyens techniques spécialisés pour prévenir, éliminer, catastrophe, gestion des catastrophes et organisations civiles volontaires pour sauver la vie humaine » se présents dans le domaine de la défense contre les catastrophes naturelles et civilisée.

Les organisations de sauvetage ont une tâche conformément aux points définis à l'article 52 de la Loi sur la protection contre les catastrophes afin d'assurer la préparation, l'information, l'avertissement, l'alarme et la protection individuelle de la population, la fourniture de dispositifs de protection individuels et la protection collective, locale et longue distance. [1]

La forme de la protection collective de la population, qui implique des ressources humaines plus importantes, des organismes professionnels coopérants, des organismes de bienfaisance contributives et des citoyens et leurs petites communautés, est déterminée par l'ampleur et la portée des dégâts. Dans le domaine de la protection contre la protection locale et la protection de la garde, l'emplacement de la défense est identique à la zone dangereuse ou

vulnérable. En vertu de la législation, en cas de prophylaxie, de risque de catastrophe ou d'urgence, l'effet menaçant et les conséquences attendues, la protection locale s'applique tout d'abord comme moyen de protection de la population. En même temps, en soulignant la primauté de la protection de la vie humaine désignée par la loi, la constatation de László Teknős est correcte, selon laquelle, dans le domaine des dommages où la protection ne peut pas être fournie sur le terrain, la protection des habitants de plusieurs personnes ou des établissements entiers, est la protection de distance. [6]

La commande, l'exécution, les règles et les responsabilités d'expulsion, de réception et de rapatriement dans le domaine de la protection interurbain sont définis dans les chapitres 31 à 35 du décret gouvernemental. [2] L'élimination temporaire de la population et du matériel de subsistance d'une zone vulnérable telle que définie dans le plan d'intervention d'urgence et son logement temporaire sur un site d'accueil est un système de tâches complexe qui nécessite la coopération de toutes les forces d'intervention qui fournissent des capacités de protection locales. Selon la définition de Júlia Hornyacsek, "la capacité de défendre est la totalité des activités, des forces, des dispositifs et des matériaux qui aident à prévenir l'émergence de menaces et, le cas échéant, à remédier au danger et à soutenir le travail des forces professionnelles de sauvetage". [7, 5.o] Les organismes de sauvetage bénévoles participent à l'élaboration de cette capacité de défense avec leurs ressources financières, leur système de gestion, leur préparation et leurs compétences de préparation.

LES TACHES D'INTERVENTION LORS DE L'ENLEVEMENT ET DE LA RECEPTION

Les organisations de sauvetage auront la chance de coopérer à l'évacuation, à l'évacuation et à l'accueil, qui seront coordonnées par le président du comté, la capitale et les comités de défense locaux, dans la mise en œuvre du maire et dans la participation de l'organe local et régional de l'organisation professionnelle de gestion des catastrophes.

Le processus d'expulsion

Les compétences des petites équipes de sauvetage communautaires, généralement formées pour les tâches de prévention des dommages causés par l'eau, sont la connaissance personnelle de la majorité des membres de la communauté résidentielle du règlement, ainsi que la cartographie de l'infrastructure de transport et des solutions de rechange, ainsi que les organismes de sauvetage du comté ayant des compétences en recherche et sauvetage en milieu urbain.

Les tâches administratives, sécurité de la communication

La transmission de l'information peut être faite entre l'agent d'expulsion et la population, sous la forme d'une alerte, sous la forme d'informations ou parmi les groupes impliqués dans le déploiement de la tâche d'expulsion.

Au cours d'une alerte, les activités de soutien des organisations volontaires de protection civile peuvent apparaître dans le lieu normal de publication des alertes de la population, des organisations commerciales et des propriétaires de matériel de transport.

Les organisations de sauvetage peuvent fournir une communication entre les équipes travaillant dans le déploiement d'escortes en déployant un parc d'outils conçu pour la communication de localisation. Ici, nous pouvons désigner des systèmes de communication mobile pour la gestion de groupes de sauvetage volontaires tels qu'un client extérieur mobile, une tour de communication mobile auto-construite, des stations de base IP de 2,4 GHz et 5 GHz ISM ou des radios EDR.

Sur la base de l'enquête sur les données téléchargées dans HELIOS Civil Protection Administration, [8] on peut affirmer que les organisations de protection civile volontaires ne présentent pas de couverture unifiée dans le parc de périphériques de communication, les équipements radio EDR ne sont pas disponibles pour toutes les organisations. Cela affecte à la fois l'échange d'informations sur place, d'une part, et la capacité d'interagir avec les forces professionnelles en utilisant le système EDR.

Les tâches administratives

L'organisation volontaire de protection civile peut prendre part à la gestion de la population déportée, en fonction de la préparation logistique et des ressources humaines de son personnel.

Les tâches de livraison

Les organisations de sauvetage peuvent interférer avec le transport de la population au moyen d'une seringue anti-incendie ou d'une capacité de transport de véhicules, du matériel, des biens culturels, du bétail, de l'alimentation et d'autres matériels transportant des fournitures et de la capacité de la remorque à transporter le matériel.

Sur la base de l'examen de la capacité des organisations de protection civile volontaires, la répartition suivante peut être mesurée :

Dans le cas de 81 équipes de sauvetage, 24 organisations ont une voiture ayant la capacité fixe pour 4-5 personnes, 25 organisations sont de 6 à 21 microbus, 17 organisations ont 20 à 165 autobus et 42 pompiers peuvent transporter de 6 à 9 personnes.

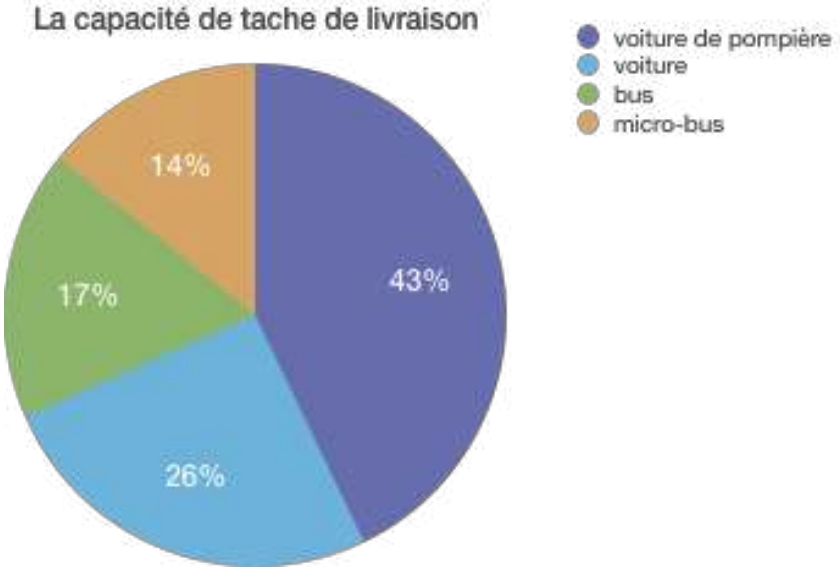


Diagram 1. Créé par les auteurs.

Sur la base de l'échantillon, on peut affirmer que la capacité des passagers des bénévoles des passagers correspond à la réalisation d'activités de soutien dans le processus d'expulsion.

Les outils spécifiques de ces outils, de l'hospitalisation et de l'équipement technique utilisés pour transporter les patients hospitalisés dans les établissements désignés. Il s'agit notamment des berceaux de sauvetage, des lits squelettiques et des véhicules utilisés pour le transport d'ambulances.

Il nécessite un équipement et une formation spéciaux pour aider à la circulation des matériaux déposés dans les pharmacies, dans les entrepôts toxiques et dans les dépôts

d'engrais dans un endroit sûr. Le déplacement des matières dangereuses, la réalisation de la tâche de transport est un risque important qui doit être disponible sur le site pour fournir les dispositifs de protection nécessaires à l'élimination des dommages fournis par l'opérateur. Tel qu'exprimé par le manuel éditorial de Kátay Urbán Lajos - Bognár Balázs, il existe un risque important de déplacer les marchandises dangereuses lorsque l'emballage du produit peut conduire à l'environnement, à l'environnement et au transport où le danger est causé par l'accident du véhicule pour quelque raison que ce soit. [9]

L'exécution de la tâche suppose un équipement de protection spécial contre les effets nocifs des produits chimiques. Lors de l'examen de l'équipement adapté à cette tâche, le registre de protection civile contient des vêtements de protection antistatiques et des équipements de protection contre les incendies.

Dans le cadre des tâches de transport, nous pouvons également gérer les outils utilisés pour exécuter la tâche d'évacuation. En vertu des dispositions du Décret Gouvernemental § 50 (1) " en cas de risque direct de vie et de risque imprévu dans la zone vulnérable, il n'y a aucun moyen de mener à bien les tâches d'expulsion, la protection de la population doit être assurée par une évacuation. " [2, 50§(1)] L'émergence d'une menace directe pour la vie est causée par un changement radical des facteurs environnementaux lors de l'évacuation, les situations spéciales qui peuvent être résolues par le comté et les organisations nationales de sauvetage organisées pour la mission de recherche et de sauvetage. Par exemple, l'évasion de la zone inondée où la tâche est effectuée avec des navires, des bateaux de secours et des embarcations de sauvetage. Les navires de déploiement capables d'accueillir 12 à 20 personnes dans la gestion de certains groupes de sauvetage peuvent être installés comme exemple d'assemblage. En tant que tel, nous pouvons considérer l'intervention dans la zone affectée par l'impact extérieur (tremblement de terre, explosion) causant la dégradation urbaine où les organismes de protection civile volontaires sont impliqués dans l'évacuation en utilisant leur technologie de corde.

Les tâches de recherche

Les organismes de recherche et de sauvetage sont responsables de leur formation pour trouver des résidents, des sans-abris et des déménagements dans le processus, même s'ils sont susceptibles d'être déplacés. Lors de la recherche de personnes dans des zones gratuites, l'utilisation de dispositifs de détection aérienne accélère, ce qui rend la tâche plus efficace. Avec l'aide d'un personnel formé au développement et à l'utilisation d'un outil de reconnaissance aérienne, l'organisation de sauvetage peut obtenir des informations sur la situation et l'état du sans-abris, ce qui permet de soutenir l'intervention en explorant les options de sauvetage et d'approche. À titre d'exemple, la Drone Hexa-6 dans la gestion du groupe de sauvetage peut servir de modèle pour l'efficacité de l'application de la reconnaissance aérienne par organisation de sauvetage.

Les travaux de recherche en fonctionnement pour fournir des structures d'éclairage de fond dans la mise en œuvre interprétées du déploiement d'évacuation, le temps d'évacuation de la journée est lié à l'endroit où le service d'éclairage public n'est pas établi ou est temporairement suspendu. En utilisant des réflecteurs et des lampes d'éclairage de danger, les capacités d'intervention des organisations de sauvetage se reflètent dans l'illumination des voies d'évacuation et la création de conditions de circulation sûres. Lors de l'examen de l'équipement pour la réalisation de cette tâche, les outils suivants se trouvent dans le registre de protection civile.

Comté	Description
Bács-Kiskun	Réflecteur
Bács-Kiskun	Système de réflecteur de projecteur 2,5 KW
Baranya	Réflecteur d'halogène
Győr-Moson-Sopron	Lampe d'illumination
Borsod-Abaúj-Zemplén	Réflecteur d'halogène
Győr-Moson-Sopron	Réflecteur

Table 1. Créé par les auteurs.

Le processus d'inclusion

En vertu de l'article 52 (3) du décret gouvernemental, lors de la déportation, il faut s'efforcer de minimiser les conditions de vie de la population touchée par la réception, ce qui peut être réalisé par une coopération coordonnée entre les forces intervenantes. La coordination est établie par le Président du Comité de Défense du Comté dans sa juridiction. [2]

Les fonctions d'hébergement et de maintenance

En établissant ou en maintenant un site de réception, les organisations de sauvetage peuvent être un participant efficace au déploiement de leurs moyens techniques. Fournir une alimentation électrique est une exigence fondamentale pour les tâches d'approvisionnement et de santé publique ou de sécurité publique. Pour le dépôt de ces actifs, nous trouvons la distribution suivante :

1. Les établissements où la gestion de la logistique (entreposage, gestion du cycle de vie) de l'actif n'est pas résolu par l'organisation de sauvetage est la propriété et le maintien du gouvernement local et les organisations locaux de protection civile volontaires ont le droit d'utiliser et ont le droit d'utiliser.

Comté	Outil á robot - Performance du
Hajdú-Bihar	8,20 (kW)
Hajdú-Bihar	4,00 (kW)
Hajdú-Bihar	7,00 (kW)
Veszprém	200,00 (kW)

Table 2. Créé par les auteurs. Source de données:

2. Les actifs techniques sont dans la majorité de la maintenance et le dépôt des organisations de sauvetage dans la gestion de la sous-unité exécutant la tâche de logistique. Le tableau 3 résume l'emplacement de l'agrégateur le plus performant dans les comtés donnés.

Comté	Outil á robot - Performance du générateur
Bács-Kiskun	6,50 (kW)
Békés	4,50 (kW)
Borsod-Abaúj-Zemplén	4,80 (kW
Budapest	1,00 (kW)
Győr-Moson-Sopron	1,50 (kW)
Heves	8,00 (kW)
Jász-Nagykun-Szolnok	5,50 (kW)
Nógrád	3,80 (kW)
Pest	4,00 (kW)
Somogy	10,00 (kW)
Vas	5,00 (kW)
Zala	2,60 (kW)

Table 3. Créé par les auteurs.

Grâce à ces exemples, nous pouvons voir que les agrégateurs dans l'utilisation des organisations de sauvetage occupent une échelle de 1.00 kW à 10 kW, ce qui peut effectuer la tâche en tant que source d'alimentation supplémentaire lors de l'exécution de la tâche en fournissant l'alimentation en énergie ininterrompue ou des systèmes d'éclairage plus petits.

Dans la liste des générateurs de puissance, des dispositifs performants, tels que le générateur de puissance de 350 kW dans le comté de Csongrád, ou la centrale électrique de 176 kW dans le comté de Zala, pour des équipements électriques, des systèmes de nettoyage ou d'éclairage à économie d'énergie Ils peuvent également fournir une énergie adéquate pour leur nutrition.

Les tâches administratives, sécurité de la communication

Les organisations de sauvetage peuvent participer à la mise en œuvre des tâches administratives locales de réception, en tenant compte des documents nécessaires à la gestion du nombre de personnes hébergées, du bétail et des biens matériels figurant dans la liste des matériaux pour la réception de la population sur le site d'atterrissage.

Les tâches sociales

Les tâches sociales comprennent la fourniture d'assistance dans la formulation et le maintien des conditions sociales d'inclusion. Dans cette tâche, les bénéficiaires reçoivent la connaissance de la politique, le soutien spirituel et les soins de base des enfants et d'autres métiers spéciaux et, le cas échéant, la partie de la mise en œuvre de la désinfection et de la décharge.

LA DEVELOPPE D'UN CADRE DE QUALIFICATIONS

Le niveau d'assistance fourni par les organisations bénévoles de protection civile dans le domaine de l'accueil de la déportation est déterminé par les qualifications et la réactivité des ressources humaines. En évitant les obstacles à une intervention efficace, la résolution immédiate des problèmes ne peut être réalisée que par la connaissance des mécanismes d'action, de l'analyse des dangers, de la réponse au danger donné et de l'accumulation des connaissances existantes. "Les tâches sont généralement une chaîne de tâches logiquement liées, nécessitant une mise en œuvre cohérente des conclusions tirées de la mise en œuvre du plan, de la concentration des forces, du suivi continu, de l'évaluation et du résumé de l'expérience. Des mécanismes efficaces de rétroaction sont en place ". [10, 182.o] Par conséquent, des efforts devraient être faits pour inclure dans les informations sur la formation des problèmes qui peuvent être utilisés par les organisations de sauvetage pour soutenir la population touchée dans un environnement altéré dans la mesure du possible dans un cycle de vie quasi normale et donc pour atteindre l'intérêt individuel dans la réglementation en tant qu'objectif objectif.

"Afin de défendre efficacement les effets destructeurs des catastrophes ou d'autres menaces, les municipalités doivent participer efficacement à la mise en œuvre des tâches de sauvetage et de restauration, soutenues adéquatement par les organisations coopérantes, elles doivent disposer du système et des capacités de défense appropriés et bien équipés qui ont déjà été" [11, 88.o]

Étant donné que tout est considéré comme spécifique à l'intervention afin de protéger la population, la situation changeante nécessite une adaptation et un développement constant des procédures standard. Par conséquent, la conception et la maintenance des compétences vont au-delà de la préparation pour le respect de la mise en œuvre de l'activité principale et nécessitent un développement continu des exigences de la protection civile.

Selon les Instructions du Directeur Général 20/2012, les organisations de sauvetage volontaire sont offertes sous la forme d'une formation initiale, d'une formation professionnelle et d'une formation continue. [12]

Éléments de protection de la population de l'éducation de base

Le matériel de la formation de premier cycle est assuré par l'exploitation du système de protection contre les catastrophes et le rôle et la responsabilité des organisations de protection civile dans ce système. Les éléments de cette forme de formation comprennent des éléments

de la participation des organisations bénévoles à la protection de la vie privée, de la réinstallation et de l'inclusion de la population, qui apparaissent dans les thèmes suivants.

1. En ce qui concerne la gestion des catastrophes et la législation, les volontaires peuvent définir les antécédents juridiques pour l'utilisation de leur organisation de sauvetage, le système d'intervention et les obligations de défense prévues par la réglementation légale pour la protection civile et la protection de la population.
2. Les droits et les obligations des membres du matériel de formation devraient être explorés avec la coopération des organismes professionnels avec la culture et la formalité des organes de comportement des organismes d'application de la loi, en présentant et en passant sur la base de la coopération sur place, élément important de la mise en œuvre effective de mesures massives de protection de la population dans des circonstances modifiées.
3. Le sujet des effets menaçants, les possibilités de défendre les sources de danger les plus importantes dans le domaine d'exploitation et la présentation des plans d'intervention d'urgence fournissent un cadre pour planifier l'orientation et l'appui fondamental des interventions.
4. En vertu des dispositions de la Loi sur la Sécurité du Travail, un employé ne peut se voir confier un travail qui lui convient, possède les connaissances, les compétences et les aptitudes nécessaires pour travailler sans risque et sécurité. [13] Selon cela, les travaux sur le thème de la sécurité et de la santé au travail couvriront les règles à observer lors de la détection des dommages, les règles à respecter dans le sauvetage technique, la sécurité incendie et les règles d'hygiène de l'activité critique. Au cours de la formation initiale, la zone de transfert des connaissances de base sur les tâches de déménagement et d'évacuation peut être expliquée dans la partie sécurité des travaux des consignes de sécurité pour la sauvegarde de la zone contaminée et l'utilisation d'équipements de protection individuelle.
5. Lors du traitement des tâches de protection civile réglementées à l'article 52 de la Loi sur la protection contre les catastrophes, les organismes de sauvetage connaissent bien le système d'alerte, les méthodes d'information et d'alerte de la population et les bases d'exécution des tâches qui peuvent être couvertes par leur capacité de montage. [1]
6. Informations sur les premiers soins sur les connaissances fondamentales en matière de santé, qui est la règle des soins primaires pour les résidents touchés par le matériel chimique, biologique et radiologique dans le déclenchement résultant du mouvement des patients hospitalisés et des éventuels accidents radiologiques.

La formation professionnelle est une protection élémentaire

Sur la base de la Direction générale 20/2012, la formation professionnelle implique la préparation d'unités spécialisées des organes pour des tâches spécifiques. [12] Le matériel de connaissances présentant dans le processus de transfert de connaissances de cette forme de formation, la protection de distance de la population, est présenté comme une série de tâches spéciales :

1. Pendant la déportation et la réception, l'unité de santé est impliquée dans la protection de l'ABV préventive de la population et des biens matériels, la décharge et la désinfection, les premiers soins, la recherche des blessés et le transport des blessés.
2. Intervention de l'unité de protection de la population selon les articles 46-54 du Décret Gouvernemental, est la mise en œuvre de l'évacuation, de l'évacuation et de l'accueil. L'intervenante devrait s'efforcer de se conformer au libellé de l'article 48 du décret gouvernemental afin que la vie familiale et communautaire de la

population touchée par la déportation ne soit pas entravée jusqu'à ce que la réintroduction soit faite et, par conséquent, la formation doit inclure, en plus des connaissances juridiques et techniques fournies dans la formation initiale, les aspects psychologiques, les éléments sociologiques qui permettent aux membres de l'organisation de sauvetage de répondre aux besoins individuels découlant de l'âge, du sexe ou d'autres biens des personnes déplacées lorsqu'ils sont en contact avec la population. [12]

3. L'unité d'info communication intervient en fournissant des informations rapides, précises et crédibles, le soutien de la formation pour la mise en œuvre de cette tâche, conformément aux dispositions du Chapitre VII du Décret Gouvernemental, fournissant des informations d'urgence pour la population, traitant des outils d'information et de communication et transmettant la connaissance de l'exécution de l'alerte. La formation pour fournir une coopération avec les forces professionnelles et la fourniture de connaissances techniques, en particulier, devrait inclure la connaissance du système d'information de l'organisation de sauvetage pendant le contrôle des catastrophes, qui nécessite l'accès au système et la coordination de son utilisation, comme prévu à l'article 61 du décret gouvernemental.
4. L'unité logistique a pour mission de soutenir l'intervention de l'organisation de sauvetage, la capacité d'intégration adéquate, la capacité de travailler dans toutes les situations, la rapidité et la flexibilité, l'interopérabilité appropriée, la rentabilité et la conception des processus logistiques. [14] Dans le programme de formation professionnelle, il convient de préciser la planification des tâches correspondant à l'engagement dans la mise en œuvre de l'inclusion, la fourniture de conditions financières et techniques aux organisations bénévoles de protection civile et la planification des tâches de la période de préparation, la préparation directe et la période de mise en œuvre.
5. L'unité technique effectue la tâche d'enquêter et d'économiser l'élimination des dommages techniques et le cambriolage dans les bâtiments en ruines. La connaissance des tâches liées à l'activité de la période de déclassement est la technique consistant à sauver des éléments protégés du patrimoine culturel dans le domaine d'exploitation et à mettre en place des structures de protection pour la réception pendant la réception et le maintien de l'entretien technique et de l'accueil des établissements entrants pendant la période de destruction.

L'éducation complémentaire est un élément fondamental de la protection de la population

Les changements socioéconomiques ont créé de nouvelles menaces, qui ont mis les menaces des établissements dans un système de protection de conception basé sur de nouvelles perspectives. L'élément clé de la protection de la population du 20ème siècle, la gestion des abris, a été remplacé par les institutions d'accueil, la principale source de danger, alors que les placements militaires sont devenus naturels (inondations, tremblements de terre, conditions météorologiques d'urgence) et de plus en plus civilisation (accidents industriels, terrorisme, problèmes de migration). Comme l'affirme István Endrődi dans son article, les risques et les risques les plus complexes qui menacent la sécurité ont radicalement changé le système de défense domestique. [15]

Selon les articles publiés par les auteurs d'Enikő Hevér - Árpád Muhoray, il est indiqué que la responsabilité première des organismes d'application de la loi est de protéger la population, de concevoir, d'organiser et de mettre en œuvre des moyens de défense par une correction

appropriée des changements sociaux, économiques et naturels [16]. Par conséquent, de nouveaux défis et réponses à cette nécessité doivent être reflétés dans le matériel de formation, en préparant ainsi les organismes de bénévolat à des mesures correctives efficaces.

Conformément aux instructions du Directeur général du 20/2012, le but de la formation complémentaire est d'accroître les connaissances et d'améliorer le niveau de préparation des participants, de répéter et d'organiser la formation de base et professionnelle. [12] Ainsi, cette forme de formation fournit un cadre pour évaluer les situations de gestion de crise dans les circonstances changées, en détectant les faiblesses et en modernisant les procédures et en mettant en œuvre sa capacité à la mettre en œuvre.

SUGGESTIONS

La complexité du processus d'évacuation, d'évacuation et de réception est due au grand nombre de facteurs physiques, psychologiques et psychologiques de la population affectée et à l'état excité et perturbé résultant de la population touchée, d'autre part, les différents niveaux des forces intervenantes, Selon László Teknős, au cours des dernières années, comme excédent dans l'exécution du travail de défense, ils sont restés chez eux malgré la relocalisation. À son avis, ceux qui ne suivaient pas l'évacuation organisée pourraient les mettre en danger pour la vie. Les actions de sauvetage suppriment les forces, l'équipement, l'énergie et le temps d'intervention. [17]

La formation continue des ressources humaines des organisations de sauvetage doit développer la connaissance des contacts avec les personnes concernées, développer la connaissance de la population moderne et résumer la bonne et la mauvaise expérience des interventions passées. Par conséquent, dans le cadre d'une formation complémentaire, l'éventail des connaissances à traiter devrait également s'étendre à cette zone.

L'exigence de base de l'intervention spéciale des organisations, l'efficacité du système de gestion et le système de soutien logistique pour l'arrière-plan était la définition de l'exécution des tâches et de son environnement. À cette fin, il est recommandé de traiter dans le matériel de formation à la fois théorique et pratique les domaines suivants liés aux tâches des tâches de protection de la population de l'évacuation et de la réception d'évacuation :

1. Recherche et sauvetage.

Selon les conclusions des auteurs du document, László Földi- Norbert Körmendy, les conditions environnementales de la civilisation et les risques naturels, ainsi que la mise en œuvre technique du site de l'événement, impliquent la nécessité du développement des organisations de sauvetage. [18]

Lors de l'examen de l'équipement technique des organismes de sauvetage, la détection du dispositif de reconnaissance aérienne a été démontrée. Dans le même temps, le dossier de protection civile montre que toutes les organisations de sauvetage volontaires n'ont pas cette technique, de sorte que leur participation à la reconnaissance aérienne n'est pas assurée. Étant donné que l'utilisation de dispositifs drone lors de la réinstallation, de l'évacuation et de la détection de l'approche sécurisée des itinéraires d'évacuation est une solution innovante dans le domaine de l'utilisation, il est justifié de l'utiliser dans toutes les organisations de sauvetage au niveau de la formation. La disponibilité de l'actif peut être résolue en assurant une organisation qui la gère.

2. Fournir des tâches spéciales de protection populiste.

Julia Hornyacsek déclare dans son rapport scientifique que la catastrophe a créé la peur, l'augmentation de la tension et de l'anxiété chez l'homme. Le changement d'état négatif résultant et la crise personnelle pendant les interventions du public ont été précédemment ignorés et l'accent mis sur l'organisation technique du sauvetage. [19] Les changements radicaux dans l'environnement résidentiel, l'effondrement des services publics, la destruction des routes, la perturbation ou le manque temporaire de soins de base, les obstacles pour répondre aux besoins fondamentaux, l'émergence forcée des situations extraordinaires en cours de déportation, l'engagement de l'individu dans la communauté, les influences environnementales intenses: tons, lumières, á la suite de la vue de mort, des animaux gravement blessés, tombés, le sentiment d'impuissance et d'impuissance peut apparaître chez l'homme. En ce qui concerne la protection du logement, le matériel de formation devrait être utilisé pour résoudre l'effet de panique massif et la psychose de masse causé par les impacts psychologiques de ceux dans la zone sinistrée et pour mener à bien des tâches de protection civile dans ces circonstances. Bien sûr, le bénévole intervenant n'a pas la tâche de faire face à des phénomènes psychiques tardifs suite à des catastrophes ou d'entreprendre une intervention de crise visant à rétablir l'équilibre. Leurs activités sont limitées à aider à surmonter la crise et à surmonter le stress, ce qui crée les conditions d'intervention. L'aide doit développer son rôle et développer la capacité à identifier de manière excessive. La tâche de l'intervention est d'accepter le soutien et la situation réelle (crise). [20]

CONCLUSIONS

Les organismes de sauvetage bénévoles ont la possibilité d'intervenir avec le soutien de leur équipement et de leurs capacités spéciales et de toute la gamme de la zone de protection de la population. Au cours de la mise en œuvre des tâches de protection civile dans le système de déportation et de réception, elles assurent le travail des organismes professionnels grâce à leur équipement technique, leur capacité personnelle et de leur cargaison, leurs ressources humaines qualifiées et leur logistique. Sur la base des données enregistrées dans le registre de la protection civile, on peut affirmer que les organisations de sauvetage disposent du matériel technique qui peut être utilisé dans le processus de réception et de déménagement et les règlements dans lesquels la gestion logistique et l'entreposage d'un actif donné d'une organisation de sauvetage ne sont ni détenus ni gérés par l'administration locale Les organisations de protection civil volontaires ont le droit d'utiliser et ont le droit d'utiliser.

La formulation d'une réponse efficace aux défis de la création de sécurité, la mise en œuvre de tâches de protection civile dans un environnement social en constante évolution, oblige les organisations bénévoles à maintenir leur capacité à poursuivre et à développer leurs qualifications. Ils devraient être inclus dans la formation, dans l'exercices de coopération, les pratiques de coopération et la conception de l'utilisation d'outils techniques. La participation des organisations bénévoles de protection civile est une condition préalable aux capacités d'intervention, qui sera développée dans le processus de formation défini par les régulateurs internes de la prévention des catastrophes.

Les formations examinées comprennent des informations sur le rôle des organisations de sauvetage dans leur situation d'engagement. Afin de mettre à jour le curriculum, des mesures devraient être prises pour souligner le développement de la capacité de l'organisation de sauvetage à jouer un rôle particulier dans la protection de la population, sa capacité à soutenir

la crise et la coopération avec les organisations coopérantes, l'absence d'un environnement de service de base et la capacité de répondre aux circonstances changeantes de sa civilisation.

Sur la base d'une revue de la littérature pertinente publiée sur ce sujet, on peut affirmer que les structures générales d'intervention en matière de protection de la population des organismes de sauvetage axés sur les bénévoles sont étudiées en profondeur, alors que le développement d'outils techniques et le développement de compétences d'intervention basées sur ces outils sont nécessaires

LITTERATURE UTILISEE

[1] *2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról*

[2] *234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról*

[3] *62/2011 (XII. 29.) BM rendelet a katasztrófák elleni védekezés egyes szabályairól*

[4] *2011. évi CXIII törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről*

[5] 290/2011(XII. 22.) Korm. Rendelet a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény egyes rendelkezéseinek végrehajtásáról

[6] TEKNŐS L.: *A kitelepítés, kimenekítés általános és speciális feladatai Magyarországon* Bólyai Szemle: A NEMZETI KÖZSZOLGÁLATI EGYETEM KATONAI MŰSZAKI TUDOMÁNYÁGI FOLYÓIRATA XXIII. évfolyam, 2014/3. szám pp. 109-123

[7] HORNYACSEK J.: *A polgári védelmi szervezetek alkalmazási lehetőségei a tömeg közlekedési katasztrófák felszámolása során*., in: New Challenges in the Field of Military Sciences 2010 7th International Scientific Conference. Budapest, Magyarország, 2010.09. 28-30. pp. 1-19. http://www.drhornyacsek.hu/2.htm (Letöltés: 2016. 03.10.)

[8] HELIOS Polgári védelmi adattár

[9] BOGNÁR B., BONNYAI T., GÖRÖG K., KÁTAI-URBAN L., VASS GY.: *Létfontosságú rendszerek és létesítmények védelme, Kézikönyv a katasztrófavédelmi feladatok ellátására*, Dr. Bognár Balázs, Dr. Katai-Urban Lajos, (szerk.) NEMZETI KÖZSZOLGÁLATI EGYETEM Katasztrófavédelmi Intézet Budapest, 2015, 147 p.

[10] KOZÁK A., HORNYACSEK J.: *A polgári védelem kialakulása, szerepe a katasztrófavédelem egységes rendszerében*, Bolyai Szemle 21:(2) pp. 157-184. (2012)

[11] HORNYACSEK J.: *A települési védelmi képességek a katasztrófa-kihívások tükrében*, Budapest: „Biztonságunk érdekében" Oktatási- és Tanácsadó Tudományos Egyesület,2010.

[12] *BM Országos Katasztrófavédelmi Főigazgató 20/2012. (VIII.30) számú utasítása a polgári védelmi szervezetek állományának katasztrófavédelmi képzési programjáról*. http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_jogszabaly (letöltés: 2016.03.28)

[13] *1993. évi XCIII. törvény a munkavédelemről 50. §* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99300093.TV (letöltés: 2016.03.28)

[14] MUHORAY Á., TEKNŐS L.: *A HUNOR hivatásos nehéz kutató - mentő mentőszervezet alkalmazásának logisztikai feladatai,* Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata 25: (E-szám) pp. 14-23

[15] ENDRŐDI I.: *Egy lehetséges új veszélyhelyzeti információs és tájékoztató rendszer bemutatása, jelentősége a veszélyhelyzeti tájékoztatásba.* Bólyai Szemle: A NEMZETI KÖZSZOLGÁLATI EGYETEM KATONAI MŰSZAKI TUDOMÁNYÁGI FOLYÓIRATA XXIII. évfolyam, 2014/3. szám pp. 109-123

[16] HEVÉR E., MUHORAY Á.: *A rendőrség bűnügyi szakterületének együttműködése a katasztrófavédelemmel a civilizációs katasztrófák során*, Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata 24: (1) pp. 169-184.

[17] TEKNŐS L.: *A kitelepítés, kimenekítés általános és speciális feladatai Magyarországon* Bólyai Szemle: A NEMZETI KÖZSZOLGÁLATI EGYETEM KATONAI MŰSZAKI TUDOMÁNYÁGI FOLYÓIRATA XXIII. évfolyam, 2014/3. szám pp. 109-123p

[18] FÖLDI L.-KÖRMENDY N.: K*atasztrófaveszély felderítés 1. Általános felderítési feladatok*.http://www.zmne.hu/tanszekek/vegyi/docs/fiatkut/pdf/korm_04_03.pdf (Letöltés: 2016. 03.10.)

[19] HORNYACSEK J.: *A tömegkatasztrófák pszichés hatása a beavatkozó állományra, az alapvető korai és késői pszichés jelenségek, valamint a negatív következmények elkerülésének lehetséges módjai*, Műszaki Katonai Közlöny (Online) 22.:(1. szám) pp. 143-189. (2012)

[20] BOLGÁR J. - SZEKERES GY.: *Katasztrófa és kríziskommunikáció lélektani alapjai elektronikus jegyzet a védelmi igazgatás szereplői számára* Zrínyi Miklós Nemzetvédelmi Egyetem Kossuth Lajos Hadtudományi Kar 2009)

MENTŐSZERVEZETEK FELADAT VÉGREHAJTÁSA A KITELEPÍTÉS, BEFOGADÁS FOLYAMATÁBAN

Absztrakt

A kárhelyszínen, az együttműködő és közreműködő szervezetek, a közigazgatási egységek, az állami hivatásos és önkéntes erők feladatmegosztásában a mentőszervezetek speciális felszerelésükkel, képzett humánerőforrásukkal és logisztikai képességeikkel vesznek részt.
A biztonság megteremtésének kihívásaira való hatékony válasz megfogalmazása, és a polgári védelmi feladatok egy folyamatosan változó társadalmi környezetben történő végrehajtása, folyamatos képesség fenntartást és képzettség fejlesztést kíván az önkéntes szervezetek részéről, amely meg kell, hogy jelenjen a képzések, továbbképzések, együttműködési gyakorlatok rendszerében, illetve a technikai eszközök felhasználási koncepciójának kialakításában.
Jelen publikációjában a szerző az önkéntes mentőszervezetek kitelepítés-befogadás rendszerében történő szerepvállalásának lehetséges területeit, az azt támogató jogi szabályozási hátteret, illetve a feladat végrehajtásra való felkészülés struktúráját, fenntartható finanszírozásának lehetőségeit vizsgálja.

Kulcsszavak: *önkéntes polgári védelem, képzések, gyakorlatok, kitelepítés-befogadás*

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

TŰZOLTÓI BEAVATKOZÁSOK NEMZETKÖZI KÖRNYEZETBEN

FIRE INTERVENTIONS IN INTERNATIONAL CONTEXT

KUK Enikő Eszter; PÁNTYA Péter

(ORCID ID: 0000-0003-3365-5989); (ORCID ID: 0000-0003-2732-2766)

kuk.eniko.eszter@uni-nke.hu; pantya.peter@uni-nke.hu

Absztrakt

A legtöbb országban a tűzoltóságok szervezete felelős az elsődleges műszaki mentési és természetesen a tűzoltási beavatkozások széles körénél. A széles körű szakmai tudásigényt tovább mélyíti a nagyszámú külföldi látogató, átutazó, akik nem beszélik az adott ország nyelvét. Magyarországot tekintve jelen írás ismertet olyan körülményeket, ahol olyan sérültekkel lehet találkozni, akik nem beszélnek magyarul. A szerzők rámutatnak az idegen nyelvtudási követelményekre a tűzoltói beavatkozások során és ismertetik azokat a tűzoltósági beosztásokat, ahol a tűzoltótisztek nagyobb eséllyel találkozhatnak külföldiekkel, így ezekben a helyzetekben az idegen nyelvi tudás segítheti a beavatkozás hatékonyságát.

Kulcsszavak: *tűzoltóság, beavatkozások, nemzetköziség, idegen nyelvek*

Abstract

In the majority of the countries, fire departments are responsible for a wide variety of interventions, including fire incidents and technical rescue. In the wide range of skills and knowledge a potential one is the high number of foreign visitors who do not speak the language of the country. By taking a look at Hungary, the paper specifies certain features of countries that increase the likelihood of non-natives getting involved in incidents. In response, the authors highlight foreign language knowledge as an asset during fire interventions and specify those positions within the fire service who might get in contact with foreigners, resulting in a situation when the knowledge of a foreign language can support the effectiveness of their work.

Keywords: *fire service, interventions, internationalism, foreign languages*

A kézirat benyújtásának dátuma (Date of the submission): 2017.10.01.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.10.31.

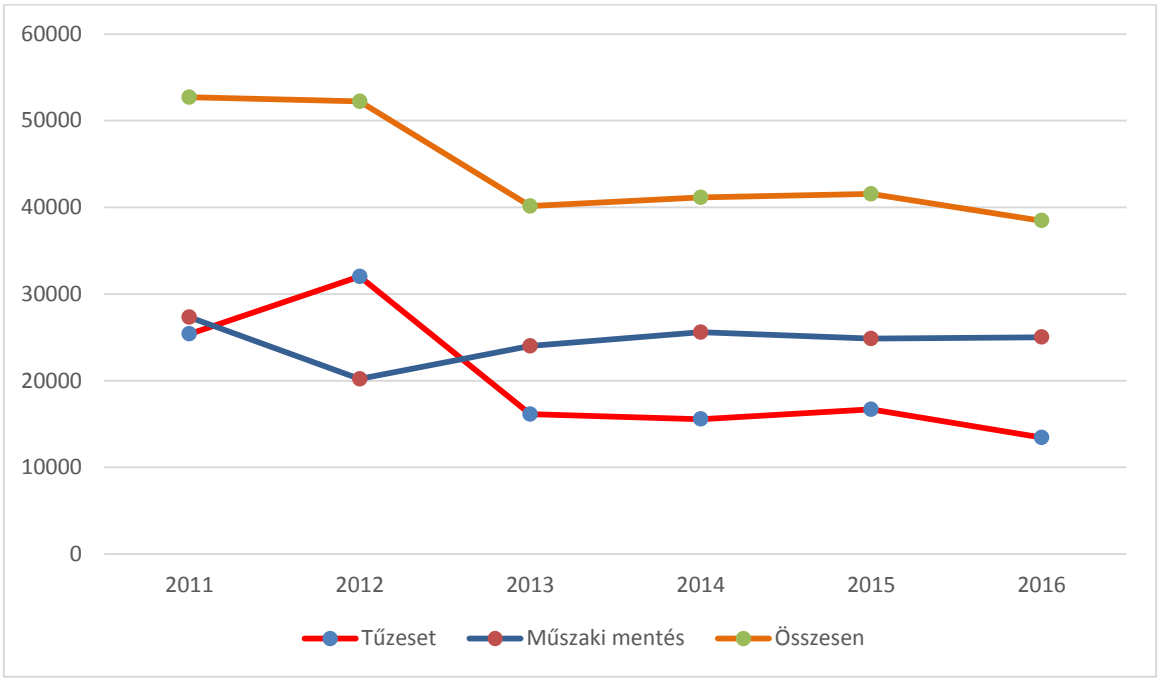
BEVEZETÉS

A növekvő turizmus és nemzetközi szállítás egyben növeli az igényt az idegen nyelven kommunikáló személyek felé, ami biztonságot nyújthat mind az állampolgárok, mind a külföldi utazók felé. Mint minden országban, Magyarországon is felelősséget kell vállalnia az államnak a területén tartózkodók biztonsága érdekében. A tűzoltói beavatkozás hatékonyságára hatással van a beavatkozók képzése, a technikai eszközfejlesztés és egy másik mód, a minél szélesebb körű információszerzés a felderítés során. Az információk érkezhetnek a segélykérő telefonhívás során, a szemtanuktól és a sérültektől is. A beavatkozási kör ismertetését követően látható, hogy a turizmus és a nemzetközi szállítmányozás milyen hatással van erre a területre. A szerzők ismertetik a hivatásos katasztrófavédelmi szervezet, a hivatásos tűzoltó-parancsnokságok azon beosztásait, amelyekben a beavatkozások során idegen nyelv használatára fokozottan szükség lehet.

A TŰZOLTÓSÁGOK BEAVATKOZÓ TEVÉKENYSÉGEI

A tűzoltási és műszaki mentési területen a tűzoltóságok az elsődleges felelősök, az elsődleges beavatkozók. A műszaki mentés a balesetek széles körét tartalmazza úgy, mint épületomlás és sérülés, viharkár, közlekedési baleset (esetleg veszélyes anyag jelenlétében) akár közúton, akár vasúton. Ezek csak néhány példák a műszaki mentési terület ismertetésére és a tűzoltósági tevékenység részvételére. [1]

Az 1. számú ábra ismerteti azokat a magyarországi tűzjelzéseket, ahol a tűzoltóságok részéről is beavatkozás is történt 2011 és 2015 között. Több, mint fele a beavatkozásoknak a műszaki mentés, amely tevékenység a lakosság által is a tűzoltósághoz kapcsolódik.



1. ábra Tűzoltói beavatkozások száma 2011-2015 között Magyarországon
(Forrás: KAP Online, a BM OKF statisztikai adatbázisa Pántya P. által kutatva és szerkesztve)

A mentési tevékenységben résztvevő hivatásos tűzoltóknak a képzésük folyamán számos területen kell szakértelmet szerezniük, valamint egészségügyi, pszichológiai és fizikai alkalmassági feltételeknek kell megfelelniük. A szakmai kiképzést folyamatos továbbképzés követi minden szakmai szinten. Az idegen nyelv tudása nincs jelenleg a képesítési követelmények között, kivételt a felsőoktatásban részt vevők képeznek, a speciális

felsőoktatási szabályok miatt. [2] Amennyiben azt a környezetet nézzük, ahol a tűzoltói beavatkozások történnek, láthatóvá válik, hogy könnyen bekövetkezhet idegennyelv-tudást igénylő káreset, ahol ez az ismeret hatással lehet a beavatkozásra közvetlenül. A káreset felszámolásának sikeressége függ a megmentett értéktől, a sérültek vagy életveszélybe kerültek mielőbbi megmentésétől és ezt befolyásolja a természeti környezet vagy a káresemény közvetlen környezete is. Minél több ismerettel rendelkeznek a beavatkozók előzetesen és a beavatkozás során, annál nagyobb esély van a minél sikeresebb kárfelszámolásra.

A TURIZMUS ÉS A SZÁLLÍTMÁNYOZÁS HATÁSA A TŰZOLTÓSÁGOK BEAVATKOZÁSAIRA

A műszaki mentésekre leggyakrabban a közúti balesetek során van szükség, ahol nagy valószínűséggel lehet találkozni sérült személyekkel is. A jelen cikk témájának megfelelően vizsgálva a közúton – különösen az Európai Unióban – igen nagy számban vannak jelen különböző nemzetiségű személyek.

Az Európai Unió statisztikái alapján a népesség 61,1%- szokott részt venni a turizmusban, 25% külföldre is utazik [3]. A magyar Statisztikai Hivatal adatai alapján a Magyarországra érkező külföldiek száma 2014-ben közel 46 millió fő volt. [4]. A Magyarországon tartózkodók száma 139.700 és 206.909 között volt az elmúlt tíz évben [5]. Ámbár erre nincsenek közvetlen kimutatásaink, azonban a nagyszámú külföldiek hazánkban tartózkodása előrevetíti a tűzoltói beavatkozásokban való érintettségüket, akár mint szemtanú, jelzést adó személy is. Értékes információkat adhatnak a káresetek környezetéről bejelentőként. Kijelenthető, hogy a legtöbbet beszélt nemzetközi nyelvek Magyarországon az angol és a német.

A külföldiek számát tekintve egy tűzoltói beavatkozást érintő terület a közút és vasúthálózat, ahol a nemzetközi személy és áruszállítás történik (benne veszélyesáru-szállítmányozással). Magyarország lehet célpontja vagy csak átkelési területe ezen mozgásoknak. Közép-kelet európai elhelyezkedése okán az ország kapcsolatot teremt nem csak a szomszédos, hanem távolabbi országok számára, akár Ázsiával is. A tárgyalt témakör szempontjából ezekre a nemzetközi tranzitútvonalakra – amelyek nagyszámú és jellemzően nem magyar anyanyelvű utazók által is használva vannak – mindenképpen érdemes figyelemmel lennünk.

MAGYARORSZÁG KÖZLEKEDÉSI HÁLÓZATA

Magyarország több nemzetközi szervezetnek is a tagja, egyezménynek a részese, melyek a különböző szállítmányozási formákat (közúti, vasúti, vízi, légi) szabályoznak. Egyértelműen megjelenik itt a vasúti szállításban az Ázsia felől vagy felé történő személy vagy árumozgás. Az európai vasúthálózatban Magyarország két szállítási folyosóval is részt vesz. Az egyik az Orient, amelyik a Cseh Köztársaságtól egészen Görögországi tart, míg a Mediterrán vonal Spanyolországtól egészen Záhonyig, Magyarország keleti határáig húzódik.

Figyelemmel az úthálózatra megemlítendő, hogy a teljes – nemzetközi szempontból is érdekes – vonalak igen hosszúak. Ha csak az autópályákat vizsgáljuk, a magyarországi szakaszok megközelítik a nyugat-európai átlagot. Az elmúlt évtizedekben a teljes magyar autópálya vonal hossza megháromszorozódott.

Egy ország elhelyezkedése és szállítási, mindenféle úthálózati fejlettsége vonzóvá tehetnek egy országot fuvarozók, átutazást tervezők számára. A fentiek alapján a magyarországi nemzetközi forgalom megnövekedett, ami magában hordozza a nagyobb számú közlekedésben részt vevőket érintő baleseteket. Szerencsére a veszélyes áruk szállítása hosszú

idő óta szabályozott nemzetközi szinten. Ilyenek az ADR[1] közútra, a RID[2] vasút esetében, az ADN[3] a belföldi hajózásnál és az ICAO TI[4] valamint az IATA DGR[5] a légiszállításnál. Szabványosított jelek, piktogramok és UN számok segítenek azonosítani a különböző veszélyes anyagokat, árukat akkor is, ha a jármű vezetője, kísérője nem tud információt adni (akár a körülmények miatt) vagy amennyiben nem beszéli az adott ország nyelvét.

AZ IDEGEN NYELV TUDÁSÁT IGÉNYLŐ BEOSZTÁSOK A HIVATÁSOS KATASZTRÓFAVÉDELMI SZERVEKNÉL

Az előzőekben tárgyaltak alapján látható, hogy az egyes káreseti helyszíneken, például vasúti tűzesetnél vagy közúti műszaki mentésnél beavatkozó tűzoltók jó eséllyel nem csak az anyanyelvüket kell, hogy használják ahhoz, hogy információkat szerezzenek vagy kommunikáljanak a sérültekkel, a jelzést adó személlyel. A beavatkozó egységek számára a jelzés vételekor az adott káreset teljes körülménye nem ismert és a gyors döntéshozatalhoz (például a megfelelő erők és eszközök riasztása) hasznos a minél több előzetes információ. Az idegen nyelv tudása – különösen a legjellemzőbben előfordulóké – segítheti eszközként a minél több előzetes, a döntéshozatalhoz szükséges információhoz jutást.

Szükséges lehet, hogy azonosítsuk azokat a tűzoltói – jellemzően tiszti - beosztásokat a hivatásos katasztrófavédelmi szervezetnél, ahol gyakrabban, nagyobb eséllyel találkoznak olyan sérültekkel, akik nem magyar anyanyelvűek. A következő táblázat összegzi a magyar katasztrófavédelem vonatkozó munkaköreit a hierarchikus szintnek valamint helyi, területi szintnek megfelelően. Az országos, központi szint a cikk téma szempontjából nem releváns, nem valószínű az ott létesített beosztásoknál a nagyobb arányú közvetlen kapcsolat sérült vagy jelzést adó személyekkel.

Helyi szint	**Megyei szint**
szerparancsnok Egy tűzoltógépjármű parancsnoka, amennyiben, több tűzoltó tartózkodik rajta. Középfokú állami és szakmai végzettség szükséges.	*műveletirányító referens* A műveletirányítást végző beosztott, adott esetben közvetlenül kommunikál a sérültekkel vagy a jelzést adókkal. Középfokú állami és szakmai végzettség szükséges.
szolgálatparancsnok Az adott tűzoltóság aznapi készenléti szolgálatának parancsnoka, jellemzően vonul a káresetekhez. Szükséges a beosztás betöltéséhez legalább egy felsőfokú alapképzés, BSc oklevél.	*főügyeletes és ügyeletvezető* a műveletirányítási tevékenységet végzi, azt vezeti, adott esetben közvetlenül kommunikál a sérültekkel vagy a jelzést adókkal. Szükséges a beosztás betöltéséhez legalább egy felsőfokú alapképzés, BSc oklevél.

[1] European Agreement concerning the International Carriage of Dangerous Goods by Road, Európai megállapodás a veszélyes árúk nemzetközi szállítására.

[2] Regulations concerning the International Railway Transport of Dangerous Goods, A veszélyes árúk nemzetközi vasúthálózaton történő szállításának szabályai.

[3] European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways, Európai megállapodás a veszélyes árúk nemzetközi, belföldi vizeken történő szállítására.

[4] The International Civil Aviation Organization Technical Instructions for the Safe Transport of Dangerous Goods by Air, Műszaki előírások a biztonságos légi szállításért a Polgári Nemzetközi Légi Szervezet által

[5] Provisions concerning Transport of Dangerous Goods in the International Air Transport, Megállapodás a veszélyes árúk légi szállítmányozására vonatkozóan.

tűzoltóparancsnok és helyettese, esetlegesen a műszaki-biztonsági tiszt Az adott tűzoltóság vezetője vagy a vezetési törzs tagja. Magasabb riasztási fokozat esetén vonul a helyszínre.	*megyei katasztrófavédelmi igazgatóság kijelölt vezetője, tisztje* A megyei igazgató által készenléti jelleggel megbízott személy az esetleges kiemeltebb esetek személyes, helyszíni irányítására
katasztrófavédelmi kirendeltség-vezető A kirendeltségek első számú vezetője, kiemeltebb esetekben vonul a helyszínre.	

2. ábra . Azon beosztások a hivatásos katasztrófavédelmi szervezetnél, ahol idegen nyelvtudásra lehet szükség egy káreset helyszínén. (Forrás: szerzők)

A táblázatban ismertetett beosztásoknál a váltásos szolgálati rend esetében hasznos, ha minden szolgálatra jut elérhető, idegennyelv-tudási képességgel rendelkező tűzoltó. Idegen nyelvi követelmény jelenleg csak a felsőfokú alapképzésben részt vevők számára kötelező, a táblázatban láthatóan pedig csak a tiszti beosztásokhoz szükséges ilyen felsőfokú képesítés. Magyarországon a készenléti jellegű tűzoltó szolgálat háromváltásos rendszerű, A, B és C jelű szolgálati csoportokkal, amelyek folyamatosan, 24 óránként váltják egymást. A szolgálati napot követően 48 óra szabadidő kerül biztosításra. Ez a rendszer biztosítja, hogy folyamatosan a riasztásra készen álljon a megfelelő számú és képzettségű tűzoltó. Az egyes szolgálati csoportokat a szolgálatparancsnokok vezetik legalább felsőfokú alapképzési oklevéllel (BA), ez biztosítja, hogy bármely napon a megfelelő képesítésű tiszt lássa el az irányítói feladatokat. Távollét esetén (pl.: szabadság, betegség, képzés) helyettesíthetőek ideális esetben rajparancsnokkal, aki szintén az említett képesítésekkel rendelkező tiszt. Egy tűzoltóparancsnokságon – egy megyei katasztrófavédelmi igazgatósághoz viszonyítva – jellemzően sokkal kevesebb a tiszti beosztás, ami egyben a várhatóan kevesebb idegen nyelveket beszélők arányát okozza.

A 2015. évi XLII. számú törvény a szolgálati jogviszonyban állók szolgálati körülményeit, előmenetelét, belső sajátos életét szabályozza. [10] Hasonlóan az előzőleg hatályban lévő törvényhez meghatározza, hogy legalább felsőfokú alapképzési oklevél (régebben főiskolai diploma, BA) szükséges a tiszti kinevezéshez (hadnagytól). Ennek az állami oklevélnek a megszerzése nyelvvizsga megszerzéséhez kötött, amely a cikk témájának szempontjából nem csak angol vagy német, tehát a leggyakrabban előforduló lehet. Az említett törvény nem csak a hivatásos tűzoltókra vonatkozik – akikről jellemzően szól a jelen cikk – hanem az egyéb rendvédelmi szervezetek tagjaira is (pl.: rendőrség, büntetés-végrehajtás). [11]

Az új kihívások, mint az idegen nyelvtudási képességeket oktatni szükséges. A Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézeténél a hallgatók (jellemzően a nappali képzési formában) elsajátítják a tűzoltósági, vagy bővebben katasztrófavédelmi szaknyelvi ismereteket. [12] [13] Emellett az idegen nyelvi vizsgák megszerzésére is nagy hangsúlyt helyeznek. A hároméves felsőfokú alapképzés alatt (nappali rendszerű katasztrófavédelem szak), az idegen nyelvi órák öt féléven át tartanak 300 órában, amelynek célja, hogy a hallgatókat felkészítse a nyelvvizsgára és hogy megadja a szükséges szaknyelvi ismereteket. Az elsőéves hallgatók, amennyiben nem rendelkeznek nyelvvizsga bizonyítvánnyal, a korábban tanult idegen nyelvet folytatják. A 2016-2017-es tanévtől a két szakirány esetében – katasztrófavédelmi műveleti és iparbiztonsági – már bementi követelményként lett meghatározva a nyelvvizsga bizonyítvány. Ezen hallgatók esetében lehetőség van egy második idegen nyelvet tanulni vagy a korábban tanultat folytatni magasabb szinten, szaknyelvi elemekkel is bővítve. Ezen a módon a hagyományos nyelvtanulás mellett kibővülnek az ismereteik a szakmájuk idegen nyelvi aspektusaival is. A Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézetén belül a Tűzvédelmi és Mentésirányítási szakirányon lehetőség volt már többször a hallgatók számára részt venni külföldi szakmai

gyakorlatokon, köszönhetően az Erasmus+ programoknak vagy egyéb pályázatoknak. Ezen a módon kombinálva jelentősen növelhető a szakmai gyakorlat és egyben az idegen nyelvtudási készség. Ebben a kérdéskörben a katonai felsőoktatásban zajló idegen nyelvi képzés jó tapasztalatokkal szolgál. Tekintettel arra, hogy a személyek között együttműködés a NATO egyik alapköve, a közös, országok közötti képzési rendszer ezt megalapozza a nemzeti katonai oktatásban és a gyakorlatok során. Ez később megfelelően ráépíthető az úgynevezett törzstiszti terminológiai nyelvtanfolyamra. [14]

KÖVETKEZTETÉSEK

A jelen cikk ismertette Magyarország helyzetét a nemzetközi közlekedési viszonylatban. Itt külön hangsúlyt kaptak a nemzetközi szállítmányozási vagy a személyek turisztikai és egyéb célú átutazásai az ország területén, amely által megnő a magyar nyelvet nem beszélők jelenléte. Magyarország példáján keresztül a szerzők ismertették ennek hatásait a katasztrófavédelmi, tűzoltósági beavatkozásokra. Ismertették továbbá azokat a beosztásokat az elsődlegesen beavatkozóknál, ahol az idegen nyelvek tudására jellemzően szükség lehet és annak megléte hatással lehet a beavatkozásra is a sérültekkel való kapcsolattartás vagy az információk beszerzése során. Végül, a szerzők bemutatták, hogy a tűzoltó szakmai felsőoktatásban hogyan történik a hallgatók idegen nyelvi felkészítése a várható kihívásokra.

FELHASZNÁLT IRODALOM

[1] KALAMÁR N., PÁNTYA P.: *A magyar katasztrófavédelem által végzett beavatkozások*, Védelem Tudomány: Katasztrófavédelmi Online Tudományos Folyóirat 1:(4) pp. 88-99. (2016)

[2] RESTÁS Á., PÁNTYA P., HORVÁTH L., RÁCZ S.R, HESZ J.: *A tűzvédelem komplex oktatása a Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézetében,* In: Restás Ágoston, Urbán Anett: Tűzoltó Szakmai Napok 2016. 186 p., Konferencia helye, ideje: Szentendre, Magyarország, 2016.03.02 Budapest: BM OKF, 2016. pp. 177-181. 1-2., (ISBN:978-615-80429-0-1)

[3] Eurostat: *Tourism statistics* http://ec.europa.eu/eurostat/statistics-explained/index.php/Tourism_statistics (21/01/2017)

[4] *Hungarian Central Statistical Office: Number and expenditure of foreign visitors in Hungary* http://www.ksh.hu/docs/hun/xstadat/xstadat_evkozi/e_ogt002c.html?down=95 (11/01/2017)

[5] Hungarian Central Statistical Office: *Number of foreign nationals in Hungary* http://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_wnvn001b.html?down=525 (11/01/2017)

[6] MÁV Zrt.: *Memberships, partnerships* http://www.mavcsoport.hu/mav/tagsagok-egyuttmukodesek (12/01/2017)

[7] Rail Net Europe: *Rail Freight Corridors* http://www.rne.eu/rail-freight-corridors-rfcs.html (12/01/2017)

[8] European Conference of Ministers of Transport: National Peer Review Hungary http://internationaltransportforum.org/pub/pdf/04UrbHungary.pdf (12/01/2017)

[9] Hungarian Central Statistical Office: The Length of Motorways http://www.ksh.hu/docs/hun/eurostat_tablak/tabl/ttr00002.html (11/01/2017)

[10] *Act XLII of 2015 on the Service Status of Professional Members of Law Enforcement*

[11] PÁNTYA P.: *What could help for the firefighting, technical rescues*?, In: Stefan Galla, Andrea Majlingova, Boris Toman, Advances in Fire, Safety and Security Research 2015. Bratislava: Fire Research Institute of the Ministry of Interior Slovak Republic, 2015. p. 60.

[12] RESTÁS Á. – BLESZITY J. – GRÓSZ Z. – KRIZSÁN Z.: *New Training for Disaster Management at University Level in Hungary:* Presentation of the multi-cycle system on the field of public administration, law enforcement and military training concerning the faculty of disaster management; *NISPAcee Government vs. Governance in Central and Eastern Europe: From Pre-Weberianism to Neo-Weberianism? Presented Papers from the 22nd NISPAcee Annual Conference*, Budapest, 2014 ISBN: 978-80-89013-72-2

[14] UJHÁZY L.: *Allied Joint Force Command Headquarters Brunssum's Deployed Joint Forces Headquarters Trainin*g. AARMS, 2008/3, pp. 445–451 ISSN: 1588-8789

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

RELEVANT DECONTAMINATION TASKS CARRIED OUT BY FIREMAN UNITS

TŰZOLTÓ EGYSÉGEK ÁLTAL VÉGZETT VEGYIMENTESÍTÉS AKTUÁLIS FELADATAI

KUTI Rajmund

(ORCID ID:0000-0001-7715-0814)

kuti.rajmund@sze.hu

Abstract

Classical decontamination is a process aims to eradicate the environment-damaging effects of human, natural and constructed environment. It has been carried out primarily by military units, therefore the action steps have been developed accordingly. However in recent years, during eliminating the consequences of several industrial and traffic accidents, the activity performed most often by firefighter units has come into view. Special tools and discharge materials were provided to perform their duties, so it was necessary to change the steps of the procedure. To perform effective decontamination, specially trained executive staff is required, people who are qualified for operating special equipment, devices, and for applying the latest methods. To maintain the expertise and practical skills of the staff, a high level theoretical and practical training is required, where the steps need to be improved continuously. In this article, I systematized and compiled basic tasks which are necessary for firefighter units to execute theoretical and practical training of decontamination, in such a way, that with their application the simplified decontamination tank designed by myself can be safely operated. With this research, I would like to contribute to increasing the efficiency of theoretical and practical training.

Keywords: *chemical decontamination, training, training levels, practices, control*

Absztrakt

A klasszikus vegyimentesítési eljárás a mérgező vegyi anyagok humán, természeti és épített környezetet károsító hatásainak a felszámolására irányuló folyamat, elsősorban katonai egységek végezték, lépései ennek megfelelően kerültek kifejlesztésre. Az utóbbi években a különféle ipari és közlekedési balesetek következményeinek felszámolása során került előtérbe a tevékenység, melyet leggyakrabban a hivatásos tűzoltó egységek végeznek. A feladatokhoz speciális eszközök és mentesítő anyagok kerültek rendszeresítésre, ennek megfelelően kellett az eljárás lépéseit módosítani. A hatékony vegyimentesítéshez a speciális eszközöket működtető, a legújabb módszereket alkalmazó, különlegesen kiképzett végrehajtó állomány szükséges. Az állomány szaktudásának, gyakorlati készségeinek szinten tartásához, magas szintű elméleti és gyakorlati kiképzésre van szükség, melynek lépéseit folyamatosan fejleszteni kell. Cikkemben a tűzoltó egységek vegyimentesítésre történő elméleti és gyakorlati kiképzéséhez szükséges alapvető feladatokat rendszereztem és állítottam össze olyan módon, hogy alkalmazásukkal az általam tervezett egyszerűsített vegyimentesítőhely biztonságosan üzemeltethető lehessen. Kutatásaimmal az elméleti és gyakorlati kiképzés hatékonyságát kívánom növelni.

Kulcsszavak: *vegyimentesítés, kiképzés, képzési szintek, gyakorlatok, ellenőrzés*

A kézirat benyújtásának dátuma (Date of the submission): 2017.05.15.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.08.

INTRODUCTION

Due to the development of science, the amount of produced and used chemicals is constantly increasing. Unfortunately, this process also involves the occurrence of chemical-related accidents. The units of organizations dealing with various remediation are exposed to the presence of increasing number of special and hazardous substance during interventions. Investigators come into contact most likely with hazardous materials within the scope of ADR[1], when transportation accident occurs. These materials contain compounds which are harmful to human health and environment as well. In these cases, interventions are operated in special protective equipment due to toxicological effects of the hazardous substances, and full personal and equipment decontamination shall be carried out as the closing phase of the works. Decontamination covers efforts to eliminate or minimize adverse impacts on the environment, designed to remove or neutralize toxic materials from persons, different landmarks, surfaces of devices, water and air within a minimum amount of time [1]. Decontamination requires special equipment and material which is effectively applied by specially trained personnel [2]. L. Földi [3] and Z. Grósz [4] deal with the steps of decontamination in detail, but they only applied it in military environment. I have to point out that the process carried out by firefighter units differs from the classical military decontamination process as per the tools used and as per executive staff as well, so there is a difference in training tasks also. I deal with the current tasks of this special training.

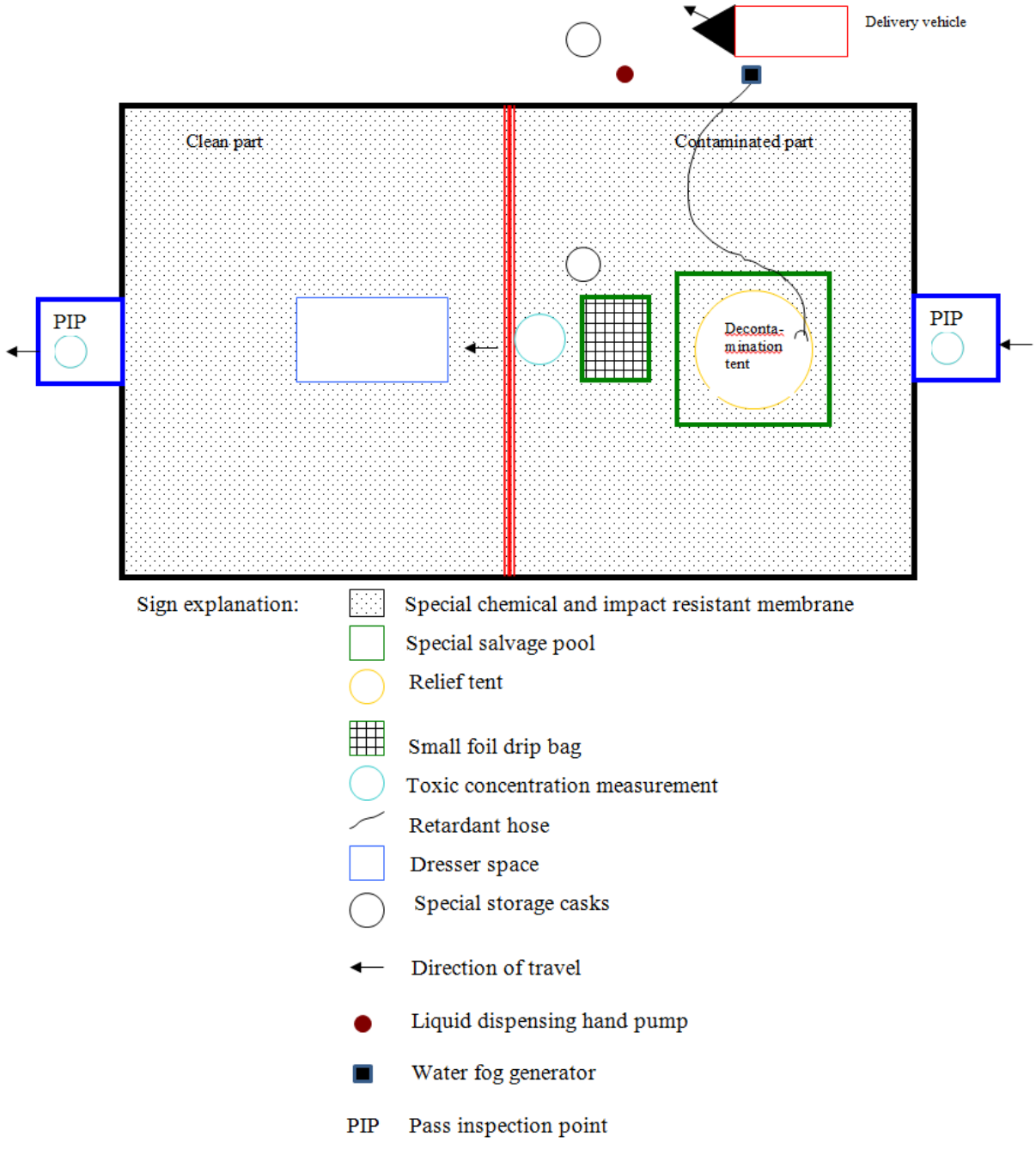
DESIGN REQUIREMENTS OF SIMPLIFIED CHEMICAL DECONTAMINATION

For the efficient and environmentally friendly chemical discharge, there is a need of formation of special discharge space regarding to person and equipment. One of the most appropriate tool to spray out decontamination liquid is mobile water fog generator and the DS 10 manual pumping liquid dispenser [5]. The minimum equipment necessary to design decontaminating site, to ensure the safe disposal of the process and to store hazardous substances, are the following:

- Special chemical and impact resistant membrane 10x4 meter 1pcs, (+1 spare),
- Special Salvage Pool 1.5x1.5x0.2 meters,
- Special plastic Damage Rescue 0,5x0,5x0.2 meters,
- Relief Tent,
- UNIJET FOG Water mist extinguishing equipment with removable console,
- Hand pump fluid dispensing unit (DS10),
- In a container, at least 100 liters of water (for mixing solution in unit),
- Universal decontaminating Emulsion (Kärcher TDE 202),
- Universal hazardous material storage, lockable container 200 liter (+1 pcs.),
- Hazardous material storage, lockable barrel of 120 liters (+1 pcs.),
- Special chemical storage foil bag 200 liters 2 pcs. (+2 pcs),
- Special chemical storage foil bag 120 liters 2 pcs. (+2 pcs),
- Single Use Protective Clothing (TYVEK), 2 pcs. (+2 pcs),
- Complete Respirator (2pcs.) + reserve bottle (2 pcs.),
- Liquid dispensing hand pump,
- Disinfectant/Antiseptic hand wash unit for the exempted/disabled person.

1 Accord europeen relatif au transport international des marchiandises dangereuses par route (European Convention on the international carriage of dangerous goods by road)

The disposal of the devicesmentioned above is preferably carried out in the loading space of a carrying vehicle, thereby creating the conditions for the establishment of discharge site as soon as possible. The outline of the decontaminating site from the above-mentioned devices can be seen in the following figure:



1. Figure: Schematic diagram of the design of decontamination site.

(Source: Composition of the author)

THE PURPOSE OF TRAINING

Some subtasks of the decontaminating tasks performed by the forces of Hungarian Armed Forces are carried out by separate subunits. There are no available separate subunits for simplified decontamination tasks carried out by firefighting forces, to form and operate the

discharge area described above, moreover to operate the devices, only five persons are necessary. It is of particular importance that the interveners are able to complete all the subtasks and manage all the tools. The qualitative education of firefighters is the most important social aspect of disaster management, which covers the area of general and special training based on the latest results of disaster science [6].

It is important to accomplish these tasks carefully, without fail, and if an accident or technical failure occurs, the staff needs to be aware of what to do when necessary. During interventions involving dangerous substances it is particularly needed to implement a thorough decontamination because material spill or incomplete removal could lead to health damage and in severe cases to death [7]. It is also a main objective to enable involved staff to master the steps for identifying hazardous substances, the use of necessary equipment and devices, proper use of equipment used during decontamination and in addition to learn to fulfil tasks safely in the presence of hazardous substances.

LEVELS OF TRAINING

Emergency situations may arise during hazardous material accidents, where liquidation needs greater preparedness and perfect training. The specialized training – like decontamination training – means practical application of the acquired theoretical knowledge and creation and development of skills [8].

Taking into account the aspects of decontamination, the following knowledge should be acquired for the staff involved:

Knowledge level:

- Structure, functions and administration of the organizations intended to damage recovery,
- Basic knowledge of hazardous materials,
- Grouping specialized equipment for different interventions.

Comprehension level:

- Service levels stratification, formalities, contact rules and the order of the instruction implementation
- Requirements, rules relating to the presence of hazardous substances,
- Equipment used during interventions, applicability of specialized equipment, properties of release agents,
- The use of Intervention Policy, physical requirements on persons who carry out the intervention.

To know at the level of proficiency:

- Various remedial implementation of complex tasks,
- Decontamination-related tasks professional completion.

Readiness / skill level:

- Rules applied in the use of personal protective equipment, protective clothing during interventions depended on the presence of hazardous materials
- The application of the procedure is necessary to identify dangerous substances, comprehensive technical devices, rules of instruments.

The only way to guarantee success during intervention in the presence of hazardous materials is when the fastest possible installation of technical tasks are performed equipment relying on the use of specified. Every step of the process is based on a theoretical education, properly described above in the planned levels of knowledge and practical training. This especially refers to each step of decontamination [9].

THE PHASES OF TRAINING

For relevant training, the application of the following stages is essential:

- At theoretical level, it is necessary to master the rules for mixing the solutions required for the decontamination, the use of necessary technical equipment and technology tools, and each step of the discharge process,
- The theoretical knowledge must be transposed into practice, for which practices should be planned and organized. The exercises should be extended to the exercise of the various sub-processes, it should be implemented over a complex exercise according to the following sub-processes.
- The complex practices should always imitate realistic conditions as far as possible.

During each exercise, attention shall be paid to avoid finishing the practice by performing the decontamination duties, the staff needs to master the handling, copying, storage and post-work tasks of the hazardous substances.

COMPLEX REMEDIAL EXERCISES

Intervention performing organizations might not be prepared to a possible elimination of consequences of terrorist acts or a protracted and complex remediation in the presence of hazardous substances [10]. For effective remediation, it is extremely important to maintain the simulation exercises whereby the logistical, medical and technical assistance tasks should also be addressed. Transported hazardous materials could be in solid, liquid and gaseous consistency. During an accident, it must be taken into account that the substances could be released to the environment or transhipped which can cause more problems for liquidation investigators. These problems are needed to be aligned for the participants in the practice also. It is important to acquire the use of additional equipment, special hoses, pumps and drip equipment to trans load, absorb and clear away various hazardous substances. The staff must be prepared of the rules of operation of flares equipment because the trans loading is not easy at the case of frozen liquefied flammable gases. During practices, all attention should be paid on the strict adherence to the necessary precautions while trans loading and transhipping, keeping in mind the environmental safety issues and the environmental tasks should also be addressed [11]. The staff must be prepared to face the challenges resulting from the effects of global warming as well [12].

Considering the facts above, it can be concluded that those remedial exercises which includes intervention and then discharge, in the presence of a hazardous substances where all the steps in handling hazardous materials can be exercised, are not easy to perform regularly. Accordingly, the training should be accomplished in smaller units. It is necessary to separate the practise of smaller steps (e.g.: development of chemical decontamination place, preparation of decontamination solutions, operation of disposal facilities, working in full-body protective clothing, personal and equipment decontamination) which should lead through the whole exercise. Every step must be checked section by section, only flawless execution allows to proceed, and then, in conjunction with the subtask, to examine the whole process in a complex exercise.

THE PLAN OF EXERCISES

During my professional career, I have participated in several interventions in the presence of hazardous substances, so I managed to get liquidation-related experiences, which I could exploit later during missions and planning exercises. As more organizations took part in the remediation, the key objective in the phase of planning and implementing during the exercises was to understand all organizations rescue capabilities and tools, joint problem solving, communication and developing flexible management mechanism.

Therefore, that is why the planning of complex exercises is important, so that chemical decontamination could be inserted exactly into the intervention or the algorithm of remediation [13].

When planning the practices of these functions, it is appropriate to mention:

- Steps after the elimination of hazardous materials accident should be acquainted with the staff concerned according to guidelines set out,
- Exercise intervention in full personal protective equipment (protective gas tight suits, respirators, gas masks),
- Fast, professional implementation of life rescue tasks,
- Practice tactical steps set out on the subject, mounting types,
- Solving Communication Problems,
- Exercise the steps of the chemical discharge procedure, application necessary time constraints of installing and commissioning the equipment [14].

It is advisable to elaborate thoroughly the tasks of the participants in control and the executers, and to revise them later depending on their practical experience. The plans shall be supplemented with power calculation and tactical asset-site drawing [15].

MONITORING THE EFFICIENCY OF DECONTAMINATION

The exercises should be monitored closely when controlling the effectiveness of chemical decontamination. It has a great importance at personal exemption. Protective full-body clothing is made of special materials, which repellent the liquid got on its surface. This phenomenon is easy to observe in practice, water should be sprayed on the protective cloth and water should be watched how it quickly runs off the material. It is hard to tell if the water got on all parts of the clothing, because of its repellent effect. The special discharge solutions contain surfactants, precisely in order to be able to stay on the contaminated surface until the chemical process is complete.

These substances increase the wettability of the solution discharge and improves dispersion on surfaces being exempted. The presence of surfactants on the cloth is not able to quickly repel the discharge solution from the surface, so it can be examined where are those places where the liquid has not reached, and the discharge there must be continued. During the procedure, the check passes (EÁP) should also be subjected to instrumental checks for which the necessary instruments are available in Disaster Relief Mobile Laboratories (KML).

CONCLUSIONS

The intervening staff of damage elimination organizations is often confronted with hazardous substances at various exposed locations. I found that in the case of staff training for these tasks has ongoing and outstanding actuality. In order to ensure a smooth and effective damage elimination, the emphasis should be placed on the training of controlling and intervening staff, particularly with regard to the interventions on hazardous chemicals and chemical discharge tasks.

SUMMARY

The challenges and threats of today's modernization all justify the need for the continuous development of tools and tactics needed for elimination of damages in the presence of dangerous substances.

At present, the greatest threat is caused by fire events and extreme weather conditions due to global climate change, and beyond these accidents involving hazardous chemicals and chemical disasters. To eradicate all these damage events, a highly skilled and experienced personnel is required.

In my article, I have systematized and constructed the basic tasks of the theoretical and practical training required for safe operation of simplified chemical discharge space I designed so that the process can be efficiently implemented by applying them.

It is essential to ensure the necessary intellectual and financial conditions for quality education and effective training, as well as to maintain knowledge level of executive staff.

REFERENCES

[1] KUTI R.: Vegyimentesítőhely kialakításának követelményei, az eljárás személyi és technikai feltételei, Védelem katasztrófa- tűz– és polgári védelmi szemle, XVIII. / 1. (2011) 26-27. p. http://vedelem.hu/letoltes/ujsag/v201101.pdf (downloaded: 06. 04. 2017.)

[2] HALÁSZ L., FÖLDI L., PADÁNYI J.: Climate change and CBRN defense. *Hadmérnök*, VII./ 3. (2012), http://hadmernok.hu/2012_3_halasz_padanyi_foldi.pdf 42 –49. (downloaded: 13. 04. 2017.)

[3] FÖLDI L.: A Magyar Honvédség tevékenysége a vegyi katasztrófák elleni védelem összefüggés rendszerében, PhD értekezés, ZMNE Budapest, 2003

[4] GRÓSZ Z.: ABV Védelem alapjai, Tankönyv, ZMNE Budapest, 2003

[5] KUTI R., FÖLDI L.: Possible use of mobile water fog generators for decontamination tasks, AARMS Academic and Applied Research in Military Science Vol. 8, Issue 1 (2009) 127–132. p. http://www.zmne.hu/aarms/docs/Volume8/Issue1/pdf/12kuti.pdf (downloaded: 13. 04. 2017.)

[6] PAPP B.: Az állami szintű katasztrófavédelem elemzési szempontjai nemzetközi környezetben. Védelem Tudomány 2, (2017/1) 263-284. p. http://www.vedelemtudomany.hu/articles/19-papp.pdf (downloaded 02. 10. 2017.)

[7] KUTI R.: Milyen mentesítő anyagokat használjunk, milyen eljárásokat alkalmazzunk veszélyes anyag beavatkozások után? Védelem Online: Tűz-és Katasztrófavédelmi Szakkönyvtár 203, (2008) 1-6. p. http://www.vedelem.hu/letoltes/tanulmany/tan203.pdf (downloaded: 13. 04. 2017.)

[8] MÉSZÁROS L: Pedagógia I. Egyetemi jegyzet, ZMNE Budapest, 2004

[9] HORVÁTH G., KUTI R.: Об опыте базовой подготовки профессиональных пожарных к проведению аварийно-спасательных работ в Венгерской Республике, УДК 614.8, АКАДЕМИЯ ГПС МЧС России (Москва 2011), 1-6. п. http://agps-2006.narod.ru/ttb/2010-5/03-05-10.ttb.pdf (downloaded: 13. 04. 2017.)

[10] KUTI R.: Terrorcselekmények kárfelszámolási lehetőségeinek vizsgálata tűzoltói aspektusból, Védelem katasztrófa- tűz– és polgári védelmi szemle, XIV. / 3. (2007) 34-35. p. http://vedelem.hu/letoltes/ujsag/v200703.pdf (downloaded: 13. 04. 2017.)

[11] FÖLDI L., HALÁSZ L.: Környezetbiztonság, Complex Kiadó Budapest 2009, 20.p.

[12] HALÁSZ L., PADÁNYI J., FÖLDI L.: Improving the CBRN defence of combat vehicles as a response to the challenges of climate change, Economics and Management, Published by the University of Defence in Brno, VII. / 3. (2013) 31-38. p. http://www.unob.cz/en/Eam/Documents/EaM%203-2013.pdf (downloaded: 13. 04. 2017.)

[13] PADÁNYI J., FÖLDI L.: Tasks and Experiences of the Hungarian Defence Forces in Crisis Management, CONTEMPORARY MILITARY CHALLENGES/SODOBNI VOJASKI IZZIVI 17 / 1. (2015) 29-46. p.

[14] KUTI R: Műszaki Mentések I.-II- Egyetemi jegyzet, ZMNE Budapest, 2007,

[15] KUTI R.: Komplex műszaki mentések tervezésének lehetőségei, Védelem Online: Tűz- és Katasztrófavédelmi Szakkönyvtár, 233, (2010) 1-7. p. http://www.vedelem.hu/letoltes/tanulmany/tan233.pdf (downloaded: 13. 04. 2017.)

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

AZ INFORMÁCIÓBIZTONSÁG ALAPKÉRDÉSEI

THOUGHTS ON INFORMATION SECURITY

GÉMES Csaba

(ORCID: 0000-0003-3012-2175)

gemes.csaba@uni-nke.hu

Absztrakt

A hírekben mind sűrűbben megjelenő hacker-támadások, vagy a médiában szereplő külföldi és hazai kibervédelmi feladatok hallatán, tudományos munkákban, munkahelyi tájékoztatókon, de még iskolai tananyag-tervezetként is egyre gyakrabban találkozhatunk az elektronikusan kezelt adatok biztonsági kérdéseivel, egy szóval az információbiztonsággal.
De mi is az az információbiztonság? Múló divat, vagy valóban fontos kérdés, amellyel foglalkozni kell? Mit és miért kell védeni? Kinek és mit kell, vagy lehet tennie? A cikk szerzője ezekre a kérdésekre keresi a választ.

Kulcsszavak: *információbiztonság, informatikai biztonság*

Abstract

As more frequently appearing the news of hacker attacks, and foreign and national cyber defence tasks in the media were found, over and above in the scientific works, job briefings, and even the school curriculum draft more and more often we can meet electronically handled data security issue, in one word: information security.
But what is information security? Only fashion, or indeed important to deal with it? What should be protected and why? Who and what you should or can do? The author seeks to answer these questions.

Keywords: *information security, Information Assurance INFOSEC, IT security*

A kézirat benyújtásának dátuma (Date of the submission): 2017.07.03.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.27.

BEVEZETÉS

A hírekben mind sűrűbben megjelenő hacker-támadások, vagy a médiában szereplő külföldi és hazai kibervédelmi feladatok hallatán, tudományos munkákban, munkahelyi tájékoztatókon, de még iskolai tananyag-tervezetként is egyre gyakrabban találkozhatunk az elektronikusan kezelt adatok biztonsági kérdésivel, egy szóval az információbiztonsággal. A téma aktualitását mutatja, hogy 2016 júniusában a NATO varsói csúcstalálkozóján az elektronikus formában lévő információ létezési közegét jelentő kiberteret hivatalosan is elismerik ötödik műveleti dimenzióként a korábbi négy fizikai (szárazföldi, légi, tengeri, kozmikus) hadszíntér mellett. [1]

A téma egyre magasabb szinten és egyre gyakoribb megjelenése indokolttá teszi, hogy kiemelt figyelemmel foglalkozzunk az információbiztonsággal. Már a téma szakirodalmának felületes tanulmányozásából is megállapítható, hogy a megoldandó probléma igen összetett, megoldására különböző biztonságszervezői (menedzsment) módszerek vannak, amelyek megértéséhez, további tanulmányozásához elkerülhetetlen az információbiztonság alapkérdéseinek tisztázása. E cikk célja az információbiztonság alapkérdéseinek áttekintése, a biztonság kialakítására és fenntartására alkalmazható módszerek vizsgálatának megalapozása érdekében.

AZ INFORMÁCIÓS TÁRSADALOM

Az információbiztonság alapkérdéseinek vizsgálatát kézenfekvő egy rövid történeti áttekintéssel kezdeni, amely rávilágit az információbiztonság fontosságára is.

Az ősidőkig visszatekintve megállapítható, hogy az információk megszerzésére, illetve annak megakadályozására való törekvés – vagyis az információ védelme – a beszéd megjelenésével párhuzamosan, az első emberi társadalmak kialakulásával egyidős tevékenység: „Már az ősközösségi társadalmakban is „lopták” az információkat, amikor megpróbálták kifürkészni a másik közösség vadászati szokásait vagy túlélési praktikáit”. [2: 251]

Ebből következően az információbiztonság története az őskorig vezethető vissza. Természetesen a társadalmi fejlődéssel együtt a megszerzendő információk köre, megjelenésének formája, keltezésének módja, valamint ebből következően az információ megszerzéséhez felhasználható, illetve ennek megakadályozásához szükséges módszerek is folyamatosan fejlődtek.

Az ókorban az írás megjelenésével az információ rögzített formában is tárolhatóvá és továbbíthatóvá vált, ezzel átlépve az emberi emlékezőképesség és a személyes közlés határait. Az írás megjelenésével lehetőség nyílt az információ változatlan formában és emellett nagyobb mennyiségben való tárolására és továbbítására is. Az információ pontos és bizalmas átadása többé már nem igényelt a személyes találkozást. A hírnökök, futárok a szóbeli helyett már írásos közleményt továbbítottak, így a korábban jellemzően kis mennyiségű, esetenként torzítottan átadott hír helyett nagy mennyiségű, sértetlenül átadott információ hordozóivá válhattak ráadásul úgy, hogy annak tartalmát sem kellett megismerniük. Lényegében megállapítható, hogy az írás megjelenése forradalmasította az információ kezelését. Természetesen, mint minden új technológia, az írásos közleménytovábbítás is rejtett magában új kockázatokat, ahogyan a hírvivő elfogásával a teljes és valós szövegű üzenet elfogása történt meg, amelyet felhasználhattak. Fennállt annak a veszélye is, hogy az elfogott üzenet helyett, vagy akár előzmény nélkül is küldhető olyan félrevezető üzenet, amelyet a címzett az írás hiteleségében bízva valósnak vélt.

Biztonsági szempontból nézve az új információkezelési módszerek új biztonsági lehetőségeket is nyújtottak, amelyek kiaknázására szükség is volt az új kockázatok csökkentése érdekében. Az írásos közleménytovábbításnak voltak önmagában rejlő biztonsági funkciói is, mint ahogyan a hírvivő hozzáférésének lehetősége már eleve korlátozottabb egy lezártan továbbítandó üzenet esetében a szóbeli információhoz képest. Kezdetben az írástudók alacsony számából eredően maga az írás is védettséget jelentett, majd megjelentek a különböző algoritmusú titkosítások, jelszavas, és rejtjelzési megoldások is. [3]

Az írás megjelenése szerepet játszott az ókori államok kialakulásában is, amelyek irányításában, működésében meghatározó szerepe volt hatalmi szempontból érzékeny információk kezelésének. Ennek fényében nem meglepő, hogy már az első ókori államok eszközrendszerében megjelenik a kémkedés és ezzel együtt az elhárítás is. [4]

A középkor jeles eseményei közül témánkhoz kapcsolóan ki kell emelni a könyvnyomtatás feltalálását,[1] amely információtechnológiai szempontból a nagy mennyiségben való sokszorosítás és a széles körben való hozzáférés előnyei és az ezzel járó biztonsági problémák megjelenése szempontjából jelentős. Másrészt – a tudomány oldaláról megközelítve – a könyvnyomtatás az újkori technológiai fejlődést megalapozó műszaki tudományok kialakulása, fejlődése és elterjedése szempontjából is kiemelt szerepet játszott.

Az újkori társadalom fejlődésébe a tudományos, majd ennek hatására a több hullámban országonként akár néhány évtizedes eltéréssel végbemenő ipari forradalmak számtalan technikai újítást hoztak. A megjelenő új technológiák közül a távíró, a telefon és a rádió megjelenésével létrejön elektronikus hírközlés, amely az információk gyors és nagy távolságra való eljuttatásának következményeként összezsugorodik a világ. Itt kell megjegyezni, hogy a rádió katonai alkalmazásával szinte egyidejűleg megjelenik a kisugárzott információ lehallgatása és a zavarása is, majd megtörténnek az ezek elleni első válaszlépések, amelyekről már elektronikus információvédelmi intézkedésként beszélhetünk.

Az ipari forradalmak a technológiai fejlődésen túl komoly társadalmi-gazdasági változásokat is eredményeztek A munkaerő megoszlás változásainak vizsgálata alapján megállapítható, hogy 19–20. század fordulóján a mezőgazdaságban dolgozók számát meghaladta az iparban, majd az 1960-as évektől[2] az információs szektorban dolgozók száma. [5]

A távközlés fejlődése, a műsorszóró rádióadások, a televízió elterjedése már a 20. század közepétől hajtotta az információs technológia fejlődését, amely a századvégre a személyi számítógépek, hálózatok, internet, multimédia elterjedésével robbanásszerű mértéket öltött. A fejlődéshez szükséges ipari termelés, az információtechnológia magán, vállalati, és állami szférában egyre elterjedtebb alkalmazása, komoly társadalmi változásokat is hozott. A gépipari tömegtermelésre épülő ipari társadalom fokozatosan átalakult a tudásra, információra és információtechnológiára alapuló „posztindusztriális”[3] vagy az 1970-től elterjedő kifejezéssel[4] „információs társadalommá”. [6]

---

[1] Európában Johann Gutenberg mainzi aranyműves által, a korábbi ázsiai nyomtatási módszerektől feltehetően függetlenül 1450 körül megalkotott, mozgatható nyomóelemek széles körű használatával történő technikai eljárás. (Wikipédia: Johann Gutenberg)

[2] Országonként eltérő a technológia fejlettség függvényében Az USA-ban 1967 Daniel Bell munkája [Bell] alapján.

[3] Daniell Bell amerikai szociológus preindusztriális – indusztriális – posztindusztriális felosztása alapján.

[4] Yoneji Masuda japán származású szociológus használta egy konferencián.

Napjainkban a rohamosan fejlődő technológia, illetve az általa nyújtott lehetőségek, szolgáltatások egyre nagyobb mértékű kihasználásának elkerülhetetlen következménye az ezzel járó veszélyek – szakmai szóhasználattal élve a fenyegetések – hatványozott mértékben történő növekedése is. Ezen fenyegetések által okozható károk kiemelt jelentőséggel bírnak, amelyek elkerülése illetve csökkentése érdekében lépéseket kell tenni.

BIZTONSÁG ÉS VÉDELEM

Az előző történeti áttekintéssel képet kaphattunk az információbiztonság kialakulásáról és fontosságáról. Ebben a fejezetben körül járjuk, hogy egyáltalán mi is az a biztonság, milyen területei vannak, illetve kialakulásához milyen alapelveket kell figyelembe vennünk.

A biztonság és védelem közötti különbség

Az információs társadalom kialakulásának folyamata mutatja, hogy hogyan és milyen történelmi távlatokban gyökerező kihívásokra való válaszlépésként jött létre az információbiztonság (vagy információvédelem). Szinte magától értetődő, hogy a témakör további részletezéséhez elkerülhetetlen a „biztonság” a „védelem” illetve a külföldi szakirodalomban használt megfelelőjük értelmezése.

A biztonság és védelem, különböző megközelítésből született megfogalmazásaiból színes képet mutat a szakirodalom. [7: 5–9] [6: 19] A két kifejezés használata közötti különbség a magyar nyelvben jól körvonalazódik. A biztonság egy megkívánt – kialakítandó és fenntartandó – állapotot jelent, a védelem pedig a biztonság eléréséhez és fenntartásához szükséges tevékenységet. Az angol nyelvű szakmai terminológiában mindkét értelemben a „security” (biztonság) szót használják. Habár a „defence” szó néha az információ „védelem”-ként is előfordul, leginkább a fizikai és katonai értelemben vett védelemként használatos, hasonlóan a „safety” (biztonságos) kifejezéshez. A NATO és az USA terminológiájában a magyar „biztonság” és „védelem” szavak mindegyikét kifejező „security” mellett leggyakrabban a „Information Security” rövidítéséből származó „INFOSEC” kifejezést használják. Ezen kívül egyre gyakrabban találkozhatunk a garanciának, garantált vagy szavatolt védelemnek fordítható „assurance” kifejezéssel is.

Az információt az „Information Assurance” (a továbbiakban: IA) elveit alkalmazva kell védeni, amely védelmi intézkedésekkel teszi elérhetővé a kommunikációs, informatikai és egyéb elektronikus és nem elektronikus információs rendszerek, valamint a tárolt, feldolgozott és továbbított információk elvárt biztonsági szintjét a bizalmasság sértetlenség, rendelkezésre állás, letagadhatatlanságát és hitelesség vonatkozásában. [8: Ann. 1]

Az INFOSEC és az IA fogalomkörét összehasonlítva elmondható, hogy az INFOSEC kimondottan az elektronikus információs rendszerek és az abban kezelt adatok védelmét tűzi ki céljául [9] egyenértékűen a magyar „elektronikus információbiztonság” fogalomkörrel, míg az IA az információk és információs rendszerek mindegyikére értelmezendő, beleértve a nem elektronikus rendszereket is. [10]

Az információbiztonság területei

A biztonság alanya szerint számtalan „biztonság” létezik, amelyekből jelen írásban csak az információbiztonsággal foglalkozunk, azon belül leginkább az elektronikusan kezelt információk biztonságára fókuszálva. Joggal merül fel a kérdés, hogy az információbiztonságnak milyen egyéb területei vannak és azok milyen viszonyban állnak egymással.

Az információbiztonság általánosan elfogadott nézet szerint személyi- fizikai- dokumentum- (vagy adminisztratív) biztonsági, valamint elektronikus információbiztonság területekre osztható fel.

A hazai és a külföldi terminológiák összegzésével az elektronikus információbiztonság (INFOSEC) területeiként az átvitelbiztonságot (TRANSSEC), a kompromittáló kisugárzás elleni védelmet (EMSEC/TEMPEST), számítógép és hálózati biztonságot (COMP&LANSEC), valamint a rejtjelzést [CRYPTOSEC] tekinthetjük, de ettől eltérő felosztással is találkozhatunk. [11]

Az elvárt szintű információbiztonság csak úgy alakítható ki, illetve tartható fenn, ha az az információbiztonság, és ezen belül az elektronikus információbiztonság valamennyi területén egyaránt biztosított az ehhez szükséges védelem. Ezt nevezzük a biztonság komplexitásának. [12] A komplex védelem fogalma így egyaránt értelmezhető az információbiztonság, illetve ezen belül az elektronikus információbiztonság valamennyi területére, amelyek összefoglaltan az 1. ábrán láthatók.

1. ábra A komplex információbiztonság elemei [12.]

Biztonsági alapelvek és célkitűzések

Az információbiztonság kialakulásához és fenntartásához elengedhetetlen definiálni azokat a biztonság három attribútumaként, aspektusaként, tulajdonságaként vagy biztonsági célkitűzésként nevezett, kezdőbetűik alapján BSR-nek (angolul CIA-nak[5]) rövidített kritériumokat, valamint egyéb biztonsági alapelveket, amelyek megfelelő szinten történő teljesítése esetén a biztonságot megvalósultnak tekinthetjük.

Ezen biztonsági célkitűzések és alapelvek alapján került meghatározásra a vonatkozó nemzeti jogszabályban [13] az elektronikus információs rendszer biztonságának fogalmai is, amely „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.”

[5] BSR: Bizalmasság, Sértetlenség, Rendelkezésre állás CIA: Confidentiality, Integrity, Availability

A meghatározásban szereplő biztonsági célkitűzések és alapelvek az alábbiak szerint értelmezhetőek.

A bizalmasság az elektronikus rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. [13: para. 1 bek. 8]

A sértetlenség az adatra vonatkozóan azt jelenti, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot, abban, hogy az az elvárt forrásból származik (hitelesség) és a származás megtörténtének bizonyosságát (letagadhatatlanság) is. A sértetlenség a rendszerre vonatkozóan azt jelenti, hogy a rendszerelem rendeltetésének megfelelően használható. [13: para. 1 bek. 39]

A rendelkezésre állás annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek. [13: para. 1. bek. 38]

A zárt védelem elve szerint a védelem kialakítása az összes számításba vehető fenyegetést figyelembe veszi. [13: para. 1 bek. 48]

A teljes körű védelem elve szerint a védelmi intézkedések a rendszer összes elemére kiterjednek. [13: para. 1 bek. 44]

A folytonos védelem elve az időben változó körülmények és viszonyok ellenére is folyamatosan megvalósuló védelmet jelenti. [13: para. 1 bek. 21]

A kockázatokkal arányos védelem alapelve rögzíti, hogy a védelem költségeinek arányosnak kell lenniük a fenyegetések által okozható károk értékével. [13: para. 1 bek. 31]

A fejezet összegzéseként megállapítható, hogy az információbiztonság egyidős az emberi társadalommal, ahogyan az elektronikusa információbiztonság is az elektronikus adatkezelés megjelenése óta létezik. Az új technológiák új kockázatokat hordoznak magukban. Ebből következően napjaink információs társadalmában az életünket egyre szélesebb körben átszövő és egyre összetettebb információs technológia alkalmazása egyre magasabb kockázattal jár, amelyet megfelelő biztonsági intézkedésekkel csökkenteni kell. A fogalmak vizsgálata során megállapítható, hogy a terminológia elég vegyes képet mutat. Megfigyelhető, hogy akár eltérő jelentésű kifejezések akár egymás szinonimájaként is használhatóak, valamint előfordul, hogy egyazon fogalom jelentése még az egymással szorosan összefüggő szakterületek szóhasználatában is eltérő területet fed le. A szakterületek biztonsági szabályzóit vizsgálva még a biztonság területeinek, feladatrendszerének felosztásában is eltéréseket találhatunk. Ugyanakkor az eltérések ellenére megállapítható, hogy az információbiztonság kialakítása és fenntartása szempontjából jelentős biztonsági alapelvek és célkitűzések azonosak.

VÉDENDŐ ÉRTÉKEINK

Adat és információ

A védendő értékek sorában elsődleges fogalomként találkozunk az „információ”-val, illetve a köznyelvben és néha még a szakemberek körében is szinonimaként használt „adat” kifejezéssel. A különböző információelméletekből és szakirodalmi forrásokból eredően mindkét fogalomnak számos definíciója van. [14] Ezek közül szakmai megfontolásból az információbiztonsági törvényben [13] (a továbbiakban Ibtv,) rögzített meghatározásokat célszerű mérvadónak tekinteni, amelyben utalást találunk a két fogalom viszonyára is:

Az *„adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.”* [13: para. 1 bek. 1]

Az *„információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét,*

annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti." [13: para. 1 bek. 25]

A két fogalom információelméleti összehasonlításaként megállapítható, hogy az információ, az adatok értelmezett jelentéssel bíró formájaként magasabb tudati szintet képvisel. [12] Műszaki megközelítéssel vizsgálva ugyanakkor megállapítható, hogy az elektronikus információbiztonság szempontjából elektronikus jelek formájában az információ hordozójaként valójában az „adattal" találkozunk. Ennek ellenére a szakmai szóhasználatban az „információ"- biztonság és védelem a jellemző. „Adat"-biztonságról vagy védelemről szakmai szempontból legfeljebb az elektronikus adathordozók kapcsán eshet szó, ezekkel a szóösszetételekkel jellemzően a személyes és a közérdekű adatok védelmének területén találkozhatunk. A fogalmak angol megfelelőjeként a „data" és az „information" kifejezések használata között ugyanezen különbségek figyelhetők meg.

A két fogalom jelentése a fentiek alapján látszólag egyértelműen elhatárolható, ugyanakkor szövegkörnyezettől függően előfordul, hogy a kifejezések felcserélt használata sem módosít a szöveg értelmén.

A rendszer

Az információ, vagy az annak hordozójaként tekinthető adat biztonságának garantáláshoz elengedhetetlen, hogy az azokat feldolgozó elektronikus információs rendszerek biztonságáról is gondoskodjunk. A különböző rendszerelméletek szerint számos meghatározást találunk az általános értelembe vett információs rendszerekhez is, és ezen belül az elektronikus rendszerre is. A kimondottan elektronikus információkezelő rendszerekre (a továbbiakban: rendszer) vonatkozó fogalom is többféle kifejezés formájában jelenik meg. Csak az általános szóhasználatot alapul véve beszélhetünk „informatikai technológiák" (IT), vagy ennek a szabványok és ajánlások terminológiáiban megjelenő „Információ- és kommunikációs technológiák" (ICT és IKT) kifejezésekről is.

A rendszer fogalmánál érdemes kihangsúlyozni, hogy az elektronikus rendszer fogalmába az „tisztán" informatikai rendszereken és hálózatokon kívül beleértendők az alábbi infokommunikációs rendszerek mindegyike, függetlenül attól, hogy az adott rendszer milyen arányban tartalmaz informatikai komponenseket.

Így elektronikus rendszerként értelmezendők a vezetékes, a mobil, a rádiós és műholdas távközlés; a vezetékes, a rádiófrekvenciás és műholdas műsorszórás; a rádiós vagy műholdas navigáció, automatizálási, vezérlési és ellenőrzési rendszerek (SCADA), távmérő, távérzékelő és telemetriai rendszerek, valamint ezek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek. [15: 124–208]

Az elektronikus információbiztonságra vonatkozó nemzeti, külföldi és nemzetközi szabványok, ajánlások, direktívák, jogszabályok és egyéb szabályzókat megvizsgálva gyakran találkozhatunk s szóhasználatukat tekintve gyakran „informatikai biztonság" címekkel és terminológiával, ugyanakkor tartalmilag szinte minden esetben a bővebb értelemben vett IKT rendszerek biztonságáról esik szó.

A rendszer kifejezés különböző rendszerelméleti és szakterületi megfogalmazása közül a minősített adatok védelméről szóló törvényben [16] (továbbiakban: Mavtv.) szereplő rövid, tömör, lényegre törő megfogalmazást kiemelni, amely szerint az elektronikus adatkezelő rendszer a *„minősített adat elektronikus, elektromagnetikus vagy optikai úton történő kezelésére alkalmas berendezés, módszer és eljárás együttese*". Mindenképpen érdemes még rendszer fogalmát jobban részletező, a személyzettel szabályozással és kapcsolód folyamatokkal kiegészített az Ibtv. szerinti megfogalmazást is megemlíteni, amely szerint az *„elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver*

és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese" [13: para.1 bek. 14b]
A részletes megfogalmazás mellett az Ibtv. az információs önrendelkezési jogról és az információszabadságról szóló törvénnyel [17] való összhangot megteremtése érdekében az adatgazdával összefüggésben is definiálja a rendszer fogalmát az általános megfogalmazással azonos módon. [13: para. 1 bek. 48 (3)]

Egyéb védendő értékek

Az információ biztonságát veszélyeztető fenyegetések csak viszonylag ritkán irányulnak közvetlenül az információra. A véletlen vagy szándékos fenyegetések jelentős része a rendszeren, vagy az azzal kapcsolatban álló tényezőkön keresztül éri a rendszert. Már a rendszer fogalma Ibtv. szerinti megfogalmazásából is látható, hogy a rendszer klasszikus hardver és szoftver komponensein kívül megjelenik az ember, a környezeti infrastruktúra, a hálózat, – a nem feltétlenül elektronikus – adathordozó, mint például a kinyomtatott papír. A megfogalmazás szerint ide tartozik még a rendszer működéséhez szükséges szabályozás és az összes kapcsolódó folyamat is. Következtetésként a védendő értékek közé kell sorolni minden olyan tényezőt, ami a rendszer biztonságos működését befolyásolja. [13: para. 1. bek. 14b]
Természetesen így történik az a minősített adatkezelés esetében is, azzal az eltéréssel, hogy a Mavtv.-hez kapcsolódóan két külön végrehajtási rendelet szabályozza az elektronikus biztonság, [18] illetve a biztonság egyéb területeit. [19] További eltérést jelnet, hogy az elektronikus biztonságról szóló rendelet a Mavtv. által szűkebben értelmezett „rendszer" biztonsága mellett a külön tevékenységként foglalkozik rendszer részeként tekintett rejtjelzéssel, és a hálózatbiztonsággal. A rendeletek tartalmát és szakterületek viszonyát vizsgálva mégis megállapítható, hogy – a rendeleti és a szakterületi elkülönítés ellenére – a személyi-, fizikai-, adminisztratív-, és az elektronikus információbiztonság, illetve ez utóbbi részterületei egymással szoros kapcsolatban állnak a biztonság komplexitásának megfelelően.
A fejezet összegzéseként megállapítható, hogy az elektronikus információbiztonság kialakítása és a fenttartása csak úgy valósítható meg, ha védendő információ mellett gondoskodunk az azt feldolgozó rendszer biztonságáról is, valamint – a biztonság komplexitásának megfelelően – a kapcsolódó személyi-, fizikai-, és adminisztratív biztonságról is. Továbbá a védelemi intézkedéseknek a biztonság garantálásához szükséges mértékben ki kell terjednie minden a rendszer biztonságát befolyásoló személyre, folyamatra, szabályozásra, eszközre, infrastruktúrára és annak használatára.

KÖVETKEZTETÉSEK

Megállapítható, hogy az információbiztonság egyidős az emberi társadalommal, ahogyan az elektronikusa információbiztonság is az elektronikus adatkezelés megjelenése óta létezik. Az információbiztonság aktualitását mutatja, hogy az információs technológia rohamos fejlődéséből adódó lehetőségek kihasználása egyre nagyobb jelentőséggel bír a társadalmi élet minden területén, beleértve a magán-, a vállalati- és a kormányzati szférát is. A technológia fejlődésének, illetve az általa nyújtott lehetőségek, szolgáltatások egyre nagyobb mértékű kihasználásának elkerülhetetlen következménye az ezzel járó veszélyek (fenyegetések) hatványozott mértékben történő növekedése is. Ezen fenyegetések által okozható károk kiemelt jelentőséggel bírnak, amelyek elkerülése illetve csökkentése érdekében a biztonsági alapelvek és célkitűzések megfelelő védelmet kell alkalmazni.

A biztonság tárgyát képező védendő értékek vizsgálata során megállapítást nyert, hogy az információ biztonsága érdekében gondoskodni kell az információt feldolgozó rendszer biztonságáról is. Ezen kívül a biztonság komplexitásából adódóan a védelmi intézkedéseknek

a biztonság garantálásához szükséges mértékben ki kell terjednie minden a rendszer biztonságát befolyásoló személyre, folyamatra, szabályozásra, eszközre, infrastruktúrára is.

A fogalmak vizsgálata során megállapítható, hogy a terminológia elég vegyes képet mutat. Megfigyelhető, hogy akár eltérő jelentésű kifejezések akár egymás szinonimájaként is használhatóak, valamint előfordul, hogy egyazon fogalom jelentése még az egymással szorosan összefüggő szakterületek szóhasználatában is eltérő területet fed le. A szakterületek biztonsági szabályzóit vizsgálva még a biztonság területeinek, feladatrendszerének felosztásában is eltéréseket találhatunk. Ugyanakkor az eltérések ellenére megállapítható, hogy az információbiztonság kialakítása és fenntartása szempontjából jelentős biztonsági alapelvek és célkitűzések azonosak.

A biztonság kialakításához és fenntartásához hozzáértő biztonságszervezői munka szükséges, amelynek támogatására számos menedzsment módszer létezik. Ezen módszerek – az adott szervezet és az elektronikus rendszerei sajátosságainak megfelelő – kiválasztása, önálló vagy együttes alkalmazása igen összetett problémákat vet fel, amelyek hatékony megoldásához a téma részletes vizsgálata szükséges.

FELHASZNÁLT IRODALOM

[1] SZENES Z.: *Meglepetések nélkül. A varsói NATO csúcs értékelése.* http://biztonsagpolitika.hu/kiemelt/meglepetesek-nelkul-a-varsoi-nato-csucs-ertekelese (A letöltés dátuma: 2016. 11. 06.)

[2] MUHA L. (szerk), Az *informatikai biztonság kézikönyve.* 10. javított kiadás. Budapest: Verlag Dashöfer, 2004.

[3] SINGH, S.: *The Code Book – The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* SZENTGYÖRGYI J. (ford.), *(Kódkönyv – A rejtjelezés és rejtjelfejtés története.)* Budapest: Park, 2002.

[4] PIEKALKIWICZ, J: *A kémkedés világtörténete I.* Budapest: Zrínyi Kiadó, 1997.

[5] BELL, D.: Az információs társadalom társas keretrendszere. In. *Információs társadalom I.* 3–33. Budapest: Infonia, 2001.

[6] HAIG Zs.: *Információ, társadalom, biztonság.* Budapest: NKE Szolgáltató Kft., 2015.

[7] MUNK S.*:* Információbiztonság vs. informatikai biztonság. In. *Robothadviselés 7 Konferencia.* Budapest, 2007. 11. 27. http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.pdf (A letöltés dátuma: 2016. 11. 06.)

[8] *C-M(2007)0118 NATO Information Management Policy (NIMP).* Brussels: North Atlantic Council (NAC) – NATO HQ Document, 2008.

[9] *NIST SP 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations.* Gaithersburg: NIST Special Publication National Institute of Standards and Technology – U.S. Department of Commerce, 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (A letöltés dátuma: 2016. 11. 09.)

[10] *SP 800-59, Guideline for Identifying an Information System as a National Security System.* 2003. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf (A letöltés dátuma: 2016. 11. 09.)

[11] *AC/35-D/2004-REV2 Primary Directive on INFOSEC.* NSC and the C3 Board (C3B) – NATO HQ Document, 2010.

[12] HAIG ZS.: *Az információs társadalom információbiztonsága.* Budapest: ZMNE, 2009. jegyzet https://ludita.uni-nke.hu/repozitorium/handle/11410/8514

[13] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV (A letöltés dátuma: 2016. 11. 09.)

[14] MUNK S.: Információs színtér, információs környezet, információs infrastruktúra. *Nemzetvédelmi Egyetemi Közlemények,* 2 (2002). http://m.ludita.uni-nke.hu/repozitorium/handle/11410/1083 (A letöltés dátuma: 2016. 11. 09.)

[15] HAIG ZS., VÁRHEGY I.: *Információs műveletek I. Információs korszak hadügyi forradalma és információs rendszerei.* Budapest: ZMNE, 2004.

[16] *2009. évi CLV. törvény. a minősített adat védelméről.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0900155.TV (A letöltés dátuma: 2016. 11. 11.)

[17] *2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV (A letöltés dátuma: 2016. 11. 11.)

[18] *161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1000161.KOR (A letöltés dátuma: 2016. 11. 11.)

[19] *90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1000090.KOR (A letöltés dátuma: 2016. 11.11.)

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

THE NEED FOR BYOD SECURITY STRATEGY

A BYOD ESZKÖZÖK BIZTONSÁGI STRATÉGIÁJÁNAK IGÉNYE

KADËNA, Esmeralda; KOVÁCS Tibor

(ORCID: 0000-0002-3808-6909); (ORCID: 0000-0001-7609-9287)

kadenaesmeralda@gmail.com; kovacs.tibor@bgk.uni-obuda.hu

Abstract

With the recent advancements in technology and the rapid adoption of smartphones, tablets and laptops, it has become increasingly common for employees to use their own personal devices to perform work-related tasks. This is known as Bring-Your-Own-Device (BYOD). Permitting employees to utilize their own preferred device in the work-place also brings some risk of data loss for the enterprises, whether by employees losing devices or compromising cybersecurity.
This work is based on literature reviewing and two research questions are held: "What are the security risks associated with implementing BYOD in the workplace?" and "What are best practices to create a BYOD strategy in workplace?". Formulating a BYOD strategy is only one side of the equation, the other is the employee education.

Keywords: *BYOD, security risks, strategy.*

Absztrakt

A technika újkeletű fejlődésével, az okostelefonok, tabletek és laptopok gyors átvételével egyre elterjedtebb lett a munkavállalók körében, hogy saját személyes eszközeikkel hajtsanak végre munkához kapcsolódó feladatokat. Ezt a jelenséget BYOD-ként ismerjük (Bring Your Own Device: hozd a saját eszközödet). Az alkalmazottak számára annak engedélyezése, hogy saját, előnyben részesített eszközeiket hasznosítsák az munkahelyen, a vállalati adatvesztés kockázatát is magában hordozza, akár az eszköz elveszítésével, akár a biztonság veszélyeztetése által. Jelen munka a vonatkozó irodalmi áttekintésen alapul, miután két kérdést vet fel: Melyek azok a biztonsági kockázatok, amelyek a BYOD munkahelyi bevezetésével együtt járnak? Valamint: Melyek azok a legjobb gyakorlatok, amelyek a BYOD stratégia munkahelyi megteremtésére irányulnak? A BYOD stratégia megteremtése a kérdés csupán egyik oldala, a másik a munkavállalók oktatása.

Kulcsszavak: *BYOD, biztonsági kockázat, stratégia*

A kézirat benyújtásának dátuma (Date of the submission): 2017.07.12.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.22.

INTRODUCTION

Nowadays the use of the Internet has assumed omnipresence, affecting the way we live and work. New concepts and concerns come with it and here I will concentrate on the emerging concept of Bring-Your-Own-Device (BYOD). According to the defining of Ghosh et al., BYOD is a new development in the workplace through which the employees are encouraged to access organization resources like corporate e-mails, calendars and scheduling, documents, applications, etc., with their personal devices, either for work or for personal use [1].

The relative low cost of the smartphone and also its ease of use at the workplace for voice and data services, contribute also to the adoption of BYOD concept. The characteristics of smartphone have to do with its contemporary advanced features and the numerous applications (apps). From the point of view of computer architecture, basically it is an embedded portable computer, equipped with interactive, mostly Java-based Apps, running on flexible operating systems (OSs) such as Android, iOS, Windows Mobile, etc. The paradigm of running these smartphones on mostly free-and open-source software (FOSS), have made its adoption and use very reliable and universal [2].

According to this, different organizations are coming to terms with the need for a BYOD strategy to authenticate and authorize employees to use BYOD on enterprise networks, which would inure to the benefits of the organization. On the other hand, BYOD presents network externalities which could impact on the corporate security framework of re-defining the uncertainties of network perimeter and to safeguard the information assets to ensure confidentiality, integrity and availability (CIA) [3], [4].

A key concern with BYOD is the case where management of the organization may not be aware of personally-owned devices accessing corporate resources. Furthermore might happen that the needed technical support may not also provided. According to past related- studies, it is shown that there is an increased cyber-risk posed to the sensitive corporate information assets of any business when “foreign” and/or unauthorized devices access the corporate network [5].

The research of Onwubiko and Owens shows that employees compliance with security policies and guidelines is taken for granted in many companies. Instead they prefer a formalistic approach of the security [6]. Actually these provides some directives on where to extra resources should be used to improve the employees (regarding security awareness) as one of the most important lines of the defense. A compromised mobile device with access to the enterprise network could serves as vulnerable entry points for nefarious activities within the network and possibly with access to sensitive information. Therefore is very important for any organization while adopting BYOD, to put in place the appropriate security measures in order to mitigate against the disadvantages of this phenomenon.

It was reported that in a study from Alcatel-Lucent’s Motive Security Labs, 16 million mobile devices worldwide have been infected by malware and mobile infections are said to be growing at a disturbing rate, with an increase of 25% in 2014 comparing with 20% in 2013 [7]. CEBR reported that mobile-related cyber-attacks cost UK businesses about £18 billion in lost revenue and £16 billion in increased IT expenditure per year resulting from breaches [8]. As we can see, the report indicates that the mobile devices compromises are a widespreas risk, where 81% of UK businesses recording a breach in 2014 [8].

Actually experts believe that if nothing is done about the cyber-risk threats, the organizations in all parts of the world are faced with cybersecurity breaches and will continuously remain faced with these concern. These breaches resulting mostly in breach cost such as incident response forences, clean up, legal; reputation and brand damage as a consequence; and lost on their revenue due to downtime and so on [3]. To aggravate the already unsafe situation, the major part of SMEs in developing economies consider

themselves as not having any data attractive to threat agents, and they have not face any attack. Actually the contrary is true, it can be imagined/believed, big companies usually have data on employees, clients, suppliers, partners, etc., and it is with much more interest for attackers to have that large information on their hands [3]. Although this, there are no limits for attackers, the potential risks and countermeasures to stay on the safe side should be taken not only in consider but also to implement them in the appropriate way.

BYOD CHALLENGES AND SECURITY RISKS

The BYOD concept implemented in different kind of organizations can bring about many advantages such as increased efficiency and convenience. But what might be convenient for us (users) can be also convenient for attackers. Thus this phenomenon as it was mentioned above led to/bring a number of security risks for IT infrastructure and data of the enterprises and users also.

Actually there are certain factors that increase the occurrence of BYOD risks. To start, when the enterprise and personal data are allowed to coexist on the same device, then it becomes very problematic and challenging to find a balance between security control of enterprise and privacy of personal data, especially when the device is not a corporate asset. Furthermore, it is not easy for IT departments to support different phone/OS version/carrier combinations [9], which are also constantly changing with technical advancement and get outdated very quickly [10], [1], [11]. We should also keep in mind that because of the increased processing power and memory of smartphones and tablet computers, increased data transmission capabilities of the mobile phone networks, and open and third-party extensible operating systems for mobile devices, they become an interesting target for attackers [12].
Below are listed and more explained some associated risks related with BYOD in enterprises.

Data leakage

Data Leakage can result from different causes. Considering a lost/stolen device case. Data leakage can happen when an attacker access data on a lost or stolen device with unprotected memory. If data on the BYOD memory or its removable media is not adequately secured by encryption it is possible that an attacker can easily gain access to information [13]. Another case is when enterprise information is sent to personal contacts by mistake [11]. Usually and very often BYODs contain also important and valuable information such as credit card data, bank account numbers, passwords/PINs and so on. Because of their portable nature, they are the main store for the user's personal information and also corporate sensitive data. Moreover there are chances that some disgruntled employees may also share confidential business data on personal devices with competitors, leading to a competitive disadvantage for the organization [1].

Another case has to be with improper decommissioning. It means the transfer of a mobile device to another user without removing sensitive data may result in an attacker gaining access to the data on it [5]. Due to a growing awareness of identity theft many people and organizations now destroy or wipe computer hard drives prior to decommissioning. Unfortunately, the same is not yet happening with mobile devices used in the workplace with sensitive corporate data.

Reminding that personal devices are not part of the business's IT infrastructure, and due to that, these devices are not protected by company firewalls and systems (unless the company takes countermeasures against this). So it is clear that data leakage can led to not only problems for users but through BYOD they can be transmitted also to company causing company's system vulnerable to data breaches.

Data Disclosure by accident

It is possible that data can be disclosed unintentionally by the user of a mobile device. Data is transmitted or received and many users are either unaware, tend to forget that or ignore the privacy settings. Even though they may have given a clear approval, their naivety about functionality of device applications led to problems with their awareness on the fact that an application collects and publishes personal data [3], [14].

Phishing and SMishing

Phishing or SMiShing can result from an attacker using phony applications, SMS, or email that appear unpretentious to collect user credentials like password, PINs, or credit card information [15]. Phishing attacks are well-known threats for users of traditional computers and are increasingly becoming a concern for mobile devices and platforms alike for several reasons. What is more, the reduced screens sizes of these devices, makes it convenient for attackers to camouflage useful hints like whether the website uses SSL, that users rely on to decide whether or not to submit credentials. Also, application stores provide a new way of phishing by giving attackers the chance to place counterfeit apps in the app-store, looking like authentic apps, as well as these devices provide additional channels that can be used for phishing, using SMS in the case of SMiShing. Users may be less cautious about SMS phishing messages, and finally even though users may be aware of the risk of phishing in traditional computers, most are unaware of the same type of risk in mobile devices.

Hackers can infiltrate system

It can result from network resource overload due to many mobile devices connecting to the corporate network and exhausting resources and making them unavailable to legitimate users. Thus, the availability security dimension is said to have been compromised of breached. The uptake of smartphones usage and mobile Internet, have increased the risk of network congestion through either signaling overload or data capacity overload [16].

Network congestion

Vulnerabilities

Several kinds of vulnerabilities still remain a crucial concern for BYOD. It was reported from Enterprise Apps Tech News, that CyrusOne outlines malware, device theft and phishing as among the key risks for organizations [17].

Malware: There are many types of malicious software (malware) and are referred to by different names depending on the function. It tends to disturb users by entering at private specific information, they may cause breakdown of the device and lead to stolen or to become unusable the information/documents of the users [18]. Common malwares include Spyware, Virus, Financial Malware, Surveillance Malware, Trojan horse, etc. They are a big problem when implementing BYOD strategies into a business. While using personal devices, employees can access whatever sites or download any mobile applications that normally business would restrict to protect its system.

"Jailbreaking" or "rooting" a device also puts company's systems at risk because it removes limitations imposed by the manufacturer to keep the mobile software updated and protected against external threats. It's best to understand that as employees have the freedom to choose whatever device they want to work with, the process of keeping track of vulnerabilities and updates is considerably harder. Through this method hackers are allowed to have access to the OS of the mobile and as a result creates a vulnerability. Furthermore

these devices do not receive the necessary security updates and become vulnerable to threats [19].

POSSIBLE SOLUTIONS AND STRATEGY

Taking in consider that BYOD is applied in many companies and the risks and challenges that this phenomenon brings, it is very important for organizations, especially for IT departments to have a strategy to create a balance between a great user experience and effective information security.

To avoid risk one option might be the strategy of "Here is your own device (HYOD)". Here the devices are provided by the organization where the enterprise has total control on the device. It can happen that employees are resistant against this approach and they may use workarounds as using a company-owned device may be considered inconvenient for them [20]. Furthermore Earley et al., note "the trick is to use transparent approaches and a light touch, rather than intrusive approaches that will only encourage workarounds" [21].

An acceptable use policy may be used alone or in conjunction with installed software for managing the device [22]. In case that a software option is chosen, then a mobile device management (MDM) application can enforce the policies required by the organization prior to providing the employee's device with access to the company network [20]. It was noted from Chang et al., that the "BYOD policies include identifying which devices can be used in the company network, listing both allowed and banned apps, and describing classes of data that shouldn't be stored locally after being used by a mobile application" [20, p. 2]. A whitelist and blacklist of applications should be maintained with an understanding that the blacklisted applications will never be installed on a managed device [1].

In case the device is lost or stolen the user need to back up his/her personal information before and during enrollment in the MDM [23]. The MDM should adhere to the company security policy to enforce passwords and screen lock capabilities also.

The U.S. White House suggests three virtualization methods:

- Remotely access the computing resources so the data is not stored on the personal devices;
- Implement a walled garden that separates the personal and corporate apps processes;
- Apply limited separation of the employee personal and corporate data with a requirement of security controls [20].

It was suggested by Ackerman [22], that: "keeping corporate data on the device in a separate software container (which allows the user's and the business's programs to run simultaneously without accessing each other's data)". Can be taken in consider also mandatory installation of security software, configuration of auto-update for software updates and security patches, the creation of security codes, the use of VPN protocols when using public Wi-Fi connections, the encryption of all company data, and the enabling of remote deletion capabilities.

Another important issue is related with employees and their responsibilities regarding securing policies. Their security awareness should be taken in consider in every enterprise. Organizations and especially IT departments need to create material to train their employees on different practices such as:

- What devices will be supported?
- What mobile operating systems (Android or iOS) will be supported?
- What apps, if any, will be supported?
- Address security issues with BYOD policy, including:

- Password policies;
- Public Wi-Fi security and awareness;
- Loss and/or phone theft policies.

Employees need to understand how security threats affect them personally in order to have successful operations. Why not considering the possibility that employees can should also sign an agreement after completing BYOD training to eliminate any future questions about ownership, loss, or confidentiality breaches.

Despite the effort governance, compliance and security functions put into managing information security, employees often remain the weakest link in an organization's defense. But even a basic level of risk understanding and awareness can prevent simple failures in control that are often the root cause of security breaches. This doesn't mean to force them to read and agree the policies. It is about connecting different integral parts within organization and explaining why is really important to stay in the safe side.

After a two-year transition, from May 2018, General Data Protection Regulation (GDPR) will come into effect [24]. It aims law updating to better address challenges of privacy for a better security protection for individuals and companies. And BYOD will meet it as well. Companies with inappropriate BYOD policies may run the risk of non-compliance with GDPR and paying up to 4% of global turnover, as well as the risk of insider threat and data breaches [25]. So the need to strengthen BYOD policies must be to the top of priority list and it is needed that these policies must be conform to industry regulations and correctly implemented, especially into employee training.

CONCLUSIONS

This work was developed with focus on BYOD concept. Constantly organizations attempt to improve their strategies for better management and higher returns. But one of the major challenges they must take not only in consider but also to prevent is bring your own device (BYOD) risk. It was presented that this phenomenon brings a number of security risks for IT infrastructure, data of the enterprises and users also.

The occurrence of BYOD risks are increasing and there are certain factors. Starting from the fact that the enterprise and personal data are allowed to coexist on the same device, then it becomes very problematic and challenging to find a balance between security control of enterprise and privacy of personal data, especially when the device is not a corporate asset. Maybe the balance will never be created as the technology is becoming more and more convenient and in the same time risky. But always should be taken countermeasures. Organizations and especially IT departments should have a strategy to create a balance between a great user experience and effective information security. HYOD might be a solution but it is shown that is same cases employees are resistant against this approach.

In the case of BYOD a MDM application can enforce the policies required by the organization prior to providing the employee's device with access to the company network. Also the employee's awareness is a big problem. The really intention is not to enforce but to put them and companies in the safe side. Their collaboration is needed and the companies should put more emphasize on the security training.

These policies are mentioned as solutions on in this work but normally they might have some limitations. So the future work might be providing a best view of security risks of BYOD and to see how the BYOD policies are changing and how will they change, when GDPR will come into effect.

BIBLIOGRAPHY

[1] P. K. GAJAR, A. GHOSH AND S. RAI, "Bring Your Own Device (BYOD): Security risks and mitigating," *Journal of Global Research in Computer Science,* vol. 4, no. 4, April 2013.

[2] G. HOGBEN AND M. DEKKER, "Smartphone Security: Information Security Risks, Opportunities and Recommendations for Users," ENISA, London, 2010.

[3] E. O. YEBOAH-BOATENG, "Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA)," Institut for Elektroniske Systemer, Aalborg Universitet, Aalborg, 2013.

[4] ERNST & YOUNG, "Security & Risk Considerations for your Mobile Device Program," EY, 2013.

[5] E. O. YEBOAH-BOATENG, "Using Fuzzy Cognitive Maps (FCMs) to Evaluate the Vulnerabilities with ICT Assets Disposal Policies," *International Journal of Electrical & Computer Sciences,* vol. 12, no. 5, pp. 20-31, 2012.

[6] C. ONWUBIKO, T. J. OWENS, "Situational Awareness in Computer Network Defence: Principles, Methods and Applications," IGI Global, 2012.

[7] P. PAGANINI, "More than 16 million mobile devices are infected worldwide," Security Affairs, 2015.

[8] CEBR, "The business and economic consequences of inadequate cybersecurity," Centre for Economics and Business Research Ltd, 2015.

[9] C. ROSE, "BYOD: An Examination of Bring Your Own Device in Business," *Review of Business Information Systems – Second Quarter 2013,* vol. 17, no. 2, pp. 65-70, 2013.

[10] E. B. KOH, J. OH AND C. IM , "A study on security threats and dynamic access control technology for BYOD, Smart-work Environment," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, Hong Kong, 2014.

[11] C.-C. CHANG, W. CHENG-CHIEH AND S.-C. CHEN, "The Influence of Bring Your Own Device on the Psychological Climate at Workplace," in *ICEC '14 Proceedings of the Sixteenth International Conference on Electronic Commerce*, Philadelphia, PA, 2014.

[12] G. COSTANTINO, F. MARTINELLI, A. SARACINO AND D. SGANDURRA, "Towards enforcing on-the-fly policies in BYOD environments," in *9th International Conference on Information Assurance and Security (IAS)*, Gammarth, 2013.

[13] B. CAUSEY, "Strategy: How to Conduct an Effective IT Security Risk Assessment," InformationWeek Reports, 2013.

[14] M. E. WHITMAN AND H. J. MATTORD, Principles of Information Security, 4th ed., Boston, MA: Cengage Learning, 2011.

[15] E. O. YEBOAH-BOATENG AND P. M. AMANOR, "Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices," *Journal of Emerging Trends in Computing and Information Sciences,* vol. 5, no. 4, pp. 297-307, April 2014.

[16] A. T. KARYGIANNIS AND L. OWENS, "Wireless Network Security: 802.11, Bluetooth and Handheld Devices," National Institute of Standards and Technology (NIST), 2002.

[17] J. BOURNE, "Malware and 'connection hijacking' remain biggest BYOD risks, report warns," Enterprise Apps Tech News, 2016.

[18] A. FELT, M. FINIFTER, E. CHIN, S. HANNA AND D. WAGNER, "A survey of mobile malware in the wild," in *Proc. of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2011.

[19] P. RUGGIERO AND J. FOOTE, "Cyber Threats to Mobile Phones," United States Computer Emergency Readiness Team (US-CERT), 2011.

[20] M. J. CHANG, P.-C. HO AND T.-C. CHAN, "Securing BYOD," *IT Professional,* vol. 16, no. 5, pp. 9-11, 24 September 2014.

[21] S. EARLEY, R. HARMON, M. R. LEE AND S. MITHAS, "From BYOD to BYOA, Phishing, and Botnets," *IT Professional,* vol. 16, no. 5, pp. 16-18, 2014.

[22] E. ACKERMAN, "The bring-your-own-device dilemma: Employees and businesses seek to balance privacy and security," *IEEE Spectrum,* vol. 50, no. 8, pp. 22-22, August 2013.

[23] P. FIORENZA, "Mobile Technology Forces Exploration of Bring Your Own Device," *Public Manager,* vol. 42, no. 1, p. 12, 2013.

[24] Council of the EU, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," Council of the European Union, Brussels, 2015.

[25] S. BLACKMER, "GDPR: Getting Ready for the New EU General Data Protection Regulation," InfoLawGroup LLP, 5 May 2016. [Online]. Available: https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/.

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

AZ IOT KATONAI FELHASZNÁLÁSI LEHETŐSÉGEI ÉS A FEJLESZTÉS IRÁNYAI

POSSIBILITIES OF USING IOT FOR MILITARY PURPOSES AND THE DIRECTIONS OF DEVELOPMENT

KOLLÁR Csaba

(ORCID: 0000-0002-0981-2385)

kollar.csaba@uni-nke.hu

Absztrakt

Teoretikus, hazai és külföldi forrásokat feldolgozó tanulmányom célja, hogy az IoT információbiztonsági fókuszának katonai aspektusait, illetve a fejlesztés lehetséges irányait mutassam be. A téma bevezetését követően az IoT katonai döntési folyamatban elfoglalt lehetséges helyéről írok, majd az IoT katonai technikai rendszerének egyik elfogadott ábrája alapján három katonai alkalmazási megoldást ismertetek. Külön alfejezet foglalkozik az IoT és az információbiztonság problematikájával, illetve a fejlődés és a sebezhetőség lehetőségeivel. Tanulmányom zárásaként az eredmények összefoglalása után az IoT civil-katonai fejlesztéseinek lehetséges forgatókönyveiről értekezem.

Kulcsszavak: *digitális kor, információbiztonság, IoT, katonai alkalmazás, hálózatos katona*

Abstract

My theoretical study, which deals with domestic and foreign sources, aims to present the military aspects of IoT's information security focus and the possible directions of development. Following the introduction to the topic, the possible place of IoT in the military decision-making process is described, then three solutions for military exploitation is discussed on the basis of an approved figure regarding the military-technical system of IoT. Separate sub-chapter deals with the issues of IoT and information security, as well as the possibilities of development and vulnerability. My study ends with the summary of outcomes and the possible scenarios of IoT civil-military development trends.

Keywords: *digital age, information security, IoT, military applications, networked soldier*

A kézirat benyújtásának dátuma (Date of the submission): 2017.10.10.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.21.

BEVEZETÉS

Az IoT nemzetközi katonai – elsősorban USA/NATO – jelenlegi és tervezett felhasználási területei közül a fontosabbak a következők: (1) a katonai teljesítmény nyomon követése, (2) a katonák egészségügyi felügyelete, (3) a pilóta nélküli rendszerek elterjedése, (4) a populáció nyomon követése [1], (5) a logisztikai feladatok hatékonyabb elvégzése [2], valamint (6) a műveleti döntések meghozatalához szükséges nagymennyiségű adat biztosítása, illetve (7) a katonai objektumok és kritikus infrastruktúrák védelmét elősegítő megoldások bevezetése. Ez utóbbi védelméről magyarul többek között Munk [3, 4] értekezett.

Suri és Tortonesi [5] felsorolás jelleggel foglalja össze az IoT eszközök katonai felhasználásával kapcsolatos fontosabb elvárásokat:

1. Decentralizált infrastruktúra
    a. nem lehet támaszkodni központosított infrastruktúrára
    b. taktikai felhőkre van/lenne szükség, ezek azonban még fejlesztési fázisban vannak
2. Hálózat felhasználása
    a. a polgári/kereskedelmi környezetben ez nem kihívás
    b. könnyen és gyorsan hozható létre kapcsolat az internethez
3. Együttműködési képesség
    a. néhány általános protokoll létezik, amelyik magába foglalja a szabványokat
4. Bizalom és biztonság
    a. az adatvédelem az elsődleges szempont, de a gyártók teljes hozzáférést szeretnének
5. Eszközök használata
    a. továbbra is kihívást jelent a tápellátás (különösen harci körülmények között)
6. A szemantikus web technológiára épülő alkalmazások
    a. segíthet az interoperabilitásban, az adatelemzésben és -hasznosításban

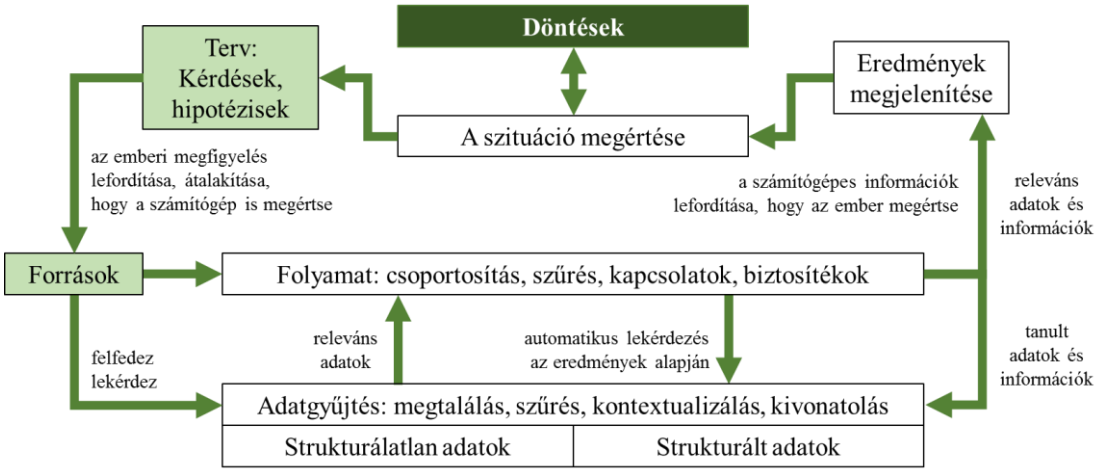
Külön figyelmet érdemel a katonai felhasználásra tervezett IoT eszközök autonómiája (önjáró, automatikus működése). Az Amerikai Védelmi Minisztérium a legfontosabb követelményként az autonómiát fogalmazta meg, különösen az olyan helyzetekre utalva, amikor az eszközök informatikai/elektronikai támadásoknak vannak kitéve. Ilyenkor az eszköznek gyors reakcióidő mellett fel kell ismernie az illetéktelen hozzáférést és meg kell azt akadályoznia (A2AD – anti-access/area-denied).

A hadiipari vállalkozások közleményei alapján megállapítható, hogy az USA hadseregében egyre komolyabb figyelmet kap az információs- és adathadviselés [6]. Ennek az oka az, hogy amint egy adat, vagy információ létrejött, azonnal továbbítható a hírszerző, megfigyelő és felderítő rendszerek felé, ami nagymértékben tudja növelni a hadsereg és az adott egység katonai hatékonyságát. A hadiipari cégek egyre komolyabb erőforrásokat fordítanak arra, hogy az IoT eszközökre épülő megoldások révén elősegítsék a gépi tanulást, illetve automatizálják a döntéshozatalt. Az IoT révén a C2BMC rakétavédelmi rendszer hatékonyabban tud működni, mivel a sok száz szenzorból, radarból és műholdból származó adatokat egy közös kommunikációs nyelv, illetve protokoll szerint továbbítják, illetve dolgozzák fel, ami a rendszerelemek közötti folyamatos kommunikáció mellett a fenyegetésekre és támadásokra történő eredményesebb és gyorsabb reagálást is lehetővé teszi. Az amerikai védelmi hivatal, a DARPA is egyre többet foglalkozik az IoT és a hadiipar kapcsolatával [7]. Olyan fejlesztések kapnak támogatást, amelyek fókuszában a szenzorok és a mesterséges intelligencia áll. Az eredmények révén a hadsereg az eddiginél hatékonyabban lesz képes felderíteni az ellenséges eszközöket és kommunikációs csatornákat, ami helyzeti előnyt jelent a számukra. A tervek között szerepel az is, hogy a már jelenleg működő nagyobb fizikai mérettel (és akár nagyobb

pontossággal) rendelkező fix, vagy telepített érzékelők mellett okostelefon méretű, hordozható eszközökkel lássák el a védelemmel foglalkozó polgári és katonai felhasználókat, illetve olcsó, s így tömegesen kihelyezhető IoT érzékelők monitorozzák folyamatosan a fontosabb út- és vasútvonalakat, hidakat, illetve a kritikus infrastruktúrák környezetét. Az IoT behálózottságnak köszönhetően olyan védelmi rendszer alakítható ki, amelyik még időben képes felfedezni a piszkos bombákat, a radioaktív sugárzást és egyéb, a társadalomra/infrastruktúrára veszélyes eszközöket, anyagokat. A környezeti monitorozás révén nagyon sok adat áll majd rendelkezésre. A hatékonyság, s így a téves riasztások arányának csökkentése érdekében fontos feladat lesz az adatzaj szűrése, az adattisztítás még mielőtt a tényleges és mélyreható elemzés megtörténik.

AZ IOT ÉS A KATONAI DÖNTÉSI FOLYAMAT

Az IoT katonai területeken történő megjelenésének egyik legfontosabb haszna az, hogy sokkal több adattal és a belőlük képzett információval, illetve tudással képes támogatni a döntési mechanizmusokat, valamint magát a katonai vezetők, parancsnokok döntéshozatalát, ahogy az az 1. ábrán is látható.



1. ábra Az IoT a katonai irányításban és ellenőrzésben (saját szerkesztés [5] alapján)

A katonai döntési folyamatban az IoT megjelenésével nagyobb hangsúly helyeződik a környezeti tényezők és hatások vizsgálatára. A műveleti területeken kihelyezett (telepített, szétszórt) IoT eszközök, illetve a támogató hálózati és egyéb infrastruktúra révén a szenzorok nagyon sok adatot tudnak szolgáltatni a környezet fizikai, kémiai, biológiai és egyéb jellemzőiről, s ezek az adatok az idősoros feldolgozásnak köszönhetően sokkal jobban értelmezhetővé teszik a változások időbeli lefolyását.

A rendelkezésre álló adatok akár strukturáltak, akár strukturálatlanok lehetnek. Az előbbibe tartoznak többek között a szöveges dokumentumok, a felhasználói/katonai tapasztalatok, a weblapok, a különböző multimédiás tartalmak, a közösségi hálón megtalálható információk, míg a strukturáltat elsősorban az adatbázistáblák, a térinformatikai adatok és koordináták, valamint a különböző szenzorok által rögzített adatok alkotják. Az adatok feldolgozása során csak a döntés szempontjából releváns strukturált, szemantikus adatok (információk), az absztrakcióra és felfogásra alkalmas tudás, illetve az intelligenciát jelentő bölcsesség kerülhet a katonai vezetők elé. Ezt szolgálják a folyamat egyes elemei, melynek végén olyan eredmény jelenik meg, ahol a számítógépes információkat a katonai döntéshozók által érthető formában (adatvizualizáció) kell bemutatni. Ennek alapján a vezetők képesek a szituációk gyors megértésére, további lekérdezési parancsok megfogalmazására a számítógép által érthető nyelvezet-

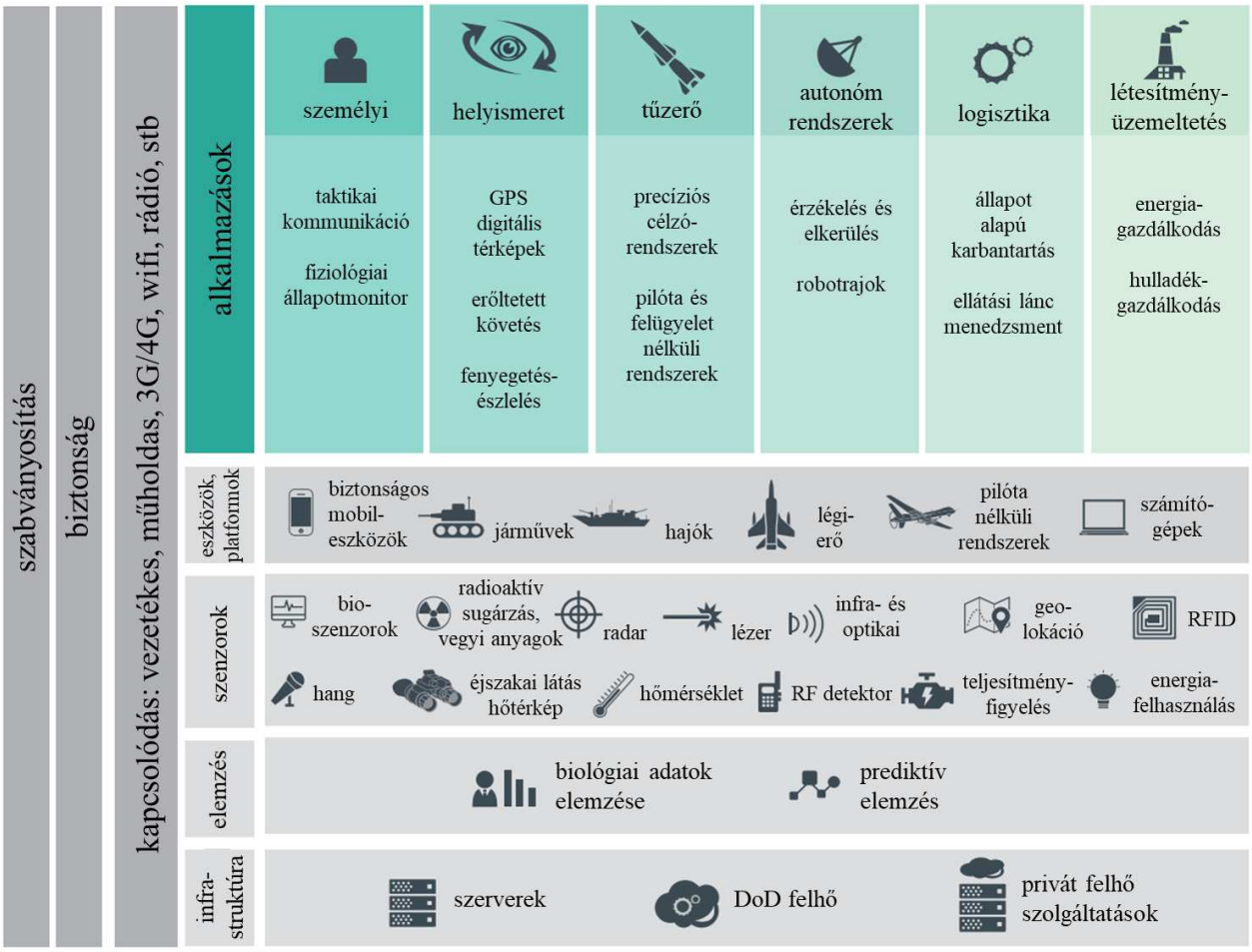
re. Így egyfelől újabb adatok gyűjthetők, másfelől a már rendelkezésre álló adatok új szempontok szerint strukturálhatók a közöttük levő szemantikai kapcsolatok révén. A szituáció megértése és a döntés meghozatala között – amennyiben a katonai vezetők megbíznak az IoT és egyéb támogató technikák által szolgáltatott adatok relevanciájában – kevesebb idő telik, ami különösen éles harci helyzetekben növeli a hatékonyságot, s így helyzeti előnyhöz juttatja a saját erőket.

Ahogy arra tanulmányom későbbi részeiben még utalni fogok, azt az idealizált állapotot, miszerint a katonai/parancsnoki döntéseket az IoT, a szemantikus adatfeldolgozás, a döntési folyamatok automatizálása, a mesterséges intelligencia megkönnyíti, s egyben jobban meg is alapozza, jelentősen árnyalja az, hogy az IoT technológia biztonsági szempontból – a civil felhasználási területekhez hasonlóan – a katonai területeken is meglehetősen sebezhető.

AZ IOT KATONAI TECHNIKAI RENDSZERE

Az IoT katonai technikai rendszerének alapját – a 2. ábra szerint – a szabványosítás, illetve a technikai-technológiai keretrendszer jelenti. Publikus forrás [8] szerint a NATO által 2015-ben indított „Az IoT katonai alkalmazhatósága” elnevezésű, IST-147 jelzésű, Lengyelország vezetésével működő munkacsoportjának (tagok: Belgium, Finnország, Németország, Hollandia, Lengyelország, Románia, Egyesült Királyság, USA) feladatai négy terület köré szerveződnek az IoT fókuszában. Ezek:

1. Meg kell vizsgálniuk az IoT katonai felhasználhatóságát az olyan területeken, mint az alapfeladatok ellátása, a helyzetfelismerés, a határőrizet, vagy az energiaellátás.
2. Fel kell térképezniük az IoT katonai felhasználhatóságának kockázati tényezőit, javaslatot kell tenniük a fontosabb kockázati tényezők konkrét kezelésére. Megoldást kell találniuk többek között a személyazonosság és az okmányok/belépőkártyák kezelésének, az objektumok védelmének, valamint a kereskedelmi biztonsági módszerek jelenlegihez képest lényegesen hatékonyabb módszereire.
3. Meg kell határozniuk azokat a kommunikációs követelményeket, amelyek az IoT által biztosított gép-gép kommunikációhoz köthetőek. Javaslatokat kell megfogalmazniuk a kommunikációs architektúrák vonatkozásában (fejlett gép-gép kommunikáció, robosztusság, skálázhatóság).
4. Technológiákat kell definiálniuk, amelyek hasznosítani tudják az IoT lehetőségeit, többek között az adatelemzés, illetve a rengeteg adat gyors feldolgozása vonatkozásában.



2. ábra Katonai technikai rendszer (saját szerkesztés [9] alapján)

Tervek szerint az említett munkacsoportnak 2018. december 1-ig kell elkészülniük a kitűzött feladatokkal. Megállapításaikat elsősorban két korábbi projektre, az IST-ET-076-ra (IoT katonai felhasználásának releváns témái), illetve az IST-ET-075-re (szenzorok és kommunikációs hálózatok integrációja) alapozzák majd.

Az ábra soron következő részével, az IoT és biztonság kapcsolatával nem ebben, hanem egy másik fejezetben foglalkozom részletesebben, míg az IoT rendszerek kapcsolódási lehetőségeiről, az infrastruktúráról, az adatok elemzéséről, valamint a szenzorokról Kollár [10] már korábban említést tett. Az eszközök és platformok egy része funkcióját, felhasználási területeit illetően nem tér el jelentősen a polgári életben használt társaitól. A polgári élethez képest azonban valamennyi katonai felhasználási területen a biztonságos működés, az energiaellátás, a meghibásodásból eredő esetleges károk minimalizálása még nagyobb hangsúllyal szerepel. Az alábbiakban a katonai alkalmazási lehetőségek közül ismeretetek hármat.

A hálózatos katona és a helyismeret

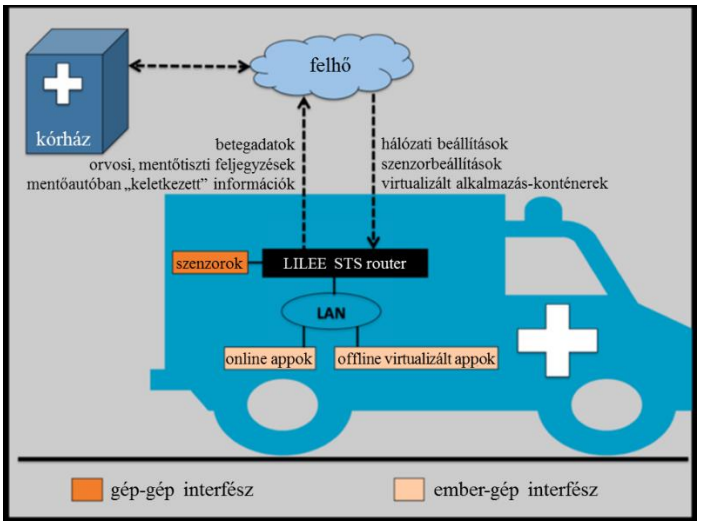
Manapság már senki nem kérdőjelezi meg az információalapú hadviselés fontosságát, illetve azt sem, hogy ennek aránya a többi hadviselési formához képest folyamatosan növekszik. A 2010-2030 közötti időszakot tekintjük az új hadügyi forradalom második hullámának, amelynek egyik fontos jellemzője tanulmányom fókuszában az, hogy „megkezdődik a hálózatos harceszközökkel rendelkező és magasabb hálózatba köthető katona, az úgynevezett hálózatos katona programok kifejlesztése, amellyel befejeződik a haderő digitalizálásának komplex programja” [11; 137. o.]. Hiba lenne azt állítani, hogy a hadügyi forradalmi korszakokat megelőzően a katonákat nem látták el olyan személyi felszereléssel, amelyik vezeték nélküli ösz-

szeköttetés segítségével támogatta a katona, a többi katona, illetve a parancsnok között a kapcsolattartást. A technika fejlődésével ezek az eszközök (pl.: katonai rádió-adóvevők) méretüket és tömegüket tekintve egyre kisebbek lettek (az elektroncsöveket leváltotta a tranzisztor, majd az integrált áramkör), csökkent a fogyasztásuk, miközben – köszönhetően az adás- és vételtechnika, illetve a híradástechnika fejlődésének – hatótávolságuk megnövekedett. Az sem szorul különösebb magyarázatra, hogy az említett forradalmak előtt is használtak a katonák különböző műszereket (pl.: hőmérsékletmérő, szélsebességmérő, Geiger–Müller-csöves sugárzásmérő), de a mért értékeket a katona rendszerint manuálisan rögzítette (papírra, vagy később számítógépre), vagy ugyan az eszköz rögzítette, de az adatok további feldolgozása érdekében az eszköznek el kellett jutnia a parancsnokságra, hogy vezetékes kapcsolaton keresztül rácsatlakozzon a megfelelő számítógépre.

A modern katona arzenáljában megjelentek, vagy meg fognak jelenni mindazok az infokommunikációs megoldások, amelyek a ma, vagy a jövő polgárait is jellemzik. A hálózatos katonák, illetve az általuk használt eszközök között a kommunikáció szélessávú, vezeték nélküli hang és adatátvitelre egyaránt alkalmas taktikai rádióval történik. Az elképzelések szerint a katona testén, ruházatán, sisakjában, esetleg bőre alatt elhelyezett szenzorok által rögzített állapotok (pl.: földrajzi koordináták, testhőmérséklet, pulzus, verejtékezés és annak 1-2 kémiai jellemzője) folyamatosan a személyi hálózatába (body-LAN) kerülnek, ahol megtörténik az adatok elsődleges és gyors feldolgozása, majd az előfeldolgozott adatok továbbítódnak a távolabb, vagy akár felhőben levő adatbázisokba a komolyabb, szemantikus feldolgozás érdekében. Az adatfeldolgozást követően a katona szükség szerint gyors visszajelzést kap akár a többi bajtársától, akár a parancsnoktól, akár a mesterséges intelligenciára épülő szoftveres megoldásoktól. A pontos helyismeret céljából számos olyan alkalmazást tud a katona az okoseszközére tölteni, amelyik lehetővé teszi a számára a harctéren folyó események valós idejű 3D-s nyomonkövetését. A katona sisakjában elhelyezett szenzorok, illetve a szenzorok adatait folyamatosan és valós időben feldolgozó élettani állapotmonitor révén idejekorán felismerhető a traumás agysérülés, a veszélyes kimerülés, vagy bármilyen olyan állapot, ami miatt az egészsége és harctéri aktivitása veszélybe kerülhet. A harctéri katonáról szóló adatok az irányítóközpontba kerülnek, ahol dönthetnek a katonai további sorsáról.

A harcszíntéren sebesült katona ellátásának előkészítése

Ahogy arról a hálózatos katonáról szóló részben már szó esett, a harctéri katonák egészségi állapotát folyamatosan monitorozni lehet, illetve szükség esetén be lehet avatkozni a folyamatokba (pl.: vissza lehet rendelni a bázisra). Gazdasági és praktikus megfontolásokból a katona bőrén, ruházatán, sisakjában elhelyezett egészségügyi szenzorok feladata az alapvetően egészséges katona állapotának a felügyelete, s a biológiai státusában nem várt, hirtelen bekövetkezett változások feldolgozása, az előfeldolgozott adatok továbbítása. Ezek a szenzorok alapvetően nem alkalmasak arra, hogy a sérült, sebesült katona állapotáról részletesebb és komplexebb képet nyújtsanak.



3. ábra A harcszíntéren sebesült katona ellátásának előkészítése (fordítás [12] alapján)

A kialakult gyakorlat szerint a harctéren megsebesült katona elsődleges ellátását a harctéri elsősegélynyújtók oldják meg. A jövő harctéri elsősegélynyújtóinál olyan hordozható vizsgálati eszközök lesznek (noninvazív és invazív egyaránt), amelyeket rá tudnak helyezni a beteg katonákra, így a részletes állapotmonitorozás azonnal elindulhat. Miközben a sérült katonát a kórházba szállítják, kétirányú adatkommunikáció is zajlik (3. ábra). A mentőautóból a felhőbe, s onnan a kórházba küldik a statikus betegadatokat (pl.: név, azonosítószám), a harctéri elsősegélynyújtó, mentőtiszt, orvos feljegyzéseit, illetve a mentőautóban, a beteg állapotával kapcsolatban keletkezett dinamikus adatokat (pl.: várnyomás, pulzus, EKG). A kórház így időben fel tud készülni a traumás beteg katona ellátására (pl.: műtők, szakszemélyzet, specialisták), s arra is lehetősége van, hogy a felhőn keresztül távvezérelje az IoT szenzorokat, illetve letöltesse a mentőautó lokális szerverére a speciális egészségügyi alkalmazásokat (appok) az alkalmazás-konténerekből.

Kiképzés

A katonai kiképzésben a kiterjesztett és virtuális valóságra, illetve egyéb, kevert valóságokra épülő módszerek és eljárások nem ismeretlenek, különösen, hogy a hadtudomány evolúciójában a valós és a virtuális világok egyaránt megjelennek [13]. A pilóták/űrhajósok repülőgép-, illetve űrhajószimulátora, a tantermi/tornatermi körülmények között megvalósított harcászati feladatok (pl.: taktikai tervek realizálása, VV-sisakkal felvértezve a virtuális ellenség megsemmisítése) egyaránt ide sorolhatóak. Az IoT megjelenése és katonai elterjedése annyiban fog változást hozni, hogy a kiképzés valódi terepen történik meg, ahol a különböző szenzorok, s az általuk szolgáltatott és feldolgozott adatok révén a kiképzőtisztek valós időben tudják áttekinteni valamennyi katona tevékenységét, s azonnali visszajelzést tudnak neki adni szükség esetén. A katona ruházatán elhelyezett szenzorok érzékelik majd, ha viselőjét eltalálják, s jelzik, hogy ez a találat az adott virtuális fegyver használata miatt halálos sérülést okozott-e, vagy sem. A katonák folyamatosan rögzített GPS-koordinátái, fiziológiai monitorozásának adatai a hadgyakorlatot követően akár személyre szabottan, akár az adott kötelék közös tevékenységét illetően kielemezhetőek, összevethetőek a kötelék korábbi teljesítményével, s a kiképzők így még jobb tanácsokkal tudják segíteni a katonák szakmai-gyakorlati fejlődését.

AZ IOT ÉS AZ INFORMÁCIÓBIZTONSÁG

Számos szerző ért egyet azzal, hogy a jövőben nagyon sok IoT eszköz veszi majd körül az embert – bár ahogy arra korábban is utaltam az IoT elterjedési dinamikáját illetően komoly

nézeteltérések is vannak. A korábban csak az asztali számítógépekre, majd később a hordozható eszközökre (laptop, tablet, okostelefon) vonatkozó információbiztonsági elvárásokat ki kell terjeszteni az IoT eszközökre és rendszerekre is [14] akár a polgári, akár a katonai felhasználási területekről is legyen szó. Daly [15] négy fontos tanácsot nevez meg a katonai IoT és a biztonság fókuszában. Ezek a következők:

1. Legyünk biztosak benne és ellenőrizzük, hogy az információ hiteles forrásból származik, a rendszereink pedig rugalmasak.
2. Tartsunk lépést a technológiával.
3. Fókuszáljunk a belső fenyegetésekre.
4. Végezzünk folyamatosan adatelemzést.

Az alábbiakban a négy tanács gyakorlati tartalmát ismertetem részletesebben.

Legyünk biztosak benne és ellenőrizzük, hogy az információ hiteles forrásból származik, a rendszerek pedig rugalmasak. A katonai vezetőknek – különösen a katonai információbiztonsággal és kiberhadviseléssel foglalkozó vezetőknek – az IoT által generált hatalmas adatmennyiséggel kapcsolatban fel kell tenniük a kérdést, hogy honnan tudják, hogy a rendszer által generált adatok megbízhatóak? A választ az információbiztonsági stratégiában kell keresniük. Az adatok természetesen kódolt, titkosított formában kerülnek továbbításra az egyes IoT rendszerelemek között. A titkosítás mellett az adatok szétválogatásával és megfelelő csoportosításával is csökkenthető a kockázat. A polgári életben is elterjedt virtuális gép technológia, adatbázis konténerek és egyéb fejlett megoldások a katonai területeken is használhatóak, a katonai fejlesztéseknél és alkalmazásoknál azonban az információbiztonság érdekében a szükségtelen szolgáltatásokat és alkalmazásokat el kell távolítani, s a megmaradt szoftvereket a céloknak megfelelően kell beállítani. Mivel (1) viszonylag sok rendszer épül(t) az IoT kiszolgálása érdekében, (2) a felhőalapú és hagyományos megoldások és szolgáltatások számos operációs rendszer alatt működnek, (3) megannyi felesleges tulajdonság is fut (vagy a tudtunk nélkül futtatható) – ezért a felesleges kockázat szintje magas.

A digitális kor velejárója, hogy egyre több és több, IoT-hez köthető technikai és technológiai újítás jelenik meg, melyek egy része – magától értetődően – ha időben egy kicsit megkésve is, de a katonai területekre is átterjed. A polgári életben, különösen, ha az IoT eszközök sérülékenysége konkretizálható és jelentős anyagi kárral jár, ugyancsak fókuszba kerül a biztonság, a katonai területen azonban ez még markánsabban jelenik meg. Ahogy a katonai rendszerekhez újabb és újabb IoT eszközök csatlakoznak, úgy növekszik a sérülékenység és a fenyegetettség. Ez a biztonsági rések növekvő számában, s ezzel összhangban a katonai szerverek ellen irányuló IoT eszközökkel, vagy azokon keresztül megvalósított támadásokban realizálódik. Szükség van olyan katonai kísérleti laborokra, ahol nem csak az új eszköz és a már meglevő katonai informatikai infrastruktúra kapcsolatát és a kapcsolat sebezhetőségét vizsgálják meg, hanem azt is, hogy a beágyazott rendszerek és rendszerelemek révén milyen adatok keletkeznek, azok hova továbbítódnak, illetve ezek az elemek hogyan kapcsolódnak más eszközökhöz. Ez olyan komoly probléma, amivel a katonai vezetőknek foglalkozniuk kell, különösen azért, mert ha az IoT eszközökkel felruházott katona pillanatnyi adatait (pl.: GPS koordinátái, egészségi állapota, közelében levők száma, egymáshoz viszonyított helyzete) az ellenség megszerzi, akkor a harctevékenység során könnyedén helyzeti előnyre tud szert tenni, vagy akár a katonák kiiktatása révén meghiúsítja az akciót.

Az ellenség információs műveletei az adott kötelék belső rendszereit is érinthetik az IoT eszközök révén. Az összekapcsolt IoT eszközök, s az általuk generált, s a felhőbe küldött adatok, valamint a felhőben végzett adattárolás és adatfeldolgozás révén számos automatizált katonai rendszer működik. Az IoT, mint informatikai rendszer határainak védelme ugyan csökkentheti a fenyegetettség és a kockázat mértékét, de a belső elhárítás révén nem felderített kémek és árulók a digitális kort megelőző korokhoz képest sokkal nagyobb károkat tud-

nak okozni az adatszivárogtatással, az adatok átírásával, az adatfolyam lassításával, vagy blokkolásával, stb.

Az ilyen hibák és (belső) támadások jelentős része kiküszöbölhető lenne azáltal, ha az eddiginél lényegesen szofisztikáltabb és gyakoribb adatelemzést (Big Data Analitika) végeznének a katonai informatikai rendszerekben. A sikeres adatelemzés során számos olyan algoritmus futtatható le, amelyek eredménye segítségével feltárhatóak a rendszerben azok a működési folyamatok, amelyek a nem elvárt és megszokott működésre vezethetőek vissza (pl.: minden ok nélkül hirtelen megnövekszik a felhőből küldött adatok mennyisége az egyik végpont felé). Az analitika arra is lehetőséget biztosít, hogy megjósoljanak (predikció) bizonyos folyamatokat és fenyegetéseket, mielőtt azok megtörténtek volna.

Az IoT és az információbiztonság technikai fókusza mellett érdemes megemlíteni a társadalomtudományos aspektust is. Pomerleau [16] cikkében James Cartwright-ra, az USA Stratégiai és Nemzetközi Tanulmányok Központ védelempolitikai tanulmányokkal foglalkozó részlegének a vezetőjére hivatkozva azt állítja, hogy az IoT, illetve a hozzá kapcsolódó technológiai fejlesztések (pl.: intelligens hűtőszekrények, intelligens termosztátok) gyökeresen fogják megváltoztatni az emberek életét. Cartwright úgy véli, hogy annak ellenére, hogy az IoT több szinten fog hasznosulni akár a polgári, akár a katonai területeken, a fő kérdés nem technikai, hanem kulturális. A biztonság, illetve az eszközök biztonságos használata, valamint a használatukhoz fűződő biztonságtudatosság és annak fejlesztése messze komolyabb feladat, mint a különböző IoT eszközök hardverének a kifejlesztése, illetve a hozzá kapcsolódó megfelelő programkódok megírása.

FEJLŐDÉS ÉS SEBEZHETŐSÉG

Sajnos az IoT eszközök katonai informatikai infrastruktúráját érintő információbiztonsági hiányosságok mellett azzal is számolni kell, hogy az IoT bevezetése és alkalmazása területén lemaradás tapasztalható. Pomerlau [17] Zheng és Carter [9] tanulmányára – melyben 29 kormányzati/katonai és ipari vezető döntéshozó véleményét elemzik – hivatkozva megállapítja, hogy ugyan az IoT (technológiával támogatott) olyan területeken, mint a drónokkal végzett megfigyelés, vagy a felderítés, az USA hadserege a polgári fejlesztésekhez képest előnyben van, általánosságban azonban a polgári élet generálja az IoT fejlesztéseket. Miközben a polgári életben a légjármű-karbantartás, az ellátási lánc menedzsment, vagy az intelligens otthonok területeken megannyi sikeres példával lehet találkozni, addig ezeknek a rendszeres katonai megjelenése és elterjedése még várat magára. Hivatkozott szerzők szerint a jelen valósága az, hogy az adatok gyűjtése és megosztása gyakran attól függ, hogy a mérőeszközök által mért adatok kézi felvitele (vagyis a látott mért eredmények rögzítése valamely informatikai/számítástechnikai rendszerben) mennyire gyorsan történik meg. A másik probléma az, hogy ha meg is történik az adatok rögzítése, a hadsereg sokkal kevesebb tudást és bölcsességet tud ebből kinyerni, mint amennyire egyébként a polgári életben használt algoritmusok és egyéb elemzési módszerek révén lehetősége lenne. A harmadik problémát a széttöredezett és különálló informatikai architektúra jelenti. Ez ugyanis nehézkessé teszi a protokollok és a különböző hálózatok közötti fejlesztéseket, illetve magát a közös használatot is. Negyedik problémaként azt sem szabad figyelmen kívül hagyni, hogy a katonai célú informatikai rendszerek fejlesztése és bevezetése rendszerint a tenderkiírásoktól és a közbeszerzési eljárásoktól függ, aminél gyakran már az igények megfogalmazásakor sem járnak el kellő körültekintéssel és integrált rendszerszemlélettel a katonai felhasználói oldal szereplői.

Campbell [18] úgy véli, hogy a polgári és a katonai informatikai rendszerek összekapcsolódása, vagy legalábbis funkcionális átfedése (pl.: a katonák telefonjain a polgári életben is használatos operációs rendszerek és alkalmazások futnak) sokkal sebezhetőbbé és támadhatóbbá teszi a nem polgári célpontokat, objektumokat. Világviszonylatban megnövekedett a hackerek, a social engineerek, s az általuk a vállalatok, kormányhivatalok ellen elkövetett

támadások száma. A jövőben számítani lehet arra, hogy a katonák és a katonai létesítmények is a támadások fókuszába kerülnek. Nevezett szerző munkájában hivatkozik az egyik, katonai megrendeléseket is kiszolgáló, egészségügyi vállalattal kapcsolatos információbiztonsági tanulmányra, mely megállapította, hogy hackereknek sikerült olyan érzékeny egészségmonitorozási területeken, mint például a kardiológia átvenni az irányítást az eszközök fölött, s manipulálták a gyógyszeradagoló pumpát. Ez előrevetíti annak gondolatát, hogy a harctéren megsebesült katonát az IoT technológiát használó távmonitorozó rendszer eredményes támadását követően akár a halálba is lehet küldeni (pl.: rossz gyógyszer adagolása, vagy túladagolás), mialatt a tábori kórházba szállítják.

Solomon [19] az IoT eszközök fejlesztésével kapcsolatban azon az álláspontonvan, hogy alapvető kritérium – akár van, akár nincs szabvány – hogy a fejlesztők az eddiginél lényegesen nagyobb odafigyeléssel dolgozzanak a biztonság tekintetében. A fejlesztés mellett is nagyobb fókuszt kell, hogy kapjon a biztonság, többek között a statikus kódelemzés (SCA), illetve a statikus alkalmazás-biztonság tesztelés (SAST) során. A fejlesztők és tesztelők információbiztonsági fókusza megtalálható a fejlesztői munkakörnyezetben és a következő előnyökkel jár:

- A programozók olyan fejlesztőkörnyezetben dolgoznak, amelyik elősegíti, hogy a biztonság a fejlesztés valamennyi szakaszában megjelenjen és figyelmet kapjon, így csökken a hanyag kódolásból eredő kockázat.
- Olyan modern, zökkenőmentes fejlesztési módszerek is használhatóak, mint az Agile, a DevOps, vagy a CI (Continuous integration).
- A biztonsági folyamat alapvetően automatizált, mindenki aktívan részt vesz benne. A fejlesztőket a munka megkezdése előtt részletesen felvilágosítják arról, hogy mik a biztonsági alapelvek, amelyeknek meg kell felelniük. Ez különösen a katonai IoT alkalmazások esetében követelmény.
- A fejlesztés során lehetőség van biztonsági küszöbszinteket definiálni. Ennek segítségével ellenőrzőlista-szerűen lehet kontrollálni, hogy az adott lépés, programrész, illetve -elágazás megfelel-e az alapvető biztonsági előírásoknak.
- A biztonságos munkamódszer kedvezően hat a megtérülési mutatóra (ROI), gyorsabban és hatékonyabban lehet a sérüléseket javítani, kevesebbet kell költeni karbantartásra, illetve csökken az adatszivárgásból eredő kár.

EREDMÉNYEK

Tanulmányom legfontosabb eredményének azt tartom, hogy a hivatkozott szerzők véleménye alapján megalapozottnak látom azt a kijelentést, hogy a hálózatos katona az utópisztikus távoli jövőből kézzelfogható távolságba, több területen pedig már a jelen valóságába került. A katonai területen hálózatba kötött emberek, gépek, berendezések, eszközök, járművek, stb. a vezetékes, s egyre gyakrabban vezeték nélküli kommunikációs protokolloknak köszönhetően akkor is képesek a folyamatos kapcsolattartásra, ha földrajzilag egymástól távol helyezkednek el. A katonákról, az általuk használt technikáról, a környezetről az IoT eszközök révén nagyon sok adat gyűjthető össze, ugyanakkor úgy gondolom, hogy a katonai-vezetői döntés támogatásában az IoT technológia még nem játszik döntő szerepet. Ennek okait abban láttam, hogy (1) a szenzorok, a lokális, illetve a távoli adattovábbítás és adatfeldolgozás védelme egyelőre nem megoldott, (2) a keletkezett adatok szofisztikált, szemantikus feldolgozása és közérthető vizuális megjelenése még várat magára, illetve (3) emiatt a katonai vezetés nem tud megbízni a technológiában. Véleményem szerint még egy ok megnevezhető, ami gátolja az IoT katonai elterjedését, ez pedig a róla alkotott meglehetősen heterogén katonai (NATO, USA) álláspontok elegye. Bár tanulmányomban mindvégig kongruens vélemény megalkotására törekedtem, sajnos több helyen is éreztem a publikus nyilatkozatok mögött megtalálható nézetkülönbségeket, melyekről nem gondolom, hogy a kommunikációs hadviselés (tudatos

félrevezetés, összezavarás) része lenne. Legvégül pedig az eredmények között tartom számon azt is, hogy az IoT katonai elterjedésével kapcsolatban rávilágítottam arra, hogy a polgári életben tapasztalt technikai fejlődés/fejlettség szintjéhez képest a katonai fejlődés/fejlettség az IoT területén lemaradást mutat. Ezért is tartottam fontosnak, hogy tanulmányom következő alfejezetében, a „következtetések"-ben nem egy hagyományos summázatát adjam írásművemnek, hanem négy forgatókönyvet vázoljak fel.

KÖVETKEZTETÉSEK

Következtetéseimet tanulmányomban két „tiszta", egy „nem tiszta" és egy „kevert" forgatókönyv köré kívánom rendezni. Kérdéses ugyanis, hogy előbb a polgári/üzleti területeken dolgozó fejlesztők dolgozzanak-e ki az IoT használatára vonatkozó biztonsági megoldásokat (szabványokat), amiket aztán már mint elvileg biztonságosnak mondott rendszereket a katonaság is átvesz, vagy – a hagyományos civil-katonai fejlesztések sémáját alapul véve – a megfelelő biztonsággal ellátott, a katonai elvárásoknak és követelményeknek megfelelő IoT rendszerek majd csak a katonai bevezetést követően jelennek meg a polgári életben.

Ha az első „tiszta" forgatókönyvet vesszük alapul, akkor a katonaság az informatikai technikai/technológiai szintjét tekintve mindig is lemaradásban lesz a polgári területekhez képest. Azzal, hogy az IoT rendszerek/szabványok csak később jelennek meg a katonai területeken azt is jelenti, hogy később ismerkednek meg vele a felelős üzemeltetők, s az adott rendszer gyenge pontjait ismerő polgári (vagy a polgári életből verbuvált) hackerek viszonylag könnyebben tudják feltörni az adott megoldásra támaszkodó katonai rendszereket.

A második „tiszta" forgatókönyv ugyan a katonai információbiztonság fókuszában jónak tűnik, hiszen a katonai területen dolgozók előbb ismerik meg a katonai IoT fejlesztéseket és javítják ki a tesztek során tapasztalt hibákat, tehát a polgári támadók előtt járnak tudásban és tapasztalatban. Ugyanakkor nincs semmi garancia arra, hogy a dinamikusan és exponenciálisan fejlődő IoT területén tevékenykedő fejlesztők és gyártók elsőként a katonai megrendeléseket szolgálják ki, lemondva a polgári megrendelők által kínált nagyobb, globális profitlehetőségéről. Ez a forgatókönyv természetesen nem zárja ki annak a lehetőségét sem, hogy akár nemzeti (pl.: USA), akár szövetségi (pl.: NATO, Visegrádi Négyek) szinten a kimondottan hadiiparra szakosodott vállalatok akár katonai műszaki egyetemekkel, karokkal, tanszékekkel közösen dolgozzanak az IoT fejlesztéseken, de a publikusan elérhető információk alapján erre jelenleg nem nagyon lehet példát találni.

A „nem tiszta" forgatókönyv szerint vannak és lesznek olyan területek – amelyekre már a jelen tanulmányomban is utaltam – amelyeken a katonai fejlesztések dominálnak, s csak ezek katonai bevezetése után jelenik meg az IoT haditechnika (akár egyszerűbb változatban is) a polgári életben. Az információbiztonság szempontjából ez jó megoldásnak tűnik, de nem csökkenti jelentős mértékben az informatikai eszközökre és megoldásokra épülő haditechnikai ágazatok lemaradását a polgári informatikai fejlesztésekhez képest.

A „kevert" forgatókönyv szerint a hadiipari fejlesztésekben polgári és katonai szereplők (katonai és polgári egyetemek, vállalatok, programozó csapatok, projektek, stb.) szoros együttműködés révén vesznek részt, ami azt jelenti, hogy a fejlesztési eredmények közel azonos időben jelennek meg a katonai és a polgári alkalmazásokban. Ez egyfelől elősegíti, hogy a katonai informatikai rendszereket üzemeltetők időben némiképp előbb ismerjék meg a fejlesztési eredményeket, mint a támadók, ugyanakkor felveti az információbiztonság fogalmát egy másik dimenzióban. A többszereplős fejlesztésekben a csapattagok nem azonos megbízhatósági szinten vannak. A nemzetbiztonsági átvilágításon átesett egyetemi oktatók, katonai vállalatok fejlesztői magasabb megbízhatósági szintet képviselnek azokhoz képest, akik szabadúszóként csatlakoznak a polgári fejlesztőkhöz. Az ő esetükben meglátásom szerint ugyan olyan átvilágítás szükséges. Kérdéses persze, hogy egy lezser, a szabadsághoz maximálisan ragaszkodó Z generációs programozó (aki kreativitásában akár messze felülmúlja a többi,

idősebb csapattagot) engedélyezi-e az átvilágítást, illetve elfogadja-e a munkavégzéssel kapcsolatos, számára feleslegesnek tűnő szigorításokat és szabályokat, vagy a felismerve a területen világviszonylatban tapasztalható munkaerőhiányt, idő előtt továbbáll.

A négy forgatókönyv közül meglátásom szerint a modern, infokommunikációs eszközöket használó hadseregek számára a „kevert"forgatókönyv nyújtja a legnagyobb innovációs potenciált. Ha ez az előny kellő információbiztonsággal és biztonságtudatossággal társul, akkor összességében optimális megoldás születhet.

FELHASZNÁLT IRODALOM

[1] KENNY, R.: *All Seeing Sensors – It's About the Data, Stupid*; https://militarycommunicators.org/2015/07/14/all-seeing-sensors-its-about-the-data-stupid (letöltve: 2017.10.10.)

[2] SELTZER, L.: *The internet of military things: Logistics dream, security nightmare?*; http://www.zdnet.com/article/the-internet-of-military-things/ (letöltve: 2017.10.10.)

[3] MUNK S.: *Kritikus információs infrastruktúrákhoz kapcsolódó, sajátos katonai (védelmi szférabeli) képességeket igénylő feladatok*; Hadmérnök, III. évfolyam, 3. szám (2008) 130-146 o.

[4] MUNK S.: *A kritikus infrastruktúrák védelme információs támadások ellen;* Hadtudomány, 2008/1-2. 95-106. o.

[5] SURI, N. – TORTONESI, M.: *Session 13: Military Internet of Things (IoT), Autonomy, and Things to Come*; https://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/57e41eac8419c2f2791befb5/1474567857321/Panel+-+Military+IoT%2C+Autonomy%2C+and+Things+to+Come.pdf (letöltve: 2017.10.10.)

[6] FEARN, N.: *US Army is using IoT tech and data to transform warfare;* https://internetofbusiness.com/us-army-iot-warfare (letöltve: 2017.10.10.)

[7] MURISON, M.: *DARPA wants to militarise the IoT;* https://internetofbusiness.com/darpa-wants-militarise-iot (letöltve: 2017.10.10.)

[8] NATO**:** Military Applications of Internet of Things (IST-147). 2015. https://www.cso.nato.int/activity_meta.asp?act=8647 (letöltve: 2017.10.10.)

[9] ZHENG, D. E. – CARTER, W. A.: *Leveraging the Internet of Things for a More Efficient and Effective Military;* CSIS (Center for Strategic and International Studies), 2015.

[10] KOLLÁR Cs.: *IOT A GYAKORLATBAN, AZ INFORMÁCIÓBIZTONSÁG FÓKUSZÁBAN I. Az IoT működése, fejlődési tendenciái;* Bolyai Szemle (kézirat megjelenésre elfogadva)

[11] HAIG Zs. – VÁRHEGYI I.: *Hadviselés az információs harcszíntéren;* Zrínyi Kiadó, 2005.

[12] PURI, D.: *Mobile IoT provider applies military techniques to improve IoT resiliency;* http://www.networkworld.com/article/3122129/internet-of-things/mobile-iot-provider-applies-military-techniques-to-improve-iot-resiliency.html (letöltve: 2017.10.10.)

[13] FEKETE K.: *Evolution of Military Science: Real and Virtual World;* Fekete Károly (szerk.): Kommunikáció 2015: Communications 2015. NKE Szolgáltató Kft., 2015, 141-148 o.

[14] KUMAR, S.: *Who Hacked Into Your Smart Device?* http://electronicsofthings.com/expert-opinion/hacked-smart-device (letöltve: 2017.10.10.)

[15] DALY, M. K.: *Internet of Things: 4 Security Tips From The Military;* http://www.darkreading.com/mobile/internet-of-things-4-security-tips-from-the-military/a/d-id/1297546 (letöltve: 2017.10.10.)

[16] POMERLEAU, M.: *For the military, the Internet of Things isn't about 'things';* https://defensesystems.com/articles/2015/11/12/internet-of-things-dod-cartwright-csis.aspx?m=1 (letöltve: 2017.10.10.)

[17] POMERLEAU, M.: *Report: Military lagging in IoT adoption;* https://gcn.com/articles/2015/09/25/military-lags-internet-of-things.aspx (letöltve: 2017.10.10.)

[18] CAMPBELL, S.: *Military Security in the Age of the Internet of Things;* http://www.afcea.org/content/?q=Article-military-security-age-internet-things (letöltve: 2017.10.10.)

[19] SOLOMON, S.: *Internet of Things (IoT) – Hack My Army;* https://www.checkmarx.com/2016/03/14/internet-things-iot-hack-army (letöltve: 2017.10.10.)

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

A KÖZÉP-KELET EURÓPAI GENERÁCIÓK DIGITÁLIS KOMPETENCIA ÉS BIZTONSÁGTUDATOSSÁG VIZSGÁLATÁNAK EREDMÉNYEI

RESULTS OF THE DIGITAL COMPETENCY AND SAFETY AWARENESS ASSESEMENT IN MIDDLE EAST EUROPE

NYIKES Zoltán

(ORCID: 0000-0001-5654-5120)

nyikes.zoltan@hm.gov.hu

Absztrakt

A digitális kompetencia a 20. század végétől egyre nagyobb társadalmi és egyéni fontossággal bír. Napjainkban a digitális eszközök és az internet elterjedése miatt elengedhetetlen a legalább alapszintű informatikai ismeret mindenki számára.
A materiális világ veszélyeivel szemben már kialakultak a különböző védekező mechanizmusok. A kiber korszak csak néhány évtizedre nyúlik vissza. A kibertérben megjelenő támadásokra, a hétköznapi emberek nincsenek felkészülve és nem tudják felmérni annak a veszélyességét.

Kulcsszavak: *digitális kompetencia, biztonságtudatosság, kibertér, digitális írástudás, digitális intelligencia*

Abstract

Digital competence has become increasing importance for social and individual since the 20th century. Due to the spread of digital devices and the Internet, the basic IT knowledge is essential for everybody. Different defense mechanisms have emerged against the danger of the material world. The cyber era started only a few decades ago. Civil people are not aware of attacks in the Cyber space and they can't survey its danger. In Hungary the information technology and the Internet penetration started in the last some decades.

Keywords: *digital competence, safety awareness, cyber space, digital literacy, digital intelligence*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.11.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.19.

BEVEZETÉS

Magyarországon az informatika és az internet rohamos elterjedése az elmúlt évtizedekre tehető. Az X és az azt megelőző generációkhoz tartozó magyar felhasználók csak felnőtt korukban találkoztak digitális ezközökkel és azok használatával. Az 1965 és 1979 között születetteket nevezi a szociológia az X generációnak. Ezen korosztályok munkába állásához nem volt elvárás a digitális kompetencia, hiszen sem a digitális eszközök sem a digitális infrastruktúra nem volt mindenki számára elérhető. Mindezeken túl ennek a korosztálynak nem volt megfelelő motivációja arra, hogy fejlessze a digitális kompetenciáját és ezzel együtt fejlődjön digitális biztonságtudatossága.

Ezért az említett korosztályok jelentős segítségre szorulnak abban, hogy napjaink digitális kihívásainak megfeleljenek. A digitális kompetencia és ezzel együtt a biztonságtudatosság képzéssel fejleszthető. Az ismeretek szintje jelentős eltérést mutat az azonos korú felhasználók között. Ennek felmérése, a szintek meghatározása összetett feladat. Kérdőíves felméréssel a felhasználók készségük és jártasságuk szerint különböző szintű csoportokba oszthatók. A különböző szinten lévő felhasználók digitális kompetenciájának és biztonságtudatosságának fejlesztése eltérő ismeret átadásával valósítható meg.

Jelen dolgozatban a kutatásaim eredményeként a vizsgált korosztályok szintjeinek felmérését és a felhasználók ezen szintekhez történő besorolását mutatom be.

AMIT TUDNI KELL AZ X GENERÁCIÓRÓL

Az X generáció elnevezést először Robert Capa (Fiedmann Endre), magyar származású fotós használta egy 1953-as, II. világháború után születettek szereplésével készült fotósorozatának elnevezésére. Az X az ismeretlent jelöli, ami később Douglas Coupland: X generáció című regénye nyomán került a köztudatba. Az X generáció a szellemi, spirituális ébredés alatt születetteket jelöli, akiknek szüleik már kevésbé óvták, védelmezték gyermekeiket, mint az őket megelőző generáció. Az X generáció eszes, gyakorlatias és jó ítélőképességű. A korosztály többsége szüleiknél iskolázottabb, és már nem csak a kötelező orosz nyelvet tanulta. A hetvenes évek végétől születettek már kamaszként is használják a számítógépet, és mindenki saját tempójának megfelelően elkezdi használni a technika legújabb vívmányait. A munka területén a pénz, a karrier, a státus, motiváló erő. Marc Prensky (2001) találóan digitális bevándorlóknak címkézi ezt a nemzedéket. Az elnevezés véleményem szerint találó metafora, hiszen sokan nem a mai modern világban születtünk, hanem gyorsabban vagy lassabban, bosszankodva vagy lenyűgözve használni kezdtük a digitális világ új vívmányait. [1]

A BIZTONSÁGTUDATOSSÁG ÉS A DIGITÁLIS KOMPETENCIA KAPCSOLATA

A biztonságtudatosság fontossága a mai világunkban nem kérdőjelezhető meg. Az informatika és az internet robbanásszerű fejlődése társadalmi változásokat hozott magával. Az iskolás- korúak számára az informatika oktatása és a digitális kompetencia fejlesztése már egész kora gyermekkortól kezdődően biztosított. Azonban nem csak az említett korosztálynak szükségesek a felsoroltak, hanem a társadalom teljes egészének. A mai kor emberének az élethosszig tartó tanulás biztosítja azt a tudást, amivel piacképes lehetőséget tud teremteni magának. [2] Az ipar digitalizációja korunk kihívása, mely új lehetőségeket nyit meg, ezt a modernizálódási folyamatot Ipar 4.0-nak vagy negyedig ipari forradalomnak nevezik. [3] Korunkban a legfontosabb digitális vívmányok, mint a felhő technológia (cloud technology) a dolgok internete (IoT), a mesterséges intelligencia (virtual rality), stb. egyre szélesebb körben ismert és alkalmazott. A hagyományos gyártórendszerek és gyártási eljárások optimális

működtetése már az internetes alkalmazások támogatásával valósul meg. Ahhoz, hogy az „Ipar 4.0" által forradalmasított gazdaság jól működjön, elengedhetetlen a rendszerek „leggyengébb láncszemének", az ember tudásának és tudatosságának az elvárt szintre történő emelése. [4] Hiába alkalmaznak a gyárak modern technológiát, technikát, hogyha azt a felhasználó tudásának, vagy a tudatosságának hiányában nem tudja optimálisan, biztonságosan üzemeltetni. [5] A biztonságtudatosság és a digitális kompetencia kapcsolatának kutatása céljából, egy olyan kérdőívet állítottam össze, amelynek a kérdéseire kapott válaszok kiértékelésével és ebből megállapított összefüggések alapján javaslatokat tudok kidolgozni a képességek és készségek fejlesztése érdekében a digitális-társadalom egyenlőtlenségeinek felszámolására.

A kérdőív aktualitása

A kérdőív a biztonságtudatosság és a digitális kompetencia kapcsolatáról azt a célt szolgálja, hogy a válaszadók körében hogyan érvényesülnek és milyen arányban vannak jelen korunk kihívásainak megfelelő informatikai ismeretek és a hozzá kapcsolódó biztonság. A kérdőív válaszai alapján levont következtetésekkel az Európai Unió által felállított digitális kompetencia keretrendszerének általam történt módosítását, kiegészítését kívánják alátámasztani. A fent említett keretrendszer, az aktív munkavállalók és a munkáltatók sikeres egymásra találását segíti. [6] Erre a feladatra teljesen alkalmas, azonban általában a nyugat-európai munkavállalók képességeit veszi alapul. Sajnos, a Közép-Kelet európai munkavállalók a történelmi sajátosságokból adódóan a nyugatitól eltérően szocializálódtak. Ebből kifolyólag, különbözik az értékrendjük, mások a társadalmi szokásaik, az oktatási körülményeik, a lehetőségeik, a viselkedésük. Eltérő lehet a kulturális beállítottságuk, és különbözik az intelligencia szintjük is. Ami szembetűnően hatalmas szakadékként látszik, az a társadalmak közötti jövedelemarány. Ebből adódóan más elvárásokat kell a Közép-Kelet európaiakkal szemben felállítani, mint a nyugati társadalmakban élők esetében. Így a keretrendszert is ki kell egészíteni azokkal a jellemzőkkel, amelyek erre a társadalomra jellemző tulajdonságokat is tartalmazzák. [7] Véleményem szerint, ha azok a szempontok is érvényesülnek, amelyekkel kiegészítettem a meglévő keretrendszert, akkor teljes mértékben alkalmazható lesz mindannyiunk számára. Ennek alapján a munkavállalók fel tudják mérni a saját digitális képességeiket, a munkaadók pedig képet kapnak arról, hogy a munkavállalóik milyen szintű digitális ismeretekkel rendelkeznek. Fény derülhet mindenki számára arra, hogy hol vannak hiányosságok a képességekben és mely területek azok, amelyeket már nem kell vagy nem szükséges fejleszteni. Ezáltal jelentős időt és pénzt lehet megspórolni, valamint optimalizálni lehet a munkavállalók oktatását, képességeik fejlesztését.

A kérdőív háttere

A kérdőívet először papír alapon készítettem el, amelynek kitöltésében azon rétegek válaszaira számítottam, akik valamilyen oknál fogva nem túl aktívak a digitális térben. Digitális megoldásként rátaláltam a GoogleForm alkalmazásra, amely praktikussága, hatékonysága miatt alkalmasnak bizonyult az online formájú válaszadásra, annak gyűjtésére és kiértékelésére is. A kérdőívet először magyar nyelven készítettem el, alapvetően a magyar nyelvű felhasználók válaszainak felmérésére. Ezt követően készítettem el a nemzetközi válaszadók elérése érdekében az angol nyelvű változatot. [8] A kérdőív linkjének a potenciális kitöltőkhöz történő eljuttatásban az e-mail formátumot választottam. Mivel úgy ítéltem meg, hogy a felhasználók megszólítása egy ilyen jellegű megkeresés esetén a személyes hangvétellel hatékonyabb, mintha egyéb közösségi médián keresztül kerestem volna meg őket. Természetesen én voltam az, aki minden egyes lehetséges válaszadónak elküldem a linkeket tartalmazó e-mail. Erre, úgynevezett kulcsfelhasználókat kerestem meg. Az általam a

kulcsfelhasználók részére kiküldött e-mailek száma nem haladta meg a 100-as nagyságrendet. Ez természetesen nem jelenti azt, hogy minden kulcsfelhasználó továbbította volna a levelet, akinek én elküldtem. Az általam választott kulcsfelhasználók mindegyikével személyes ismeretségben állok. A tanulmányaim során megismert hallgatótársaimnak, tanáraimnak, más egyetemek tanárainak, hallgatóinak küldtem el a kérdőívet. Segítségként használtam még az Óbudai Egyetem NEPTUN rendszerét is, melyen keresztül az egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, valamint az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallgatói és tanárai részére a Kar dékánjának engedélyével került kiküldésre a kérdőív linkjét tartalmazó e-mail. Kifejezetten ügyeltem arra, hogy általánosságban ne tegyem közzé semmilyen közösségi médián a kérdőívet. Továbbá, nem küldtem el olyan személy részére a kérdőívet tartalmazó levelet, aki nem válaszolt a segítségkérésemet tartalmazó üzenetre. A válaszadók többsége magyarországi magyar személy volt. A magyar nyelvű kérdőívet határon túl élő szerbiai és romániai magyarok is kitöltötték. Az angol nyelvű kérdőív kitöltésében elsősorban Közép-Kelet európai felhasználók aktivitására számítottam. A kérdőívet nagy számban orosz és román felhasználók töltötték ki, e mellett szerb, szlovák, cseh, lengyel, albán, macedón felhasználók is megtiszteltek a válaszaikkal. A külföldiek számára szánt angol nyelvű kérdőívet a nemzetközi kapcsolatok segítségével, általában a korábbi határon túli konferenciák alkalmával kialakított kapcsolatrendszerek segítségével sikerült szétküldeni. Az angol nyelven megküldött segítségkérő email, amit én küldtem el, megközelíti a tizenötöt. [9] Azonban előfordult az is, hogy az egyetemi ismerőseim külföldi kapcsolatainak segítségével került kiküldésre a külföldieknek szánt kérdőív. Arról sajnos nincs tudomásom, hogy a megkeresett ismerőseim mennyi angol nyelvű emailt küldtek szét a külföldi ismerőseiknek. Ebben az esetben arra ügyeltem, hogy a kérdőív a Közép-Kelet európai régió országaiban maradjon elsősorban, és a kapott válaszokkal bizonyítani tudjam azt a hipotézisemet, hogy az Európai Unió által készített keretrendszer nem minden esetben fedi le a Közép-Kelet európai régió és benne a magyarországi munkavállalók digitális kompetenciáit. Sajnos arról sincs információm, hogy mennyi külföldihez jutott el a megkeresés pontosan és abból arányaiban hányan válaszoltak. [10]

A KÉRŐÍVBŐL NYERT INFORMÁCIÓK FELHASZNÁLÁSA

A keretrendszer tökéletesítésének érdekében további célom még az volt, hogy azon felhasználók számára, akik már nem az aktív munkavállalói rendszerhez tartoznak, is elérhető legyen egyfajta képességmérő rendszer. A válaszadók kulturális és egyéb különbségeiből fakadó válaszai alapján megállapítható, hogy a keretrendszer kiegészítése, a válaszok alapján megfogalmazott szempontokkal szükséges. Az időskorú felhasználók, akik életük során nem találkoztak még a digitális eszközökkel és az azok által elérhető lehetőségekkel, vagy nem voltak rákényszerülve arra, hogy ezeket használják, ők az egyik említett felhasználói réteg. Jelen korunkban, ezzel szemben – habár már hosszú évtizedekre tehető a digitális kor kezdete – ezek az emberek egyfajta robbanásszerű dologként élik meg azt, hogy most már bárki zsebében ott lehet az internet. [11] Ennek a felhasználói rétegnek a biztonságtudatosságával igazából nincs probléma, mert bennük már kialakultak a reflexek a fizikai világban. Viszont, ha használják a digitális technológia által nyújtott lehetőségeket, nem tudják, hogy hogyan védekezzenek a digitális veszélyekkel szemben. Amennyiben nem használják ezeket a lehetőségeket, akkor saját magukat rekesztik ki a társadalmi élet újszerű formájából. Mindezt teszik úgy, hogy sokszor nincsenek tisztában azzal, hogy miről is mondanak le azzal, hogy önként, vagy külső kényszerből kirekesztik saját magukat. Fennáll azonban annak a veszélye ezen felhasználók esetében, hogy ezzel a választásukkal olyan mély társadalmi szakadékot generálnak, amely egyéb társadalmi problémákhoz is vezethet. [12]

A gyermekkorú felhasználók

Az Egyesült Királyságban gyermekkorúak (7-19 éves) internetes szokásainak felmérése során kiderült, hogy az egyes alkalmazások (közösségi hálózatok, kommunikációs csatornák és játékok) használatában igen jó kompetenciát mutatnak, azonban a felugró ablakokban megjelenő reklámok frusztrálják és félelmet keltenek bennük, pedig ezek kellő számítógépes ismerettel kikapcsolhatók. Tehát a gyermekkorú felhasználók esetében, függetlenül attól, hogy ők már a digitális világba születtek bele, nem beszélhetünk olyan szintű digitális kompetenciáról, ami elégséges lehetne a tanulás nélküli felhasználáshoz. [13] Tévhit ugyanis az, hogy ez a korosztály már úgy, olyan tudással született, hogy ők már rendelkeznek azon képességekkel, amelyekkel könnyedén elboldogulnak a digitális térben. [14] Tény, hogy sokkal gyorsabban tanulnak, mint a náluk idősebb generációk, de minden másfajta tudás elsajátítására is sokkal fogékonyabbak, legyen az az idegennyelv, vagy akár a matematikai ismeretek. Így ennek a korosztálynak a digitális kompetenciáját gyorsan és hatékonyan lehet(ne) kellő szintűre fejleszteni. Azonban nem csak lehet, hanem szükséges is azt fejleszteni. A fiatalok esetében nem elegendő csupán az ösztönös, a kíváncsiságból adódó, valamint az egymás, vagy a felnőttek utánzásán alapuló tudásra hagyatkozni, mert az beláthatatlan veszélyeket rejt magában. Vegyük figyelembe azt, hogy a gyerekek veszélyérzete jóval alacsonyabb, mint a felnőtteké, ezáltal a naivitásukból adódóan sokkal bátrabban használják a digitális eszközöket. Nem ismerik a veszélyt jelentő tényezőket, nem ismerik fel a gyanús jeleket, ezáltal könnyebben válhatnak áldozattá. [15] Szükséges ezért számukra is a mielőbbi és rendszeres, szervezett képzés-oktatás, mivel csak ilyen módon lehet felkészíteni őket a digitális világ biztonságos használatára.

A felnőttkorú felhasználók

A felnőtt korú felhasználók esetében, már általánosság az, hogy rendelkeznek valamilyen szintű digitális ismeretekkel. Ezt a tudást vagy az iskolai rendben, különböző tanfolyamok útján, vagy tapasztalati úton szerezték. [16]

Az időskorú felhasználók

Az időskorú felhasználók digitális kompetencia szintéjek a növelése azért is fontos, hogy az egységes, vagy a homogénhez közelítő digitális ismeretek révén növelhető legyen a társadalmi információbiztonság. [12] Amennyiben a társadalom ezen rétege nem rendelkezik megfelelő szintű biztonsági ismeretekkel, abban az esetben rajtuk keresztül a többi, egyébként biztonságtudatos felhasználó is veszélybe kerülhet saját tudtán kívül. Gondoljunk arra amennyiben akár egy családot, akár egy céget veszünk alapul, akik egy hálózatot használnak, hogy ott a védelem szintjét a leggyengébb felhasználó szintjéhez kell mérni. Amennyiben, például a nagymama kap egy zsaroló vírust tartalmazó kéretlen üzenetet a családi wi-fi hálózatán bejelentkezett okostelefonjára, és azt a nagymama gyanútlanul megnyitja, abban az esetben a családi hálózatra kötött összes, arra érzékeny eszköz megfertőződhet. Hiába alkalmazta a családfő, vagy a digitális-bennszülött unoka a legjobb védelmi megoldásokat. [17]

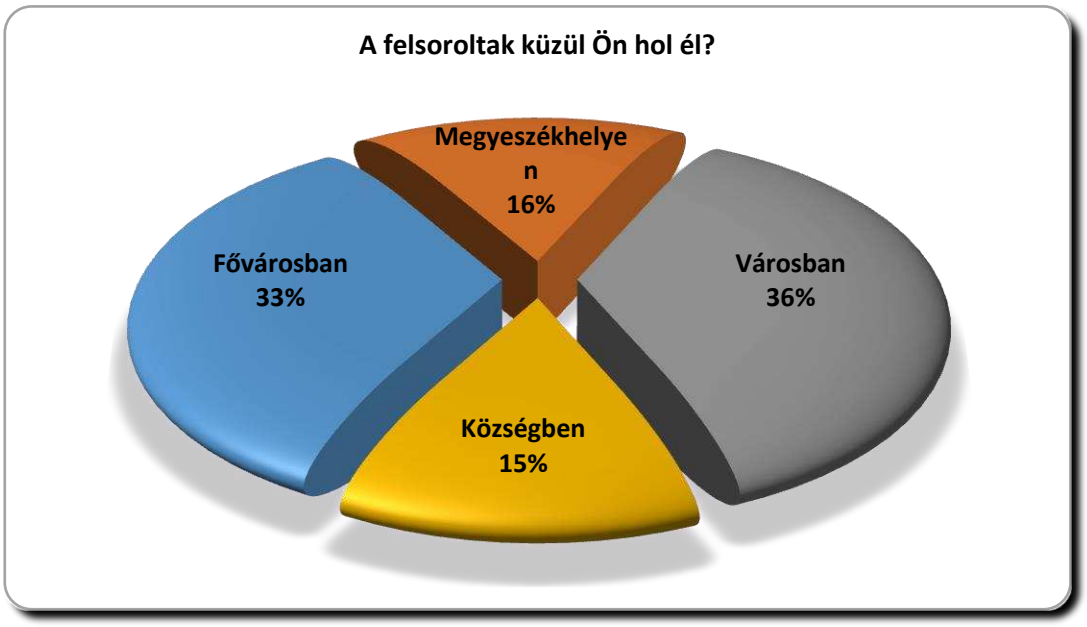
A KÉRDŐÍV KÉRDÉSEI ÉS AZOK VÁLASZAI

A kérdőívet összesen 1537-en töltötték ki, ebből a magyar nyelvűt 1274-en, amiből az online kérdőívet 1195-en, a papíralapút 79-en, valamint az angolnyelvű online változatot 236-an.

A válaszadók nemzetiségét tekintve a magyar mellet a legtöbb kitöltő orosz, román, szerb, szlovák, cseh, lengyel és macedón volt. De volt belorusz, koszovói, albán, horvát, német, luxemburgi és portugál kitöltő is.

Lakóhely szerinti eloszlás.

Az első kérdés „A felsoroltak közül Ön hol él?” volt. A kérdés feltevésével az volt a célom, hogy megtudjam azt, hogy a válaszadók milyen szerkezettípusú településen élnek. Abból a célból tettem fel ezt a kérdést, hogy láthassam azt, hogy milyen fejlettségű informatikai infrastruktúrával rendelkezhet az adott településforma, amelyet a felhasználó elérhet. Erre a kérdésre 1496 válasz érkezett. A válaszok szerint, amelyek az 1. ábrán találhatóak, a fővárosban 494-en, megyeszékhelyen 232-an, városban 545-en, míg községben 225-en élnek a válaszadók szerint.

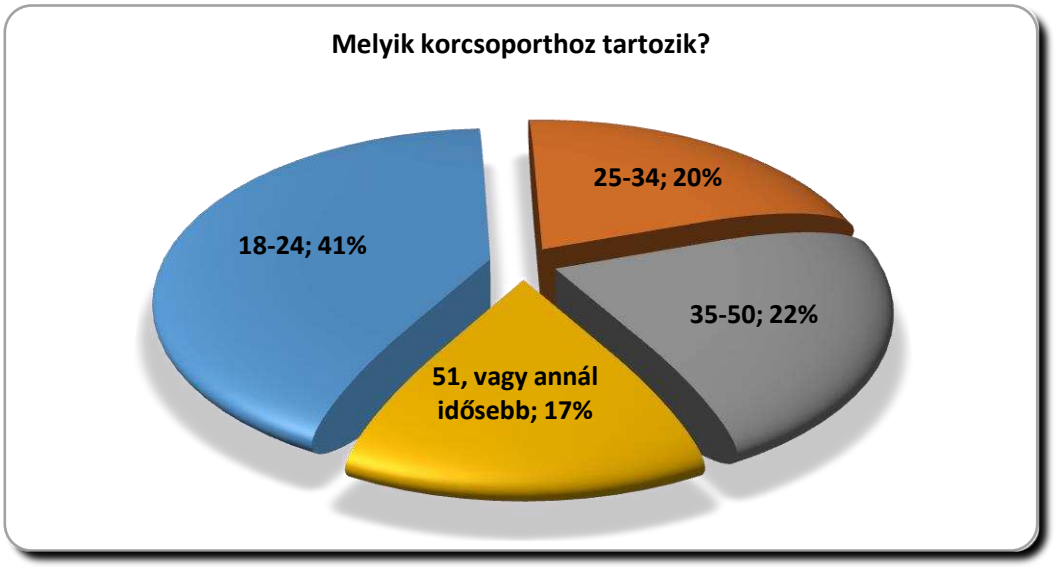


1. ábra A kérdőív „A felsoroltak közül Ön hol él?” kérdésének kiértékelése (saját szerkesztés)

Életkor szerinti eloszlás.

„Melyik korcsoporthoz tartozik?” kérdésre, amit a 2. ábra mutat be, összesen 1496-en adtak választ. A korcsoportokat az informatika fejlődésének és a felsőoktatásban résztvevők életkorának figyelembe vételével határoztam meg. Az első válasz a „18-24” korcsoport volt, ami a nappali rendű felsőoktatásban résztvevők életkorára utal. Ezt a választ összesen 614-en jelölték be. A következő válaszlehetőség a „25-34” korcsoport volt, ami látható, hogy az 1982 és 1993 között született felnőttek csoportja. Ennek a korosztálynak a tagjai, akik már az Y generáció és még a World Wide Web nyilvánossá tétele előtt született. Ezt a választ 304-en jelölték meg. A „35-50” korcsoport megjelölése volt a következő, amit 327-an jelöltek meg. Ennek a korcsoportnak a meghatározása a X generációhoz köthető. Ők azok, akiknek ahogyan korábban is említettem, felnőttként kellett megismerkedniük a számítógéppel, a mobiltelefonnal, az internettel, az e-maillel. Fel kellett venniük a tempót a digitális technológia rohamos fejlődésével. Az „51, vagy annál idősebb” választ 252-en jelölték meg. Ez a korcsoport a „Baby-boom” generációhoz tartozó felnőtteket jelenti. Ehhez a generációhoz tartozók azok, akik a digitális szakadék másik, távolabbi felén vannak. Ennek a

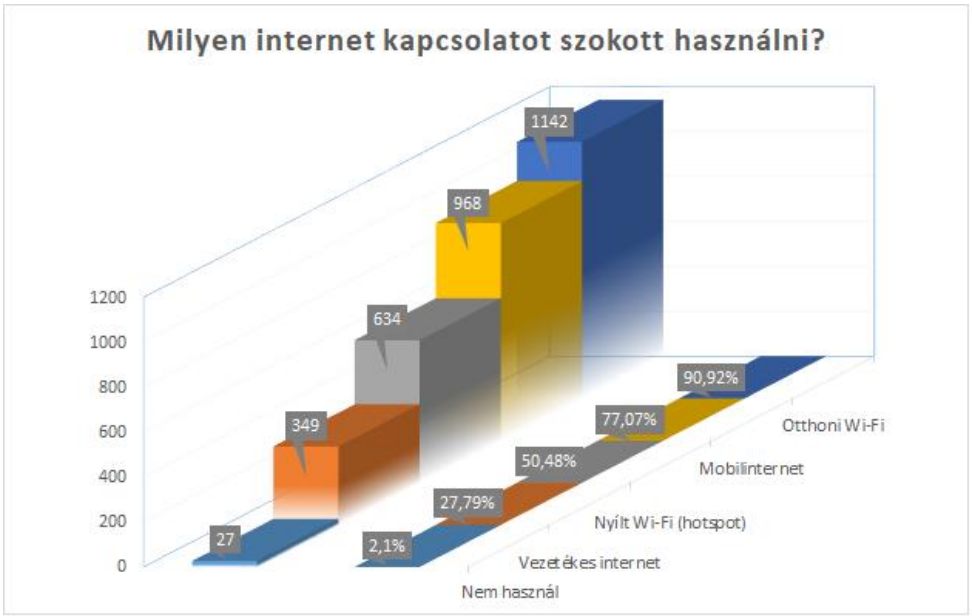
generációnak a legfiatalabbjai is már fiatal felnőttek voltak a PC korszak beköszönte idején. Az ő számukra a legnehezebb a digitális kor nyújtotta lehetőségeket beleilleszteni a mindennapjaikba.



2. ábra A kérdőív „Melyik korcsoporthoz tartozik?” kérdésének kiértékelése (saját szerkesztés)

Az internet infrastruktúra használatának eloszlása.

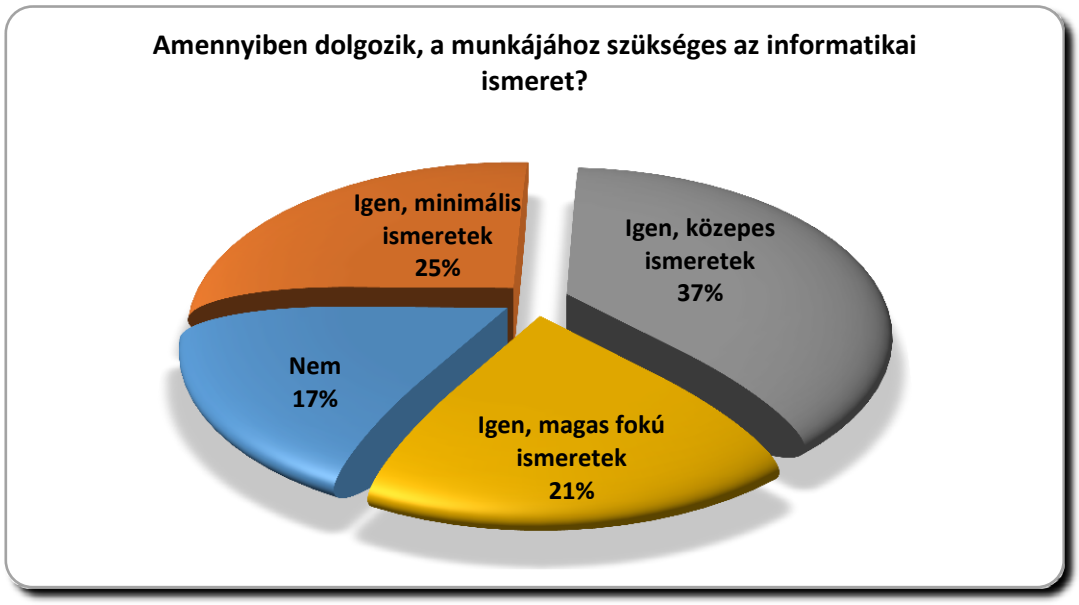
Arra a kérdésre, amelyben azt kérdeztem meg, hogy milyen típusú internet kapcsolatot szokott használni, összesen, 1256 válasz érkezett. A válaszok eloszlása a következőképpen alakult, „Előfizetéshez kapott mobilinternetet” 968-an, „Otthoni Wi-Fi hálózatot” 1142-en, „Nyílt Wi-Fi (hotspot) hálózatot” 634-en, „Vezetékes internetet” 349-en használnak, és 27-en „nem használnak” mobil eszközön internetet. A 3. ábrán található válaszokból jól látszik, hogy a válaszadók többsége az otthoni internetet használja.



3. ábra A kérdőív „ Milyen internet kapcsolatot szokott használni?” kérdésének kirétékelése (saját szerkesztés)

Az informatikai ismeretek szükségessége a munkavégzéshez.

Az már korábban is köztudott volt, hogy egyre több szakmához válik elengedhetetlenné az informatikai ismeretek megléte. A digitalizálódó világban prognosztizálható az, hogy a közeljövőben a szakmák szinte mindegyikéhez szükséges lesz a legalább alap szintű informatikai ismeretekre. Valamint, az is látható, hogy a jelenleg meglévő és elégséges informatikai ismereteknél is magasabb szintű ismeretre lesz szükség az adott szakmában a technológia egyre gyorsabb fejlődésének köszönhetően.



4. ábra A kérdőív „ Amenniben dolgozik, a munkájához szükséges az informatikai ismeret?” kérdésének kiértékelése (saját szerkesztés)

A kérdőívem egyik kérdése arra irányult, hogy jelenleg a válaszadóknak milyen szintű informatikai ismeretekre van szüksége a munkájához. A válaszok összességében megdöbbentőek, amelyet a 4. ábra mutat be, és egyben alátámasztják azt a feltételezést, amelyet az előzőekben leírtam. Az összes válaszadó közül 1399 válaszolt. Ebből a “Nem” 236, az “Igen, minimális ismeretek” 357, az “Igen, közepes ismeretek” 517, az “Igen, magas fokú ismeretek” 289 válasz volt.

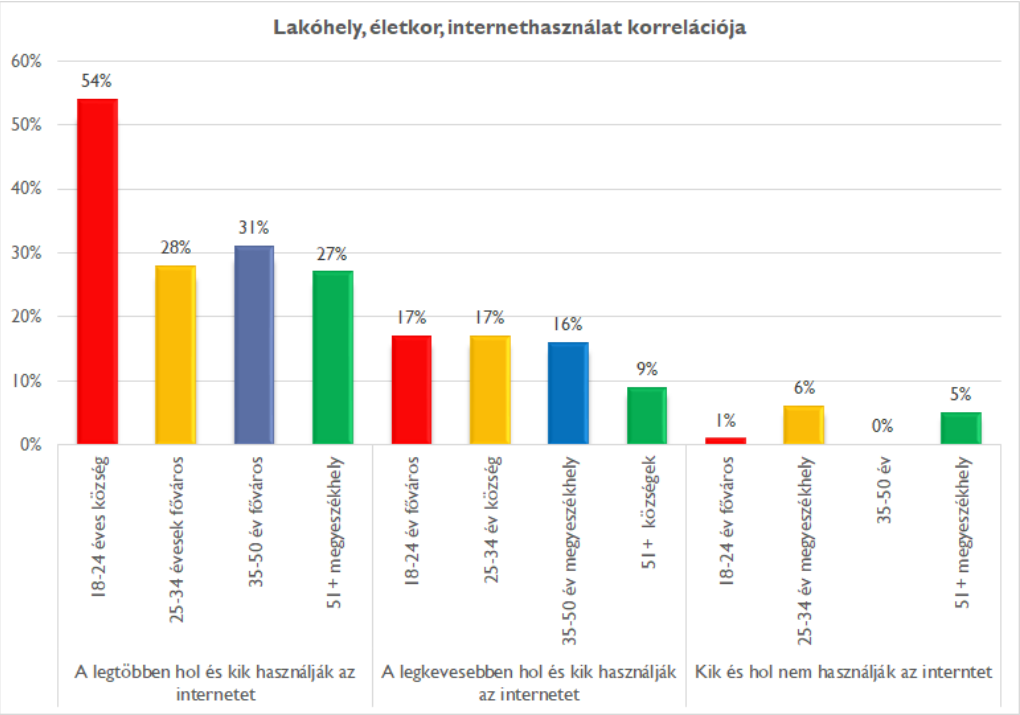
A BIZTONSÁGTUDATOSSÁG ÉS A DIGITALIS KOMPETENCIA KORRELÁCIÓJÁNAK VIZSGÁLATA

Az alábbi részben a biztonságtudatosság és a digitális kompetencia közötti összefüggéseket vizsgálom különböző értékelési szempontok alapján. A vizsgálatomhoz korrelációs mátrixot használtam, amely alapján a vizsgálati szempontok szerinti korrelációkat sikerült megtalálni.

A jó digitális kompetenciával rendelkező felhasználók biztonságtudatosságának vizsgálata.

A vizsgálatom arra irányult, hogy képet kapjak arról, hogy a lakóhely és az életkor alapján felmérjem, hogy mennyi felhasználót ért már vírustámadás, olyan összetevők alapján mint, aki gyakran internetezik, használja a hotspot-ot, használ vírusvédelmet, gyakran változtatja a jelszavát.

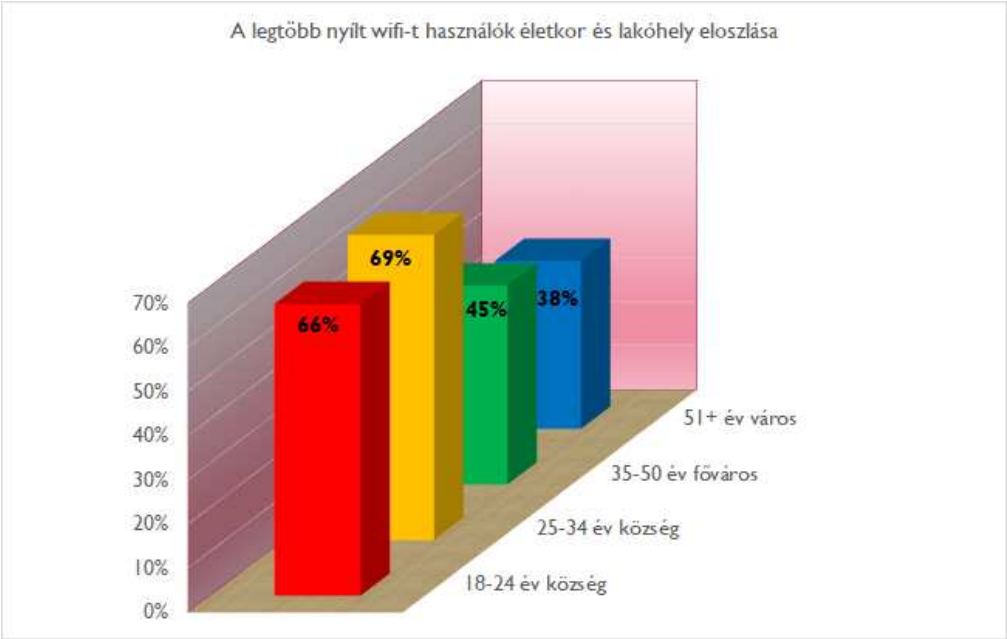
Az alábbi szempontokat tekintve megállapítható az életkort figyelembe véve a legtöbben a 18-24 év közötti válaszadók 54 %-a községekben él, a 25-34 évesek 28 %-a és a 35-50 évesek 31%-a fővárosban él, míg az 51 feletti életkorú válaszadók 27%-a megyeszékhelyeken él. A legkevesebben a 18-24 évesek közül (17%) a fővárosban, a 25-34 évesek (17%) és az 51 évnél idősebbek (9%) községekben, a 35-50 évesek (16%) megyeszékhelyeken él. Az internetet a válaszadók szinte mindegyike használja, kivéve a fővárosi 18-24 éveseknek 1%-a, a 35-50 évesek 6%-a és az 51 évnél idősebb válaszadók 5%-a megyeszékhelyeken élőknek nem használja az internetet, amely az 5. ábrán látható.



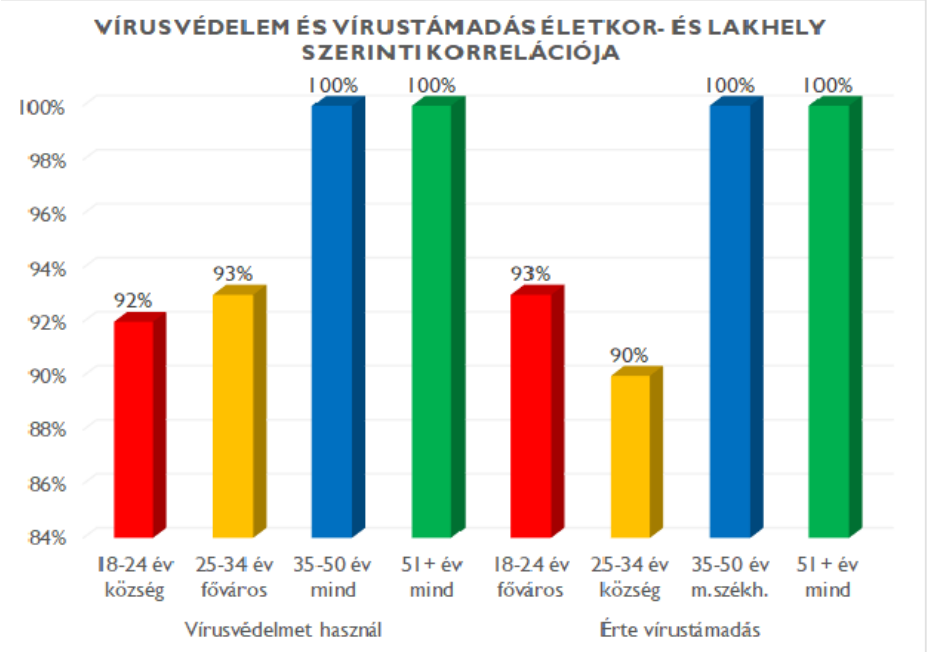
5. ábra A kérdőív válaszainak a lakóhely, életkor, internethasználat korrelációja (saját szerkesztés)

Hordozható mobil eszköze, amin internetezni szokott, a 18-24 év közötti válaszadók közül csak a városban élő mindegyikének van, a 25-34 évesek közül a fővárosban élők kivételével mindegyiknek van. Csak a 35-50 év közötti és az 50 évnél idősebb városban és községben lakó válaszadók mindegyikének van ilyen mobil eszköze. Ezek közül a nyilvános wi-fi hálózatokat, a hotspot-okat a legtöbben a 18-24 éves (66%) és a 25-34 éves (69%) válaszadók közül községben élők, a 35-50 éves fővárosiak (45%) és az 51 évnél idősebb városban élők (38%) szokták használni, ami a 6. ábrán látható.

Vírusvédelmet, a fenti szempontokat is figyelembe véve, a 35-50 és 51 évnél idősebbek mindegyike használ. Ezzel szemben a 18-24 évesek közül a községben élők (92%), a 25-34 évesek közül a fővárosban élők (93%) használnak vírusvédelmet. Ezen válaszadók közül a legtöbb vírustámadás a 18-24 éves fővárosi válaszadót (93%) és a 25-34 évesek közül a községben élő válaszadót (90%) érte. Míg a 35-50 évesek közül a megyeszékhelyeken élők és az 51 évnél idősebb fővárosi és megyeszékhelyen élők mindegyikét érte már vírustámadás, ami a 7. ábrán látható.



6. ábra A kérdőív válaszai alapján, a legtöbb nyílt wifi-t használók életkor és lakóhely szerinti eloszlása (saját szerkesztés)



7. ábra A kérdőív válaszai alapján, a legmagasabb számú vírusvédelmet használók és vírustámadás-károsultak életkor és lakhely korrelációja (saját szerkesztés)

A vizsgálat következtetései

A felmérésem eredményeként megállapítottam, hogy a vizsgált népesség digitális kompetenciáját és biztonságtudatosságát tekintve jelentős eltérés mutatható ki a lakóhely és az életkor szerint. A lakosság digitális jólétének, biztonságos internet használatának növelése képzéssel növelhető. A fiatalabb korosztály digitális kompetenciája magasabb fokú, mint az idősebb korosztályoknak. Ezzel szemben az idősebb korosztály rendelkezik magasabb biztonságtudatossággal, ami fizikai valós térben az évek során kialakult „reflexeknek” köszönhető, mert azt könnyebben át tudták ültetni a kiber térre. A probléma csak az, hogy a

biztonságtudatosságukat a digitális kompetencia alacsonyabb megléte miatt nem tudják olyan szinten alkalmazni, mint a fiatalabb generációk, akik a digitális kompetenciája magasabb fokú, de nem alakult még ki megfelelően biztonságtudatosságuk.

A fenti adatokból jól kirajzolódik, hogy azon válaszadókat érte a legnagyobb arányban vírustámadás, akik:

- 18-24 év közötti fővárosi válaszadók, a legkisebb arányban értékelték a saját biztonságtudatossági és digitális kompetencia szintjüket legalább jóra;
- 25-34 év közötti községben élő válaszadók, folyamatosan használják az internetet és a legnagyobb arányban használják a hotspot-ot.

Továbbá:

- a 35-50 év közötti megyeszékhelyen élő válaszadók mindegyikét, akik legkisebb arányban változtatják csak meg a jelszavaikat;
- az 51 évnél idősebb fővárosi és megyeszékhelyeken élők mindegyikét, akik a legkisebb arányban változtatják meg a jelszavaikat, és a legkisebb arányban értékelték legalább jóra a saját biztonságtudatossági és digitális kompetencia szintjüket.

A DIGITÁLIS KOMPETENCIÁT ÉS A BIZTONSÁGTUDATOSSÁGOT SEGÍTŐ KUTATÁSI CÉLOK

A jelenlegi társadalmi berendezkedés megkívánja a kormányzattól és a társadalom tagjaitól azt, hogy tegyenek meg mindent annak érdekében, hogy a digitális javakhoz minél többen és minél magasabb minőségben tudjanak hozzáférni. Ahhoz, hogy ez optimális lehessen, elengedhetetlen az, hogy a biztonságtudatosság és a digitális kompetencia magas szintű legyen a felhasználók esetében.

A lakosság digitális kompetencia szintjének felmérése

A felhasználók egyéni digitális kompetencia szintjének felméréséhez az Európai Unió elkészített egy keretrendszert. A kérdőíves kutatásom rámutatott, hogy ez sajnos önmagában, a meglévő szintjeivel és osztályaival nem elegendő ahhoz, hogy a Közép-Kelet európai felhasználók képességeit besorolja. [18] Ezt a keretrendszert felülvizsgáltam és elkészítettem annak módosítási javaslatát a saját eredményeim alapján. A keretrendszer felhasználásával szükséges lenne – Magyarország vonatkozásában – egy reprezentatív felmérés a fiatalok, a munkavállalók és az idősebb korúak digitális kompetenciájának felmérése. Ez alapján a teljes lakosságra vonatkozóan azok a szükséges stratégiák kidolgozhatók, illetve felülvizsgálhatóak lennének, amelyek a jelenlegi és a következő munkavállalói korosztály minél alaposabb digitális ismeretinek elmélyítését szolgálnák a versenyképes gazdaság megteremtése és fenntartása érdekében. Továbbá ez az idősebb korúak digitális szegregációját is csökkenthetné.

A digitális eszközök biztonságos használatát elősegítő fejlesztések

A tapasztalatok alapján, a jelenlegi digitális eszközökön használt operációs rendszerek és a rajtuk használt alkalmazások, sok esetben tartalmaznak olyan hibákat, amelyek a rendszer működését önmagánban nem befolyásolják, de a felhasználó hiányos ismereteiből, vagy egyéb kompetencia hiányából, valamint az éleslátás romlásából biztonsági kockázatot jelent. Az ilyen jellegű hibák, a felugró ablakokban megjelenő információk téves, vagy nem megfelelő értelmezéséből, illetve az azokra adott válaszok, utasítások megadásából erednek.

Az ilyen jellegű biztonsági rések kiküszöbölésére kidolgozom annak a lehetőségét, hogy a felugró ablakok olyan információt tartalmazó piktogramot, vagy animációt tartalmazzanak, amelyeket a felhasználók könnyen megértenek és beazonosítanak. Ennek alkalmazásával a nyelvi-, az olvasási- nehézségekkel, vagy hiányával élők biztonságos digitális eszközhasználata könnyen fejleszthető lehetne. Továbbá a gyengén látók is könnyebben tudnák használni a digitális eszközöket. Ennek, az általam megkezdett, kidolgozandó, de még nem publikált, digitális akadálymentesítésnek a lehetőségével a lakosság szinte mindegyike számára elérhetővé válna a kibertér biztonságos használata.

KÖVETKEZTETÉSEK

A fenti kutatás egyes eredményei és azokból készített korrelációk alapján is jól látható, hogy a Közép-Kelet európai lakosság biztonságtudatossági- és digitális kompetencia szintje mennyire szerteágazó. A lakóhely és az életkor alapján elkészített korrelációk jól ábrázolják azt, hogy melyek azok a gyenge pontok, amelyek alapján akár kormányzati, vagy akár társadalmi összefogással szükséges segítséget nyújtani a felhasználók számára. A felhasználók jó digitális kompetencia- és biztonságtudatossági szintje elengedhetetlen az ipari termelés optimalizálásához, valamint az jelenleg már zajló Ipar 4.0 forradalomnak a társadalom egésze számára történő kiaknázásához. Ezt segítheti az a digitális kompetencia keretrendszer, amely alapján a felhasználók ismeretszintje beazonosítható. Az Európai Unió által kidolgozott keretrendszer és a digitális intelligenciában megfogalmazottak alapján kidolgozom a magyar sajátosságokat is figyelembe vevő digitális kompetencia értékelési rendszerét. A magyar társadalom sajátosságait figyelembe vevő digitális kompetencia értékelési rendszer kidolgozásának elsődleges célja, hogy segítse a magyar gazdasági jólét szintjének emelését, annak fejlődését és a társadalom nyugati életszínvonalra történő mielőbbi felzárkózását. Továbbá biztosítsa a társadalom tagjainak a biztonságtudatossági szint növelését, amely a mindenki számára újdonság erejével ható kiberteret jellemzi. [19]

FELHASZNÁLT IRODALOM

[1] ZOMBAINÉ TARNÓTZKY, K., *"Generációk összehasonlítása, különös tekintettel a Z generáció és tanáraik között fellelhető különbségekre",* Budapesti Gazdasági Főiskola, Szakdolgozat, 2015, http://dolgozattar.repozitorium.bgf.hu/2395/1/Zombaine_Szakdolgozat.pdf, (letöltve: 2017.05.15.)

[2] *"Recommendation of The European Parliament and of The Council of 18 December 2006 on key competences for lifelong learning*" (2006/962/EC), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006H0962&from=HU , (letöltve: 2017.03.20)

[3] TOKODY, D. AND FLAMMINI, F., "*Smart Systems for the Protection of Individuals", Key Engineering Materials*, Vol. 755, pp. 190-197, 2017, DOI: 10.4028/www.scientific.net/KEM.755.190, https://www.scientific.net/Paper/Preview/525154 (letöltve: 2017.08.21.)

[4] LAZÁNYi, K., "*Stressed Out by the Information and Communication Technologies of the 21st Century*", Science Journal Of Business And Management, 4:(1-1) pp. 10-14. 2016, http://article.sciencepublishinggroup.com/pdf/10.11648.j.sjbm.s.2016040101.12.pdf (letöltve: 2017.02.06)

[5] BALÁZS, D. Á. et al., "*Building Protection with Composite Materials Application*", Key Engineering Materials, Vol. 755, pp. 286-291, 2017, 10.4028/www.scientific.net/KEM.755.286, https://www.scientific.net/KEM.755.286.pdf (letöltve: 2017.08.21.)

[6] *"Measuring Digital Skills across the EU: EU wide indicators of Digital Competence*", 2014, https://ec.europa.eu/digital-single-market/en/news/measuring-digital-skills-across-eu-eu-wide-indicators-digital-competence (letöltve: 2017.02.06)

[7] "*A common European Digital Competence Framework for Citizens. Europen Commision,* Europen Union, 2016, " https://www.openeducationeuropa.eu/sites/default/files/DIGCOMP%20brochure%202014%20.pdf (letöltve: 2017.02.06)

[8] GUTIÉRREZ PORLÁN, J., SERRANO SÁNCHEZ, J. L., „Evaluation and development of digital competence in future primary school teachers at the University of Murcia", Journal of New Approaches in Educational Research, 5(1), 51-56. doi: 10.7821/naer.2016.1.152 https://naerjournal.ua.es/article/view/v5n1-8?platform=hootsuite (letöltve: 2017.02.06)

[9] "*Digital competences - Self-assessment grid. European Union*", 2015 | http://europass.cedefop.europa.eu/sites/default/files/dc-en.pdf , (letöltve: 2017.01.21)

[10] VUORIKARI, R., PUNIE, Y., CARRETERO, S., DEN BRANDE, L. V., *„DigComp 2.0: The Digital Competence Framework for Citizens"*, 2016, DOI: 10.2791/11517, ISBN: 978-92-79-58876-1, http://www.ecdl.cz/data/ECDL-DIGCOMP-update.pdf (letöltve: 2017.03.20)

[11] ERMALAI, I. L.,"*IT Gaining Ground in Learning*", Advanced Engineering Forum, Vols. 8-9, pp. 37-44, 2013, DOI: 10.4028/www.scientific.net/AEF.8-9.37, https://www.scientific.net/AEF.8-9.37 , (letöltve: 2017.03.20)

[12] PORUMB, C., PORUMB, S., ORZA, B., VLAICU, A., "Blended Learning Concept and its Applications to Engineering Education", Advanced Engineering Forum, Vols. 8-9, pp. 55-64, 2013, DOI: 10.4028/www.scientific.net/AEF.8-9.55, https://www.scientific.net/AEF.8-9.55 (letöltve: 2017.03.20)

[13] *"Safer Internet Day Report - Have your Say: Young people's perspectives about their online rights and responsibilities",* Childnet International and the UK Safer Internet Centre, 2013, https://www.saferinternet.org.uk/safer-internet-day/sid-2013/have-your-say-survey-results, (letöltve: 2017.05.15)

[14] HOLLOWAY, D., GREEN, L., LIVINGSTONE, S., "*Zero to Eight, Young children and their internet use",* August 2013, ISSN 2045-256X http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx, (letöltve: 2017. 05.15)

[15] PORUMB, S., PORUMB, C., VLAICU, A., ORZA, B., "*Advanced Learning Tools for (Non) Formal Education*", Advanced Engineering Forum, Vols. 8-9, pp. 65-74, 2013, DOI: 10.4028/www.scientific.net/AEF.8-9.65, https://www.scientific.net/AEF.8-9.65 (letöltve: 2017.03.20)

[16] SIMON J., „*Industrial Data Acquisition Applications Using Relational Databases, IoT Environment and Multi Criteria Decision Making Systems, International Journal of Current Research in Engineering", Science and Technology 1, 2016, 34-41,* https://www.researchgate.net/profile/Janos_Simon2/publication/311257938_Industrial_

Data_Acquisition_Applications_Using_Relational_Databases_IIoT_Environment_and_Multi_Criteria_Decisio n_Making_Systems/links/584028d908ae8e63e61f756b.pdf (letöltve: 2017.03.18)

[17] TOKODY D., SCHUSTER GY., *"Driving Forces Behind Smart City Implementations-The Next Smart Revolution.",* Journal of Emerging Research and Solutions in ICT 1.2, 2016, pp. 1-16., http://eprints.fikt.edu.mk/171/ (letöltve: 2017.03.18)

[18] NYIKES Z., *"Creation Proposal for the Digital Competency Framework of the Middle-East European Region*", Key Engineering Materials, Vol. 755, pp. 106-111, 2017, DOI: 10.4028/www.scientific.net/KEM.755.106, https://www.scientific.net/KEM.755.106.pdf (letöltve: 2017.08.21.)

[19] KIM, M. K., XIE, K., CHENG S. L., „*Building teacher competency for digital content evaluation", Teaching and Teacher Education*, Elsevier, Volume 66, August 2017, Pages 309–324, https://doi.org/10.1016/j.tate.2017.05.006, http://www.sciencedirect.com/science?_ob=ShoppingCartURL&_method=add&_eid=1-s2.0-S0742051X16304140&_ts=1496105080&md5=e7240273e9c6716c47e9e5ac4baeb977 (letöltve: 2017.03.18)

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

THE CURRENT STATE OF INFORMATION COMMUNICATION TECHNOLOGY IN CRITICAL INFRASTRUCTURE: THE CASE OF VIETNAM

AZ INFORMÁCIÓ KOMMUNIKÁCIÓS TECHNOLÓGIA JELENLEGI HELYZETE A VIETNÁMI KRITIKUS INFRASTRUKTÚRÁBAN

NGUYEN, Huu Phuoc Dai, RAJNAI Zoltán

(ORCID: 0000-0003-1523-0856); (ORCID: 0000-0002-9139-736X)

phuocdaitt@yahoo.com; rajnai.zoltan@bgk.uni-obuda.hu

Abstract

Critical infrastructure (CI) is the most important key component of a national security and economic development. It involves some sectors like energy; finance; transportation; oil; gas and water distribution; health; government and emergency services. These critical infrastructures are becoming increasingly interconnected by the Information communication technology (ICT). This paper reports on the current state of ICT in the critical infrastructure of Vietnam. Moreover, the authors expressed that how the ICT influenced on CI development of Vietnam.

Keywords: *critical infrastructure, critical, infrastructure, ICT, Vietnam*

Absztrakt

A Kritikus Infrastruktúra a legfontosabb összetevője a nemzetbiztonsági és közgazdasági fejlesztésnek. Magában foglalja például az energiai, pénzügyi, közlekedési, olaj-, gáz-, és vízhálózati; egészségügyi; kormányzati és vészhelyzeti szektorokat. Ezek a kritikus infrastruktúrák egyre jobban összekötődnek az Információ kommunikációs technológiák (Information Communication Technology - ICT) által. Ez a cikk az ICT jelenlegi helyzetéről szól - a vietnámi kritikus infrastruktúrában. Kifejtjük, hogyan hatott az ICT a Kritikus Infrastruktúra fejlesztésére Vietnámban.

Kulcsszavak: *kritikus infrastruktúra, kritikus, infrastruktúra, ICT, Vietnám.*

A kézirat benyújtásának dátuma (Date of the submission): 2017.08.29.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.03.

INTRODUCTION

Internet of Things (IoT) and ICT play an important role in many aspects of our lives. With the boosting of ICT in the world, the Vietnamese government has seen the pressing the inclusion of the telecommunication services and Internet services. In particularly, ICT can offer several services or resources such as reduced operating cost; diminished paper process and improved effectiveness; and efficiency of governmental activities. However, Vietnam is a developing country and among the poorest countries in the world, as a result, Vietnam ICT industry has been recently developed. Additionally, little research has been conducted into the interconnectedness between internet services and critical infrastructure. This paper; therefore, focuses on the operationalization of current state of ICT in Vietnam critical infrastructure as well as the influence of ICT in Vietnam critical infrastructure system.

BACKGROUND

Critical infrastructure

Critical infrastructure is a combination of two words: "critical" and "infrastructure". The term "critical" involves the infrastructure that offers support for economic, public health, social well-being, and for the functioning of key government responsibilities (e.g. C. Alcaraz and S. Zeadally, 2015). The word "infrastructure" refers to physical infrastructure like transport, services, technology, communication, network, assets and so on [2]. In another hand, critical infrastructure is known as "a wide array of public facilities and equipment required to provide social services and support private sector economic activity" [3]. It includes electrical power systems; gas and oil storage and transportation; banking and finance; transportation; healthcare; information and communications; water supply system [4]; emergency services (medicine, fire and law enforcement); law enforcement and internal security; foreign affairs; government; national defense and intelligence [5]. Although critical infrastructure has many aspects, an essential thing is that internet communication technology (ICT). As a result of ICT, it can connect to all other aspects of the national critical infrastructure system. Specifically, Though ICT and IoT have positive impacts on many aspects of our modern lives, they may generate potential vulnerability as a honey pot for attackers to exploit. Thus, critical infrastructure is very important for the national security because once this operating system is damaged or disrupted, it will seriously influence not only citizens but also threaten other essential national services including the government.

Types of critical infrastructure

According to the research of (S. M. Rinaldi, 2004 and G. Giannopoulos et al, 2012), there are four types of interdependencies of critical infrastructure in Europe:

Physical: the state of one infrastructure is dependent on the output of the other. In another way, a commodity of one infrastructure (an output) was made from another infrastructure (an input). For example, water and hydro electricity generation plant are interdependent. Water provides the power to make the rotation of turbine in order to produce electricity. If the drought happens and leads to not enough water, it will directly influence hydro electricity generation plant.

Cyber: the state of each infrastructure depends on information transmitted through the information infrastructure. For instance, air transportation control system relies on the computerized control system and it needs information transmitting by the information infrastructure.

Geographic: the dependency on local geography influences that affect simultaneously several infrastructures. The fiber optic communication cables, electricity lines, and telephone lines are hung on the lamp-posts. The flow of electricity, the information transmitting on telephone lines do not influence to the fiber optic cables; however, physical damage to lamp-posts, it can be the corruption for electric power and communications.

Logical: the entire of dependency types are not a physical, cyber or geographic connection. When the price of gasoline goes down in summer holidays, travelers may flock the high ways and it can cause the traffic congestion. Therefore, logical interdependency between gasoline and transportation is not a physical process but it is due to a human decision and their actions.

ICT STATE IN VIETNAM

In VietNam, there are some ICT projects which were applying in many aspects such as:

E-government

In 2010, this year was a peak point in the development of e-government in Vietnam. Regarding the implementation of Decision 43/2008/GD-TTG and 48/2009/QD-TTG of ICT application in state agencies period 2011-2015 with a total investment of 1700 billion Viet currency[8]. Vietnamese e-government mainly focusses on four main target clients such as individuals, enterprises, governmental officials and governmental agencies. It can help Vietnamese officials to diminish time and expense; reduce stagnation, bureaucracy, and extortion; operate 24/7; satisfy the demand of social needs; increase transparency and decrease paper and so on [9]. During last 26 years, there were 5 big projects implemented, two of them was supported by French government (in 1991-1993 and 1994-1996); one was provided by State budget (1996-1998), another one was under the Prime Minister's Decision in 1997 and the last one was considered as the milestone for e-government in Viet Nam from 2001 to 2007. Although all achievements were not as expected [8], Vietnam's position rank has increased every year regarding the global rank of e-government readiness [10].

E-commerce

Vietnam has built some typical systems such as Vietnam cyber mall, real estate exchange, e-business, blue sky, book store, electronics and mechanical appliances supermarket and so on. Vietnam's IT industry is quite young and the lack of E-commerce law is one of the barriers for foreign enterprises in trading with Vietnamese firms. Therefore, during the 4th ASEAN summit in Singapore (Nov 22nd to 25th, 2000), Vietnam signed the e-ASEAN framework agreement to facilitate e-commerce in ASEAN [11]. Moreover, Vietnamese Political Bureau promulgated a Politburo's Directive No.CT58BCT on Oct 17th, 2000, followed by the government's decision No 81/2001/QDTTG to develop information technologies in the cause of industrialization and modernization [11]. With the objectives toward the year of 2020, the ICT of Vietnam will reach the advanced level in the region to make economic branch increase at the high growth rate in order to contribute to the GDP growth.

Challenges

Although Vietnam ICT human resources are rich, their IT professional skill is not enough to well compete with the other countries in the same region and in the world [12]. Moreover, the online legislative framework; for examples, legal laws or regulations for e-business, e-government, e-marketing and the like didn't get completely [11]. In addition, the current internet service providers (ISPs) also skip the security standards of their networks; hence, the computer security and information assurance issues are a major challenge for Vietnam ICT development not only for officials and providers but also for users [13]. In another way, ICT training projects for staffs, workers, and citizens are not paid attention, as a result, the qualification and capacities of IT staffs are at a low level [14]. In briefly, Vietnamese government needs to invest more budgets in some IT training projects not only for organizations but also for individuals in order to upgrade IT skill levels.

Threats / Security Concerns

According to A. Ahmad and M. A. Elhossiny,2012) and (M. U. Bokhari, et al,.), there are a lot of potential threats or security issues deal with ICT systems such as malicious attacks and hackers. Firstly, malicious attacks are related to the small program or some codes that can monitor all your online activities and capture all personal information like spywares, Trojans, adware, and so on. Moreover, they can change and damage your laptop seriously without the user's permission as virus threats. Secondly, hackers who can attack the other people via the Internet by using some malicious codes to steal, change or destroy the victim's data. Attackers can put the hidden codes inside the advertisements, photos and send them to the online social network (Facebook, Twitter …etc.). In addition, the security problems for the ICT system can be defined in different ways as authentication, available, integrity and confidentiality [16], [17].

- Integrity: unauthorized users alter or modify the content of the information by executing malicious codes.
- Authentication: the attackers steal the user's authentication or the information are eavesdropped in the insecure communication.
- Availability: the intruders use DoS or DDoS technology to attack the victims.
- Confidentiality: insecure storage, information leakage.

In fact, in November 2002, during a Hacking workshop, Vietnamese hackers showed the their penetration evidence into some important systems for example the billing system of Hanoi telecom company (the largest local provider of telephone lines), VDC (national Internet Service Provider company) and more than 80 percent of domestic company website [13]. Hence, Vietnamese government began to take the security vulnerabilities into consideration of Vietnam's Internet infrastructure.

THE INFLUENCES OF ICT ON CRITICAL INFRASTRUCTURE

Internet users

In 2000, there were only 200,000 people over approximately 79 million people - likely 0.3% citizens of Vietnamese population use the Internet as a tool to serve their lives. After 5 years later, it dramatically increased from 0.3 % to 12.7 %. Moreover, in 2010, this rate peaked up nearly 2.4 times from 12.7% to 30.7%. Consequently, Viet Nam recognized that the Internet is a

useful tool in many aspects to boost the country's development; for example, Viet Nam government invested one billion and 15 million USD for information technology in 2006. Furthermore, in 2016, there were a huge number of Vietnamese people penetrated to the Internet as 52 %. In summary, Viet Nam is a country which has approximately 95 million in the population [18]; however, the speed of approaching new technology, especially Internet is extremely fast (figure 1).

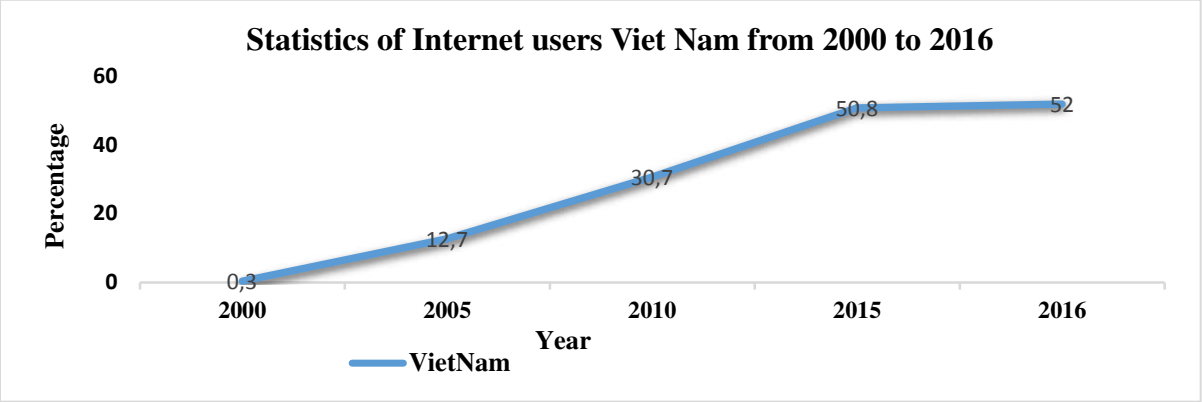


Fig.1 Viet Nam and Hungary Internet users statistics [19]; [20]

Cyber-attacks from ICT to critical infrastructure

ICT is expanding with the incredible speed in Viet Nam, especially Internet users; however, the threat of cyber-attacks in critical infrastructure also increases quickly. It threatens to not only national critical infrastructure but also national security and citizen's life. The attackers mainly use Internet as a powerful environment to hijack some parts of critical infrastructure as the government agencies, industry, and transportation. For example, in 2014, there was a report from BKAV (a famous IT and network security company in Viet Nam) said that there were more than 200 websites were attacked by Chinese hackers including six government agencies websites which have "gov.vn" domain [21]. Moreover, according to Kaspersky Lab noted that the percentage of industrial computers was attacked from 17% in July 2016 to more than 24% in December 2016. Viet Nam is the top of three targeted-attack countries with more than 66%, Algeria (over 65%) and Morocco (60%) [22]. Furthermore, the recent dangerous attack occurred on 29th, July 2016, the official website of Viet Nam Airlines was hijacked by a Trojan named (Troijan.Win32. Dropper.Encrypt.K.) and the users were redirected to another website which contained false information. It led to 400,000 Golden Lotus member's data were published on the website such as name, birthday, workplace, address, nationality, telephone number, password and so on [23]. Then, the perpetrator was identified by Chinese hacker group named 1937CN – the strongest hacker group in China. Furthermore, this group also attacked around 1000 Vietnamese websites among 15 government websites with the domain (gov.vn), 50 education websites (edu.vn) and around 200 websites of Philippines on the last two days of May in 2015 [24]. Therefore, if Vietnamese critical infrastructure is threatened or damaged, it will lead to the unimaginable effects not only for the government but also for Vietnamese citizens. These damage influenced on Vietnamese critical infrastructure, especially in air transportation.

CONCLUSION

This paper has provided an overview of how ICT is vital for the economic development and national security in Vietnam, particularly in critical infrastructure. It is hoped that ICT can help Vietnam reach the percentage of Internet users at world's average level and gain Vietnam information technologies at the advanced level in the Asian communities in 2020. Although ICT offers many chances for Vietnam to develop in the long run, it still has some security concerns. It is therefore necessary for doing further research into the security of ICT which government and individuals can rely on.

BIBLIOGRAPHY

[1] C. ALCARAZ AND S. ZEADALLY, "Critical infrastructure protection: Requirements and challenges for the 21st century," *Int. J. Crit. Infrastructure. Prot.*, vol. 8, no. 0, pp. 53–66, 2015.

[2] K. GORDON AND M. DION, "Protection of 'critical infrastructure' and the role of investment policies relating to national security," *OECD (Organisation Econ. Co-operation Dev.*, no. May, p. 11, 2008.

[3] J. MOTEFF, P. PARFOMAK, AND I. AVE, "CRS Report for Congress Received through the CRS Web Critical Infrastructure and Key Assets :" 2004.

[4] D. M. BIRKETT, "Water Critical Infrastructure Security and Its Dependencies," *J. Terror. Res.*, vol. 8, no. 2, p. 1, 2017.

[5] J. D. MOTEFF, "Critical Infrastructures : Background, Policy, and Implementation," 2015.

[6] S. M. RINALDI, "Modeling and simulating critical infrastructures and their interdependencies," *37th Annu. Hawaii Int. Conf. Syst. Sci. 2004. Proc.*, vol. 0, no. C, pp. 1–8, 2004.

[7] G. GIANNOPOULOS, R. FILIPPINI, AND M. SCHIMMER, *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art.* 2012.

[8] N. V. T. KHANH, "The critical factors affecting E-Government adoption: A Conceptual Framework in Vietnam," *Eur. J. Bus. Soc. Sci.*, vol. 2, no. 11, pp. 37–54, 2014.

[9] The S. Republic and M. O. F. Information, "SOCIALIST REPUBLIC OF VIETNAM Building e-government and applying information technology in governmental bodies ' s activities," 2008.

[10] United Nations, *E-Government Survey 2014*. 2014.

[11] B. HOANG AND M. CUONG, "Current Status of Vietnamese E-commerce."

[12] T. P. THANH AND H. M. DUC, "Truong Phuoc Thanh and Ha Minh Duc INFORMATION SOCIETY OF VIETNAM : CURRENT STATE AND PERSPECTIVE Thesis Degree Programme in Information Technology," no. April 2012.

[13] D. LE, "Challenges of Internet Development in Vietnam :" no. January, pp. 16–19, 2007.

[14] L. SCIENCE, "VIET NAM REPORT (Final report of the second phase) Institute of Labour Science and Social Affairs (ILSSA)," 2004.

[15] A. AHMAD AND M. A. ELHOSSINY, "E-Learning and Security Threats," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 12, no. 4, 2012.

[16] M. U. BOKHARI, S. KURAISHY, AND S. AHMAD, "Security Concerns and Counter Measures in E-Learning Systems."

[17] E. A. FISCHER, "Cybersecurity issues and challenges: In Brief," *Cybersp. Threat Landsc. Overview, Response Authorities, Capab.*, p. 12, 2016.

[18] "Vietnam population statistics." [Online]. Available: http://www.worldometers.info/world-population/vietnam-population/.

[19] "Vietnam internet users and population statistics." [Online]. Available: http://www.internetworldstats.com/asia/vn.htm.

[20] "Hungary internet users statistics." [Online]. Available: http://www.internetlivestats.com/internet-users/hungary/.

[21] "Vietnam and threats of cyber attacks." [Online]. Available: http://english.vietnamnet.vn/fms/science-it/155532/vietnam-and-the-threat-of-cyber-attacks.html.

[22] "Critical infrastructure targeted by cyber attacks." [Online]. Available: https://www.infosecurity-magazine.com/news/40-of-ics-critical-infrastructure/.

[23] "CMC Infosec says malware used to attack Noi Bai Airport." [Online]. Available: http://english.vietnamnet.vn/fms/science-it/161772/cmc-infosec-says-malware-used-to-attack-noi-bai-airport.html.

[24] "Chinese attacked 1000 Vietnam website." [Online]. Available: http://tuoitrenews.vn/society/28449/chinese-hackers-attack-1000-vietnamese-websites-in-two-days.

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

RADAROK ELEKTRONIKAI VÉDELME I. (ELMÉLETI MEGKÖZELÍTÉS)

ELECTRONIC PROTECTION OF RADARS (THEORETICAL APPROACH)

SZÖKRÉNY Zoltán

(ORCID ID: 0000-0001-7411-5546)

szokreny.zoltan@uni-nke.hu

Absztrakt

A rádióelektronikai zavarás elleni védelem napjaink kiemelt kutatási területe. A radarok üzemszerű működésük közben a természetes zavarforrásokon kívül harci körülmények közt szándékos radar performancia csökkentő hatásoknak vannak kitéve. A külső zajok, zavarok a hatékony felderítést megnehezítik vagy akár lehetetlenné is teszik. A cikk áttekinti a radarokra ható elektromágneses zavarokat és egy lehetséges szempontból osztályozza őket. Az alapok mellett tisztázza az elektronikai ellentevékenység elleni tevékenység (ECCM) fogalmát és lehetőségeit. A pontos gyakorlati megoldások a cikk második részében kerülnek ismertetésre. A radaregyenlet (Blake chart) számításaival elemzi a különböző teljesítményű zavaró adók különböző távolságon történő zavarás hatását.

Kulcsszavak: *radar maximális hatótávolság, Elektronikai ellentevékenység elleni tevékenység (ECCM), zavarás, Blake chart*

Abstract

The protection against radio electronic jamming is a major field of research today one of the elements of the electronic warfare. The radar performances are reduced by the effects of jamming among combat conditions, and natural sources of interference in normal operation. The external noises and interferences make the effective detection more difficult or even impossible. The article reviews the radar electromagnetic interferences and classifies them as a possible point of view. It clarifies the definition of Electronic Counter - Countermeasures (ECCM) and capabilities. The exact practical solutions are presented in the second part of the article. The radar equation (Blake chart) calculations analyzes the interferences effects at different distances of several jamming power of transmitters.

Keywords: *radar maximal range. Electronic Counter Counter Measures (ECCM), jamming, Blake chart*

A kézirat benyújtásának dátuma (Date of the submission): 2017.06.29.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.12.

BEVEZETÉS

A rádiólokátorok nagy érzékenységű elektronikus mérőberendezések, amelyek eredményességét a szándékos, vagy környezeti zavarjelek jelentősen befolyásolhatják. Mint minden elektronikai eszközt, ezeket is védeni kell a zavaró, teljesítményüket negatívan befolyásoló hatásoktól. Az elektronikai hadviselés (EW[1]) a második világháború óta folyamatos fejlődésen ment keresztül, és mára már meghatározó tényezője a modern hadviselésnek.

A jelenlegi katonai doktrínánk szerint nincs közvetlen veszély, ami Európát fenyegetné, azonban a légtérfelügyelet magas szintű biztosítása kockázatos és költséges feladat. Bármikor felléphet olyan helyzet, amikor a valós idejű információszerzés nélkülözhetetlen, ugyanakkor ez kívülről kis költséggel bénítható. Lokátoraink 1999. március 12-i csatlakozásunk óta a NATO integrált légvédelmi rendszerének a NATINADS[2] részei és az óta folyamatos készültségi szolgálatot látnak el. A békeidőben is harcfeladatot ellátó berendezéseinknél kiemelten fontos, hogy a céltárgy detektálás, útvonalba fogás és az azonosított légihelyzet-kép (RAP[3]) előállításához szükséges radar információk - egy szándékos zavarás vagy az állandóan jelen lévő természetes interferenciák ellenére is - egyértelműen rendelkezésre álljanak a felhasználók számára.

Írásomban a radarok elleni szándékos elektronikai zavarásokkal foglalkozom. Tisztázom az alapfogalmakat, majd számításokkal igazolom a zavaró eszközök hatékonyságát. A radaregyenlet alapján bizonyítom hatásosságukat és a radarokban az ellenük használható módszerek szükségességét.

A RADAROK ELEKTROMÁGNESES ZAVAROK ELLENI VÉDELMÉNEK ELMÉLETI ALAPJAI

Alapfogalmak

Elektromágneses zavarnak (EMI[4]) nevezünk bármely olyan elektromágneses jelenséget, amely ronthatja a berendezések működését. Az EMI lehet elektromágneses zaj, nem kívánt jel, vagy magában a továbbító közegben bekövetkező változás. [1]

Az elektronikai hadviselés (EW) fogalma a MH Összhaderőnemi Doktrína definíciója alapján: „Az elektronikai hadviselés: a műveleti (hadműveleti, harc-) támogatás fajtája. Azon tevékenységek összessége, amelyek az elektromágneses spektrum ellenség által történő felhasználásának meghatározására, felderítésére, csökkentésére vagy megakadályozására, illetve az elektromágneses energia és az irányított energia felhasználására, az elektromágneses spektrum saját célú felhasználására, valamint az ellenség vezetési és irányítási rendszerei támadásának támogatására, a saját csapatok védelmére irányulnak.” [2]

Az elektronikai hadviselés három egymást kiegészítő, valamint egymást részben átfedő területre osztható fel:

- elektronikus hadviselést támogató tevékenység (ESM[5]): „Az elektronikai támogatás az elektronikai hadviselés azon területe, amely az ellenség helyzetére vonatkozó tájékozottság és a fenyegetés késedelem nélküli felismerése céljából magában

[1] Electronic Warfare - elektronikai hadviselés (EHV)
[2] NATINADS - NATO Integrated Air Defense System
[3] RAP - Recognized Air Picture - azonosított légihelyzet-kép
[4] Electromagnetic Interference – elektromágnese zavar (interferencia)
[5] Electronic Support Measures - elektronikus hadviselést támogató tevékenység

foglalja az elektromágneses kisugárzások kutatását, felfedését és azonosítását, valamint a kisugárzók helyének meghatározását." [3] Ez a tevékenység az elektromágneses jelek kutatásán, elfogásán, azok térbeli meghatározásán alapul.

- elektronikai ellentevékenység (ECM[6]): „Az elektronikai ellentevékenység az elektronikai hadviselés azon területe, amely magába foglalja az elektromágneses és egyéb irányított energiák kisugárzását abból a célból, hogy megakadályozza vagy csökkentse az elektromágneses spektrum ellenség által való hatékony használatát." [3]
- elektronikai védelem (EPM[7]): „Az elektronikai hadviselés azon területe, amely biztosítja az elektromágneses spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok által okozott nem szándékos (kölcsönös) rádiózavarok előfordulása ellenére." [4] Az elektronikai felderítéssel, elektronikai ellentevékenységgel illetve az ellenfél vezetési és fegyverirányítási eszközeinek megbontására irányuló minden más tevékenységgel összhangban kell végezni. A radartechnikában az ezen a területet magába foglaló módszereket az elektronikai ellentevékenység elleni tevékenységnek (ECCM[8]) nevezzük.

„Elektromágneses kompatibilitásnak (EMC[9]) nevezzük egy készülék, berendezés vagy rendszer azon képességét, hogy elektromágneses környezetben kielégítően tud működni, és ugyanakkor nem hoz létre elfogadhatatlan mértékű elektromágneses zavar jelet." [5]

Zavarstabilitásnak nevezzük a lokátor azon tulajdonságát és képességét, amely kifejezi, hogy az adott rendszer az elektronikai zavarás viszonyai között képes-e funkcionális feladatainak végrehajtására.

Zavarvédettségnek (EMS[10]) nevezzük valamely elektronikus berendezés tűrőképességét a nemkívánatos elektromágneses energia hatásával szemben. Egy adott áramkör, egység vagy rendszer érzékenységi szintjét az a zavarkörnyezet határozza meg, amelyben az még megbízhatóan működni képes. Minél jobb a rendszeren belül a zavarvédettség, annál nagyobb a zavarstabilitás. [6]

A zavarok osztályozása

A zavarás, zavartatás szempontjából legfontosabb a jel-zaj+interferencia viszony értékelése. Ezt a radaregyenletből kiindulva tesszük meg, melyet három fő részre osztunk:

$$\frac{S_R(t)}{N_R} = \frac{P_{átl} t_o G_{tr} F_{tr}^{\ 2}}{(4\pi) L_t} \quad \frac{\sigma F_P^{\ 2}}{(4\pi)} \quad \frac{\lambda^2 G_r F_r^{\ 2}}{(4\pi) k T_s B_r L_\alpha R_{\max}^{\ 4}} \tag{1}$$

ahol :

- a radar adási szakaszára jellemző tényezők:

[6] Electronic Countermeasures - elektronikai ellentevékenység
[7] Electronic Protective Measures - elektronikai védelem
[8] Electronic Counter-Countermeasures - elektronikai ellentevékenység elleni tevékenység
[9] Electromagnetic Compatibility - elektromágneses kompatibilitás
[10] Electromagnetic Susceptibility - elektromágneses érzékenység

- $P_{átl}$ – az adó átlagteljesítménye, $P_{átl}=P_t\tau f_{PRF}$ ahol P_t az adóimpulzus teljesítménye, és τ- az adóimpulzus időtartama, $f_{PRF}=n/t_0$
- t_o – a céltárgy besugárzásának ideje „n” impulzus által,
- G_{tr} – az adóantenna nyeresége,
- F_{tr}– a hullámterjedési tényező az adótól a céltárgyig,
- L_t – adási veszteség.

− a céltárgyra jellemző tényezők:
- σ– a céltárgy hatásos visszaverő felülete,
- F_p– a polarizációs tényező az adójel polarizáció változása a céltárgy felületén.

− a radar vételi szakaszára jellemző tényezők:
- λ – a radar üzemi hullámhossza,
- G_r – a vevőantenna nyeresége,
- F_r– a hullámterjedési tényező a céltárgytól a vevő bemenetéig,
- k – a Boltzmann-állandó,
- T_s – a vevő bemenetére redukált rendszer zajhőmérséklet,
- B_r– a radar vevőrendszereinek pillanatnyi sávszélessége (az adójelre illesztett impulzus minimális veszteséggel való vételére optimalizált sávszélesség),
- L_α – atmoszféra csillapítása,
- Rmax– a maximális hatótávolság (egyenes rálátás esetén).

Az egyenletbe csoportosítva vannak azok a tényezők, amelyek a feladat elméleti áttekintéséhez szükségesek. A radarmérnök feladata a jel-zaj+interferencia viszony növelése. Ezzel szemben a radart zavarni szándékozó szakemberek jel-zaj+interferencia viszony csökkentésére törekednek, illetve ha ezt nem tudják elérni, olyan hamis céljeleket imitálnak, melynek az elvárt céljel-zaj viszonya meghaladja a céltárgyra jellemző értékeket. Ennek elérésére több módszer is ismert. Evidensnek tűnik a visszavert jelek szintjének csökkentése, például a lopakodó technológiák alkalmazása, vagy a vevő zajszínjének a növelése külső zavarás által. Ez utóbbi vizsgálata a cikk tárgya.

A zavarás részletesebb matematikai analízise

A szándékos, aktív zavarás viszonyainak részletesebb elemzéséhez az (1) egyenletet átírjuk az alábbi, a maximális szabadtéri hatótávolságot kifejező alakra [7]:

$$R_{\max}^4 = \frac{P_{átl} t_o G_t G_r \lambda^2 \sigma F^4}{(4\pi)^3 (kT_s + qJ_0) D_x(n) L_t L_\alpha} \tag{2}$$

ahol :

− q – a zaj minőségi faktora,

− $J_0 = \frac{P_j G_j G_r \lambda^2 F_j^2}{(4\pi)^2 R_j^2 B_j L_{\alpha j}}$ a zavarás spektrumsűrűsége; (3)

ahol:
- P_j – a zavaró adó teljesítménye,
- G_j – a zavaró antenna nyeresége,
- G_r – a radarantenna nyeresége,

- F_j – a zavaró jel karakterisztika terjedési tényezője,
- R_j – a zavaró hatótávolsága,
- B_j – a zavaró adó sávszélessége,
  - $L_{\alpha j}$ – a szakaszcsillapítás a zavaradótól a radarig.

− Dx (n) - detektálási tényező, ahol 'n' a céltárgyról visszaverődött és a radar által integrált impulzusok száma, (n=1 az adott céltárgyra jellemző *egy impulzushoz tartozó jel-zaj viszony*, Swerling típusok)

A radarokat zavaró eszközök általában légi hordozókon: felderítő és zavaró repülőgépeken illetve helikoptereken találhatók, melyek őrjáratozási légtérből tevékenykednek. Ma már az új repülőgépek fejlesztésekor egyre nagyobb hangsúlyt fektetnek az önálló elektronikai hadviselési képességek beépítésére. Ezek szinte kizárólag automatikus működtetésű rendszerek. A fedélzeti önvédelmi rendszerekben általában rádiólokátorokat zavaró berendezések vannak, míg a kommunikációs zavarók hiányoznak. Kiemelt gyorsasággal fejlődnek a pilóta nélküli repülőgépek, amelyek különböző kategóriás akár hadműveleti és harcászati szinten is alkalmasak a kisméretű, korszerű zavaró berendezések hordozására.

Őrjáratozási légtérből végrehajtott zavarás (SOJ11) esetén a 2. számú egyenlet egyszerűsített formája: [8]

$$R_{\max}^4 = \frac{P_{átl} t_o G_t G_r \sigma F^4}{(4\pi)^3 k (T_s + T_j) D_x(n) L_t L_\alpha} \tag{4}$$

ahol:

$$T_J = \frac{J_0}{k} = \frac{P_j G_j G_r \lambda^2 F_j^2}{(4\pi)^2 R_j^2 B_j L_{\alpha j}} \tag{5}$$

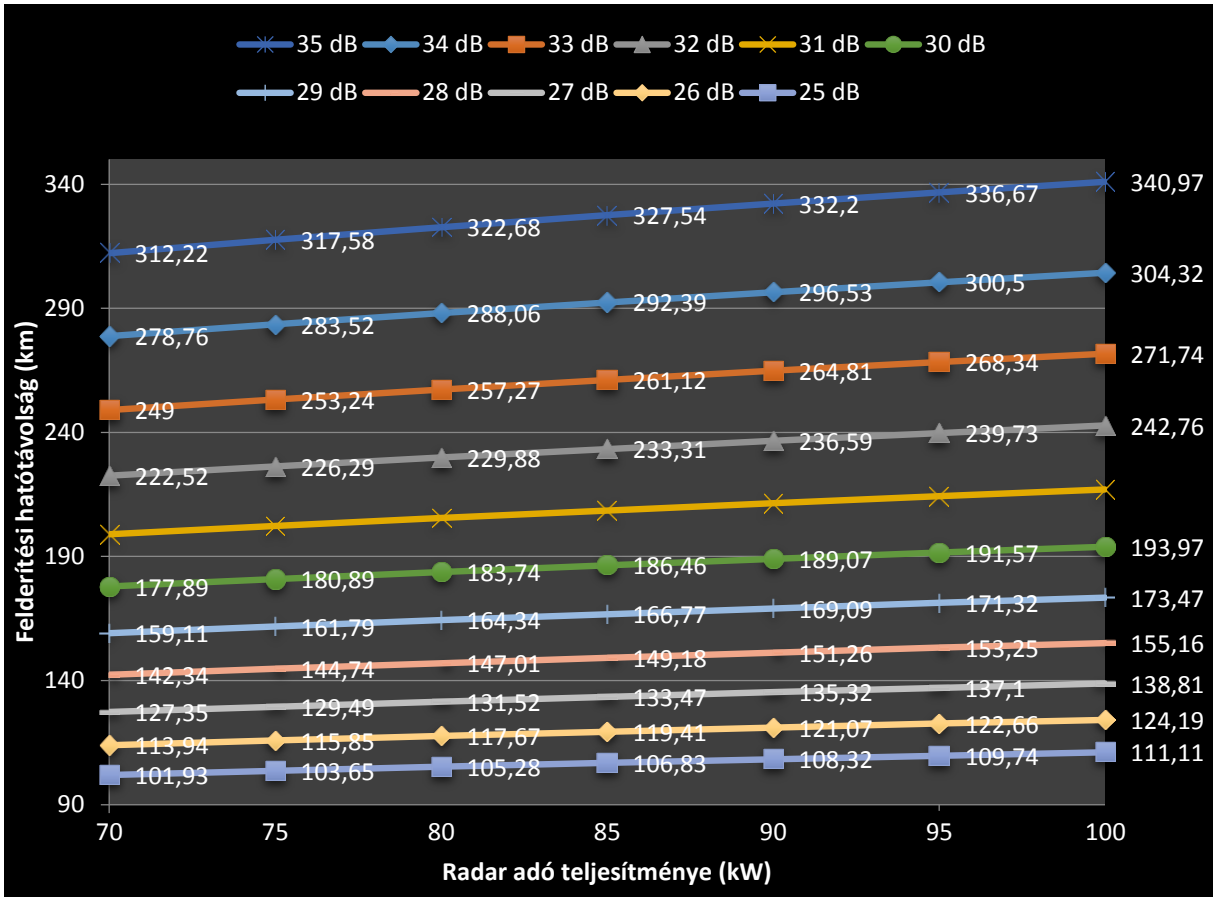
A környezeti, topológiai körülményeket és a zavaró teljesítmény jellemzőit kifejező változók nagyban befolyásolják a radar maximális hatótávolságát, melyet a következőkben Blake chart számítások segítségével szemléltetek.

Kísérő zavarás (EJ[12]) esetén a saját vagy a kíséretében tartózkodó légi járművek tevékenységének a fedése a cél a fedélzetén lévő zavaró eszközökkel.

Az (1) egyenlet első tagja a radar adótraktusának jellemzői. Ezek közül a hullámterjedési tényezővel (az adótól a céltárgyig) és nagy adási veszteséggel optimálisan megválasztott konstrukció esetén a későbbiekben egy konstans értékkel számolok. Az adóantenna megfelelő konstrukciója esetén a jel-zaj+interferencia viszony vagy a radar egyértelműségi hatótávolsága jelentősen változhat, de az egyenes láthatóság szempontjából adottnak tekinthető. Az 1. ábra mutatja a 25 és 35 dB közti antennanyereség 1 dB-enkénti változása mellett a hatótávolság növekedését. Jól látható, hogy míg 100 kW-os adóteljesítmény és 35 dB-es antenna nyereség esetén is a hatótávolság 340,97 km. Ugyanezzel a teljesítménnyel, de 25 dB-es antenna nyereséggel már csak az korábbi hatótávolság alig harmada 111,11 km. Ugyanez a kb. 30%-os hatótávolság csökkenés igaz a kisebb adóteljesítménnyel számított értékeknél is.

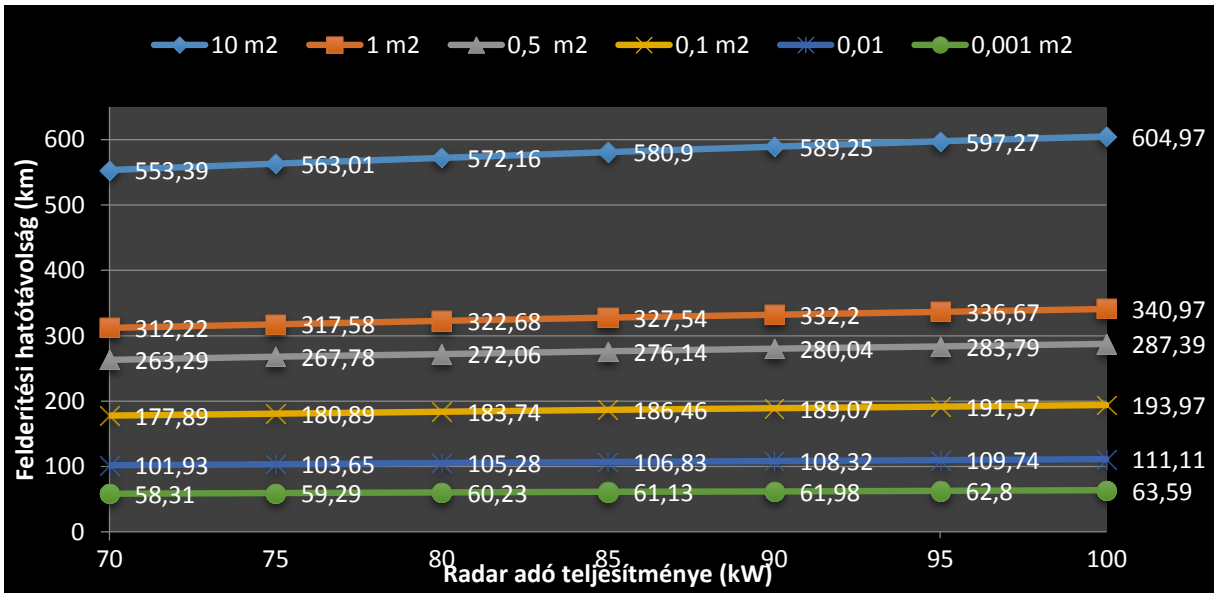
[11] SOJ – Stand-off Jamming – őrjáratozási légtérből végrehajtott zavarás
[12] EJ – Escort Jamming – kísérő zavarás

Az (1) egyenlet középső tagja a légtérben tartózkodó repülő eszközök és az azokról visszaverődő jelek paramétereit szemlélteti. A polarizációs tényező az adójel polarizáció változását mutatja a céltárgy felületén. Ezt nem tudjuk befolyásolni a számításokban konstans érték. A σ (a céltárgy hatásos visszaverő felülete) az angol nyelvű szakirodalomban RCS[13] a céltárgyra leginkább jellemző paraméter. Nagymértékben függ a repülőgép besugárzási szögétől és a visszaverő felület anyagától, minőségétől és fluktuációjától. Általánosan elfogadott érték (az „S" frekvencia sávban) hogy, a civil utasszállító, katonai csapatszállító vagy bombázó repülőgép 10-100 m^2-es, egy hagyományos vadászgép 1-5 m^2-es, egy lopakodó technológiával készült vadászgép 0,1-0,01 m^2-es, egy föld levegő rakéta, egy közepes méretű UAV, szárnyas rakéta szintén 0,1-0,01 m^2-es, míg egy kisméretű drón vagy madár 0,001 m^2-es hatásos visszaverő felülettel (RCS-el) rendelkezik. Az F–22 Raptor az USAF félrevezető állítása szerint egy üveggolyóéval megegyező, azaz körülbelül 0,0001–0,0014 m², míg egy F-35 Lightning II 0,005 m2-es hatásos visszaverő felülettel rendelkezik. A 2. ábra a különböző hatásos visszaverő felülettel rendelkező céltárgyak felderítési távolságra gyakorolt hatását mutatja növekvő adóteljesítmények esetén.



1. ábra A radar maximális hatótávolsága 25-35 dB antennanyereség esetén (saját szerkesztés)

[13] RCS – Radar Cross Section – a céltárgy hatásos visszaverő felülete



2. ábra A radar maximális hatótávolsága 0,001-10 m^2 RCS értékek esetén (saját szerkesztés)

Az (1) egyenlet utolsó tagja a radar vevőtraktusának jellemzőit tartalmazza. Monosztatikus radar összeállítást használva a vevő antenna nyeresége megegyezik az adóantennáéval. A hullámterjedési tényező (a céltárgytól a vevő bemenetéig) optimális helyzetben megegyezik az adáskori hullámterjedési tényezővel. A radarvevő pillanatnyi sávszélességének csökkentése illetve növelése szinkron zavarás esetén ugyan növelné a jel-zaj viszonyt, azonban ezt csak egy határig tehetjük meg, mert az adójelre illesztett impulzus minimális veszteséggel való vételére optimalizált a sávszélesség.

A RADAR MAXIMÁLIS HATÓTÁVOLSÁGA ZAVARMENTES ÉS ZAVAR ALATTI ESETBEN BLAKE CHART SZÁMÍTÁSOKKAL IGAZOLVA

A Blake chart [9] egy a radarok maximális hatótávolságát kiszámító egyenletrendszer, amelyet először Lamont V. Blake alkotott meg 1962-ben az Amerikai Egyesült Államok haditengerészeti kutató-laboratóriumának radartechnológiai osztályán. Az általam használt táblázat Microsoft Office Excel alapú munkalap, amelyben megadhatóak a radar valamint a zavaró adó főbb a számításokhoz szükséges technikai paraméterei. A Blake chart szimulációnál a zavaró adó sávszélessége nagyobb, mint a radarvevő sávszélessége és fehér zaj jellegű.

A radar előírt detekciós valószínűség legyen P_d=0,9, az előírt vakriasztási valószínűség legyen $P_{fa}=10^{-6}$. A radar végezzen térletapogatást 3D-ben 6 fordulat/perc sebességgel.

A radar és a zavaradó mint rendszer a következő harcászat- technikai paraméterekkel rendelkezik:

A számítások során feltételeztem, hogy a lokátor egy „átlagos” a mai kor követelményeinek megfelelő berendezés, amely a következő harcászati-műszaki elvárásoknak felel meg:

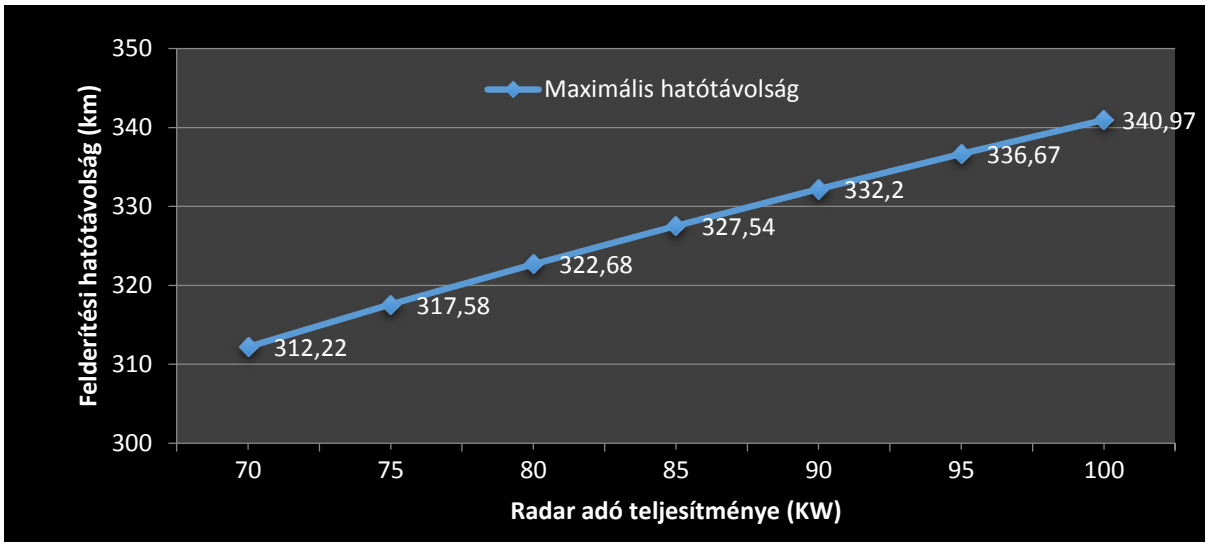
- Az adó impulzusteljesítménye: 70-75-80-85-90-95-100 kW,
- az adóimpulzus szélessége: 100 µs,
- az impulzus ismétlődési frekvencia: 500 Hz,
- az üzemi frekvencia: 1250 MHz,
- az antenna nyalábszélessége: 2^o,
- az antenna nyeresége adáskor és vételkor is: 35 dB,
- az antenna elektromos középpontjának magassága: 6 m.

A céltárgy Swerling 1 modell, σ=1 m^2 hatásos visszaverő felülettel.
A zavaró eszköz műszaki paraméterei:

- az adó átlagteljesítménye: 10-100-200-1000W,
- a zavarás fajtája: folyamatos (CW),
- az üzemi frekvencia: 1250 MHz,
- az adó sávszélessége: 200 MHz,
- az antenna nyeresége a radar irányába: 10 dB.

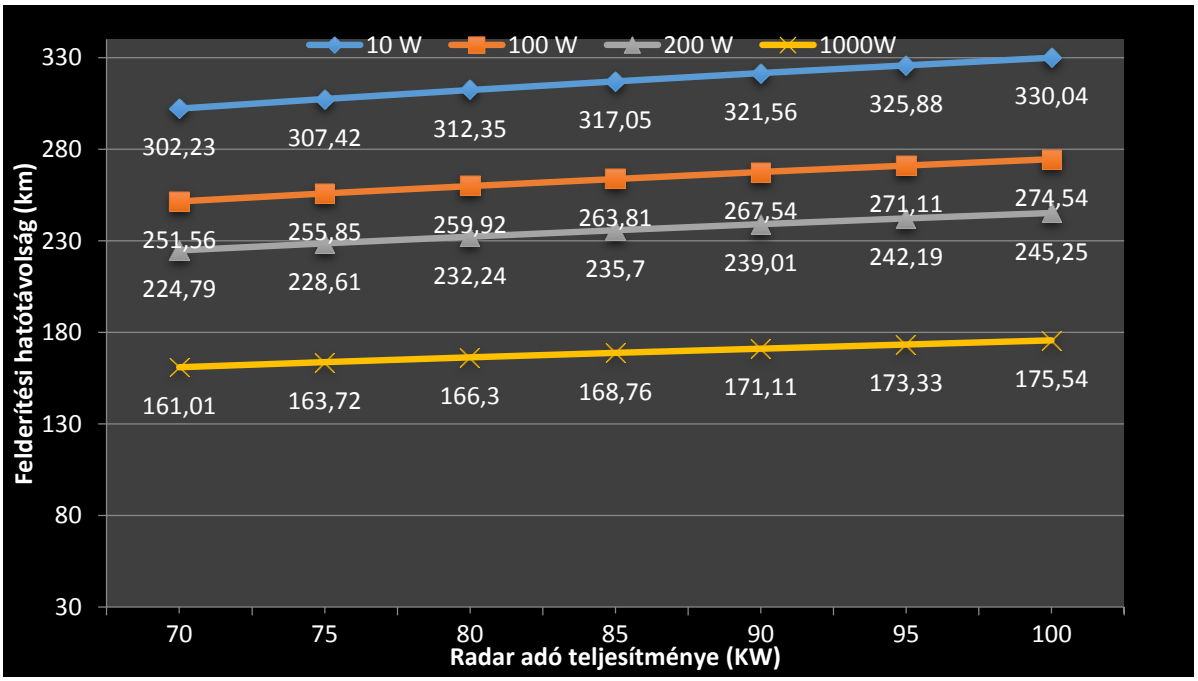
A radar és a zavaró adó közti távolságot 300, 100, 50 és végül 10 km-re választva számoltam ki a céltárgy maximális detektálhatóságát. A zavaró adó helyszöge a radarhoz képest 2,2°.

Első eset: A lokátor zavarmentes környezetben üzemel a korábban felsorolt harcászat-technikai paraméterekkel. Ebben az esetben a különböző teljesítményű adóimpulzusokkal számított maximális hatótávolságokat a 3. ábra tartalmazza.



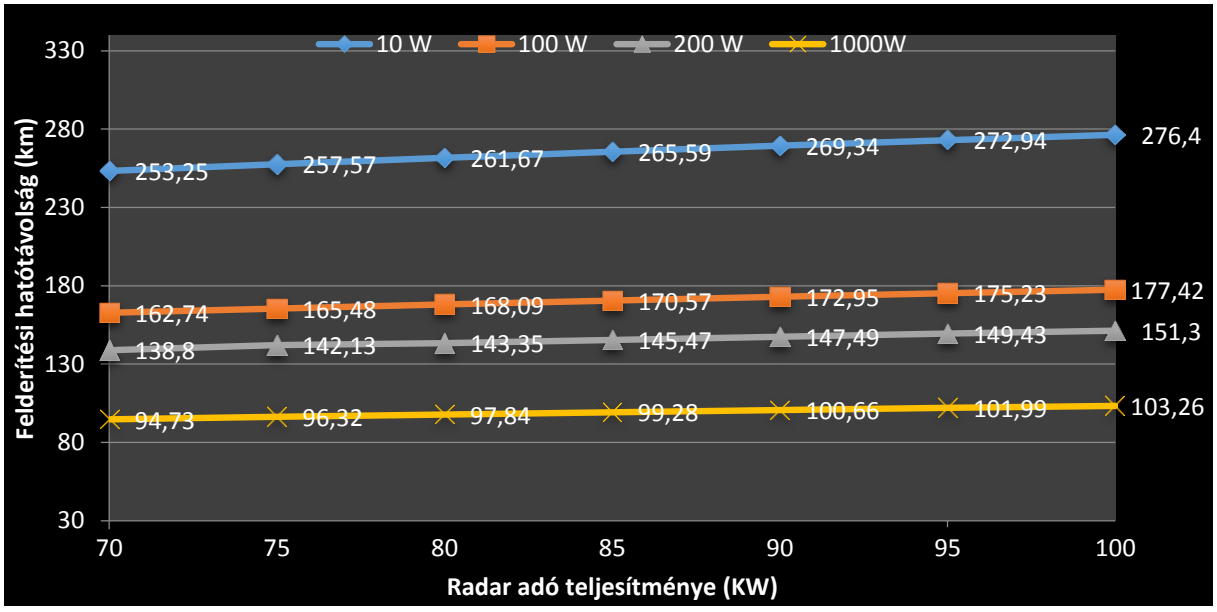
3. ábra: A radar maximális hatótávolsága zavarás nélkül (saját szerkesztés)

Második eset: A lokátor és a zavaradó távolsága 300 km (ez közel van a lokátor maximális hatótávolságához zavarás nélkül), mely megfelel az őrjáratozási légtérből végrehajtott zavarás módszerének. A zavaradó helyszöge 2.2°, sávszélessége 200 MHz (ez minden esetben nagyobb a radar vételi sávszélességénél), az effektív kisugárzott teljesítménye 100W, 1KW, 2KW és 10 KW (10W, 100W, 200W és 1 kW zavaró teljesítmény - P_j). Ebben az esetben a különböző teljesítményű adóimpulzusokkal számított maximális hatótávolságokat a 4. ábra tartalmazza.



4. ábra A maximális hatótávolság a zavaradótól 300 km-re (saját szerkesztés)

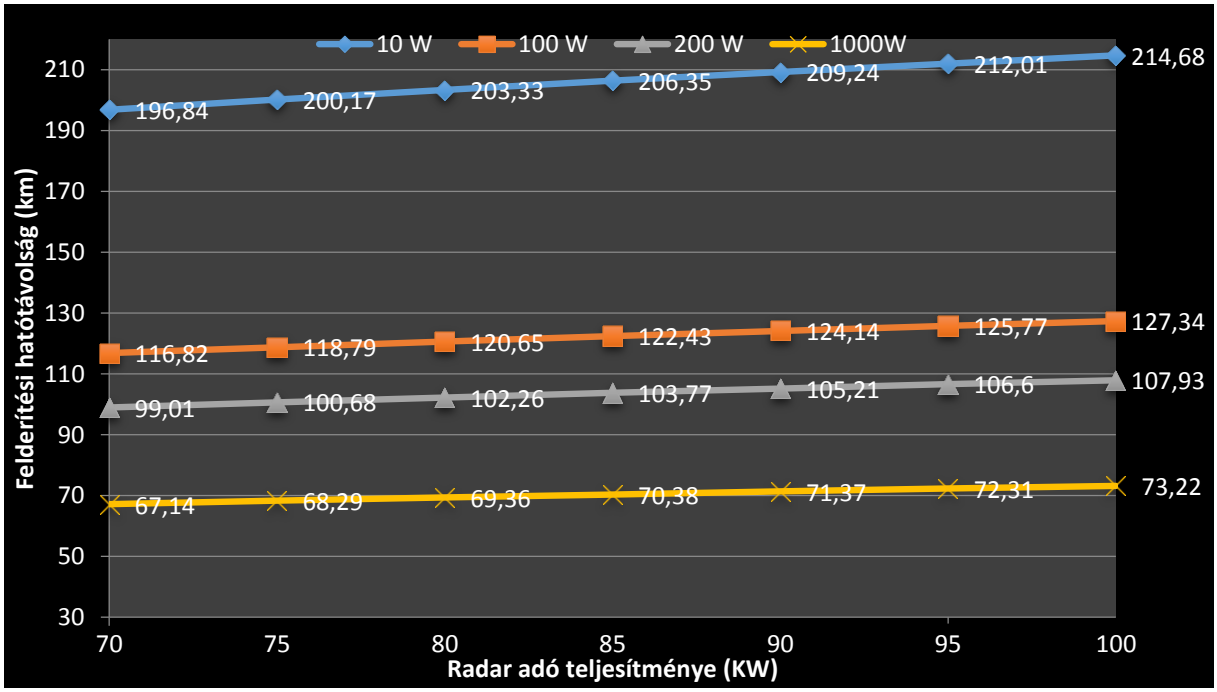
Harmadik eset: A lokátor és a zavaradó távolsága 100 km (ez belül van a lokátor maximális hatótávolságán zavarás nélkül), ami megfelel a kísérő zavarás módszerének. Az antennák által bezárt helyszög 2.2°. A zavaradó sávszélessége 200 MHz, az effektív kisugárzott teljesítménye 100W, 1KW, 2KW és 10 KW (10W, 100W, 200W és 1 kW zavaró teljesítmény - P_j). Ebben az esetben a számított maximális hatótávolságokat az 5. ábra tartalmazza.



5. ábra A maximális hatótávolság a zavaradótól 100 km-re (saját szerkesztés)

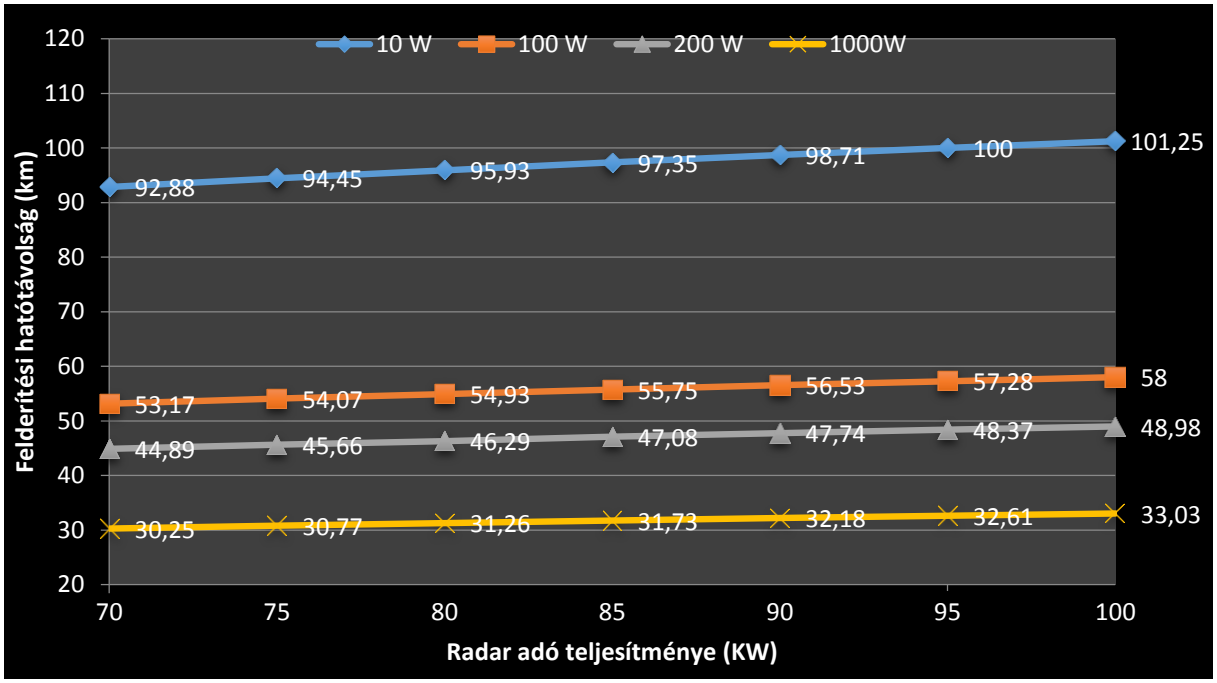
Negyedik eset: A lokátor és a zavaradó távolsága 50 km (ekkor a zavaró adó már közel van a lokátor), ami ismét a kísérő zavarás módszerének felel meg. A zavaradó helyszöge 2.2°, a sávszélessége 200 MHz (mely ismét mindig nagyobb a radar vételi sávszélességénél). Az

effektív kisugárzott teljesítménye 100W, 1KW, 2KW és 10 KW (10W, 100W, 200W és 1 kW zavaró teljesítmény - P_j). Ebben az esetben a különböző teljesítményű adóimpulzusokkal számított maximális hatótávolságokat a 6. ábra mutatja be.



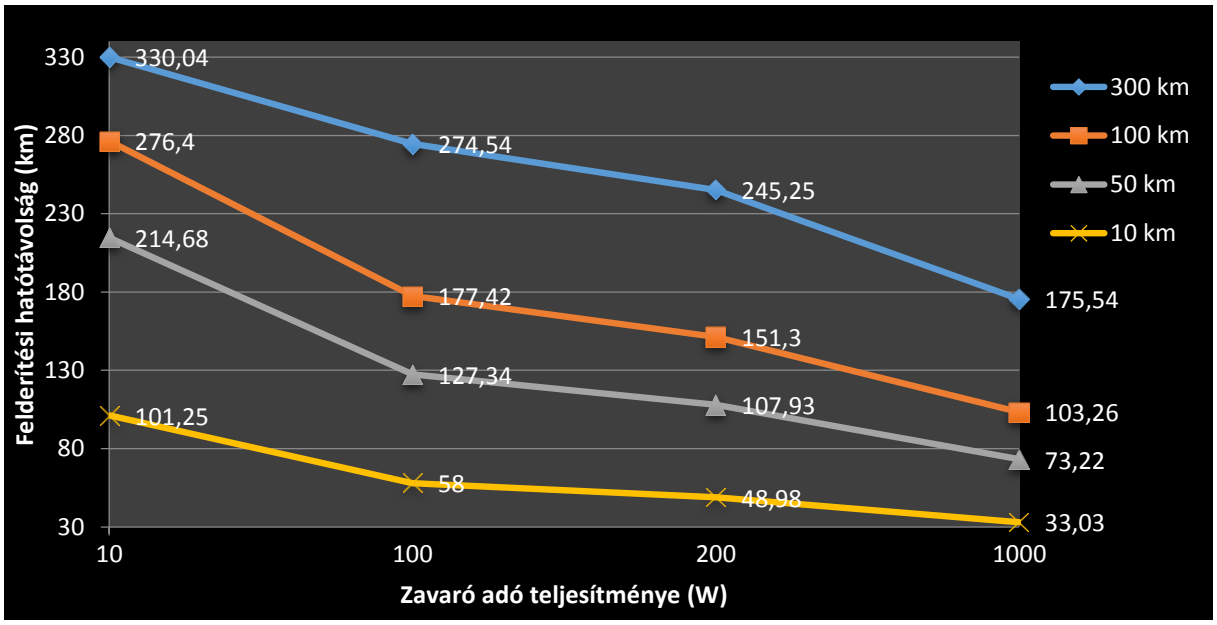
6. ábra: A maximális hatótávolság a zavaradótól 50 km-re (saját szerkesztés)

Ötödik eset: A radar és a zavaradó távolsága 10 km (a zavaró adó nagyon közel van a lokátorhoz). A zavaradó helyszöge 2.2°, sávszélessége 200 MHz, az effektív kisugárzott teljesítménye 100W, 1KW, 2KW és 10 KW (10W, 100W, 200W és 1 kW zavaró teljesítmény - P_j). A különböző teljesítményű adóimpulzusokkal számított maximális hatótávolságokat a 7. ábra szemlélteti.

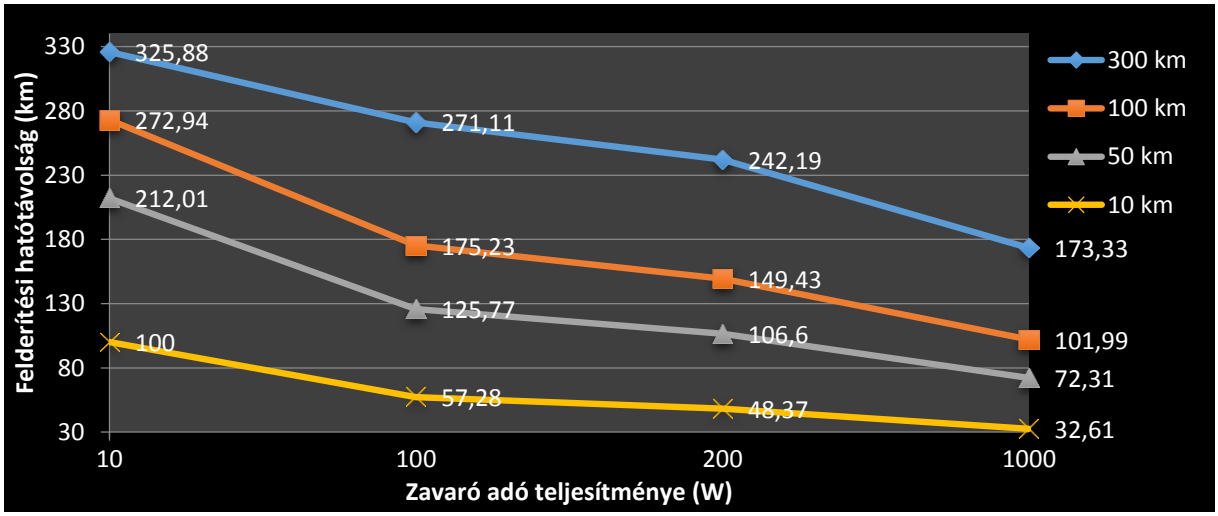


7. ábra: A maximális hatótávolság a zavaradótól 10 km-re (saját szerkesztés)

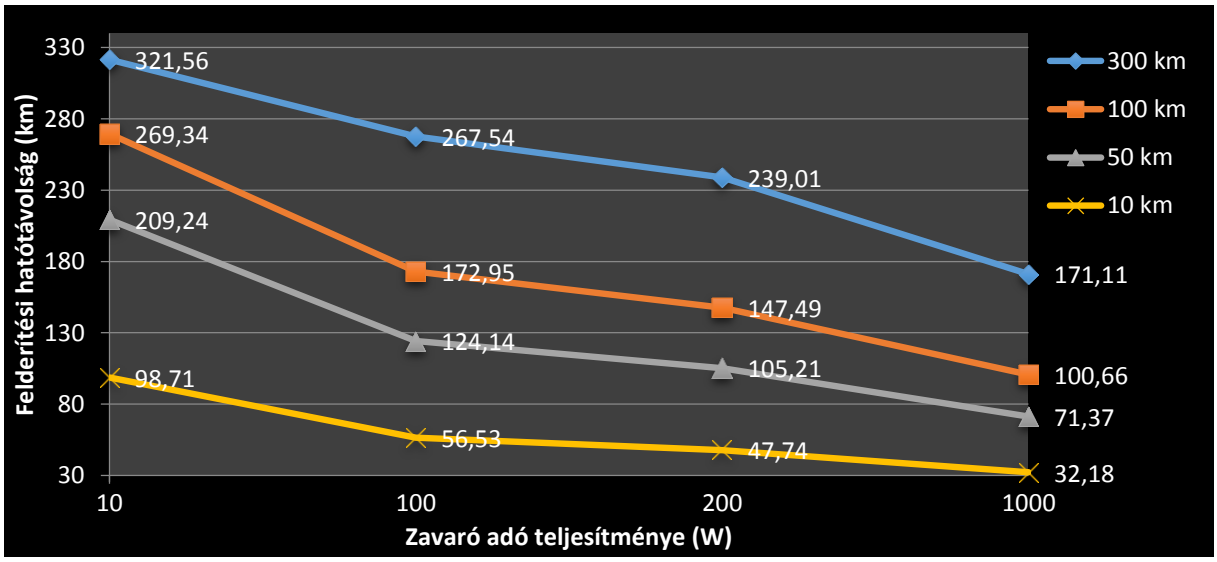
További számításokat végeztem különböző távolságokból (300, 100, 50 és 10 km) végrehajtott zavarásra különböző zavaradó teljesítmények (10, 100, 200 és 1000W) esetén. Ezen számításokat különböző radaradó teljesítmények (100, 95, 90, 85, 80, 75 és 70 kW) esetén vizsgáltam. Az eredményeket a 8, 9, 10, 11, 12, 13, 14. ábrákon ábrázoltam.



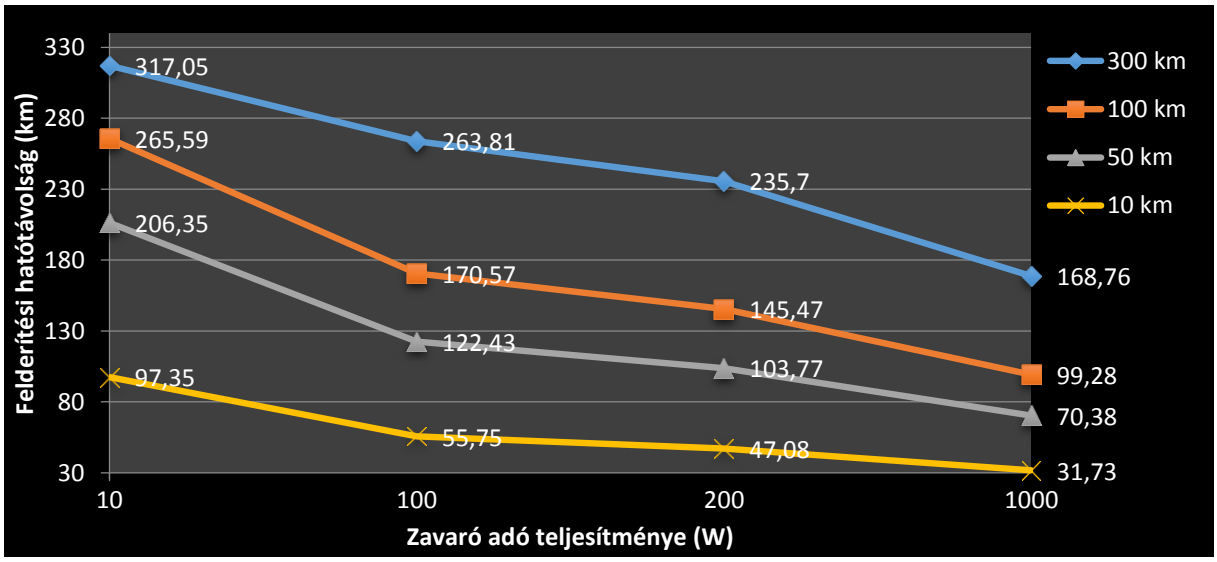
8. ábra: 100 kW radaradó teljesítmény esetén a hatótávolság (saját szerkesztés)



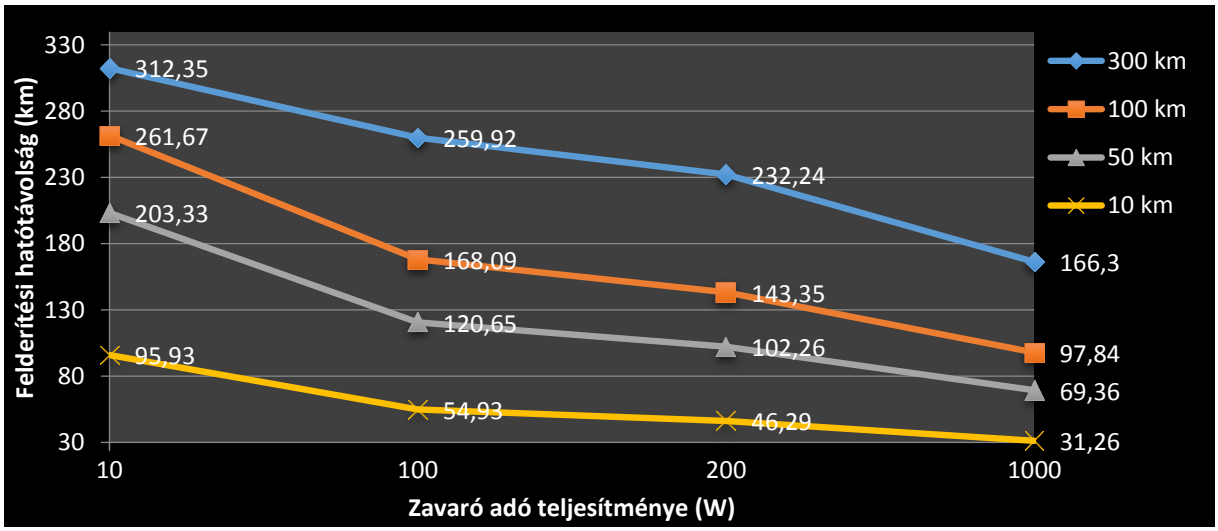
9. ábra: 95 kW radaradó teljesítmény esetén a hatótávolság (saját szerkesztés)



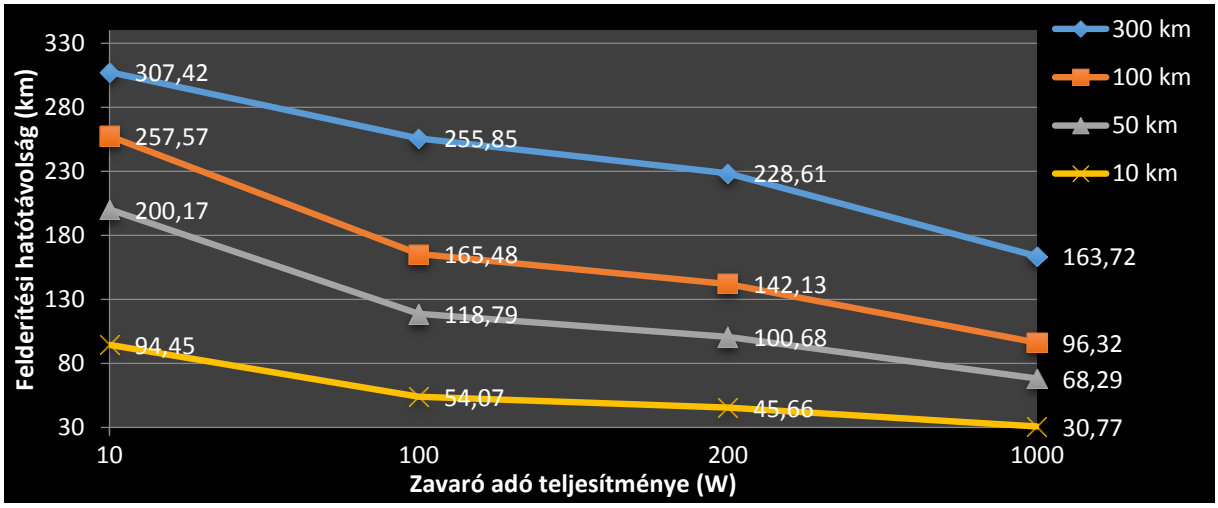
10. ábra: 90 kW radaradó teljesítmény esetén a hatótávolság (saját szerkesztés)



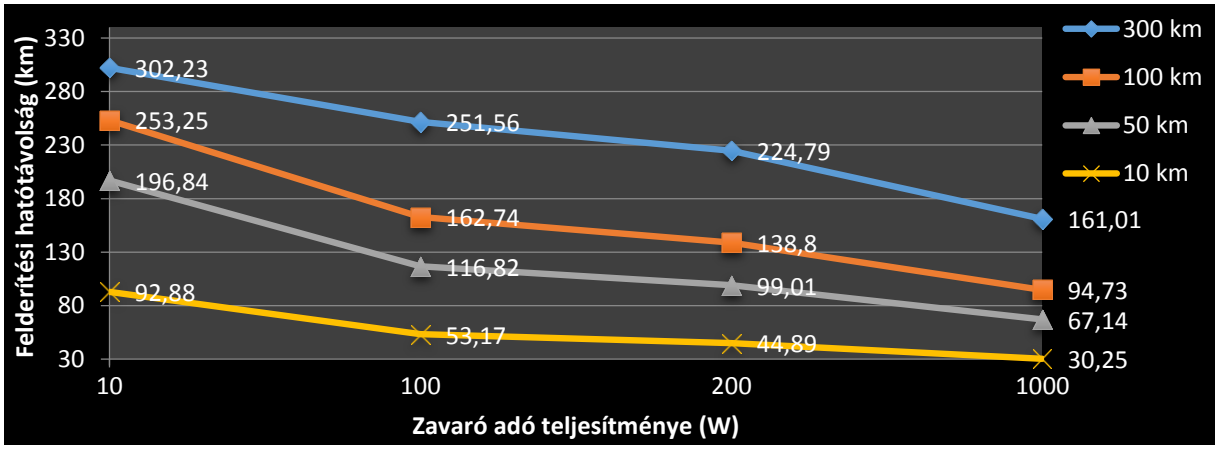
11. ábra: 85 kW radaradó teljesítmény esetén a hatótávolság (saját szerkesztés)



12. ábra: 80 kW radaradó teljesítmény esetén a hatótávolság (saját szerkesztés)



13. ábra: 75 kW radaradó teljesítmény esetén a hatótávolság (saját szerkesztés)



14. ábra: 70 kW radaradó teljesítmény esetén a hatótávolság (saját szerkesztés)

Az ábrákon látható, hogy az radar adójának teljesítményét csökkentve (100-ról 70 kW-ra) a felderítési hatótávolság nem csökken jelentősen. A visszavert jelek vételét főként a zavaró adó teljesítménye és távolsága a lokátortól korlátozza. Ez is bizonyítja, hogy mindenképp szükség van a radarberendezésekben az aktív zavarok elnyomására, szűrésére, kiküszöbölésére alkalmas technikák alkalmazására.

KÖVETKEZTETÉSEK

Ha a radar zavarmentes környezetben üzemel, akkor a maximális hatótávolsága 100 kW-os kimenő teljesítmény esetén legnagyobb 340km. Megállapítható, ha a teljesítményt a háromnegyedére csökkentjük, akkor is 320 km körüli értéket kapunk (3. ábra). Ez megfelelő rádiólokációs felderítést eredményez.

Ha a zavaradó radarhoz viszonyított távolsága 300 km (8. ábra): ugyan 100 kW-os radaradó teljesítmény mellett csökkent a hatótávolság (330,04 km-ről 175,54 km-re), de így a lokátor még mindig hatékonyan derít fel, tehát a légtér ellenőrzöttnek minősül. Megállapítható, hogy a zavarás nem hatékony. A zavaróadónak közelítenie kell a radarhoz a zavarás megvalósításához.

Ha a zavaró adó és a radar távolsága 100 km: ilyen távolságban már a kettes esetben alkalmazott zavaró teljesítmény tizede (P_j=100 W) is elég volt ugyanolyan mértékű hatótávolság csökkentéshez (R_{max}=177,42 km) (5. ábra). Amennyiben ugyanolyan

zavarteljesítményt alkalmaznak, mint a kettes esetben (P_j=1000W) akkor a hatótávolság az eredeti harmadára csökken (R_{max}=103,26 km) (5. ábra).

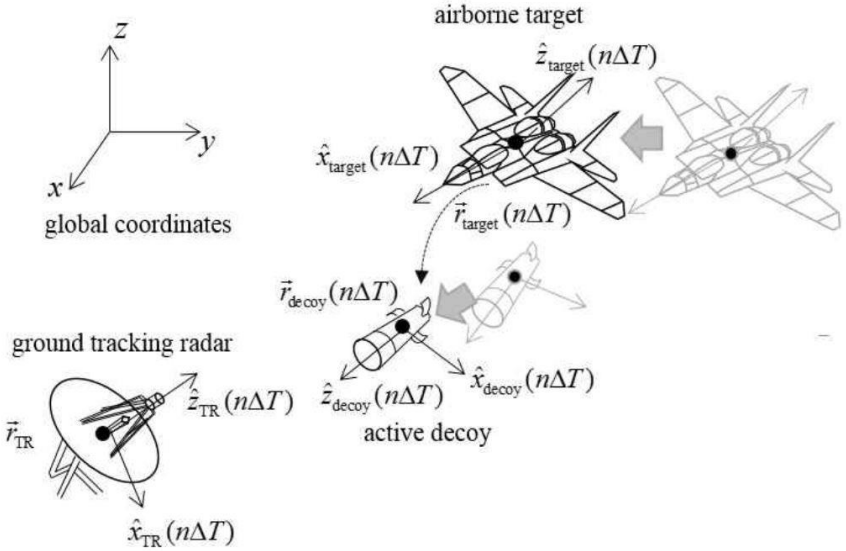
Ha a zavaradó és a radar távolsága 50 km: ez egy valós helyzetnek fogható fel mivel a lokátoraink pár darabtól eltekintve az országhatártó 50 km-en belül helyezkednek el. Ilyen távolságban már a kettes esetben alkalmazott zavaró teljesítmény tizede (P_j=100 W) már nem csak felére csökkenti, hanem harmadolja az eredeti zavarás nélküli hatótávolságot (R_{max}=127,34 km). Amennyiben ugyanolyan zavarteljesítményt alkalmaznak, mint a kettes esetben (P_j=1000W) akkor a hatótávolság kevesebb, mint az eredeti negyedére csökken (R_{max}=73,22 km) (6. ábra). Ez a távolság már kétségessé teszi az időbeni felderítést és célazonosítást valamint az információ időbeni eljuttatását a felelős magasabb szintű szervezetek és döntéshozók számára. Ebben az esetben nincs idő válaszintézkedés foganatosítására, hiszen 50-60 km-t egy 900 km/h sebességgel repülő gép 3-4 perc alatt tesz meg.

Ha a zavaró adó radarhoz viszonyított távolsága 10 km: ebben a távolságban már a kettes esetben alkalmazott zavaró teljesítmény százada (P_j=10 W) is elég, hogy harmadolja az eredeti hatótávolságot (R_{max}=101,25 km) (7. ábra). Amennyiben ugyanolyan zavarteljesítményt alkalmaznak, mint a kettes esetben (P_j=1000W) akkor a hatótávolság az eredeti tizedére csökken (R_{max}=33,03 km). Amennyiben sikerül a zavaró adót a radarhoz ilyen közel jutatni elmondható, hogy a berendezés az eredeti feladatát nem képes ellátni. A lokátor ebben az esetben csak egy szűk távolsági kapun keresztül képes felderíteni. Ebben az esetben a légvédelem reakciója lehetetlenné válik.

Számítást végeztem arra az esetre, ha az eddigi zavaradót, melynek teljesítménye P_j=10 W, 1 km közel kerül a lokátorhoz annak hatótávolsága R_{max}=32,52 km-re csökken. Gyakorlatilag a radar használhatatlan eszközzé válik.

A fentebb leírtak alapján belátható, hogy a radarok hatékony elektronikai védelem nélkül könnyen zavarható és könnyen kiiktatható tényezőt jelentenének a légvédelemi rendszerben még az olyan egyszerű zavaró eszköz, mint egy CW zavaradó számára is.

A valóságban a felsorolt eseteknél bonyolultabb - zavarással kapcsolatos - légi helyzet szimulációkat kell alkalmaznunk, hogy részleteiben feltárjuk a légtérellenőrző radarok ellen bevethető eljárások hatékonyságát. Egy ilyen esetet szemléltet a 15. ábra.



15. ábra: Kombinált zavarási helyzet ábrázolása, valós és megtévesztő céltárgyakkal [10]

A radarok különböző részegységeiben alkalmazható elektronikai védelmi elveket és gyakorlati megoldásokat ezen írásom folytatásában részletezem. Ott lesz szó az antennával

megvalósítható (SideLobe Blanking, SideLobe Cancellation), az adóval (Radar with Large ERP, Frequency Agility and Diversity, Automatic Frequency Selecting), a vevővel (Dual Frequency Conversion, Large Dynamic Range Receivers) és a jelfeldolgozó rendszerrel (Digital Coherent and Adaptive Moving Target Indication, CFAR Detection, Pulse width and Pulse Repetition Frequency Discriminator) megvalósítható ECCM technikákról.

FELHASZNÁLT IRODALOM

[1] *Az Európai Parlament és a Tanács 2004/108/EK irányelve* (2004. december 15.) http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32004L0108

[2] *Magyar Honvédség Összhaderőnemi Doktrína* 3. kiadás, 2012, MH kiadvány, p. M1-3.

[3] *Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás*, 2004, MH kiadvány, p. 6.

[4] *Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína*. MH HVK, 2005. p. 8.

[5] *Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína*. MH HVK, 2005. p. 10.

[6] BALAJTI I, VASS S: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000,

[7] BARTON D. K, LEONOV S.A: *Radar Technology Encyclopedia* (Electronic Edition), Artech House London, 1998, 64, 65, 132, 154-161, 376-385, 420. p, ISBN 0-89006-893-3

[8] BARTON D. K: *Radar system analysis and modeling*. Boston, Artech House, 2005, 545 p. ISBN 1-580536-81-6

[9] *BALAJTI I: Korszerű* katonai radarok és radaradat-feldolgozó rendszerek. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1462. 1998, p. 75.

[10] RIM J-W, KOH I-S, CHOI S-H: *Jamming Performance Analysis for Repeater-type Active Decoy against Ground Tracking Radar Considering Dynamics of Platform and Decoy*. Prague, Czech Republic, The 18th International Radar Symposium IRS 2017, June 28-30, ISBN 978-3-7369-9343-3 pp.9.

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

INFORMATION SECURITY FOR ELECTRIC CARS IN ACCORDANCE WITH NIST CRITICAL INFRASTRUCTURE CYBERSECURITY FRAMEWORK

AZ ELEKTROMOS AUTÓK INFORMÁCIÓBIZTONSÁGA A NIST KRITIKUS INFRASTRUKTÚRÁK KIBERVÉDELMI KERETRENDSZERÉNEK VONATKOZÁSÁBAN

TÓTH András

(ORCID: 0000-0001-6098-3262)

toth.hir.andras@uni-nke.hu

Abstract

The automotive cybersecurity environment is dynamic and is expected to change continually and, at times, rapidly. The security of the information is a mandatory requirement of all electric cars, which are connected to different networks to communicate among each others or connect to additional systems to get updates or road and traffic information. Some agencies have already developed cybersecurity framework to reach this goal. In this paper, I have specified the NIST Cybersecurity Framework core component functions as a vehicular cybersecurity solution, which supports the information security throughout the complete lifecycle of the vehicles.

„Supported BY the ÚNKP-17-4-IV-NKE-5 New National Excellence Program of the Ministry of Human Capacities”

Keywords: *automotive cybersecurity environment, cybersecurity framework, Vehicle-to-Vehicle (V2V), Vehicle-to-Internet of Things (V2IoT), Vehicular Ad-hoc Networks (VANETs), Vehicular Cloud Computing (VCC)*

Absztrakt

Az autóipari kiberbiztonsági környezet dinamikus, és várhatóan folyamatosan és, napjainkban, gyorsan változik. Az információk biztonsága kötelező követelménye minden olyan elektromos gépjárműnek, amely különböző hálózatokhoz kapcsolódik, hogy ez által képesek legyenek egymás között kommunikálni, vagy olyan további rendszerekhez kapcsolódni, melyek segítségével frissítéseket vagy út- és forgalmi információkat szerezhetnek be. Egyes vállalatok már kidolgozták egy-egy kiberbiztonsági keretrendszert e cél elérése érdekében. Ebben a cikkben a NIST Cybersecurity Framework által meghatározott központi összetevők funkcióit olyan járműbiztonsági megoldásként határoztam meg, melyek a gépjármű teljes életciklusa során támogatja az információbiztonságot.

„Az Emberi Erőforrások Minisztériuma ÚNKP-17-4-IV-NKE-5 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült”

Kulcsszavak: *autóipari kiberbiztonsági környezet, kiberbiztonsági keretrendszer, gépjárművek közötti kommunikáció (V2V), gépjármű és dolgok internete közötti kommunikáció (V2IoT), gépjárműves ad-hoc hálózatok (VANETs), gépjárműves felhő informatika (VCC)*

A kézirat benyújtásának dátuma (Date of the submission): 2017.08.30.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.22.

INTRODUCTION

There was organized the International Military Information-security Conference in May 2017, where Prof. László Kovács drew attention during his presentation to the importance of the information security of critical infrastructures, including the information protection of electric cars. This raised a lot of questions in me, and then I tried to deeper into the subject, to find the rules and legislations in force that directly or indirectly deal with this topic. To get to know this, I studied and analyzed a number of domestic and foreign literatures, articles and researches.

Zsolt Haig and László Kovács, in their study, Critical Infrastructures and Critical Information Infrastructures, have pointed out that the world's leading nations have begun before the millennium to pay close attention to the protection of critical infrastructures, which was followed by more robust and defense-centric measures in the early 2000s.

According to their wording, the US National Strategy for the Physical Protection of Critical Infrastructures and Key Assets was released at the beginning of 2003, which divided the critical infrastructures into the following sectors:

- agriculture and food;
- water;
- public health;
- emergency services;
- defense industrial base;
- telecommunications;
- energy;
- transportation;
- banking and finance;
- chemical industry and hazardous materials;
- postal and shipping. [1]

This division was similarly prepared by all the states, altered by merging or extending some sectors. As already seen in this compilation, the transport sector has already appeared at that time, but because of during this period there was no widespread the usage of electric cars, the transport sector did not deal with them as a critical information infrastructure. Till the last few years doctrines and standards were always not considered relevant to the automotive sector as there was no vector for cyber threats in the cars themselves. It was changed in February 2013, when the President of the United States signed an Executive Order (EO) to improve critical infrastructure cybersecurity, to counter the growing threat of cyber attacks against critical infrastructure that could threaten the economic health of the Nation and the physical safety of citizens. After this measure the leaders of other nations and international organizations started to develop their own cybersecurity framework to reduce cyber risks to critical infrastructures including e-cars.

The Barack Obama's EO was directed to the National Institute of Standards and Technology (NIST)[1] to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructures. NIST met with over 2,000 representatives of critical infrastructure sectors, state and local governments, international interests and other interested parties, holding workshops to develop the critical infrastructure cybersecurity

[1] NIST is an organization to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve the quality of life.

framework. It is needed for the framework to meet several requirements. According to these, the framework must:

- include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks;
- provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identity, assess and manage cyber risks,
- identify areas for improvement to be addressed through future collaboration with particular collaboration with particular sectors and standards-developing organizations;
- be consistent with voluntary international standards. [2]

This paper is focusing on the progress of the information security, in a narrower sense the cybersecurity, and how this affects the automotive industries, both for manufacturing, traditional IT and advanced cyber-physical systems, such as Vehicle-to-Vehicle (V2V), Vehicle-to-Internet / Vehicle-to-Infrastructure (V2I), Vehicle-to-Internet of Things (V2IoT) Vehicle-to-Everything (V2X) applications. In V2V communication, vehicles communicate with one another using On Board Units (OBU), through Omni-directional antennas and sensors. In V2I communication, vehicles communicate with infrastructure units along the road such as toll collection booths, traffic lights, petrol stations etc. Such road side infrastructure units are called as road side units (RSUs). The inter-vehicle communication takes place over a range of 300–500 m using IEEE 802.11 protocols, using the dedicated short range communications (DSRC) standard.

The National Highway Traffic Safety Administration Agency has formulated a guidance as a resource to supplement existing voluntary vehicle cybersecurity standards, principles, best practices, and lessons learned and help guide future industry efforts. In this the basic definitions of the topic were laid, which are used in this paper as well:

- attack surface: the set of interfaces (the “attack vectors”) where an unauthorized user can try to enter data to or extract data from a system, or modify a system’s behavior;
- attack vector: refers to the interfaces or paths an attacker uses to exploit a vulnerability. For instance, an exploit may use an open IP port vulnerability on a variety of different attack vectors such as Wi-Fi, cellular networks, IP over Bluetooth, etc. Attack vectors enable attackers to exploit system vulnerabilities, including the human element;
- automotive: refers to “of, relating to, or concerned with motor vehicles in general”
- Controller Area Network (CAN): a dominant serial communication network protocol used for intra-vehicle communication;
- debug: the activity of discovering errors or undesirable actions within computer code;
- digital signing: a mathematical technique used to validate the authenticity and integrity of a message, software or digital document;
- Electronic Control Unit (ECU): an embedded system that provides control functions to a vehicle’s electrical system or subsystems through digital computing hardware and associated software;
- exploit: refers to an action that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur on computer software and/or hardware. An example of an exploit would be using a diagnostic port vulnerability to take advantage of a buffer overflow that allows access over Internet Protocol (IP) networks;

- firmware: refers to the software code and data that reside on an embedded system, such as an automotive electronic control system, that implements dedicated functions and manage system resources (e.g., system input/outputs (I/O) to execute those functions. Firmware may take a variety of different forms. For example, in some cases "firmware" may refer to source code while in some cases it may take the form of a binary image consisting of a file system and compiled code;
- incident: is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system on a vehicle computing platform through the use of an exploit.
- Public Key Infrastructure (PKI): refers to a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates;
- telematics: refers to the integration of telecommunications and informatics for intelligent applications in vehicles, such as fleet management;
- vulnerability: a weakness in a system or its associated networks, system security procedures, internal controls, or implementation that could be exploited to obtain unauthorized access to system resources. For instance, an open diagnostic port on an ECU is vulnerability. [3]

THE FOUNDS OF NIST CYBERSECURITY FRAMEWORK IN E-CAR INFROMATION SECURITY

In the last years the penetration of cyber security aspects in automotive industry has widely increased and the cars are transformed from a simple mode of transport to a personalized mobile information hub. Until recently, cars have been isolated from their environment and from the internet, but the electric cars use various numbers of wireless technologies, like V2V, V2I, V2IoT, V2X communications, telematics, Near Field Communication (NFC), remote diagnostics provided by Original Equipment Manufacturers, fleet management services and multi-standard digital broadcast reception, complemented by Advanced Driver Assistance Systems (ADAS) that implement autonomous driving features.

All these electronic functions bring great benefits to the driver, increasing comfort, convenience, safety and efficiency. But these features come with new risks, too. Modern vehicles continuously generate, process, exchange and store large amounts of data. Their wireless interfaces connect the in-vehicle systems of these e-cars to external networks such as the internet, which forms entry point for hackers, opening the door for remote attacks.

The transition we are living involves mainly the massive introduction of cyber security functionalities in vehicle components. Coming generations of connected cars will differ as a result of moves toward greater convergence between automotive communications technology and connections to resources beyond the confines of the car. This is needed to deal with the increase of connectivity integrated in vehicles that is progressively exposing the vehicular network to the global hacking community. Indeed the market of aftermarket devices accessing the Controller Area Network (CAN) is wide. These devices include aftermarket head units and On-Board Diagnostic (OBD) ports to dongles, which can be Bluetooth, Wi-Fi or cellular connectivity. These devices are typically connected by the vehicle owner to the OBD port hence exposing the vehicle to remote attacks. In this view the vehicle is a set of high-level functionalities integrated through in-vehicle and out-vehicle data streams and deployed in a set of computation units. This results in the integration of cyber physical systems that provide a number of functionalities by means of wired interactions between electronic control units (ECU). So an e-car is an Internet linked device, where the awareness of online threats and the

malicious hacking of computer systems could affect the use of almost any physical entity that qualifies as a connected device.

The motivations of the hackers can be the followings:

Foreseeable motives:

- Data theft – targeted data types might include:
  - Access to online automotive apps and services – that contain banking/credit records;
  - Congestion Charge or toll payment information;
  - General personal identification data – e.g., social media users names and passwords;
  - Insurance and tax data – useful for identity theft;
  - International travel permits;
  - License plates and other vehicle registration data;
  - Lifestyle information – e.g., fitness club membership;
  - Medical records – a driver suffering from a health issue may have information about their condition either stored on a vehicle or accessible via the vehicle or a mobile device temporarily connected to the vehicle;
  - Vehicle location information – which may be used to identify patterns of use or driver behavior in anticipation of offensive action against a vehicle;
  - Vehicle physical security data.
- Extortion / denial-of-service threat;
- Fraud and deception (altering or deleting schedule logs and records);
- Freight and goods theft (activating false alarms that cause goods to be left unattended);
- Automotive 'Hacktivism' – cyber-infiltration of a vehicle's systems that is politically- or ideologically-motivated;
- Immobilization;
- Mischief and malevolence – individual hackers testing defenses and their skills; or wanting to inflict damage and/or disruption out of spite;
- Premises security and burglary – vehicle data that reveals businesses and homes are unoccupied.

Secondary motives:

- Industrial espionage – illegal access to intellectual property;
- Infliction of political or reputational damage;
- 'Script kiddies' – adversarial hackers pitting their skills against the automotive software safeguards;
- Sabotage or degrading of vehicle and connected system performance;
- Terrorism – disabling vehicles as part of an attack, for instance vehicle identification re-assignment (for stolen cars). [4]

The automotive industries can use the NIST Cybersecurity Framework components to avoid or minimize the possibilities of these attacks. It allows enterprises to identify, detect, protect, respond and recover from cyber security risks and incidents, and it provides a basic baseline set of controls which companies can use to better understand, manage, and reduce its cybersecurity risks, and to help determine "which activities are most important to assure critical operations and service delivery.

The National Highway Traffic Safety Administration Agency created a paper in this topic in 2014 (National Institute of Standards And Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles), but it only looked at the subject from the risk

management side. The Agency's multilayered approach to cybersecurity has the following goals:

- expand the knowledge base to establish comprehensive research plans for automotive cybersecurity and develop enabling tools for applied research in this area;
- facilitate the implementation of effective, industry-based best practices and voluntary standards for cybersecurity and cybersecurity information-sharing forums;
- foster the development of new system solutions for automotive cybersecurity;
- research the feasibility of developing minimum performance requirements for automotive cybersecurity;
- gather foundational research data and facts to inform potential future Federal policy and regulatory activities. [5]

They specify 6 risk management framework steps for the vehicle sector to define criticality/sensitivity of information systems, select baseline security and supplement controls, implement security controls for applying security configuration settings, determine security control effectiveness and continuously track changes to the information systems. The 6 steps are the following:

- assess threat model/use cases;
- categorize vehicle systems;
- select security controls;
- implement security controls;
- assess security controls;
- monitor security controls.

They define that the security controls are the management, operational and technical safeguards (or countermeasures) prescribed for a system to protect the confidentiality, integrity and availability of the system and its information. Security controls, also known as security requirements, will be needed to implement security controls to protect vehicles (based on safety criticality considerations. [6]

I analyzed the vehicle sector from the NIST Cybersecurity Framework core component functions, which contain cybersecurity activities and informative references and organized around particular outcomes. It is possible to identify the following areas with the five steps of the functions:

- What processes and assets need protection?
- What safeguards are available?
- What techniques can identify incidents?
- What techniques can contain impacts of incidents?
- What techniques can restore capabilities?

Functions organize basic cybersecurity activities at their highest level. These functions are identify, protect, detect, respond, and recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. [7]

Figure 1. The NIST Cybersecurity Framework core component [8]

The first step, as shown on Figure 1, is to identify what processes and assets need to protect. The companies have to do an asset management, where they can find the physical devices, the internal and external information systems, the software platforms and applications, what they have to protect against a possible attack. Also very important to do a risk assessment (as it is specified in the National Institute of Standards And Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles) to identify the possibly threats, the asset vulnerabilities, likelihoods and the impacts. Specific attacks are address for instance the cyber physical systems integrated in the vehicle. They depend on the vehicle and aim to measure the security of vehicle functions. Typical examples are traction control, ABS, automatic transmission. The likelihood is measured on the basis of five aspects which are:

- expertise needed by an attacker to implement the threat;
- motivation of the attacker;
- cost of the tools needed to implement the threat;
- effort needed by an attacker with specified expertise to implement the threat;
- availability of public available information (e.g. non-deep internet) describing the vulnerability.

The impact is measured on the basis of two aspects which are:

- impact on system functionality;
- impact on human beings interacting with the system.

The next step is the protection. When the threats are identified the companies can focus for the protection to minimize the possibility of occurrence. The users of the e-cars can use access control, where the main assets and associated facilities are limited just to authorized users, processes, or devices, and to authorized activities and transactions. It means that the access permission is managed, so the owner and other persons, who have the right to use the car, can set up for example a code for the access to the ECU, so without the car is unusable. More important questions are the data security and the information protection. The companies have to focus on the protection of the confidentiality, integrity and availability of information. To reach this it is needed to build up proper security policies, processes, and procedures, which

are maintained and used to manage protection of information systems and assets. Protecting cars against cyber threats requires disciplines and collaborations in applying security principles at each level and layer of the system. The protection is a critical layer in the overall cybersecurity defense system of the car, because it represents the border between the vehicle's internal network and the external world.

Symantec, a security software and solution company, specifies four cornerstones for protecting e-cars:

- protecting communications: particularly any modems for in-vehicle infotainment (IVI) or in on-board diagnostics (OBD);
- protecting each module: sensors, actuators, and anything with microcontrollers (MCU), and microprocessors;
- over the air (OTA) management: from the cloud to each car;
- mitigating advanced threats: analytics in the car and in the cloud. [9]

The third step is the detection, when a well-organized and built security continuous monitoring procedures help to monitor the networks, the information systems, the physical environment and personnel activities to detect potential cybersecurity events. It also can alert when a malicious code or unauthorized mobile code is detected to enter to the ECU of the car. To reach these it is needed to monitor continuously for unauthorized personnel, connections, devices and software is performed. The problem is with the e-cars, that antivirus, firewalls (they only have software-controlled firewalls in the gateways) and anomaly detection are not yet implemented in the electric vehicle, largely because of the complexity of updating policies and software regularly and frequently. Units inside vehicles have limited resources, which are often already fully utilized by the vehicle's functions. The detection is usually solved by software, applications or authentications. One of these is the Message Authentication Code (MAC), which works in the following way: each pair of nodes has a shared secrete key, which helps the sender to compute a MAC and broadcast the message with it. Then all receivers compute also a MAC with the secret key and compare it with the receiving MAC. The e-cars use HMAC, which is more secured than MAC, because with it the key and the message are hashed in separate steps.

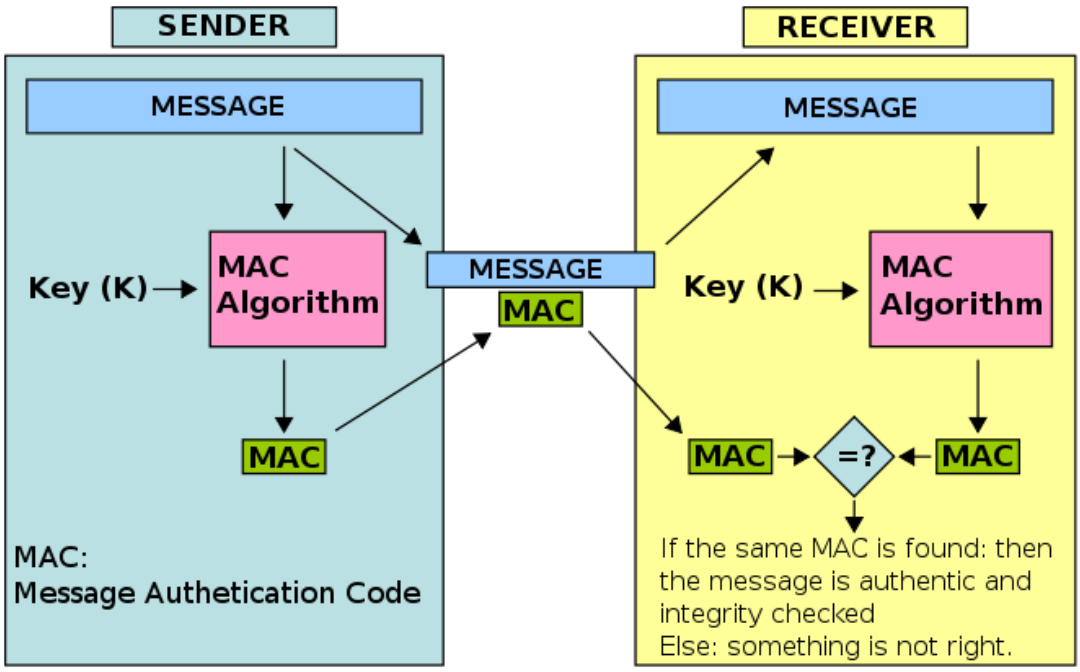


Figure 2. HMAC authentication [10]

As shown on Figure 2, during the HMAC process the sender sends a message with a MAC. When the monitor node receives this message, it can detect whether it has a MAC. If the received message has a MAC, the monitor node immediately starts to calculate the HMAC and validates the MAC on the message. If the same MAC found the authentication is done, the receiver receives the message. If the monitor node detects a MAC error, it will prevent the unauthorized frame by overwriting an error frame. This technique guarantees authentication of on-board communication proven to be resistant to spoofing and Man In The Middle and remote attack techniques, as network reconnaissance and information gathering with unauthorized access to information system/network.

The next step is the response processes and procedures, which are executed and maintained to ensure timely response to the detected cybersecurity events. It is needed to develop increased awareness and capabilities to establish communication protocols among automotive manufacturers, suppliers, cybersecurity researchers, and government agencies could assist industry stakeholders in coordinated efforts to address discovered vulnerabilities and enhance product security. If the detection system of the car is well-organized and setup, the incoming attacks are blocked, and the driver can not realize anything during the trip. The car stores this report with information of the attack, and it is able to share it with other cars in Vehicular Ad-hoc Networks (VANETs), where vehicles communicate with each other through V2V communications. Also, in VANETs, vehicles exchange data with RSUs / Infrastructure through V2I communications. With this solution the cars build up a Vehicular Cloud Computing (VCC) network with DSRC links, where RSUs act as a Gateway for the VANET to access Public Cloud. In this way the cars can share all information according the roads, traffic and executed hacker attacks, so the other cars can be prepared to reject every incoming message from the attacker. [11]

The last step is the recovery. The development of protocols for recovering from cybersecurity incidents is important for ensuring consistent approaches for making available updates to vehicles in a reliable and expeditious manner based on specific circumstances. The procedure can be a self-recovery, when the attach did not cause a huge damage in the car, and the car has an additional storage to store recovery data. For instance, when a man-in-the-middle attacker execute endless data attacks on ECUs, that have only enough space to keep the actual image of data, they can start to compare this data with the stored info. If this attacker sends an ECU random data instead of an actual image, then it is unable to boot to a working image, even though the bootloader can verify that that the random data does not match with the latest downloaded metadata. In order to solve this problem, the ECU will use the additional storage (not it's own storage), where it has enough storage to maintain not only a previous image, but also the latest downloaded image, so it can work without fail. If the damage caused so big issues that the car is not able to continue to work, it can inform the automotive manufacturers, stakeholders, suppliers or mechanics on the established communication links. They can go to the location to fix the problem, or they can try to solve it across the carcloud to update the attacked ECUs to the right version.

SECURITY FRAMEWORKS TO SUPPORT E-CAR PROTECTION

In the last few years several testing were made to analyze the security of electric cars, and to find the weakest point to strenghten the protection mechanism of the entire system against hacker attacks. One of the first and most well-known tests was when hackers killed remotely a Jeep on the highway in the US.

Examining electric cars, we conclude that typical attacks are the same as the attacks against other networks, devices or terminals. Accordingly, the attacks can be:

- data theft: user's personal data, phone numbers, other contacts, bank details;

- man-in-the-middle attack: uploading misleading information into the communications cloud used by cars, thus disrupting traffic;
- DDOS attack: thereby blocking the car's central computer and making it impossible to move;
- stealing location information: thereby tracking the driver's location;
- taking control over the vehicle: causing an accident, causing possibly attack against another vehicle or person;
- penetration: unauthorized access to resources, what can be included under the total control by the intruder, consequently modify the managed data, steal information, install malicious software on the hardware.

The above mentioned test was executed by two security researchers, and they have exposed the security vulnerabilities in automobiles by penetration tests. They have attacked an adjacent chip in the car's head unit, and rewriting the chip's firmware to plant their code. That rewritten firmware were able to send commands through the car's internal network (CAN bus) to its physical components like the engine and wheels. With the attack they could take the control over the vehicle from the radio and the windshield wipers through the accelerator to the engine. After the test the automotive industry has provided software update for the customers to secure vehicles against any potential vulnerability. [12]

It is one of the solutions against the cyberattacks, but it is much better when the industries focus on the defense and security solutions till the cars are still in the factory. There are a lot of different practices, techniques, guidelines and frameworks in this topic from companies, governments and standarnization organizations. Usually there are 4 specified security layers that lead to a highly secure vehicle network:

- secure interfaces: which connect the vehicle to the external world;
- secure gateway: which provides domain isolation (separating interfaces, infotainment, safety-critical systems etc.);
- secure network: that provides secure communication between control units (ECUs);
- secure processing units: that implement all the features of the connected car.

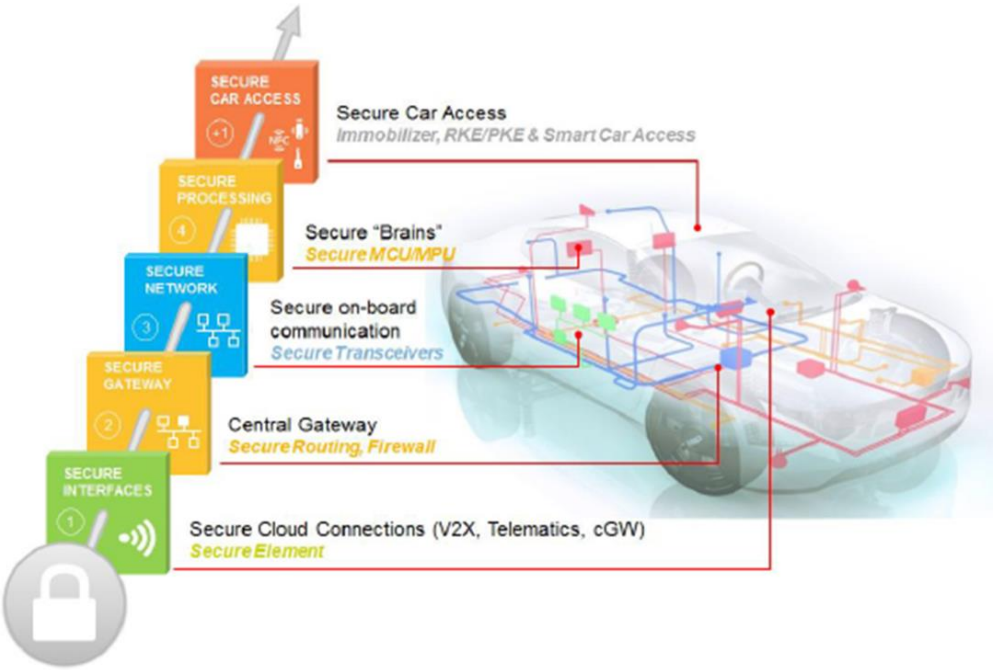


Figure 3. Automotive security framework [13]

There are also some organizations and individuals who informed the automotive industries that vehicle safety issues can be caused by cybersecurity issues, and offer security research community support. One of these was the I Am The Cavalry, which gave five recommendations for the industries in the Five Star Automotive Cyber Safety Framework. These recommendations are:

- Safety by Design – anticipate failure and plan mitigation;
  - does the industry have a published attestation of its secure software development lifecycle, summarizing the industry's design, development, and adversarial resilience testing programs for the industry's products and supply chain?
- Third-Party Collaboration – engage willing allies;
  - does the industry have a published coordinated disclosure policy inviting the assistance of third-party researchers acting in good faith?
- Evidence Capture – observe and learn from failure;
  - do the industry's vehicle systems provide tamper evident, forensically sound logging and evidence capture to facilitate safety investigations?
- Security Updates – respond quickly to issues discovered;
  - can the industry's vehicles be securely updated in a prompt and agile manner?
- Segmentation & Isolation – prevent cascading failure;
  - does the industry have a published attestation of the physical and logical isolation measures the industry has implemented to separate critical systems from non-critical systems? [14]

Examining the above issues and frameworks, and added the NIST Cybersecurity Framework, the industries can provide a well-secured network and information system to their vehicles. With a well-developed secure software development lifecycle and management, the entire system can be protected against external attacks.

CONCLUSION

The information of the e-cars and their owners are always shared among elements of the connected vehicle systems, and unfortunately it is vital, that as a user we always know who we're talking to and can be sure, that any information send or received is legitimate. The vehicle, as a member of the Internet of Things (IoT), needs to be able to authenticate itself in order to achieve accountability and so does everything in its environment. This is the only way updates, protection of intellectual property, driver identification, etc. can be carried out securely. Every vehicle owner wants to be sure, that only the online updates that he or she has tested and provided are accepted by the vehicle, and that only eligible vehicles receive updates or upgrades.

To reach this security goal the automotive industries can use the NIST Cybersecurity Framework core component functions to be sure that the information security is considered throughout the complete lifecycle of the vehicles, from the earliest stages right through to decommissioning. So they can be sure, that they protect all the necessary processes and assets, the mandatory safeguards are available, and they have all the compulsory techniques to identify incidents, contain impacts of incidents and restore capabilities.

BIBLIOGRAPHY

[1] HAIG ZS., KOVÁCS L.: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*, tanulmány, TÁMOP 4.2.2/B-10/1-2010-0001 Tudományos képzés műhelyeinek támogatása Kockázatok és válaszok a tehetséggondozásban (KOVÁSZ), Nemzeti Közszolgálati Egyetem, (2012) p. 183.

[2] LIGHTMAN, S: *The Future of the Cybersecurity Framework for Critical Infrastructure and How It May Affect the Automotive Industry*, https://www.escar.info/images/Datastore/2016_escar_usa/PAPER_2016/Lightman_Suzanne_NIST_PAPER.pdf (letöltve: 2017.07.17.)

[3] National Highway Traffic Safety Administration: *Cybersecurity best practices for modern vehicles*, (Report No. DOT HS 812 333), Washington, DC: Author (2016)

[4] The Institution of Engineering and Technology: *Automotive Cyber Security:An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles,* http://www.theiet.org/sectors/transport/documents/automotive-cs.cfm (letöltve: 2017.07.17.)

[5] National Highway Traffic Safety Administration: *NHTSA and vehicle cybersecurity,* https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/nhtsavehiclecybersecurity2016.pdf (letöltve: 2017.07.18.)

[6] McCarthy, C., & Harnett, K. *National Institute of Standards and Technology cybersecurity risk management framework applied to modern vehicles.* (Report No. DOT HS 812), Washington, DC: National Highway Traffic Safety Administration, (2014)

[7] National Institute of Standards and Technology: *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (2014) p.7.

[8] Night Lion Security: *A Baseline IT Risk Management Framework,* https://www.nightlionsecurity.com/blog/grc/2016/cyber-security-framework-csf-security-controls-download-xls-csv/ (letöltve: 2017.07.18.)

[9] FACHOT, M: *Protecting road vehicles from cyber attacks,* http://iecetech.org/issue/2017-03/Protecting-road-vehicles-from-cyber-attacks (letöltve: 2017.07.19.)

[10] Stack Overflow: *Clarification on HMAC authentication with WCF,* https://stackoverflow.com/questions/9922085/clarification-on-hmac-authentication-with-wcf (letöltve: 2017. 07. 19.)

[11] MARVY B. M., CHERIF S., HODA K. M., SHERIF A. H.: *CARCLOUD: A Secure Architecture for Vehicular Cloud Computing,* https://www.escar.info/images/Datastore/2016_escar_EU/PAPER_2016/Mary_Badr_Mounir_Mansour_CARCLOUD_A_Secure_Architecture_for_Vehicular_Cloud_Computing_PAPER.pdf (letöltve: 2017.07.21.)

[12] GREENBERG, A: *Hackers Remotely Kill a Jeep on the Highway – With Me in It,* https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (letöltve: 2017.08.30.)

[13] I Am The Cavalry: *Five Star Automotive Cyber Safety Framework,* https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf (letöltve: 2017. 09. 05.)

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

A BIZTONSÁGTUDOMÁNNYAL KAPCSOLATOS ELVEK ÉS CÉLKITŰZÉSEK AZ AMERIKAI EGYESÜLT ÁLLAMOK OKTATÁSI RENDSZERÉBEN

PRINCIPLES AND OBJECTIVES OF THE SAFETY AND SECURITY SCIENCE IN THE UNITED STATES' EDUCATIONAL SYSTEM

BEKE Éva; KOVÁCS Tibor

(ORCID: 0000-0002-8116-0422); (ORCID: 0000-0001-7609-9287)

beke.eva@kgk.uni-obuda.hu; kovacs.tibor@bgk.uni-obuda.hu

Absztrakt

A cikk azokat az Amerikai Egyesült Államokban alkalmazott komprehenzív tanítási módszereket és koncepciókat - modernt és hagyományosat egyaránt - gyűjti egybe. Ezek alapjául szolgálnak a korábban bevezetett, azóta folyamatosan bővülő biztonságtudománnyal és védelemmel kapcsolatos követelményrendszernek és oktatási irányelveknek. A tudományág széles spektrumot felölelő, szerteágazó területekre oszlik a teljesen egységes módszerek alkalmazása nem megoldható.

***Kulcsszavak**: biztonságtudomány a felsőoktatásban, módszertani elvek, új kihívások az egyetemi oktatásban*

Abstract

The article's main aim is to collect those comprehensive teaching methods and concepts – modern and traditional as well – what serve as the basis of an already launched system in regards to safety and security studies in the USA. Since the science of safety and security is a rather wide and diversified field, completely unified teaching methods cannot be introduced.

***Keywords**: safety and security science in higher education, methodological principles, new challenges in university education*

A kézirat benyújtásának dátuma (Date of the submission): 2017.07.18.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.23.

BEVEZETÉS

A klasszikus értelemben vett Maslow-féle hierarchia második szintjén helyezkedik el a biztonság, a kihívásokat szem előtt tartó, adekvát képzés e területen figyelemre méltó változásokat eredményezett. Az Amerikai Egyesült Államokban az elmúlt 50-60 év folyamatos készenléti – természeti csapások és sok száz emberéletet követelő fertőző betegségek - és versenyhelyzetre alapozott aggodalmai az orosz, kínai vagy közel-keleti veszély zónák miatt, valamint a globális gazdasági, katonai és politikai erőfölény megtartásának céljából a mindenkori adminisztráció tudatosan támogatta a biztonságtudományokkal szorosan összefüggő oktatást. Ennek célja az volt, hogy magasan képzett, jól alkalmazható munkaerő kerüljön kellő számban a szükséges biztonsági és védelmi pozíciókba. Mindezek arra kényszerítik a hosszú idő óta változatlanul működő és tanító intézményeket, hogy az újonnan jelentkező veszélyek elhárítására is alkalmas és képes szakembereket képezzenek. A biztonságtudományi tanulmányok kulcsfontosságúvá váltak a politikai, a technikai valamint a vezetői-operatív tudományok között, és mint ilyenek: interdiszciplinárisak.

A kurzusok a nemzetvédelemtől egészen az etnikai konfliktusok kezeléséig széles skálán mozognak, az egyetlen közös nevező, hogy mind a tradicionális, mind a modern biztonsági témákat tárgyalják és oktassák saját intézményi kereteiken belül vagy sok esetben külső, meghívott szakértők bevonásával.

ELVEK, TERÜLETEK, CÉLOK ÉS IRÁNYOK

Nemzetközi biztonságtudományi tanulmányok témában manapság már olyan képzéseket is indítanak, amelyek a konfliktusok valódi, nagyon gyakran emberi okait, azok végleges megszüntetését, regionális biztonsági rendszerek kidolgozását, humanitárius segélyek menedzselését valamint a nemzetközi szervezetek ebben való szerepét tanulmányozzák.

Az újabb területek közül vizsgálja a nemzetközi összefogáson alapuló titkosszolgálatok és a nemzetközi diplomácia, valamint a gazdasági és szociális egyenlőtlenségek kiváltotta viszályok kezelését - a diplomácia adta lehetőségek felhasználásával.

E folyamat a mai napig tart, jóllehet egy igen céltudatos változás figyelhető meg a biztonságtudományok fontossági sorrendjének terén. A biztonságtudományi tanulmányok (security studies) oktatása teoretikus és alkalmazott (praktikus) elemek felhasználásával egy olyan új, innovatív kontextus keretein belül oktat, amely a legmagasabb minőségi standardoknak is megfelel. Minthogy a biztonság a világon mindenütt egy összetett, valós akadályokkal és megoldásokkal szembenéző terület, fontos, hogy az oktatási módszerek kidolgozása és bevezetése olyan formában valósuljon meg, hogy a formális határok lebontásával az univerzális biztonsági stratégia kidolgozása is probléma-mentesen megvalósítható legyen.

Módszertani elvek a biztonságtudományban

Az oktatás másik legfontosabb célkitűzése az, hogy az egyes biztonságtudománnyal foglalkozó területek ne szakadjanak szét, és külön részeket alkotva a hallgatóknak választania kelljen az „either - or” elv alapján, hanem, hogy az egyes szakterületek átfedjenek egymásra és - lehetőség szerint - átmenetet képezhessenek az egyes szakágak között.

Az oktatási módszertan – bármely területet is vesszük górcső alá – kritikus pont a jövő generáció szempontjából, mert meg kell tanítania a hallgatókat e szakterületen is a kritikus gondolkodásra, a kreativitásra, a szociális készségek magas szintű művelésére, szükség esetén döntéshozatalra, a krízis-, és kockázat menedzselésére, valamint a felelős magatartásra. Ez a fajta többfunkciós perspektíva praktikusan integrálható az amerikai oktatási rendszer

különböző szegmenseibe. A képzésben használt szimulációs gyakorlatok hívatottak azt szolgálni, hogy az elemző és management technikai eszközök és megoldások készség szinten használható tudást adjanak. A gyakorlatok egyik csoportja a biztonsággal összefüggő (CTBTO, IAEA, OSCE, UN, NATO, különböző export ellenőrzési rezsimek, úgymint: Wassenar Arrangement, Nuclear Suppliers Group, Zangger Committee) nemzetközi szervezetek és intézmények szerkezetét vizsgálja, és ennek fényében, illetve segítségével dolgoz ki dinamikus stratégiai terveket - figyelembe véve a hosszú távon is megvalósítható forrás utánpótlást. Ezen elvekkel szoros összhangban működnek a globális biztonságot szolgáló nemzetközi képzések is világszerte, minthogy ezeknek a nemzetközi szervezeteknek legfőbb célkitűzéseit több nagyhatalom is ratifikálta (például a „CTBTO -… korlátlan hatályú tilalmat rendel el a katonai és más célú nukleáris robbantások végrehajtására. Tilalma légköri, a világűrbéli és a víz alatti közeg mellett, a földfelszín alatti kísérletekre is kiterjed. Semmilyen mennyiségi küszöbérték alatt nem tesz lehetővé nukleáris robbantást.”) [1]

Egy másik csoportot alkotnak azok a gyakorlatok, amelyek a nemzetbiztonsággal kapcsolatos döntéseket ölelik fel válsághelyzet esetén. A hallgatók feladata, hogy egy gyorsan kialakuló vagy már kialakult válsághelyzetben, amely az USA érdekeit éppúgy veszélyezteti, mint annak kül-, és monetáris politikáját, milyen válaszok lehetségesek diplomáciai és/vagy katonai szempontokat alapul véve, amelyek hosszú távon is formálhatják az ország stratégiáját és politikai elköteleződését.

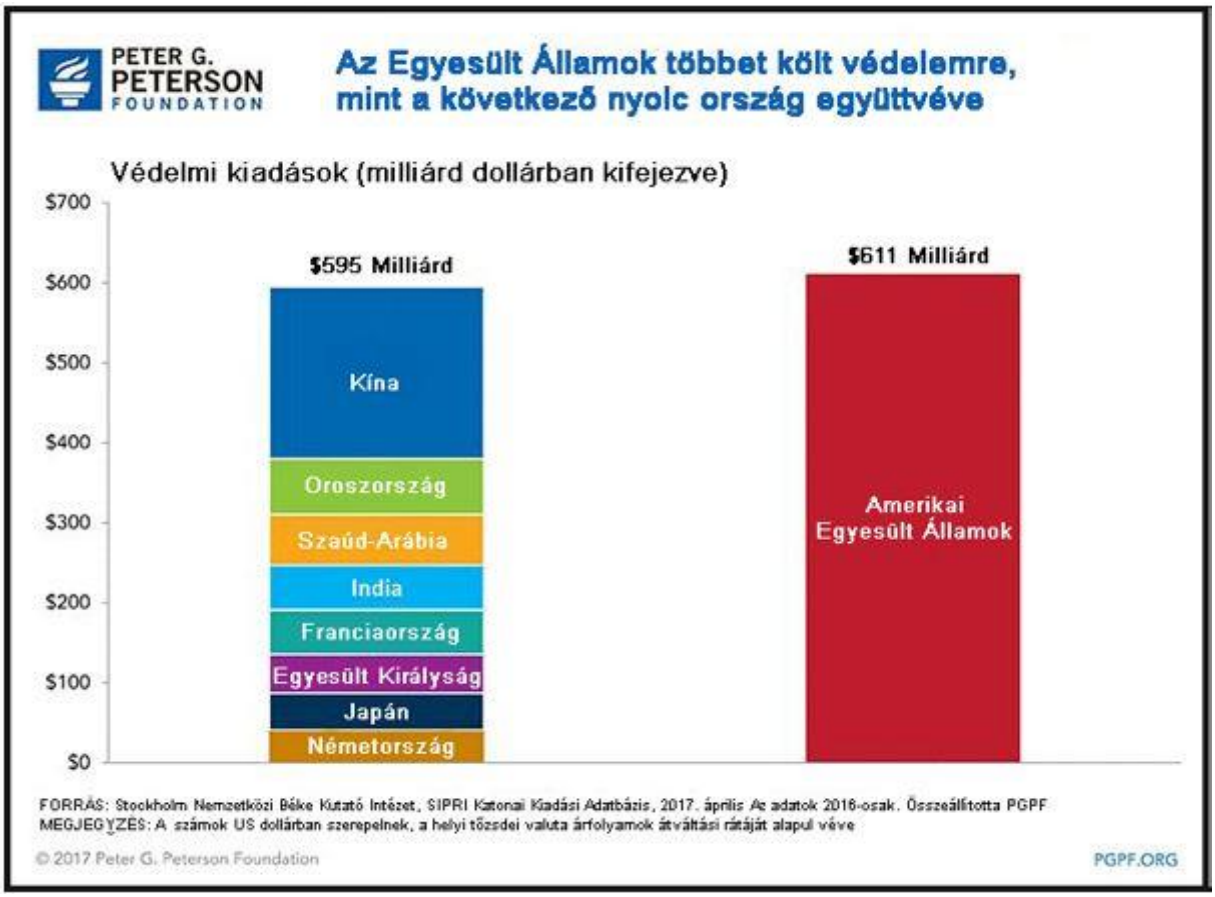
A biztonságtudomány oktatás új területei

A hagyományosan biztonságtudománynak számító szakterületek, mint például a biztonságtechnikai mérnöki tudomány, a honvédelem (homeland security), a nemzetközi biztonságpolitika és diplomácia mellé olyanok is felsorakoztak, mint a robotika és az automatizálás, a rendszerbiztonsággal foglalkozó oktatások, illetve a gazdasági és ipari drónok elleni védelem oktatása.

A 21. századi biztonságtudományi oktatás másik igen fontos területévé nőtte ki magát az információ-, és adatbiztonsági szak, a *cyber tacticians* képzés, vagyis olyan szakembereké, akik képesek az USA ellen irányuló összes, az ebbe a kategóriába tartozó támadás kivédésére. Alapvetően két csoportjuk létezik: a cyber stratéga, akinek feladata a rendszer sérülékenységének kivédése, illetve a cyber taktikus, akinek feladata a kockázat minimálisra csökkentése.

A képzési célok és irányok

A biztonságtudományi szakok egy része szorosan kötődik a politikai tudományokhoz, minthogy mindegyik kormány legfőbb célkitűzése, saját polgárainak védelme (1. diagram). A biztonsági rendszerek hibája igen gyakran az aktuális kormány politikájának hibájával kapcsolódik össze. [2] A 21. század embere egyre növekvő nyugtalansággal figyeli, hogy a hagyományos értelemben vett biztonságát új kihívások fenyegetik. Nemcsak azok, amelyeket konvencionális fegyveres konfliktusok, nukleáris fenyegetettség, avagy egyes kormányok által szponzorált terrorizmus jellemez, hanem már megjelennek a kontinenseket is áthidaló nemzetközi bűnözés, tömeges migráció vagy egész hálózatokat megbénító hackertámadások is.



1. diagram: Az Amerikai Egyesült Államok védelmi kiadásainak nagyságrendje. [3]

A biztonsági képzés másik nagy területe azon mérnökök, technikai szakemberek és a biztonság operatív részével kizárólagosan foglalkozó hallgatók oktatása, akiknek legfőbb működési területe nem az állami szféra és az ehhez szorosan kapcsolható honvédelem, terrorizmus elleni védelem, hírszerzés és elhárítás, hanem a vállalati közeg. Ennek védelmét az Egyesült Államokban három határozottan elkülöníthető, de egyúttal szorosan összefüggő, vagy egymást kiegészítő területre osztják:

- Fizikai biztonság (személyzet, áruk és létesítmények védelme);
- Informatikai biztonság (adatok és kommunikáció védelme);
- Kockázatmenedzsment (biztosítási és egyéb pénzügyi kérdések).

A biztonság és védelem működési tartománya igen széles, éppúgy, ahogy az ezekhez kapcsolódó felelősség és eljárás. Ezek igen gyakran egyes részterületeiken hiányosak, míg más részleteik átfedik egymást. Mindezek ellenére a vállalatoknak is meg kell felelniük az új biztonsági és védelmi kihívásoknak működésük minden egyes területén.

Ahogy egyre nagyobb az igény az ipari biztonság megteremtésére, úgy nő a szakemberek iránti kereslet is, ám az egyre szigorodó biztonsági követelményeknek megfelelni kívánó vállalatok egyre magasabb feltételeket szabnak a jelöltek számára, akiknek pontos ismereteket kell szerezniük és alkalmazniuk a cég biztonsági területeit átfogó vezetésben és azok részelemeiben egyaránt. Az itt megkövetelt tudás nem kizárólag technikai vagy vezetői, hanem - optimális esetben - e kettő egyensúlya. Egy maroknyi egyetem az Egyesült Államokban megalkotta a biztonságtudományi és mérnöki programokat, amelyek olyan képzési struktúrát ajánlanak, amelyeken az ipar számára szükséges tudás megszerezhető. Ezek közül a legkiemelkedőbbek a - legelőször Japánban kidolgozott - ún. belső megfelelési

programok (ICPs), amelyeknek egyik, de nem az egyetlen célja például az, hogy a titkos anyagokat gyártó cégek munkatársai tisztában legyenek azzal, hogy a technológia, a hasznosítás és fejlesztés miért „érzékeny" terület, és azokra milyen védelmi és titoktartási kötelezettségek vonatkoznak. A biztonsági oktatási programok némileg újak az egyetemeken kínált korábbiakhoz képest. Ezek között szerepel számos olyan is, amelyeket nemzeti és nemzetközi oktatási testületek akkreditálnak. Ezek az oktatási testületek megkövetelik, hogy a programokat folyamatosan javítsák annak érdekében, hogy a hallgatók elérjék az ezekben kitűzött legfőbb, a megújuló vállalati kultúrához igazodó célokat. [4]

AZ OKTATÁS LÉNYEGES ELEMEI

Módszerek

Az ember maga a „biztonsági balesetek" egyik fő okozója azáltal, hogy vezetési és tervezési megoldások védelmi követelményeit megsérti, avagy veszélyes tárgyakat működtet. Az alacsony fokú biztonsági kultúra, a gondolkodásmód és viselkedés gyakran okozza azt, hogy maga az ember a veszélyforrás. A legtöbb esetben elmondható, hogy a kultúra, a földrajzi és etnikai hovatartozás képes összehangolni az emberek és a „technológia szféra" érdekeit, míg a biztonsági kultúra ennek a harmonizációnak általános eszköze lehet. A biztonsági kultúra egyebek mellett az oktatás folyamatában alakul ki, és nagymértékben függ a munkavállalók kompetenciaszintjétől és a biztonsági kérdésekkel foglalkozó különböző pozíciókban, megfelelő hatékonysággal működő vezetéstől. [5]

A biztonsági oktatás alapjai a civilizációs változások, a kulturális értékek változásai, a tudományos és oktatási paradigmák, de éppúgy része lehet a humán, a nemzeti, vagy éppen a pragmatikus tartalom is. Külön témaként megjelenhet az emberi tényezők szerepe és a biztonsági kultúra általános és sajátos jellemzői, csakúgy, mint az emberbarát és biztonságos környezet megteremtése, mint a mérnöki feladatok egyik legfontosabbika. A képzési rendszer kiterjed az ipari és környezeti, valamint a munkahelyi biztonságra és védelmi vészhelyzetekre is. [6]

Minden társadalom nagy változásokon megy keresztül, és ez együtt jár a kulturális és tudományos oktatás elmozdulásával. Új didaktikai módszerek és elvek mentén felépülő, a hagyományos tanítási stratégiákat maga mögé utasító eljárások tűnnek fel a globális magas kockázatú társadalom megjelenésével és ennek értékrendjében bekövetkezett változásokkal párhuzamosan. A környezetre gyakorolt technológiai és antropogén hatások, valamint az egyre növekvő népesség, amelyhez hozzáadódnak a külső világ mára nagyon is valóságos veszélyei, azok az objektív tendenciák, valamint az emberi társadalom fenntartható fejlődésének szükségessége, amelyek a modern társadalmat egyre inkább a környezeti és társadalmi biztonság felé irányítják. [5]

A tudományos és technológiai változások a kockázatelmélet fejlesztését és a természeti és technológiai veszélyek tanulmányozását követelik meg, valamint annak tanulmányozását, hogy hogyan csökkenthető negatív hatásuk az emberi és természeti környezetre. Ezek a tényezők is az oktatás fejlesztését igénylik, valamint azt, hogy nagyobb hangsúlyt fektessenek a környezetbiztonsági kérdésekre, előkészítsék az egyént a gyorsan változó mindennapi valóságra, és garantálják a személyes és kollektív biztonságot. [7]

Mindezeket figyelembe véve az amerikai oktatás legjellemzőbb szakaszai a következők [8]:

A probléma felvetése

A didaktikai lépések között az első, a kérdés felvetése, nevezetesen, hogy milyen problémák megoldása szükséges és azokhoz milyen eszközök rendelhetők. Robotok prototípusának kifejlesztése, egy védelmi rendszer kidolgozása, tágabb és nemzetközi értelemben is

használható biztonság politikai elvek bevezetése vagy éppen biometrikus beléptető rendszerek használata. A lényeg az, hogy az oktató és intézménye produktív kérdésekre keressen értelmes, kreatív válaszokat és megoldásokat akár technikai akár humán tudományok alkalmazásával.

Modell-fejlesztés

A következő eleme az oktatásnak, hogy olyan modelleket fejlesszenek ki és használjanak, amelyek alkalmasak arra, hogy akár egy tudományos ötletet, vagy akár csak egy alkalmazás tudományos magyarázatát szemléltesse. Ezzel párhuzamosan az is cél, hogy új tervezési megoldásokat is kínáljon, mégpedig úgy, hogy azok a valós életben és reális környezetben is nagy valószínűséggel alkalmazhatóak legyenek. A szorosan ehhez kapcsolódó másik gyakorlat az, hogy a hallgatói modellek egy-egy oknyomozó kutatás eredményeit kell, hogy összesítsék, lehetőség szerint elkerülve a nem megbízható forrásból származó információkat és azok következményeit. Az oktató legfőbb feladata itt az, hogy kijelölje az oknyomozás helyes irányát, amelyben a hallgatóknak lehetősége nyílik tesztelni saját ötleteiket, illetve szükség esetén módosítani vagy finomítani azokat.

Szimulációs gyakorlatok

Ez ilyen típusú feladatokhoz természetesen tudniuk kell a hallgatóknak, hogy mely adatok támogatják az általuk felvázolt tervet és hogy azon belül milyen új, progresszív megoldások létezhetnek. Egy ilyen vagy hasonló feladat megoldása során nyilvánvalóan egy adott csoporton belül is többféle megoldás és interpretáció létezhet akkor is, ha a feladat ugyanaz. A legoptimálisabb eredmény kiválasztása vezeti a résztvevőket a következő lépcsőhöz, amely nem más, mint elemezni és logikus érvekkel alátámasztani a választott eljárást és az abból következő eredmények hitelességét, azok megbízhatóságát, használhatóságát bizonyítani. Matematikai, számítógép alapú vagy egyéb kalkulációkat és/vagy opciókat elemezve könnyen belátható, hogy az adatok nem mindig beszélnek önmagukért, hanem azok elemzése és a konklúziók levonása elengedhetetlen. Ennek kapcsán a hallgatók komplex rendszerek, modern és hagyományos megoldások megfigyelését és azok elemzését követhetik nyomon.

Tudományos viták

Az amerikai oktatási rendszerben a hallgatóknak képesnek kell lenniük arra, hogy koherens, logikus magyarázatot adjanak arra, hogy hogyan jutottak el a kutatási eredményekig, illetve a már létező, korábbi eredményeket be tudják építeni a saját fejlesztéseikbe. Mindazon következtetések és eredmények, amelyek ezekhez a projektekhez kapcsolódnak elengedhetetlen feltétele a kommunikáció a csoporton belül. Ez azt jelenti a gyakorlatban, hogy a közösség minden egyes tagja elmondhatja releváns reflexióit, alternatív megoldásokat kínálhat, kollaborálhat, vagy éppen ellentmondhat: így adva valóságos teret a tudományos viták gyakorlati alapjainak.

A biztonságtudomány oktatásával foglalkozó főbb intézmények

A biztonságtudományt legmagasabb szinten művelő amerikai egyetemek – felsorolásszerűen - a következők:

Georgtown University School of Foreign Service

Programjuk átfogó küldetése, hogy olyan újgenerációs elemzőket, döntéshozókat és tudósokat készítsen fel a XXI. századi nemzetközi és nemzeti biztonsági problémák és külpolitikai kérdések széles skálájának menedzselésére, akik a legbonyolultabb kérdésekben és szituációkban is képesek a legjobb döntés meghozatalára. Legújabb témáik közül kiemelkedik

a békefolyamatok veszélyei, az információs hadviselés bonyolultsága, illetve a védelem-elemzés kérdésköre. [9]

University of Massachusetts Lowell: CBRNE Security

A képzésben résztvevő hallgatók a kémiai, biológiai, radiológiai, nukleáris és egyéb robbanóanyagok (CBRNE) biztonságával foglalkoznak. A kurzusokon vizsgálják a fegyver-, és szenzortechnológiák műszaki részleteit, a non-proliferációs rezsimeket, a tömegpusztító fegyverek megszerzését és felhasználását célzó államok vagy terroristák fenyegetését, valamint a helyi, állami, szövetségi és globális erőfeszítéseket az ilyen fenyegetettség leküzdésére.

Harvard University: International Security

A képzés a globális biztonsági környezetet összetartó kérdésekkel foglalkozik elsősorban, de vizsgálja a hazai és a külpolitikát, és az ezekből származó konfliktusok okait. A Harvard Egyetem Nemzetközi Biztonsági szakképesítésén szerzett diploma lehetőséget teremt arra, hogy a hallgatók a kormánynál, egyes NGO-knál, nemzetközi szervezeteknél vagy egy multinacionális vállalatnál hasznosíthassák megszerzett tudásukat.

University of Denver: Security Management

Minthogy a biztonsági szakemberekre egyre nagyobb az igény, ez a program felkészíti őket arra, hogy megfeleljenek ennek a szükségletnek. A hallgatók megszerzik azt tudást és készségeket, amelyek a szervezetek, a munkavállalók, az ügyfelek, a fizikai eszközök és a szellemi tulajdon védelme érdekében a legfontosabbak, miközben képesek fenntartani az üzletfolytonosságot.

California State University: Industrial and Technical Studies – Organizational Security

Ez a program a hallgatóknak a szükséges technológiai hátteret oktatja, ahhoz, hogy vezetői, döntéshozói pozíciókban tevékenykedhessenek. Az ide jelentkezők három kurzus közül választhatnak, nevezetesen:

- Szervezeti biztonság: a biztonsági menedzsment fontossága a szervezetekben.
- Oktatás és képzés: a műszaki oktatás és képzés, mint karrier szerepe a biztonság megteremtésében.
- Termékek és folyamatok fejlesztése: a termék és a folyamatfejlesztés kutatása, a már meglévő adatok és a virtuális szimuláció felhasználásával.

Arizona State University: Global Security

Világunk számos különböző, összetett és folyamatosan változó biztonsági kihívással néz szembe. E kérdések megértése és az ezekre történő reagálás interdiszciplináris megközelítést igényel, amely összekapcsolja a kritikai gondolkodást a gyakorlati elkötelezettséggel. A Szabad Művészetek és Tudományok Kollégiuma által kínált kurzus, a Globális Biztonság Online áttekintést nyújt a konfliktusok okairól és költségeiről, a hazai és nemzetközi intézmények felépítéséről és működéséről, valamint a bátorítást ösztönző politikákról, amelyek lehetővé teszik a békét, a biztonságot és a stabilitást.

University of Southern California: Applied Computer Security

Az FBI arról számolt be, hogy évente több milliárd dollárt veszítenek a számítógépes bűnözés miatt, éppen ezért az IT-biztonság a technológiai iparág egyik leggyorsabban növekvő ágazatává vált. Ez a kurzus a digitális információ védelmével és biztonságával kapcsolatos aggodalmakra összpontosít, megoldásokat keres a szervezeti rendszerek védelmére és biztonságára, a hackerek elleni védekezésre és a cyber-bűnözők kézre kerítésére. [10]

Massachusetts Institute of Technology – MIT: Nuclear Science and Engineering

A nukleáris mérnöki program célja, hogy a nukleáris folyamatok hatékony megértéséhez és hasznosításához szükséges tudományos és műszaki területeken a lehető legjobb olyan oktatást nyújtsa, amely társadalom javát szolgálja - egy gazdaságilag és környezetileg fenntartható világban. Az oktatás három pillére: a tudomány, a rendszerek és a társadalom. Az érintett területek közé tartoznak a nukleáris alkalmazások az energiatermelésben, az orvosi, ipari, tudományos, környezetvédelmi és biztonsági területeken. A karon végzett kutatás kiterjed a nukleáris felhasználások széles körére, beleértve a hasadási és fúziós energiarendszereket, a nukleáris biztonságot és az orvosi, ipari és számítástechnikai eszközöket. Ezek megkövetelik a nukleáris és sugárzó anyagok folyamatainak, az anyagtudománynak, a plazmatudománynak és a kvantumtechnológiának az integrált és mélyreható ismeretét. A nukleáris rendszerek gazdasági, környezeti, társadalmi, politikai és nemzetközi vonatkozásai is központi szerepet játszanak sikeres alkalmazásukban, így ezek is a képzés részét képezik.

KÖVETKEZTETÉSEK

Minden társadalom nagy változásokon megy keresztül, és ez együtt jár a tudományos (és a kulturális) oktatás elmozdulásával. Új didaktikai módszerek és elvek mentén felépülő, a hagyományos tanítási stratégiákat maga mögé utasító eljárások tűnnek fel a globális, magas kockázatú társadalom megjelenésével és ennek értékrendjében bekövetkezett változásokkal párhuzamosan. A környezetre gyakorolt technológiai és antropogén hatások, valamint az egyre növekvő népesség, amelyhez hozzáadódnak a külső világ mára nagyon is valóságos veszélyei, az objektív tendenciák, valamint az emberi társadalom fenntartható fejlődésének szükségessége, amelyek a modern társadalmat egyre inkább a környezeti és társadalmi biztonság felé irányítják. [5]

A tudományos és technológiai változások a kockázatelmélet fejlesztését és a természeti és technológiai veszélyek tanulmányozását követelik meg, valamint annak tanulmányozását, hogyan csökkenthető ezek negatív hatásai az emberi és természeti környezetre. Ezek a tényezők is az oktatás fejlesztését követelik meg, valamint azt, hogy nagyobb hangsúlyt fektessenek a környezetbiztonsági kérdésekre, előkészítsék az egyént a gyorsan változó mindennapi valóságra, és garantálják a személyes és kollektív biztonságot. [7]

Mindazok az oktatási módszerek és irányelvek, amelyeket a cikkben felsoroltunk megteremtik a szükséges alapokat ahhoz, hogy a hallgatóknak az oktatás befejeztével megbízható tudásuk legyen az USA biztonsági kérdéseiről, a jogszabályalkotást befolyásoló legfontosabb politikai döntésekről, a külpolitikai és katonai lépésekről, a vállalati és környezeti biztonságról, a védelem megtervezéséről és szervezéséről, valamint teljes áttekintést nyújt az USA komplex biztonsági struktúrájáról és folyamatairól.

FELHASZNÁLT IRODALOM

[1] Non-proliferációs ABC Multilaterális fegyverzetellenőrzési megállapodások és exportellenőrzési rendszerek (1.2. Átfogó Atomcsend Szerződés, I. A szerződés legfontosabb célkitűzései és előírásai) Budapest, 2000, 23. oldal

[2] National Security Education Program

www.nsep.gov

[3] ETH Zürich Departement Geistes-, Sozial- und Staatwissenschaften – Center for Security Studies; www.css.ethz.ch/10.10.

[4] An investigation into HSE educational programs in the USA M. Albuti & G. Reniers Safety and Security Engineering, VI.267 WIT Transactions on The Built Environment, Vol.151., WIT Press, 2015

[5] Alexandrov, A. – Devisilov, V. A. – Ivanov, M.: A role of education system in creation of safety culture, Bauman Moscow State University https://www.researchgate.net/publication/309116168_A_role_of_education_system_in_creation_of_safety_culture (Letöltve: 2017. július 2.)

[6] Security Education and Critical Infrastructures by Cynthia Irvine, Helen Armstrong: Principle of Least Privilege www.books.google.hu/books?id=k73gBwAAQBAJ&pg=PA268&lpg=PA268&dq=security+as+as+an+object+of+education+in+the+usa&source=bl&ots=r2jrmxsAYv&sig=rJnT0ToJGdJA4AlNwpeAvKBKAxg&hl=hu&sa=X&ved=0ahUKEwjN1d3-vPLTAhXSa5oKHZsoCxcQ6AEIZTAH#v=onepage&q=security%20as%20as%20an%20object%20of%20education%20in%20the%20usa&f (Letöltve: 2017. június 20.)

[7] The Washington Post – What's the purpose of education in the 21st century? www.washingtonpost.com/news/answer-sheet/wp/2015/02/12/whats-the-purpose-of-education-in-the-21st-century/?utm_term=.0a9740b85259 (letöltve: 2017. május 12.)

[8] Maxwell School National Security Studies https://www.maxwell.syr.edu/exed/Sites/nss/About_NSS/

[9] Georgetown University www.georgetown.edu/

[10] USC University of Southern California; www.usc.edu

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

SZOMBATHELYI FERENC VEZÉREZREDES HADÁSZATI ELGONDOLÁSA A NÉMET HADVEZETÉS SZÁMÁRA AZ 1943-AS ÉVRE VONATKOZÓAN, ÉS ELEMZÉSE A MAGYAR 2. HADSEREG MŰKÖDÉSÉRŐL

STRATEGY PLAN OF COLONEL GENERAL FERENC SZOMBATHELYI FOR THE GERMAN MILITARY HEADQUARTERS AND HIS ANALYSIS OF THE 2ND HUNGARIAN ARMY'S OPERATION IN 1943

KALÓ József

(ORCID ID: 0000-0002-5022-5334)

kalo.jozsef@uni-nke.hu

Absztrakt

A tanulmány két, eddig nem publikált dokumentumot és azok keletkezési körülményeit mutatja be. Mindkét dokumentum keletkezési körülményei és létrejöttének céljai a rendelkezésre álló primer és szekunder források alapján felvázolhatók, s beilleszthetők a Szombathelyi Ferenc vezérezredes vezérkarfőnöki működésének elemzésébe, tágabb értelemben a második világháborús magyar hadtörténelem fontos, eddig homályban maradt részleteinek megvilágításába.

Kulcsszavak: *Szombathelyi Ferenc, doni katasztrófa, második világháború, önálló magyar katonapolitika, hadászat*

Abstract

The paper presents two unpublished documents and their creation conditions. The origins of the two documents and the aims of their creation can be outlined on the basis of the available primary and secondary sources, and can be included in the analysis of the General Staff of the Ferenc Szombathelyi Chief of Staff, in a broader sense, in the light of the important obscure details of WWII.

Keywords: *Ferenc Szombathelyi, Disaster on the Don River, Second World War, independent Hungarian military policy, strategy*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.02.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.15.

BEVEZETÉS

1942. november 19-én indult meg a szovjet Uránusz hadművelet, melynek célja a Sztálingrád térségében harcoló tengelyerők bekerítése és megsemmisítése volt. Az offenzíva elsöpörte a német arcvonalat, bekerítették, majd megsemmisítették a németek legerősebb hadműveleti csoportosítását, a Friedrich von Paulus[1] vezérezredes (majd vezértábornagy) vezette német 6. tábori és 4. páncélos hadsereget. A Kaukázusban lévő német erőknek is csak nagy veszteségek árán sikerült visszavonulniuk. Még a Sztálingrád térségében bekerített német erők felszámolása (1943. február 2.) előtt, a szovjet vezetés az egész keleti arcvonalra kiterjedő általános támadás megindítására adott utasítást. Így került sor a Voronyezsi Front osztrogozsszk-rosszosi, illetve a Brjanszki Front csatlakozásával a voronyezs-kasztornojei hadműveletek végrehajtására, amelyek közvetlenül a magyar 2. hadsereg és az olasz 8. hadsereg részei (Alpini hadtest), majd a német 2. hadsereg ellen irányultak. Ennek következtében 1943. január 15-én a magyar 2. hadsereg részekre szakadt, majd két nappal később a hadsereg parancsnoka, Jány Gusztáv[2] vezérezredes kiadta a visszavonulási parancsot. A hadsereg visszavonulása és majdnem teljes felmorzsolódása egészen február elejéig tartott, melyet a megmaradt részek állományrendezése után a hazaszállítás követett 1943 áprilisában és májusában. A hadsereg vesztesége a becslések szerint 93-148.000 ezer fő között mozog, nehéztechnikában közel 100%, egyéb anyagban 70%.

A magyar politikai és katonai vezetés – élükön Kállay Miklós[3] miniszterelnökkel és Szombathelyi Ferenc[4] vezérezredessel, a Honvéd Vezérkar főnökével – a katasztrófát követően el volt tökélve, hogy a magyar erők megőrzéséről[5] vallott elképzeléseit tovább képviselik, sőt, a katasztrófa még inkább erősíteni fogja erre vonatkozó hivatkozási alapjukat a németek előtt. A vezérkarfőnök szerint „*mi legalábbis egy év tartamára ki vagyunk merítve. Nem tehetünk róla, hogy a németek erőinkkel olyan rosszul sáfárkodtak*.” [1] Véleménye szerint a németek a szovjetek erejét nem kellőképpen mérték fel, melyre bizonyítékul szolgálnak a Szombathelyi vezérezredes 1942. szeptember 14-15-i, a Führer főhadiszállásán tett látogatása alkalmával elhangzottak. Ekkor maga Adolf Hitler[6] hangsúlyozta a magyar vezérkarfőnöknek, hogy „*nagyobb hadműveleteket kizárnak a tél folyamán, csak kisebb támadásokról lehet szó*”. Ebből pedig az látszik, „*hogy a téli korai és hatalmas offenzíva a németeket is bizonyára meglepte.*” [2]

A fő kérdés most az ország szempontjából ez: adunk-e további erőket a háború folytatására, vagy sem. „*Ez a kérdés most, és semmi más, mert a németek nehezen harcolnak*

[1] Friedrich von Paulus (1890-1957) vezértábornagy, 1940. szeptember 3-tól 1942. január 5-ig a német szárazföldi haderő I. főszállásmestere, egyben a német szárazföldi haderők vezérkarfőnökének (Halder) helyettese. 1942. január 5-től 1943. január 31-ig a német 6. hadsereg parancsnoka. 1943. január 31-én adta meg magát a szovjet csapatoknak, majd február 2-án sor került a német csapatok teljes sztálingrádi kapitulációjára is.

[2] vitéz Jány Gusztáv (1883-1947) vezérezredes, 1940. március 1-től 1943. augusztus 5-ig a magyar 2. hadsereg parancsnoka.

[3] Kállay Miklós (1887-1967), 1942. március 10-től 1944. március 22-ig Magyarország miniszterelnöke.

[4] Szombathelyi Ferenc (1887-1946) vezérezredes, 1941. szeptember 6. és 1944. április 19. között a Honvéd Vezérkar főnöke.

[5] Szombathelyi Ferenc Honvéd Vezérkar főnöki kinevezését az erők megőrzéséről vallott katonapolitikájának köszönhette. Ennek lényege röviden úgy foglalható össze, hogy nem kerülhetünk hasonló történelmi helyzetbe, mint 1918-19-ben, amikor a nagyhatalmak háborújában kivérzett magyarságnak nem maradt ereje saját önvédelmére, sajátságosan magyar céljai megvalósítására. Ezért arra kell törekednünk, hogy ha már szerencsétlen módon beléptünk ebbe az új háborúba, akkor csak annyi erőt bocsássunk a németek rendelkezésére, amennyit feltétlenül szükséges. „*Nekünk a fal mellett kell járnunk”, ill. „amikor a nagyok a kocsmában verekszenek, a kicsik menjenek ki*” – fogalmazta meg mindenki által érthető módon. Bővebben lásd: Kaló József: *Szombathelyi Ferenc memoranduma*. Hadtörténelmi Közlemények 2009/3. szám. 747-762.

[6] Adolf Hitler (1889-1945) a Nemzetiszocialista Német Munkáspárt (NSDAP) vezetője, 1933-tól Németország kancellárja, 1934-től Führere, azaz teljhatalmú diktátora.

és válságos küzdelemben élnek. Katonát adni pedig ma – anélkül, hogy a nemzet ellenálló képessége előbb vagy utóbb össze ne roppanna – lehetetlennek tartom. A további fegyveres részvétel nagy erőkkel Keleten, a nemzet szempontjából már eddig is túlfeszített igénybevételt teljesen kimerítené." [3] Azaz Szombathelyi vezérezredes szerint jelen helyzetben, és a belátható jövőt tekintve is ez semmi mást nem jelenthet, mint fokozott erőkifejtést a világháborúban, amely a sajátságosan magyar célok szem elől tévesztését, sőt a teljes összeomlást eredményezné!

A magyar vezérkarfőnök a német főhadiszálláson tett 1943. február 1-jei látogatása során a német-magyar sorsközösségre, a német-magyar egymásrautaltságra hivatkozott, a németek jóindulatának megtartása érdekében. Történelmi példával támasztotta alá tárgyalópartnereinek, hogy Magyarország a törökök ellen 300 évig volt Európa – benne is elsősorban a németség – védőbástyája. Ugyanazon érveket hangoztatta, mint tette ezt már 1941 nyarán, akkori memorandumában, és azóta is számtalan alkalommal. Szükség volt ezen érvekre, még akkor is, ha tisztában volt vele, hogy a völkisch gondolkodású német politikusokat és katonákat ez vajmi kevéssé érdekelné saját ambícióik kielégítésekor. De ezen érvrendszerre támaszkodva lehetségesnek látta a német támogatás kicsikarását anyagi, fegyverzeti tekintetben, és természetesen a szomszédos államokkal szemben is, a német kegyekért folytatott versenyben. Az 1941-es memorandumában megállapított módon logikusnak fogadta el a német-magyar történelmi egymásrautaltság tételét, de ennek csak a túlzásoktól mentes változatát. A magyar vezérkarfőnök fejében ez nagyjából úgy fogalmazódhatott meg, hogy a magyarság történelme során bebizonyosodott: a magyarság és a németség céljai azonosak, vagy inkább egymással párhuzamosan haladók. Ez látszott a török elleni háborúk során, az első világháborúban, majd a versailles-i békerendszer felszámolásánál is. A Duna-medence népei közül ezen utóbbiban csak a németség és a magyarság volt őszintén érdekelt, a többi nemzetiség, mint a románok, szlovákok, horvátok csak a Német Birodalom felemelkedése után lettek a németek szövetségesei. A magyarság számára az egymásrautaltság természetes módon adódott. Azonban Szombathelyi gondolatrendszerében ez nem jelentette a magyar érdekeknek a németek alá rendelését, sőt, világosan látta a németek oldaláról fenyegető veszélyeket.

1943. február 12-én Szombathelyi vezérezredes memorandumot írt Horthy Miklós[7] kormányzónak, melyben a doni katasztrófa következtében kialakult kül-, bel- és katonapolitikai helyzetet elemezte. [4] Írását azzal kezdi, hogy a doni katasztrófa után egyértelműen látható: „*A magyar hadsereg részvétele a keleti arcvonalon* […] *nem hozta meg azt a sikert, amire számítottunk*." Ahogyan Hitler február 1-jén, úgy ő is úgy fogalmaz: „*A tárgyilagos történetírásra vár az a feladat, hogy a sikertelenség okait teljesen és részletesen felderítse*." Azonban Hitlerhez képest, a németeket bírálva hozzáfűzi: „*a szövetségesek részéről a sikertelenség fő okát én abban látom, hogy a németek az oroszok erejét – dacára az 1941. év és 1941/42. év kemény harcainak, még mindig nem ismerték fel teljes mértékben, és ezért a szövetséges hadak közreműködéséhez olyan reményeket fűztek, amelyeknek ezek nem voltak képesek megfelelni*." Keserűen vethette papírra e mondatot a magyar vezérkarfőnök, hiszen éppen ő volt az, aki erre Keitel[8] vezértábornagyot egy évvel korábban, 1942. januári, a magyar 2. hadsereg keleti hadszíntérre küldését eredményező budapesti tárgyalásai során figyelmeztette.[9] Tehát most a németekre is kijózanítóan hathatott a vereség, mely által rá kellett döbbenniük, hogy „*a szövetségesektől a németekhez hasonló teljesítményeket nem*

[7] vitéz nagybányai Horthy Miklós (1868-1957) altengernagy, 1920 és 1944 között Magyarország kormányzója, a Magyar Királyi Honvédség Legfőbb Hadura.

[8] Wilhelm Keitel (1882-1946) vezértábornagy, a német véderő-főparancsnokság (OKW) főnöke 1938 és 1945 között.

[9] Az 1942. januári tárgyalásokra vonatkozóan bővebben lásd Kaló József: *A Honvéd Vezérkar főnöke és a 2. magyar hadsereg (1942-1943)*. Társadalom és honvédelem 2009/3. szám pp. 69-99.

várhatnak." Különösen igaz ez Szombathelyi vezérezredes szerint Magyarországra, amely a két háború között – ellentétben Olaszországgal és Romániával – nem fegyverkezhetett szabadon, sem anyagi, sem szellemi vonalon. Ezen felül a Szovjetunió ellen viselt háború messze esik a magyar céloktól és lélektől, már méreteiben is. „*Magyarország ilyen hatalmas külháborúra,* […] *soha nem készült, és az egész történelme folyamán ilyen háborút nem is viselt. Háborús céljait mindig is a Kárpátok medencéjén belül akarta megvalósítani, és az itteni vezető helyzetéért vívott háborúkban élte ki magát.*" Megismételve az elmúlt években általa már többször hangoztatott érvet, ismét leszögezi: „*mi magyarok ebbe a keleti háborúba tisztán ideális javakért szálltunk harcba. Semmiféle anyagi előnyt ott nem kerestünk, de nem is akartunk keresni*."

Kijózanítóan hatott a németekre az 1942 novemberében megindult hatalmas offenzíva – írja a kormányzónak a vezérkarfőnök. Szombathelyi vezérezredes, a német főhadiszálláson 1943. február 1-jén tapasztaltak alapján azt feltételezi, hogy a németek rájöttek tévedésükre a szövetséges erők felhasználása tekintetében. Ehhez a felismeréshez ő maga is el kívánta juttatni őket, amikor „*a német vezérkar főnöke számára ez év karácsonyán egy tájékoztatót állítottam össze*[10]*, amelyben rámutattam arra, hogy a magyar hadsereg felszerelése, kiképzése és a gyártási kapacitásunk olyan állapotban van, hogy újabb erőket az orosz frontra nem vagyunk képesek kiküldeni*." A tájékoztató megírásának másik okát is megnevezi: a németek nehézségeit látva félt attól, hogy az „*1943. évre újabb követelményekkel léphetnek fel*", s ezt kívánta megelőzni. De egyben rámutatott fenti tájékoztatójában arra is, hogy számolni kell egy balkáni partraszállás lehetőségével is, s mindezek miatt „*további magyar erőknek az orosz harcvonalra való kiküldését sem a nagy szempontokat figyelembe véve, de különösen a magyar szempontokból kiindulva, nem is tartanám helyesnek.*"

A MAGYAR VEZÉRKARFŐNÖK HADÁSZATI ELGONDOLÁSA AZ 1943-AS ÉVRE VONATKOZÓAN

Március első napjaiban a német hadvezetésnek még nem voltak kiforrott tervei a magyar 2. hadsereggel kapcsolatban. Szombathelyi vezérezredes úgy látta, a teljes keleti hadszíntérre vonatkozóan a németek az újratervezés fázisában vannak, s ki kívánta használni ezt az átmeneti állapotot. Március 3-án levelet írt Zeitzler[11] gyalogsági tábornoknak.[12] Lieszkovszky Pál[13] huszár alezredes visszaemlékezése szerint egy, az alábbiakban ismertetetthez hasonló,

[10] Szombathelyi vezérezredes itt az 1942. december 30-i tájékoztatójára céloz. Az iratot közli Bonhardt Attila: Hadtörténelmi Közlemények 1993/2.szám 176-190. A Bonhardt által közölt példányra Nagy Vilmos 1945 májusában egy tiszttársánál akadt rá. Szövege – a kézírásos javítások kivételével – megegyezik a Kardos hagyatékban található példánnyal. A különbség annyi, hogy a keletkezés dátuma a Bonhardt-féle iraton 1942. december, míg a Kardos-hagyatékban pontosabb: 1942. december 30. HL Personalia dr. Kardos János ügyvéd hagyatéka. 251. doboz. Orientierung über die Rüstungslage und militärpolitische Lage Ungarns. 1942. XII. 30. 1-19. Szombathelyinek a miniszterelnök úrnak tett 1943. január 17-i szóbeli tájékoztatásról készült feljegyzésében fenti iratot 1943. január 1-jére datálta.

[11] Kurt Zeitzler (1895-1963) vezérezredes, 1942. szeptember 24-től 1944. június 30-ig a német szárazföldi haderő (OKH) vezérkari főnöke. 1942. szeptember 24-től 1944. január 30-ig gyalogsági tábornok, utána vezérezredes.

[12] HL Personalia dr. Kardos János ügyvéd hagyatéka. 251. doboz. A levelet Szombathelyi Homlok vezérőrnagy útján kívánta eljuttatni Zeitzlerhez, aki azonban március elejétől Hitler kíséretében elutazott. Ezért némi késlekedés után, március 10-én vehette kezébe a levelet, melyre vonatkozó válasz előttünk nem ismert.
Kardos János regiszterében a levél a következőképpen szerepel: „*Haditerv 1943-ra Zeitzler német vkf. számára (fogalmazvány) 1943. III. 3.*"

[13] Lieszkovszky Pál Alfréd (1900-1983) huszár alezredes. 1939. október 1. és 1941. augusztus 1. között a VIII. hadtest parancsnokának személyi segédtisztje, 1941. május 1-től őrnagyi rendfokozattal. 1942. április 1-től a Vezérkar Főnökének személyi segédtisztje, 1942. október 1-től alezredes. HM Központi Irattár 59.388.
A gimnázium elvégzése után és az érettségi letételét követően 1917 és 1920 között a Ludovika Akadémia hallgatója volt. 1920–23 között a 4. huszárezred hadnagya Nyíregyházán. 1923-tól főhadnagy, s a pécsi

alapvetően a területfeladás alapelvéből kiinduló tervet egyeztetett Szombathelyi vezérezredes már 1942. szeptember 14-15-i, német főhadiszálláson tett látogatása során az OKH akkori vezérkari főnökével, Franz Halder[14] vezérezredessel. „*Halderral való beszélgetések közben hivatkozott az első világháború néhány sikeres csatájára* […]. *Színesen ecsetelte a tér és távolság hátrányait, a háttér bizonytalanságát, a sok erőt lekötő megszálló csapatokat. Azt a véleményt hangoztatta, hogy nem a birtokolt terület nagysága és szétszórt erők helyi sikerei döntik el a háború sorsát. Szombathelyi kifejtette azt a véleményét, hogy vissza kellene vonni a csapatokat és önként feladni a területet, megrövidíteni az arcvonalat. Halder valószínűleg egyetértett volna evvel, de nemhogy Hitlernek, még Keitelnek sem adhatna elő ilyen javaslatot, de még tanácsot sem nyilváníthat. Viszont nagyon szívesen venné, sőt kéri Szombathelyit, hogy egy ilyen tanulmányt nyújtson be, és azt Keitel útján juttassa el Hitlerhez. Szombathelyi független, kívülálló személy, aki ezt megteheti.*" [5] Lieszkovszky alezredes szerint a tanulmány elkészült, de annak további sorsáról nem rendelkezett információkkal. Feltételezésünk szerint az eredetileg Haldernek felvetett tervet vehette ismét elő Szombathelyi vezérezredes 1943 elején, és küldte meg az OKH akkori vezérkari főnökének, Zeitzlernek. Ugyanis Haldert az 1942. szeptemberi beszélgetést követően két héttel Hitler leváltotta beosztásából, így feltehetően akkor a magyar vezérkarfőnök „jegelte" a tanulmány ötletét.

A Zeitzlerhez írt levél német szövegű változata, fogalmazványa maradt fenn, melynek magyar fordítását teljes terjedelmében közöljük, s elemzésnek vetjük alá:

Mélyen tisztelt Tábornok Úr!

Azóta, hogy a magyar hadseregrészek az arcvonalból kivonattak, a harcot teljesen elfogulatlanul és az igazi katonáskodás történelmi szempontjából követhettem nyomon. Részben ez a nézőpont, részben katonaszívem hajt engem arra, hogy Önnek, mélyen tisztelt Tábornok Úr, írjak és a német csapatok haditettei felett érzett csodálatomat kifejezzem.

Amit csapatai teljesítenek és ahogyan a legnagyobb áldozattal a kifogyhatatlan orosz tömegek elébe dobják magukat, az a máskülönben olyan dicsőséges német hadseregnek bizonyára egyik legszebb fejezete lesz a hadtörténelemben.

Az új nemzetiszocialista német hadsereg felnőtt a régi császári hadsereg nagyságához, amely a négyéves nehéz háborúban kitartott, amely a hadtörténelem legtündöklőbb fegyvertényeit vitte véghez és amelynek csodálója mindig voltam.

---

testnevelési felügyelőségen szolgál. 1924–29 között a Zrínyi Miklós reálnevelő intézet nevelője. 1929-től századosként a 4. huszárezred századparancsnoka. 1939-ben Kassára helyezték segédtisztnek. 1941. augusztus 1. – 1942. április 1.: a HM VIII. Csoportfőnökség lovas sport előadója. Béldy Alajos segédtisztje. 1942. április 1. – 1944. április 1. között a VKF-nél személyi segédtiszt, s mint ilyen részt vett a kormányzóhelyettes halála körülményeinek kivizsgálásában. 1944. április 1. – 1944. december 31. között a HM 40. oszt. előadója. Eközben 1927-ben főtiszti tanfolyamot végzett Pécsett, 1929-ben lovagló tanfolyamot Nyíregyházán, 1941-ben törzstiszti tanfolyamot Budapesten. Őrnaggyá 1941 májusában, alezredessé 1942. október 1-jén léptették elő. 1943 decemberében nagy honvéd sportügyességi jelvényt kapott. Részt vett a Szabadság-front ellenállási mozgalomban. Bajorországban jugoszláv partizáncsapatot szervezett, 54 magyar politikai fogolynak a nyilas internáló táborból való kiszabadítására fegyveres akciót indított. 1945. május 1. – december 23.: amerikai fogságban volt. 1946. október 24.: a tényleges szolgálatból elbocsátották, ezt követően felesége játékkészítő üzemében közreműködő családtag. 1951. július 17-én kitelepítették Csány községbe. 1952-be lefokozták tart. honvéddé. Dillinger Istvánnal közösen írt munkája 1927-ben jelent meg Pécsett Illemtan és jellemnevelés címmel. https://www.arcanum.hu/hu/online-kiadvanyok/2vhSzakkonyv-magyarok-a-ii-vilaghaboruban-2/az-ihnetov-munkanaploja-vitez-beldy-alajos-vezerezredes-hadtortenelmi-leveltarban-orzott-irataibol-19411943-82D0/fuggelek-A02A/a-munkanaploban-szereplok-eletrajzi-adatai-A1B6/lieszkovszky-pal-alfred-A63F/ (letöltés ideje. 2017. november 12.)

[14] Franz Halder vezérezredes (1884-1972) a német szárazföldi haderő vezérkarának (OKH) főnöke 1938. október 31. és 1942. szeptember 24. között.

Mialatt én bámulattal (és alkalomadtán bizonyos irigységgel is) nézek fel a német katonák hőstetteire, ugyanakkor gondterhelten figyelemmel kísérem a 2. hadsereg nehéz útját, amely a szerencsétlen harcok után száz és száz kilométereket súlyos ínségben vándorol vissza. Még nem tudom, mikor és hol teszi majd az általános helyzet lehetővé, hogy a csapatrészek végül rendeződjenek és a szervezés és fegyelmezés munkáját – mely szempontjából a hosszú út biztosan nem volt kedvező – megkezdhessék.

Nagy aggodalommal tekintek a jövendő elé, mit fogunk tudni kezdeni ezzel a 2. hadsereggel. Legjobbjai elestek, megsebesültek, vagy hősiesen kitartva az ellenség kezébe kerültek. Harcos állománya a legkisebbre csökkent. Ami ottmaradt, az legnagyobbrészt a málhához, vagy a hadsereg különböző intézeteihez beosztottak. A tüzérséget, lövegeket és egyéb nehézfegyvereket, majdnem mindet, az állásokban kellett hátrahagyni és legnagyobb részben a kézi lőfegyverek hiányoznak. Az eddigi jelentések szerint a hadseregnél kb. 30.000 puska és ritkaságként csak egynéhány löveg és nehézfegyver maradt meg. Egy hadsereg fegyverek és harcoló mag nélkül. Mikor lesz ebből a szétzilált seregből ismét katonákból álló hadsereg. Különösen, ha arra gondolok, hogy a hátországban éppen fegyverben és hadianyagban hiány uralkodik.

Mihelyt a kinti viszonyokról tiszta képet kapok és a kötelékek rendbehozatalát meg tudjuk kezdeni, bátorkodom Önnek a hadsereg további felhasználására vonatkozóan konkrét javaslatokat tenni. Előzetesen szándékomat csak olyan tágan tudom megfogalmazni, hogy a fölösleges legénységet, különösen a vonattól, és mindenkit, aki fegyver hiányában nem alkalmazható, a kiegészítő parancsnokságokhoz a hátországba utasítom, már amiatt is, hogy a gazdasági életben használhatóak legyenek és ellátásuk ne a szükségszerű utánpótlást vegye feleslegesen igénybe.

Csak azokat a kötelékeket akarom kint hagyni, amelyeket fel tudok fegyverezni. A felfegyverzésre vonatkozóan – amennyiben ennek korszerűnek kell lennie, hogy teljes értékű és harcra termett kötelékeket állíthassunk fel – az Önök segítségére vagyunk utalva.[15]

Miközben most aggodalmaimmal terhelve Önnek írok, felteszem magamnak a kérdést, mik ezek az aggodalmak azokhoz képest, amelyeket Önnek most, egy új háborús év és hadműveleti szakasz kezdetén viselnie kell? Egy új haditervet kell az 1943-as évre meghatározni, amely Európa népeinek és országainak sorsát dönti el. Minő nehéz feladattal kell itt megbirkózni.

Minek és hogyan kell megtörténnie ahhoz, hogy az oroszok gyengéjét végre egyszer kitapogassuk, ez bizonyára az első kérdés.

Kérem Önt, mélyen tisztelt Tábornok Úr, semmilyen elbizakodottságot ne lásson abban, hogy ezt a kérdést itt felvetem. Távol áll tőlem a szándék, hogy Önnek bármilyen tanácsot adjak, ami éppen a katonáskodás mesterségében hálátlan szerep lenne. Egyedül véleményem összefoglalásának és Önnel való ismertetésének vágya hajt, mert ez mély rokonszenvemből és bajtársi összetartozás tudatomból fakad és tanulmányaimon alapszik, melynek eredete a cs. és kir. Hadiiskola[16] *idejére nyúlik vissza. Annálfogva mert én ezt igaznak gondolom, bátorkodom a következőket előadni.*

Az 1942-es esztendőnek nem szabad megismétlődnie, mert ez túl kevés sikert hozott. Sokkal több siker lett volna szükséges az 1941-es esztendőben ahhoz, hogy az ellenséget ismét lefegyverezzük, őt legalább annyira kimerítsük, hogy az elkövetkezendő télen hatalmas lendületét, melyet ezen a télen kifejtett, ne tudja megismételni. Ezért az ellenség zömét kell megtalálni és megverni. Ehhez, amint már Nagy Frigyes[17] *is tanította, egyik vagy másik*

[15] Tehát ismét megerősíti a német hadvezetés felé, hogy több harcoló erőt nem tudunk adni. Már a magyar 2. hadsereg maradványaiból is csak nagy nehézséggel, és csakis német segítséggel lehet harcoló erőt faragni.

[16] Az Osztrák-Magyar Monarchia Bécsben működő vezérkari tisztképző (felső szakképző) intézménye, melynek hallgatója volt Szombathelyi Ferenc is 1911-1914 között.

[17] II. (Nagy) Frigyes (1712-1786), porosz király (1740-1786). Uralkodása alatt emelkedett Poroszország regionális hatalomból a nagyhatalmak sorába. A hétéves háborúban (1756-1763) sokszoros túlerő ellen harcolt,

tartományt be kell áldozni. Ezért nem számít, milyen messzire vonul vissza az ember, ha az ellenség főerejének bekerítéséről és megveréséről van szó.

Hajlok arra a nézetre, hogy az orosz a támadást tavasszal folytatni fogja és ezáltal alkalom nyílik egy hatalmas csapásra. Nem úgy fog viselkedni, mint az előző évben, amikor főerőit visszavette és a téli offenzívára előkészítette. Csak Sztálingrádnál harcolt komolyan presztízsokokból. Idén győzelemérzetében nem fog visszavonulni. Mindent arra fog feltenni, hogy tejes győzelmet arasson. A döntésért fog harcolni és ehhez előrevonja tömegeit. Ezért ezek a tömegek sebezhetők. Adott esetben, ha szükséges lenne, még tovább vissza kell vonulni azért, hogy neki saját visszavonulási szándékot színleljünk és tömegeit előcsalogassuk.

Hol sebezhetőek ezek a tömegek? Azt hiszem az orosz hadszíntér déli részén. A hadszíntérnek ezen a részén lesz a döntés. Itt minden mozgásban van. A hó- és sármentes idő hosszabb, az időjárási viszonyok kedvezőbbek. Itt nyílik lehetőség az ellenség gyengéit kihasználni, őt megsemmisíteni és a győzelem után a termékeny területet, amelyet esetleg ki kellett üríteni, újra megszállni. Azonban a Dnyepertől keletre nem kell előrenyomulni. Még ha az előrenyomulást a hadműveletek érdekében ettől a vonaltól távolabb is lenne szükséges végrehajtani, a főerőt télre ismét a Dnyeper területére kell visszavonni.

A cs. és kir. Hadiiskolában egykoron az Oroszország elleni támadásnál a Dnyeper-vidékén kívül előrenyomulást sohasem terveztünk. Azon a nézeten voltunk, hogy ez a terület és a balti államok jelentik a határát a közép-európai katona legjobb teljesítményének. Ettől a területtől távolodva nemcsak az utánszállítási nehézségek, hanem a terület végtelen kiterjedése és a közép-európai ember pszichológiai gátlásai – akit az egészen ismeretlen klimatikus és földrajzi viszonyok aggasztanak – miatt is, nem tudunk sikeresen előrenyomulni.[18]

Az első világháborúban éppen az oroszoknál tapasztaltuk, hogy a földrajzi viszonyoknak szerepe volt a győzelem eldöntésében. A sztyeppei embert, az oroszt, a Kárpátok erdős hegyvidékének idegen viszonyai szorongással töltötték el. Nemcsak mi győztük le őket a Kárpátokban, hanem a földrajzi viszonyok is.[19] *Az orosz hadszíntér körülményein a motorizálás semmit sem változtatott, mivel ennek tartozéka, a kiépített út, éppen úgy hiányzik, mint a '10-es években, amikor a Hadiiskolába jártam.*

Nem szabad átlépni ezt a Dnyeper-vonalat, különben a végtelenbe veszünk. Ezzel szemben ebben a vonalban jól be lehet rendezkedni a védelemre és az állásokat fokozatosan fallá lehet kiépíteni. Ez a vonal kb. 1600 km hosszú. Egyharmada annak a vonalnak, amelyet a mostani

---

1761-re országa ereje kimerült és Frigyes bukása már-már biztosnak látszott. A porosz király az öngyilkosság gondolatával foglalkozott. Azonban a háború menete Frigyes számára szerencsés véletleneknek (mint Erzsébet orosz cárnő halála) is köszönhetően megváltozott, s Poroszország elkerülte a vereséget.
Szombathelyi vezérezredes nem véletlenül célzott itt Nagy Frigyesre, mint történelmi példára, hiszen – hadtudományi kiválóságán túl – köztudott volt, hogy Hitlernek ő a személyes példaképe.

[18] Szombathelyi 1941-ben hasonló megállapításokra jutott a keleti hadszíntérről Rundstedttel folytatott beszélgetésekor, és hasonló értelemben nyilatkozott a Legfelsőbb Honvédelmi Tanács 1942. október 8-i ülésén tartott előadásában is. A Rundstedt vezértábornaggyal folytatott tárgyalásai során meglepte, hogy a német tábornok milyen tárgyilagosan ítéli meg a szovjetek elleni háborút és annak esélyeit. Szombathelyi kifejezte aggályát, hogy meddig fog még a tengelycsapatok győzedelmes előnyomulása tartani, s mi az oka annak, hogy a sorozatos győzelmek ellenére bizonytalanságot érez. Rundstedt megértően bólogatott és röviden csak ennyit árult el a maga aggodalmaiból: „*Raumangst haben wir mein Lieber!*", azaz „*Félünk a tértől, kedvesem*." Az LHT előtti előadásában pedig kifejtette, hogy a magyar csapatokra bénítóan hatottak a szervezési nehézségek, a távoli hadszíntér idegen tájjellege, mely az elhagyatottság érzését keltette, de különösen a szovjet csapatok nagy haditapasztalata és jobb felszereltsége. „*Elszánt és álnok ellenség, akivel még a német csapatok is csak nehezen tudtak megküzdeni*." Bővebben lásd Kaló József: Szombathelyi Ferenc a Magyar Királyi Honvéd Vezérkar élén. Debreceni Egyetem, BTK, 2010. PhD disszertáció. https://dea.lib.unideb.hu/dea/bitstream/handle/2437/97153/ertekezes.pdf?sequence=5&isAllowed=y (letöltés ideje 2017. november 12.)

[19] Szombathelyi ezen elgondolása, és az első világháborús tapasztalatok lesznek az alapja az 1943 végén – 1944 elején megfogalmazott hadműveleti tervének, a Kárpát-védelemnek is.

orosz offenzíva kezdetén 1942 novemberében megszállva tartottunk. Ez a vonal sűrűn megszállható anélkül, hogy a hadosztályoknak 30 km-es kiterjedést adnánk.

A »belső vonalon folytatott hadművelet«[20] *is a térviszonyokkal való mértéktartásra kényszerít. A Volgánál és a Donnál a német hadsereg a »külső vonalon« állt, mert ez számára a hosszabb és rosszabb vonal volt. A belső hadműveleti vonal idén nagyobb fontosságot nyer, mert ebben az évben hadászati kisegítés szükségessé válhat. Egy erőeltolás Nyugatról Kelet vagy Délkelet felé, vagy éppen fordítva, hamarosan szükségessé válhat. A front a Volgánál és a Kaukázusban nem áll hadműveleti összefüggésben a nyugati fronttal, mert túl messze fekszenek. Egy konstruktív összeköttetést e két távoli terület között legfeljebb akkor lehetne biztosítani, ha egy 15-20 hadosztályos légi szállító flottát birtokolnánk. Természetesen ha az ember ezen a* [belső – K. J.] *vonalon áll, akkor jóval kevesebb gazdasági tér van mögötte, de annál intenzívebben tudja ezt a térséget megművelni és kiaknázni, mivel megfelelően felügyelni és biztosítani tudja.*

Az oroszoknak az 1943-as évben téli offenzívájukat nem kellene folytatni, hanem ravasz módon visszavonulni, mint azt az előző évben tették és a kezdeményezést a németeknek átengedni azért, hogy a téli játékot a következő évben még egyszer megismételhessék, ezért nem kell őket a fenti vonalon kívül üldözni, legalábbis az erők zömével nem. Még a Donyec-vonalat is csak mint előretolt állást kellene megszállni. A védelem súlya e mögött, a Dnyeper-vonalon fekszik. Semmilyen körülmények között nem tudjuk elérni és legyűrni az orosz főerőket. Nyersanyagforrásait sem tudjuk elérni, amennyiben katonailag nem válik tehetetlenné.

Mindenesetre a fentnevezett vonal tartása mindenképpen nagy hátrányokkal is jár. Az oroszok nyugodtan megerősíthetik és rendezhetik magukat. Ezzel szemben a német hadsereg is erősödhet és erőket gyűjthet, ami a 4. háborús évben szükséges is. Gondolni kell az 1944-es esztendőre is. Egyébként az oroszok erőgyűjtését még egy előretöréssel sem lehet megakadályozni. Viszont, ha az orosz a következő télen támad, akkor a Dnyeper-vonalban egy jól kiépített és megszállt vonalat talál és mögötte erős tartalékokat, melyeket a téli alkalmazásra felkészítettek és felszereltek, és így aktív védelmet gyakorolhatnának.

Egy harmonika-hadviselés, mely abban áll, hogy a németek nyáron és az oroszok télen ismét támadásba kezdenek, kerülendő. A német birodalomnak takarékoskodnia is kell, különösen a nemes germán vérrel és a kitűnő német katonákkal. A német katona az orosz hadszíntéren nemcsak a bolsevik katonák ellen harcol, hanem a földrajzi és éghajlati viszonyok ellen is, miáltal teljesítménye oly módon befolyásolható, hogy az orosz katonához – amelyet normális körülmények között messze felülmúlna – harcértékben egy az egy ellen áll. A német katonák nagy ütőképessége ezért ilyen módon nem használható ki takarékosan és hasznosan.

Ez lenne elgondolásom az Oroszország elleni hadműveleti tervet illetően az 1943-as évre. Kérem ne tekintse fenti megjegyzéseimet elbizakodottságnak, és mintha szándékomban állna az okos embert játszani. Csak azt akartam hasznosítani, amit az egykori cs. és kir. Hadiiskolában hallottam, ahol a keleti kérdéssel az akkori helyzet következtében többet foglalkoztunk, és ennek lényegét akartam Önnek továbbadni, mert hisz Ön ma ennek a vezérkarnak, tanításainak és tradícióinak is egyik továbbvivője. Főképpen, mint magam is volt cs. és kir. vezérkari tiszt fejtettem ki fenti nézeteimet.

---

[20] Szombathelyi itt a Clausewitz-i belső és külső vonal elméletére utal, mely szerint „*két hadsereg egymáshoz való viszonya két formát ölthet: 1. egymással szemben, párhuzamos arcvonallal állnak fel, vagy 2. a küzdő felek közül az egyik egy adott terület középpontjához képest belül, a másik kívül áll; ilyenkor azt mondjuk, hogy a középpontban levő fél áll a belső vonalon, míg a kerületen levő a külső vonalon*. […] *A belső vonalon lévő fél már eleve súlyt képez* […], *s e súllyal egyenként megverheti a kör kerületén levő ellenfél különálló részeit, és mindig megelőzheti – mivel a kör rádiuszán mozog – az ellenfél összpontosításra irányuló törekvéseit*.” Perjés: Clausewitz. Magvető Könyvkiadó, Budapest. 1983. 98-101.

Miközben legjobb kívánságaimat fejezem ki az eljövendő döntő hadműveletekhez, maradok mély bajtársi érzéssel

tisztelője: Sz [6]

Szombathelyi vezérezredest tehát a fenti levél megírásakor is a magyar erők megőrzésének célja vezérelte. Egyrészt a magyar 2. hadsereg tragédiája által kialakult helyzetet arra kívánta felhasználni, hogy megértesse a német hadvezetéssel: több harcoló erőt nem tudunk adni. Már a magyar 2. hadsereg maradványaiból is csak nagy nehézséggel, és csakis német segítséggel lehet harcoló erőt faragni. A magyar haderőnek tehát égetően nagy szüksége van a német felszerelésbeli segítségre. Másrészt az előző évihez hasonló nagy támadó hadművelet megtervezésétől óvja a német szárazföldi haderőnem vezérkari főnökét, ugyanis félő, hogy ez ismét a magyar erők fokozott részvételét vonná maga után. E feladatra a magyar haderő jelen helyzetében abszolút alkalmatlan, s ráadásul Szombathelyi vezérezredes meggyőződése szerint nem is magyar érdek egy fokozott részvétel a keleti hadszíntéren, hiszen nekünk a Kárpát-medencében vannak céljaink. Ezért meg kell győzni a németeket, hogy alapvetően védelmi hadászati elképzelést kövessenek: vonuljanak vissza egy jobban védhető terepszakaszra, amelyen sikerrel verhető vissza a támadó ellenség, s egyben garantálja, hogy a magyar erők megőrizhetik hadászati tartalék szerepüket a Duna-medencében. Zeitzler azonban nem tehette magáévá a magyar vezérkarfőnök tervét, mert Hitler az 1943 tavaszi helyzetet egészen másképp értékelte, mint ezt az áprilisi klessheimi tárgyalások során látni fogjuk. A haditerv sorsáról a háború után Szombathelyi ezt írta: „*A németeknek egy haditerv keretében ajánlottam, hogy az orosz hadszínteret ürítsék ki és legalább a Curzon vonalra*[21] *jöjjenek vissza, amiért Hitler nagyon megharagudott.*” [7]

1943 áprilisában sor került a klessheimi találkozóra, melynek megtartását német részről az indokolta, hogy az 1943 tavaszi, időleges hadműveleti sikereket felhasználva Hitler a csatlósállamok szövetségesi hűségének garantálására törekedett, mind gyakorlati, mind propagandisztikus szempontból. A meghívás tárgya „*megvitatni a katonai helyzetet és a magyar csapatok helyzetét*” volt. [8]

A Führer az 1943 tavaszára kialakult hadműveleti helyzetet úgy értékelte – s ezzel minden valószínűség szerint Szombathelyi vezérezredes Zeitzlernek megküldött hadászati elgondolására válaszolt –, hogy a szovjet veszteségek a háború addigi menetében tízszer akkorák voltak, mint a németeké, ezért „*őrültség volna a Szovjetunió elleni támadásokat szüneteltetni: ez csak a szovjetek föllélegzését szolgálná. Erre Németország semmi esetre sem hagy időt az oroszoknak, hanem addig veri őket tovább, amíg tökéletesen ellankadnak.* […] *Mármost azt mondhatnánk: esetleg át kellene térni keleten a defenzívára. Ez azonban csupán arra vezetne, hogy a már erősen kimerült bolsevisták újra összeszedhetnék magukat. Az a javaslat, hogy emeljenek egy »Keleti Falat«*[22]*, szintén merőben elméleti, mert télen minden keleti falat, még ha a legnagyobb tankcsapdákkal látnák is el, belep a hó és a jég, és ezzel megszűnne akadály lenni. Ebből következik a talán keserű, de elkerülhetetlen szükségszerűség: folytatni a harcot.*” [9]

[21] A Szombathelyi által javasolt Dnyeper vonal a Curzon vonaltól jóval keletebbre feküdt. Ez utóbbi nagyjából megfelelt Lengyelország 1945-ben meghúzott keleti határának.

[22] Mint fentebb már láthattuk, Szombathelyinek a Zeitzlerhez írt javaslatában ez a mondat szerepel: „*Nem szabad átlépni ezt a Dnyeper-vonalat, különben a végtelenbe veszünk. Ezzel szemben ebben a vonalban jól be lehet rendezkedni a védelemre és az állásokat fokozatosan fallá lehet kiépíteni*.”

ELEMZÉS A MAGYAR 2. HADSEREG SZEREPLÉSÉRŐL

Még zajlott a magyar 2. hadsereg hazaszállítása, mikor a vezérkar főnöke egy hosszú elemzést készített a hadsereg szerepléséről.[23] Az elkészült anyagot eljuttatta Jány vezérezredeshez is, aki írásban megjegyzésekkel reagált az elemzésre. Ezt követően, 1943. június 15-én Szombathelyi vezérezredes a berlini magyar katonai attasénak küldte meg írásbeli analízisét[24], melyet elolvasva Homlok Sándor[25] vezérőrnagy telefonon engedélyt kért, hogy az anyagot a berlini magyar követnek is bemutathassa. Sztójay Döme[26] Homlokon keresztül a szöveg bizonyos pontjainak átstilizálását, illetve enyhítését kérte a magyar vezérkarfőnöktől, mert „*az – nézete szerint akként, ahogyan jelenleg le van fektetve – a Führer hiúságát és érzékenységét erősen érintené, esetleg károsan befolyásolhatná.*" Homlok vezérőrnagy ugyancsak tompítani igyekezett bizonyos megjegyzéseket a szövegben, a különösen erősnek érzett részeket vörös irónnal jelölte meg, még a németeknek való bemutatás előtt, a Szombathelyinek vissza felterjesztett példányban. Összességében a berlini magyar katonai attasé úgy ítélte meg az anyagban foglaltakat, hogy azok „*teljes őszinteséggel tárják fel a való helyzetet, Keitel tábornagy, és kis részben Zeitzler gyalogsági tábornok VKF felelősségét is érintik, de nem teszik kritika tárgyává. Ez az Emlékirat erőssége. Másrészt, ismerve a Führer haragkitörését, kétlem hogy az, akár Keitel tábornagy, akár Zeitzler gyalogsági tábornok által a Német Birodalom Kancellárjának és Vezérének általuk bemutatásra kerülne*." [10]

Az eredetihez képest tehát feltehetően tompított elemzést Szombathelyi vezérezredes június 25-én küldte meg Keitel és Zeitzler tábornokoknak. A Keitelhez írt kísérőlevele igen szűkszavú, egymondatos tudósítás az anyag megküldéséről. A Zeitzlerhez írt levele hosszabb, annak lényege, hogy a magyar 2. hadsereg visszaszállítása alkalmából küldi meg elemzését, s abban a szilárd hitben van, „*hogy ez a sikertelen harc a Donnál katonai megerősödésünkhöz fog vezetni. Ehhez a hithez bátorságot merítek az 1806-os szerencsétlen jénai csatából.*[27] *Éppen ennek a végzetes csatának volt köszönhető a porosz hadsereg hatalmas felemelkedése vezető szerepre.*" [11]

Sajnos nem ismerjük részleteiben Szombathelyi vezérezredes elemzésének a német vezetésre gyakorolt hatását, mindössze egyetlen válaszlevél tájékoztat minket ez ügyben: Zeitzler gyalogsági tábornok július 8-án kelt válaszlevelében megköszönte a jelentést a magyar 2. hadsereg működéséről[28], és tájékoztatta a magyar vezérkarfőnököt, hogy azt a Führernek is átadta elolvasás végett. Azt ígérte, amint ideje engedi, válaszolni is fog az anyagban foglaltakra – ezt a válaszlevelet sajnos azonban már nem ismerjük. [12]

Szombathelyi vezérezredes fenti elemzését, még a német hadvezetésnek való megküldést megelőzően (június 2-án) Kállay Miklóshoz, mint a Legfelsőbb Honvédelmi Tanács elnökéhez is eljuttatta. A miniszterelnök július 20-án válaszolt a vezérkarfőnöknek, s

[23] Sajnos az iratot nem sikerült fellelnünk, de dr. Kardos János jóvoltából – aki részletes regisztert készített a perhez becsatolt iratokról – tudhatjuk, hogy Szombathelyi 1943. május 15-én zárta le az elemzését, s az legalább 55 oldal terjedelmű volt (hiszen Kardos feljegyzésében felsorolja az 53-55. oldalakat). HL Personalia dr. Kardos János ügyvéd hagyatéka. 251. doboz.

[24] Német nyelven, melynek címe „*Bericht über die Tätigkeit der 2. ungarischen Armee*", azaz „*Jelentés a 2. magyar hadsereg működéséről*" volt.

[25] Homlok Sándor altábornagy (1892-1963) 1940. május 1. és 1944. november 1. között berlini magyar katonai és légügyi attasé. 1942. április 1. és 1944. január 1. között vezérőrnagy.

[26] Sztójay Döme (1883-1946), 1936 és 1944 között Magyarország berlini nagykövete.

[27] A jénai, vagy más néven a jéna-auerstädti csatára 1806. október 14-én került sor a francia-itáliai és porosz-szász csapatok között, ahol Napóleon legyőzte ellenfeleit. Poroszország egy hat hétig tartó rövid hadjáratban döntő vereséget szenvedett, majd az ezt követő békekötés következtében területe a felére csökkent. A megalázó vereséget követően mélyreható reformokat vezettek be a kormányzat, a pénzügyek, az oktatás és a hadügyek területén, melyeknek köszönhetően Poroszország pár éven belül ismét a nagyhatalmak sorába emelkedett.

[28] Zeitzler válaszlevelében Szombathelyi levelét június 15-i keltezésűként tünteti fel, 25-e helyett. Amennyiben ez nem elírás a részéről, akkor ez azt jelenti, hogy a magyar vezérkarfőnök elemzése legelső, finomítatlan változatát küldte el a német szárazföldi haderőnem vezérkari főnökének.

levelében azt írta, „*a jelentés hű képe a megtörtént eseményeknek, a jelentéshez fűzött következtetések és megállapítások teljesen fedik az én nézetemet. Örömmel kell a jelentésből megállapítanom, hogy a 2. hadsereg zömének harca a nehéz viszonyok között semmiben sem maradt vissza szövetségeseink teljesítményei mögött*.” Kállay köszönetet mondott „*a jövőre nézve kifejezett álláspontunk világos és semmi kétséget nem hagyó vázolásáért és rögzítéséért*.” [13]

Szombathelyi vezérezredes elemzésének konkrét ismerete hiányában, a fentiek alapján csak következtethetünk annak tartalmára. Bizonyosan kritikával illette, s felelőssé tette a német hadvezetést a magyar 2. hadsereg sorsával kapcsolatosan. Különösen érdekesek azok a megjegyzések, amelyek óvtak az anyag Hitlernek való bemutatásától. A Führer véleménye ugyanis lesújtó volt a magyar 2. hadsereget illetően, s ezeket többek között Horthynak is kifejtette 1943. áprilisi klessheimi látogatása során. Hitler szerint a kudarc oka nem az volt, hogy elégtelen lett volna a magyar hadsereg fegyverzete és felszerelése. A katasztrófa leginkább annak volt köszönhető, hogy „*sem lelkileg, sem szellemileg nem tudtak helytállni a bolsevizmus elleni harcban. Ebből következett, hogy hanyatt-homlok menekültek, megfutottak az üldöző bolsevisták elől*”, ezért csekély harcértékű német alakulatokkal kellett feltartóztatni az ellenséges támadást, amely sikerült is. „*A szövetséges csapatoknál előfordultak kifejezetten lesújtó jelenetek, míg a német kötelékekben hasonló szellemi zűrzavarra sohasem került sor*. […] *Ezzel szembesítve Kállay kijelentése, hogy a honvédek ugyanúgy küzdöttek, egyenesen felháborító*.” Hitler véleménye szerint a német katonák Sztálingrádnál addig küzdöttek, „*míg fel nem fordultak az éhségtől*”, ellenben „*ilyen követelményeknek a szövetségesek nem tudtak megfelelni, nem mintha netán nem lettek volna kellően felszerelve – ez nem igaz –, hanem mert lelkileg nem voltak a feltételekhez képest erősek*.” A Führer szerint bár Jány vezérezredes igen nagy személyes bátorságról tett tanúbizonyságot, „*a magyar legénység viszont a beérkezett jelentések szerint igen rosszul tartotta magát. Tisztjeit, akik részben vitézül verekedtek, gyakran cserbenhagyta. Csúnya lehetett ez.* […] *A siralmas és undorító képről, amely ott a szemlélő elé tárult, elfogott orosz tisztek vallomásai tanúskodtak, amelyek szerint az oroszok Németország szövetségesei részéről nem ütköztek komoly ellenállásba* […]. *A szövetségeseknél nem szabad függelemsértést megtűrni, és főleg nem szabad magasztalni egy hadsereget, amely nem teljesítette a kötelességét*.” [14]

Szombathelyi vezérezredes bizonyára a fenti hitleri okfejtés hatására is kezdhetett hozzá elemzése megírásához, s fejezte be annak első változatát május közepén. A konkrét tartalom ismerete nélkül csak következtetésekre hagyatkozhatunk, amelyben segítenek minket azok az írásai, melyeket a magyar 2. hadsereg szerepléséről más helyen és időben alkotott. A Hitler által mondottakkal egyértelműen szembe menő megállapításai a következők: a magyar 2. hadsereg nem volt kellően felszerelve, páncélelhárítása elégtelen volt. „*A németek által beígért páncélvadász egységek sajnos későn érkeztek be. A magyar hadsereg védelmi szakasza az élő erőkhöz, a rendelkezésre álló fegyverzethez és felszereléshez képest túl széles volt, ezért a védelemnek nem volt elég mélysége, pedig számottevő erő támadását csakis készenlétbe helyezett erős, mozgékony tartalékok bedobásával lehetett volna visszautasítani. Hiányzott a magyar hadseregben az ellentámadást támogató rohamtüzérség, továbbá részben a nagy hatású és mozgékony légvédelmi tüzérség is.* […] *A 2. magyar hadseregnek most ismertetett harcaiból megállapíthatjuk, hogy a hadsereg csapatai – kivételektől eltekintve – derekasan, becsületesen és hősiesen megállták a helyüket, vagyis megtették kötelességüket. Ezt legjobban a már megállapított véres veszteségek nagysága igazolja*. […] *Nincs okunk a szégyenkezésre azért sem, mert az oroszok által harcba vetett erők (főleg páncélosok) sikert értek el az összes többi szövetségessel, de a német erőkkel szemben is*.” [15]

„*Hogy a csata mégis elveszett, annak oka az alábbiakban keresendő: A merev, helyhez kötött védelem, amely ellen mi mindig állást foglaltunk, addig, míg Hitler maga nem szólt közbe. A német vezetés teljes csődje különösen a tartalék alkalmazásában. Hogy a csata*

katasztrófává mélyült el, annak oka, hogy a németek visszavonuló csapatainkat a járt utakról leszorították, meleg ruháiktól és takaróitól megfosztották. Sebesülteket a kocsikról lelökték és maguk mentek azokon tovább. Községekbe őket be nem engedték, hanem a szörnyű hidegben azokon kívül kellett a magyar csapatoknak éjjelezni. Végül a hirtelen beköszöntött szörnyű hideg és a magyar hadsereg parancsnokság azon szerencsétlen intézkedése, hogy a felváltó csapatokat, amelyeknek fegyverük nem volt, mert ezt a felváltandóktól kellett átvenni, éppen az orosz támadás előestéjén rendelte az állásokba." [16]

„*Ilyen súlyos vereségre nem voltam előkészülve és ennek az okait az alábbiakban látom. Először is a német gyatra vezetésben: már régóta egy erős felfogásbeli ellentét állott fenn közöttünk és a németek között a védelem végrehajtására vonatkozólag. A németek a merev védelem mellett törtek lándzsát és ezt követelték, mi pedig a rugékony védelem mellett foglaltunk állást. Ezt a vitát azután maga Hitler zárta le egy levéllel, amelyet 1942 karácsonyán intézett a kormányzóhoz, amelyben ez felkérte arra, hogy rendelje el a magyar hadsereg számára a merev-védelmet, mert különböző harcmetódusok egy hadszíntéren csak romlást okozhatnak. Tovább igen nagy hibát követtek el a németek a tartalék alkalmazásával*. […] *Evvel a tartalékkal sem a magyar hadsereg parancsnok, de még a német harcvonal-parancsnok sem rendelkezhetett. Ezek alkalmazását a német legfelsőbb hadvezetőség kizárólag magának tartotta fenn. Ezek a tartalékok a támadás első napjaiban tétlenül álltak, tétlenül nézték frontunk felszakadását és azután pedig összekuszált menetekben szét lettek forgácsolva és apránként bevetve, úgy, hogy eredményt sehol sem érhettek el. A tartalék alkalmazásánál és a harc vezetésénél a német vezetésnek olyan csődje tárult elénk, amilyet én soha nem tudtam volna elképzelni.* […] *Teljes csődöt mondott a német vezetés abból a szempontból is, hogy a magyar arcvonal erős megerősítésére kilátásba vett és beígért különleges fegyvereket, nevezetesen páncélos rohamtüzérséget, páncélelhárító kötelékeket, amelyeknek közreműködése bennünket a legmagasabb reményekre jogosított fel, nem tudta kellő időben a hadszíntérre hozni, úgyhogy ezek az ütközetekbe csak apránként lettek bevetve. Rendkívül súlyossá, szinte katasztrofálissá tette a vereséget az időjárásnak hirtelen megváltozása. A támadás napján és a következő napokon az addig nem sokkal a mínusz alatt lévő hőmérséklet mínusz 30 és 35 fokra süllyedt le. A téli ruhák és óvócikkek Magyarországról ugyan jókor el lettek szállítva, és a harctérre meg is érkeztek, de a csapatokhoz való kiszállítás rendkívüli nehézségekbe ütközött. Itt ezen a hadszíntéren az óriási kiterjedések mellett minden, még a harcászati kérdések is szállítási kérdéssé sűrűsödtek össze. Szállítóeszközök tekintetében a németekre voltunk utalva, és vállalt kötelezettségüket nem teljesítették, nem kutatom azt, hogy nem tudták, vagy nem akarták. Így a csapatoknak egy része téli óvószerekkel és ruházati cikkekkel nem volt ellátva, amely persze szörnyű következményekkel járt. Elmélyítette még a vereség súlyosságát a németek kíméletlensége: a magyar csapatokat a jó utakról leszorították, úttalan terepre utalták. A szállásokban nem adtak nekik helyet, vagy egyáltalán nem bocsájtották be őket a községekbe. Járműveiket, lovaikat, meleg takaróikat elvették. A kocsikról a sebesülteket ledobták. Szörnyű embertelenségeket követtek el, amelyek következményei tragikusak voltak* […]. *A magyar hadseregnek a szenvedése óriási volt, de ne gondoljuk azt, hogy csak szenvedésből és pusztulásból állott, mert megnyilvánult a magyar katona ősi dicsősége és hősiessége, mely ezen szenvedéseken és pusztulásokon úrrá lett. A doni vereségért nincs mit szégyenkeznünk, emelt fővel és büszkeséggel vállalhatja mindenki a harcokban általa vitt szerepet. Magyar csapatok hagyták el utolsónak a Dont, Oszlányi*[29] *tábornok vezetése alatt. A magyar csapatok*

[29] Oszlányi Kornél (1893-1960) vezérőrnagy. 1942. november 15-től a magyar 2. hadsereg alárendeltségében működő 9. könnyű hadosztály parancsnoka (1943. augusztus 10-ig). 1943. január 28-án véghezvitt fegyvertényéért, Verhnye Turovo község védelménél tanúsított bátorságáért a második világháborúban egyedüliként megkapta a Mária Terézia-rend lovagkeresztjét. Az általa vezetett seregtest vált le utolsóként a

képezték az utóvédeket a visszavonuló német csapatok mögött, hősiesen küzdve Szügyi[30] *és Varjassi*[31] [sic!] *tábornokok alatt. Osztrogorszknál* [sic!] *kecskeméti magyar bakák kiváló lendülettel végrehajtott támadásban kivágták magukat az orosz gyűrűből és a németeknek is megnyitották az utat.*[32] *Magyar csapatoknak a harcai következménye lett az, hogy az oroszok utánlendülését feltartóztatták és időt nyertek a zömök elvonulására*. […] *Nagy elégtétellel és felfogásom igazolásául említem meg azt a körülményt, hogy mindezeket a sikereket a magyar csapatok a mozgóvédelemben érték el, amelyben ügyességük és leleményességük, valamint vitézségük teljes mértékben kibontakozhatott, és ott, ahol csak némi páncélos, vagy tüzérségi támogatásban részesültek, vitézségük szinte virtuskodásba csapott át*." [17]

Ha a fenti megállapítások bármelyike szerepelt a Szombathelyi vezérezredes által szerkesztett elemzésben, akkor az anyag bizonyosan alkalmas lehetett arra, hogy Hitler dührohamát kiváltsa. Ezen kívül még egy fontos kérdést vet fel a fenti irattal kapcsolatban Kállaynak azon kijelentése, miszerint köszönetét fejezte ki a vezérkarfőnöknek „*a jövőre nézve kifejezett álláspontunk világos és semmi kétséget nem hagyó vázolásáért és rögzítéséért*". Ez a mondat arra utal, hogy Szombathelyi vezérezredes a katasztrófa nagyságára és a magyar felszerelési helyzetre hivatkozva nyomatékosan leszögezhette ebben az anyagban is, hogy Magyarország több harcoló erőt nem tud a németek rendelkezésére bocsájtani, valamint ismételten hangsúlyozhatta a magyar hadászati tartalék szerepet a Duna-medencében.

KÖVETKEZTETÉSEK

A tanulmány két, eddig nem publikált dokumentumot és azok keletkezési körülményeit mutatja be. Az egyik teljes terjedelmében rendelkezésünkre áll német nyelven, a másik egyelőre fel nem lelhető, de a rá való hivatkozások alapján lényegileg rekonstruálható. Mindkét dokumentum keletkezési körülményei és létrejöttének céljai a rendelkezésre álló primer és szekunder források alapán felvázolhatók, s beilleszthetők a Szombathelyi Ferenc vezérezredes vezérkarfőnöki működésének elemzésébe, tágabb értelemben a második világháborús magyar hadtörténelem fontos, eddig homályban maradt részleteinek megvilágításába. A két dokumentum tovább erősíti, hogy Szombathelyi Ferenc vezérezredes az erők megőrzésnek katonapolitikáját vallotta az 1943-as esztendőben is, ahogyan tette ezt kinevezése óta, s a doni katasztrófa bekövetkezte csak még inkább megerősítette benne azt az elhatározást, hogy a német-magyar egymásrautaltság ellenére a magyar sorsot el kell választani a némettől. A történelem egy évvel később, a német megszállás pillanatában

---

Donról, január 27-én fedezve az akkor már visszavonuló német csapatokat is. 1993-ban posztumusz altábornaggyá léptették elő. Szabó Péter: Don-kanyar. Corvina, Budapest. 2001. 242.o.; 261-263. o.; 343. o.

[30] Szügyi Zoltán (1896-1967) vezérőrnagy. 1942. október 14. és 1943. február 18. között a magyar 2. hadsereg alárendeltségében működő 43. gyalogezred parancsnoka. A hadsereg visszavonulása soron egy zászlóalj erejű harccsoport parancsnoka, a szovjet áttörés lassítása és részbeni feltartóztatása miatt kitüntetették. Szabó Péter: Don-kanyar. Corvina, Budapest. 2001. 255. o., 348. o.

[31] Helyesen Vargyassi Gyula (1891-1958) altábornagy. 1942. november 15. és 1943. június 15. között a magyar 2. hadsereg alárendeltségében működő 23. könnyű hadosztály parancsnoka. A doni áttörés után, január 24-étől a (kb. 7 zászlóalj erejű) Vargyassi-csoport parancsnoka. Február 8-ig tartó védelmi és halogató harcával biztosította a megmaradt német és magyar erők visszavonulását.

[32] Helyesen Osztrogozsszk városában a német 168. gyaloghadosztály és a kecskeméti 13. könnyű hadosztály körül január 17-én zárult be a szovjet 40. hadsereg és 18. önálló lövészhadtest által képzett gyűrű. A védők kezdetben még reménykedtek a Cramer-hadtest felmentő műveletében, azonban a tartalék seregtest nem teljesítette feladatát. Ezért január 19-én este a német és magyar védők kitörésre határozták el magukat. Ennek végrehajtása során több ízben érte őket harckocsi-, repülő- és partizántámadás. A szovjet csapatok újbóli bekerítéséből Novij Olsannál a kecskeméti 13. könnyű hadosztály részei vágták ki magukat egy nádason keresztül. Szabó Péter: Don-kanyar. Corvina, Budapest. 2001. 239-249 o.

azonban egycsapásra sodorta el ezt a katonapolitikát, annak addig megnyilvánuló eredményeit, és magát Szombathelyi vezérezredest, vezérkarfőnököt is.

FELHASZNÁLT IRODALOM

[1] HADTÖRTÉNELMI LEVÉLTÁR Personalia *dr. Kardos János ügyvéd hagyatéka*. 251. doboz. *Feljegyzés Szombathelyi vezérezredesnek a magyar miniszterelnök számára 1943. január 17-én adott szóbeli tájékoztatásról*. 5-6. o.

[2] HADTÖRTÉNELMI LEVÉLTÁR Personalia *dr. Kardos János ügyvéd hagyatéka*. 251. doboz. *Feljegyzés Szombathelyi vezérezredesnek a magyar miniszterelnök számára 1943. január 17-én adott szóbeli tájékoztatásról*. 5-7. o.

[3] HADTÖRTÉNELMI LEVÉLTÁR Personalia *dr. Kardos János ügyvéd hagyatéka*. 251. doboz. *Feljegyzés Szombathelyi vezérezredesnek a magyar miniszterelnök számára 1943. január 17-én adott szóbeli tájékoztatásról*. 7-8. o.

[4] SZŰCS L.: *Horthy Miklós titkos iratai*. Kossuth Könyvkiadó, Budapest. 1972. 345-355. o.

[5] HADTÖRTÉNELMI LEVÉLTÁR Tanulmánygyűjtemény 2833 Lieszkovszky Pál huszár alezredes visszaemlékezése

[6] HADTÖRTÉNELMI LEVÉLTÁR Personalia dr. Kardos János ügyvéd hagyatéka. 251. doboz

[7] ÁLLAMBIZTONSÁGI SZOLGÁLATOK TÖRTÉNETI LEVÉLTÁRA V-101594/1. Szombathelyinek a vádirathoz írt észrevételei 33. o.

[8] RÁNKI GY.: *Hitler hatvannyolc tárgyalása*. Magvető Kiadó, Budapest. 1983. 2. k. 41. o., 67-113. o.; MAGYAR NEMZETI LEVÉLTÁR K 27 1943. április 20-i minisztertanácsi jegyzőkönyv

[9] RÁNKI GY.: Hitler hatvannyolc tárgyalása. Magvető Kiadó, Budapest. 1983. 2. k. 41., 69-70. o.

[10] HADTÖRTÉNELMI LEVÉLTÁR Personalia dr. Kardos János ügyvéd hagyatéka. 251. doboz. Homlok vezérőrnagy 1943. június 17-i levele Szombathelyi vezérezredeshez

[11] HADTÖRTÉNELMI LEVÉLTÁR Personalia dr. Kardos János ügyvéd hagyatéka. 251. doboz

[12] HADTÖRTÉNELMI LEVÉLTÁR Personalia dr. Kardos János ügyvéd hagyatéka. 251. doboz

[13] HADTÖRTÉNELMI LEVÉLTÁR Personalia dr. Kardos János ügyvéd hagyatéka. 251. doboz

[14] RÁNKI GY.: Hitler hatvannyolc tárgyalása. Magvető Kiadó, Budapest. 1983. 2. k. 71-73. o.

[15] HADTÖRTÉNELMI LEVÉLTÁR VKF 1943 1. oszt. 24/sz. n. A vezérkar főnökének 1943. február 16-i beszámolója a Legfelsőbb Honvédelmi Tanács előtt

[16] Szombathelyi Ferenc 1946. január 7-i önéletrajza. Közli KALÓ J.: *Szombathelyi Ferenc vezérezredes önéletrajza és védőbeszédének vázlata* 1946-ból. Hadtörténelmi Közlemények 124. évf. (2011. június) 2. szám 604.

[17] BUDAPEST FŐVÁROS LEVÉLTÁRA 293/1946 X. Szálasi Ferenc népbírósági pere 7. doboz Szombathelyi Ferenc feljegyzései 7129-7131.

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

INDUSTRIAL ROBOTS MEET INDUSTRY 4.0

IPARI ROBOTOK AZ IPAR 4.0 ÍGÉNYEIHEZ

MIES Gereald; ZENTAY Peter

(ORCID: 0000-0002-6332-995X); (ORCID: 0000-0002-3161-8829)

gerald.mies@icloud.com; zentay@manuf.bme.hu

Abstract

The industrial robot market has been changing significantly over the past few years. Today, the development towards Industry 4.0 and digital future factories is confronting a raising amount of industrial companies with new challenges. Industry 4.0 allows the individualization of products referred to as mass customization. In the future smart factories will be able to produce small batch sizes economically. Automation solutions, especially new kinds of robotic technologies will play a vital role in this fourth industrial revolution in terms of efficiency and productivity. Nevertheless, a comprehensive analysis of how robot technology contributes to Industry 4.0 is still lacking. In this paper a practical view on the ongoing changes will be presented and the potential of smart collaborative robots which are fully integrated in the digital infrastructure of future factories is presented.

Keywords: *automation, robots, industrial revolution, Industry 4.0, collaborative robots, smart factory,*

Absztrakt

Az ipari robotpiac jelentősen változott az elmúlt években. Napjainkban az Ipar 4.0 és az intelligens gyárak felé irányuló fejlődés egyre nagyobb kihívásokkal szembesíti az ipari vállalatokat. Az Ipar 4.0 lehetővé teszi a termékek testre szabását, amelyeket tömegméretezésnek neveznek. A jövőben, az intelligens gyárakban a legkisebb tételeket lehet majd gazdaságosan gyártani. Az automatizálási megoldások, különösen az új típusú robottechnikák fontos szerepet játszanak a hatékonyság és a termelékenység növelésében. Ennek ellenére továbbra is hiányzik egy olyan átfogó elemzés mely tárgyalja, a robottechnika hozzájárulását az Ipar 4.0 koncepciójához. A cikkben gyakorlati szempontból kívánjuk megfogalmazni a folyamatban lévő változásokat és megmutatni az intelligens együttműködő robotok azon lehetőségeit, amelyekkel integrálhatók a jövőbeli gyárak digitális infrastruktúrájába.

Kulcsszavak: *Ipar 4.0, együttműködő robotok, intelligens digitális gyár, negyedik ipari forradalom*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.09.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.29.

INTRODUCTION

Today's business environment is shaped by the ongoing globalization and the increasing use of internet-based digital technologies in production. In history of industry, three revolutions have turned the branch on its head and did fundamentally change the business environment. Considering recent developments, it is becoming extremely difficult to ignore the dawn of another paradigm shift. In the new global economy, the digitization has become a central issue for industrial manufacturers.

Initiatives of the leading industrial countries promote a new era of manufacturing. For example, the German 'Industrie 4.0' or the American 'Industrial Internet' refer to the use of smart intelligent machines and other digital assets linked in a company-wide software-based infrastructure [7, 21]. A much-debated question is whether this development is a revolution or simple evolution of existing technologies as automation, robots and the use of IT initially came up during the 1960's [10, 18]. However, the ongoing convergence of operational technology and information technology promises enormous gains in efficiency and productivity [26]. As the industrial sector is regarded to as a key driver of the economy, leading industrial country's need to drive this change and adapt to the digital environment. Based on a short historical summary of past industrial revolutions this article provides an overview about the ongoing changes on international shop floors in terms of Industry 4.0. Given the fact that a systematic and detailed understanding of how automation and robots contribute to Industry 4.0 is still lacking, the focus will then be placed on robotic technology in Industry 4.0.

FROM STEAM ENGINE TO DIGITIZATION

In history, mechanization, electricity and most recently electronics, information and automation technology have triggered three game changing revolutions. The first industrial revolution at the end of the 18th century followed the introduction of water- and steam-powered mechanical manufacturing facilities. Later, in the 19th century the second industrial revolution was caused by the electrically-powered mass production using assembly lines and the division of labour. The third industrial revolution began in the 1970's with the implementation of complex electronics and information technology (IT) on the shop floor to achieve increased automation in industrial processes [1]. They all have in common is that they had a major impact on the industrial value creation. The figure of the German Research Centre for Artificial Intelligence (AI), shows the development towards the fourth industrial revolution and the chronological sequence, as seen on Figure 1.

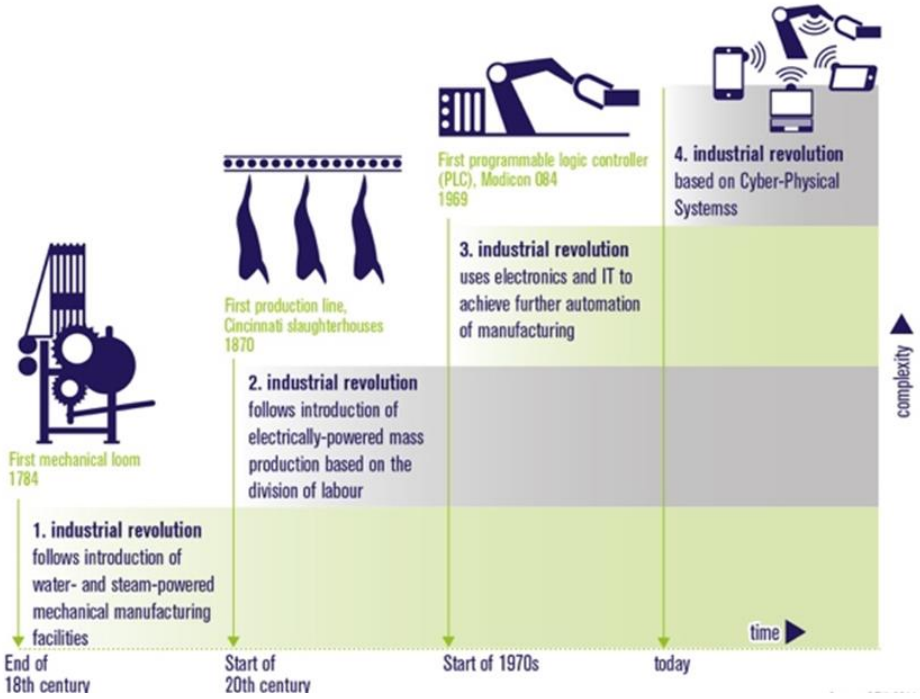


Figure 1: History of Industrial Revolutions [1]

In the course of digitization, the fourth industrial revolution now aims to connect the digital and virtual world of computer technology with the world of industrial production. This development is driven by and based on the Internet of Things (IoT). In the industrial application, the IoT enables the internet based interaction and collaboration within global networks and transcends the present borders and limits of companies. Generally speaking the IoT describes the connection of people, objects and machines to the internet [25]. Those smart, connected devices are on the rise. A glance at current statistics shows that the adoption of connected devices has been increasing over the past few years (see: Figure 2.). In 2015 the total number of connected units was about 5 billion. If this trend continues, this number is estimated to increase by 2020 to more than 20 billion connected devices [22].

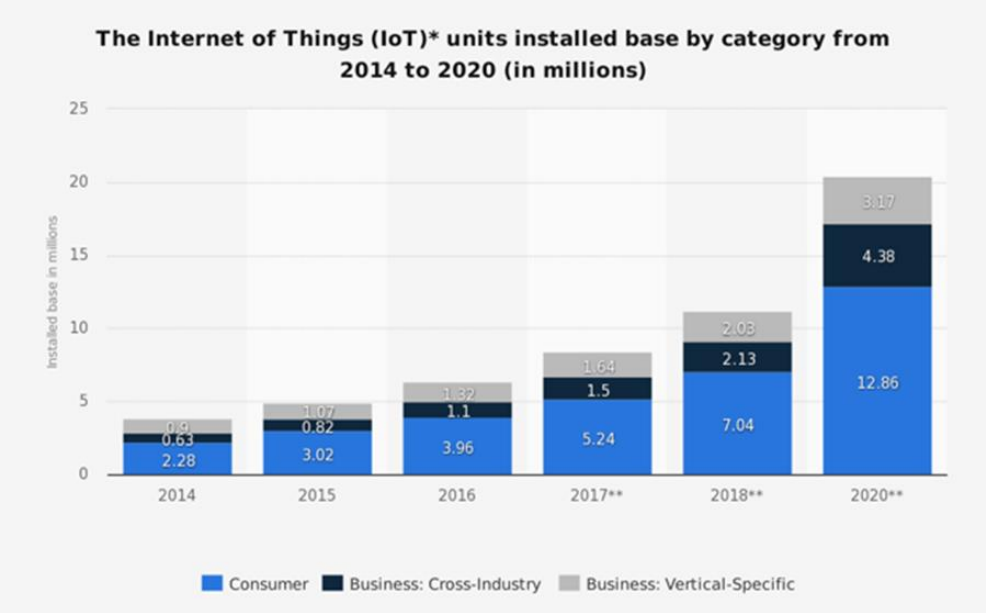


Figure 2: IoT units installed 2014 - 2020 [22]

According to Matharu et al. [15] the "*Internet of Things (IoT) can certainly be defined as the biggest revolution in the making of the IT industry. The IoT will impact our living style, the way we consume energy and all our day-to-day activities* [15]." These impacts are now so widespread that they also affect industrial value creation. The new opportunities cause significant changes in the market as the converging information and operational technology allows completely new solutions including product, service and process innovations.

INDUSTRY 4.0

Industry 4.0 refers to the industrial application of IoT technologies and is an initiative led by the German government to accelerate the industrial digitization. Taking a closer look at the industrial sector, the global competition has intensified and Germany is not the only country to have recognized the trend to deploy the Internet of Things and Services in manufacturing [1]. The 'Made in China 2025' or 'Industrial Internet of Things' programs in the Chinese and American manufacturing industry are for example two nearly similar approaches of other leading industrial nations.

The vision of Industry 4.0 and comparable concepts is to construct an open, smart manufacturing platform for industrial networked applications [1, 3]. In Germany, the development towards Industry 4.0 already has a noticeable influence on traditional business models and manufacturers cannot afford to close their eyes to reality and ignore the ongoing industrial transformation [6, 24]. The constantly changing market and customer requirements are confronting manufacturers with new challenges and affect almost every strategic decision. With the realization of the vision 'Industry 4.0' major changes will occur not only for factories but also for individuals.

The Impact of Industry 4.0

Cutting-edge manufacturing solutions are the upcoming trend in industrial value creation. In the field of technologies those which allow higher efficiency, productivity and transparency have become the focus of attention

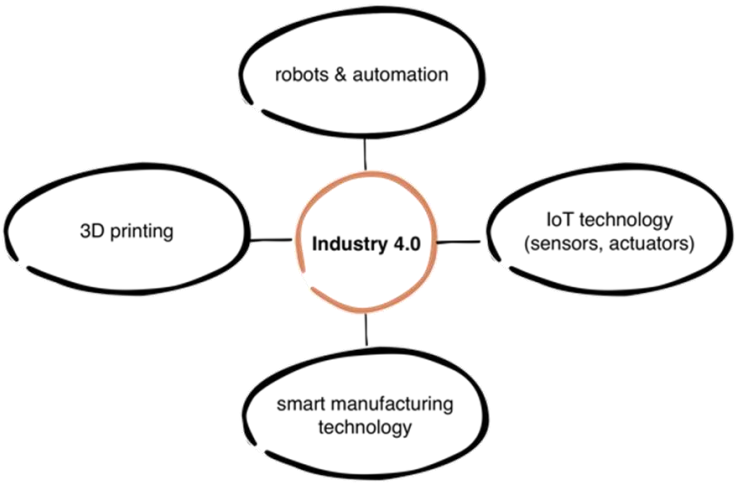


Figure 3: Industry 4.0-related Technologies (made by author)

As the figure shows, the solutions include devices such as sensors and actuators, robots, 3D-printers and manufacturing devices (such as milling-, turning-, grinding- machines etc.,) and assembly line components [5, 26]. Unlike the factories today, Industry 4.0-factories employ a completely new approach to production and transform into complex and digitized production facilities with highly automated value chains [1, 3, 20]. All assets are equipped with sensors and actuators and share data with higher level systems [4]. This convergence of

the operational technology and modern information technology results in so called cyber-physical systems (CPS), which are referred to as the driving force behind the fourth industrial revolution [6, 26].

In Industry 4.0 factories become smart and enable the fast response to market changes through flexible and demand-driven production of goods. In those smart factories the work pieces, tools, machines and robots are capable of autonomously exchanging information, triggering actions and controlling each other independently, which holds a huge potential for several improvements [1, 4]. The CPS are constantly connected, which is why the data gathered by various sensors can be used to cut costs and optimize processes [11]. A new generation of 'smart' products shares information about the status, history and the target state which enables them to manage their own production process [1, 6]. Another interesting part are new forms of human machine interaction. Workers could be supported with the information they need 'on demand' and would be able to make the right decision in every possible situation. The smart technologies will help manufacturers to increase their competitiveness through further efficiency gains and flexible fabrication of high quality products [1, 6]. Using advanced technology, companies can benefit from entirely new supply chain structures with higher equipment efficiency and flexible processes which offers strategic advantages such as the better handling of complex goods, shorter time to market and manufacturing on demand [8]. In future smart factories, batch sizes starting from one can be manufactured economically which allows individual customer needs to be met, additionally the dynamic business and engineering processes enable last-minute changes to production [1]. This will aide the process of mass-customisation.

Horizontal and Vertical Integration

Industry 4.0 is a topic with a strong interdisciplinary character. This paradigm shift in the traditional manufacturing industry requires a holistic and sustainable digital reorientation of the entire corporation, especially in the field of factory organization.

To realize the vision of smart factories, the holistic integration of all machines into a company-wide digital infrastructure is necessary. In smart factories manufacturing processes, but also the engineering and business processes from the 'office floor' need to be integrated in the digital infrastructure [25]. In order to meet the vision of an open, smart manufacturing platform the manufacturing systems need to be vertically networked and horizontally connected [1].

Vertical integration in this context refers to the connection of business and manufacturing processes including resources such as material across all levels of the organization [2]. Process data is collected and analysed in real-time, to react and adapt to environmental changes such as unexpected production stops or failures in the supply of material. The production lines are constantly connected and always optimally adjusted to the specific situation. The smart factory is driven and controlled by real-time data and therefore guarantees that all necessary decisions can be taken as efficiently and rapidly as possible.

The horizontal integration moreover describes the connection of machines and production systems across company borders [2]. All stages of the supply chain share data and communicate in a digital production network.

COLLABORATIVE ROBOT TECHNOLOGY

The development towards smart factories goes hand in hand with higher degrees of automation. Surveys such as conducted by the VDE (*Verband der Elektrotechnik, Elektronik und Informationstechnik*) [22] have shown, that in the future automation is seen to be the most important key technology for the companies interviewed. High rates of automation are often

associated with the replacement of human labour by machines. Industry 4.0 in contrast, rather aims at the support of human workers using new technologies. Therefore, automation and in this regard state of the art robot technology represent crucial elements of Industry 4.0.

Previous research indicates, that robots are still the key instruments in production strategies of flexible automation [16]. The Boston Consulting Group (BCG) estimates the global spending on industrial robotics to grow rapidly in the years to come. The statistic shows a spending of 16.7 billion U.S. dollars in 2020 and a total of 24 billion U.S. dollars in the year 2025 (see: Figure 4).

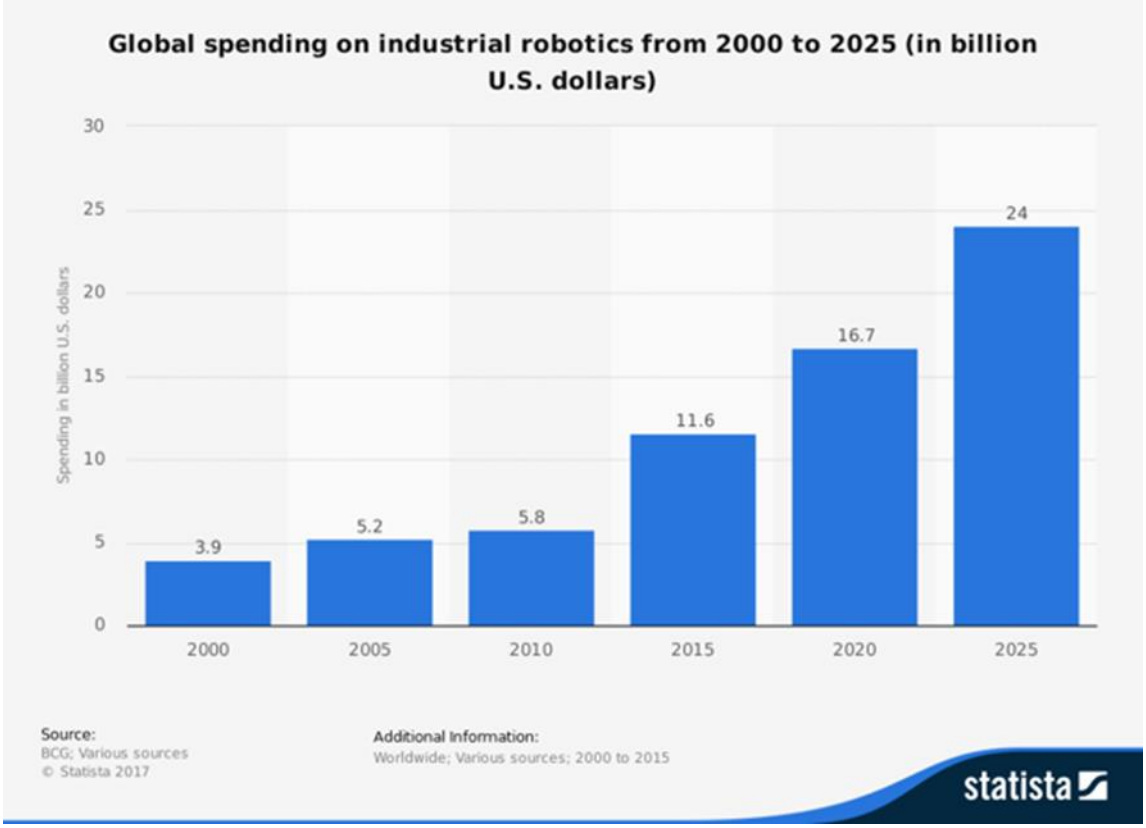


Figure 4: Global Spendings Industrial Robotics, according to [23]

Nonetheless, trying to reach ever higher levels of automation the interaction between human and machines becomes a central issue [3]. If robots are also cooperating with other activities that are distanced far away in space then time delay problems occur. Today many researches are made to handle the problem of time delay in control [27]. Today, many of the production processes cannot be easily automated – collaborative robots are able to fill these gaps [13]. In many cases such as assembly systems, parts of the process can only be automated very difficultly or the automation is not economical. These can be complex tasks that are changing rapidly, tasks that need two hands and a delicate hand-eye coordination, etc. These parts of the assembly line should be conducted by human workers. However many parts of almost any production can be easily and cheaply automated. In order to satisfy both demands, hybrid lines should be deployed. In these production line, however, conventional robots cannot be used. To satisfy this place in the market new robots were introduced that can work besides human workers. Especially the flexible mass production of individual products places new demands on the automation technology.

Recently there has been an increasing interest in those so called cobots. Traditionally a robot is defined by the IFR as „an automatically controlled, reprogrammable multipurpose manipulator programmable in three or more axes which may be either fixed in place or mobile

for use in industrial applications“[11]. In the age of Industry 4.0 computers and robotics come together in a completely new manner.

Collaborative robots enable new forms of human machine interaction. A cobot can be simply defined as „a computer controlled robot device designed to assist a person“[18]. These new collaborative robots are more flexible and are capable of learning and interact with machines and human. In contrast to traditional robots the cobots can learn new tasks through training by demonstration instead of cost-intensive programming [12].

In the field of factory automation adaptive robots create new efficiencies and change how companies produce goods and organize the shop floor [16]. For example the process costs can be reduced as the collaboration increases the productivity and efficiency and the robot requires less space as it is not isolated from the operator [8]. Unlike traditional robots, cobots need no fences around because sensors and visual systems guarantee that the robot stops before colliding with the operator [12]. This enables robots to perform tasks as humans do and allows human workers to work closely with robots [12]. Human workers can focus on complex tasks where „intelligence and dexterity “is required, in the opposite case the robots complete the tasks, which are exhausting or dangerous for the human [8].

Compared to traditional robots, collaborative robots show several benefits. They are smaller, smarter and safer. In addition, they are cheaper than stationary robots and can also be used as mobile units [13]. This flexibility enables manufacturers to use the cobot on multiple lines and easily reprogram it if necessary [12]. There are also the other side of the coin. These collaborative robots have different drawback as well. If they are compared to a conventional robots with the same capabilities we find the following: there prices are much higher because the sensorial background (sometimes even camera integration is also applied) and also the developed software background that ensures the required safety for human-robot collaboration. Their productivity is usually lags far behind conventional robots. Robots working behind a safety area (fence) can apply their full capabilities in speed acceleration and payload. Collaborative robots cannot utilise these, to ensure that the robots stops if it collides with a human. This way they work with a much slower speed that are even reduced further if a human approaches the robots. The robot has to stop if the worker enters its working envelope. This reduces the productivity of the robot considerably. The payload has to be reduced in order to have the robot safe for human collision. The so called light weight robots are design the way, that even if it hits a human they would rather brake than harm the worker. Taken these facts into consideration a human-robot production line is can be a well-functioning solution for new tasks.

CONCLUSION

Industry 4.0 has a major impact on the manufacturing industry. The paper reviews the ongoing changes and shows the potential of smart factories in the production sector. Industry 4.0 enables increased individualization of products, shorter time to market and boosts in terms of productivity, flexibility and quality.

Manufactures, not only in Germany must critically rethink their business models and strategies, keeping in mind the new technologies from the different fields. Looking at Industry 4.0 in practical context the holistic integration can be taken as the central requirement to benefit from the opportunities. The complex implementation will be one of the key tasks in the years to come.

In this new industrial world, robots will play an important role and smart and collaborative robots are on the rise and stepwise will find their way on the shop floor of manufacturing companies.

REFERENCES

[1] Acatech 2013. Recommendations for implementing the strategic initiative INDUSTRIE 4.0 http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf, (Accessed: 02.01.2017)

[2] Agiplan et al. 2015. Erschließen der Potenziale der Anwendung von ‚Industrie 4.0'http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Studien/erschliessen-der-potenziale-der-anwendung-von-industrie-4-0-im-mittelstand,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, (Accessed: 12.02.2017)

[3] BAHRIN, M.A.K. ET AL. *2016. Industry 4.0: A review on industrial automation and robotic*. ResearchGate. 78, 6–13 (2016). DOI:https://doi.org/10.11113/jt.v78.9285.

[4] BAUERNHANSL, T. ET AL. *2016. WGP-Standpunkt Industrie 4.0.* http://www.ipa.fraunhofer.de/fileadmin/user_upload/Presse_und_Medien/Pressinformationen/2016/Juni/WGP_Standpunkt_Industrie_4_0.pdf (Accessed: 14.03.2017)

[3] BAUR, C. AND WEE, D. 2015. *Manufacturing's next act.* http://www.mckinsey.com/business-functions/operations/our-insights/manufacturings-next-act (Accessed: 19.01.2017)

[6] BITKOM AND FRAUNHOFER IAO 2014. *Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland*. https://www.bitkom.org/Publikationen/2014/Studien/Studie-Industrie-4-0-Volkswirtschaftliches-Potenzial-fuer-Deutschland/Studie-Industrie-40.pdf (Accessed: 13.04.2017)

[7] BUNDESMINISTERIUM FÜR WIRTSCHAFT UND ENERGIE 2015. *Industrie 4.0 und Digitale* Wirtschaft. http://www.bmwi.de/BMWi/Redaktion/PDF/I/industrie-4-0-und-digitale-wirtschaft,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (Accessed: 16.02.2017)

[8] BURMEISTER, C. ET AL. 2015. *Business Model Innovation for Industrie 4.0: Why the "Industrial Internet" Mandates a New Perspective on Innovation*. RWTH-TIM Working Paper, Feb. (2015). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2571033 (Accessed: 08.06.2016)

[9] CORRALES, J.A. ET AL. 2012. *Cooperative Tasks between Humans and Robots in Industrial Environments*. International Journal of Advanced Robotic Systems. (2012), (1-10). DOI:https://doi.org/10.5772/50988.

[10] DR. WIESELHUBER & PARTNER GMBH AND FRAUNHOFER IPA 2015. *Geschäftsmodell-Innovation durch Industrie 4.0*. http://www.wieselhuber.de/lib/public/modules/attachments/files/Geschaeftsmodell_Industrie40-Studie_Wieselhuber.pdf, (Accessed: 27.03.2017)

[11] GORBACH, G. AND POLSONETTI, C. 2015. *Realizing value from the Industrial Internet of Things.* InTech. 62, 4 (2015), pp-(12-18).

[11] INTERNATIONAL FEDERATION OF ROBOTICS 2017. *Standardization. International Federation of Robotics*. http://www.ifr.org/standardisation/ (Accessed: 20.02.2017)

[13] LAWTON, J. *Collaborative robots*. https://www.isa.org/intech/20161001/, (Accessed: 16.01.2017)

[14] LUCKENHAUS, M. 2016. *Machine vision in IIoT: how machine vision technologies help to overcome new challenges related to connected and automated production*. Quality. 55, 5 (2016), (18-20).

[15] MATHARU, G.S. ET AL. 2014. *The Internet of Things: Challenges & security issues*. Proceedings - 2014 International Conference on Emerging Technologies. ICET 2014, (2014), (54-59). DOI:https://doi.org/10.1109/ICET.2014.7021016.

[16] MIES, G. ET AL. *Industrial Robots Worldwide Market Development: Robot Data and Robot Density Projection* for the Year of 2030. unpublished.

[17] MILLS, P. 2015. *Smarter, Smaller, Safer Robots.* Harvard Business Review. 5(2015), (28-30)

[18] NEUBERT, R. 2016. *Powering the Industrial Internet of Things*. Plant Engineering. 70, 2 (2016), (32-34).

[19] OXFORD DICTIONARIES. 2017. *Definition: Cobot*. Oxford Dictionaries | English. https://en.oxforddictionaries.com/definition/us/cobot (15.02.2017)

[20] ROLAND BERGER *Strategy Consultants and B*DI 2015. Die digitale Transformation der Industrie. http://bdi.eu/media/presse/publikationen/information-und-telekommunikation/Digitale_Transformation.pdf, (Accessed: 28.03.2017)

[21] ROCHELEAU ET AL. *Industrial Internet Consortium. Smart Factory Applications in Discrete Manufacturing*: 2017. http://www.iiconsortium.org/pdf/Smart_Factory_Applications_in_Discrete_Mfg_white_paper_20170222.pdf. (Accessed: 10.03.2017)

[12] STATISTA. 2017. *Internet of Things (IoT) in Europe*: https://www.statista.com/study/42750/internet-of-things-iot-in-europe/., (Accessed: 19.06.2017)

[22] STATISTA. 2017. *Spending forecast - industrial robotics globally* 2025 https://www.statista.com/statistics/441963/forecast-for-industrial-robotics-spending-worldwide/, (Accessed: 2017-05-22).

[24] STOCK, T. AND SELIGER, G. 2016. *Opportunities of Sustainable Manufacturing in Industry 4.0*. Procedia CIRP. 40, (2016), (536-541). DOI:https://doi.org/10.1016/j.procir.2016.01.129.

[25] STRATEGY& AND PWC 2014. *Industrie 4.0 – Chancen und Herausforderungen der vierten industriellen Revolution*. http://www.strategyand.pwc.com/media/file/Industrie-4-0.pdf, (Accessed: 14.03.2017)

[26] THAMES, L. AND SCHAEFER, D. 2016. *Software-defined Cloud Manufacturing for Industry 4.0*. Procedia CIRP. 52, (2016), (12-17). DOI:https://doi.org/10.1016/j.procir.2016.07.041.

[27] SZABOLCSI, R. -*Modeling of the human pilot time delay using Padé series*-AARMS THEORY Vol. 6, No. 3 (2007) 405–428.

HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

A KOSZOVÓI MAGASLÉGTÉRI IRÁNYÍTÁSI RENDSZER GRÁF-MODELLEZÉSE

GRAPH MODELLING OF THE KOSOVO UPPER AIRSPACE AIR TRAFFIC CONTROL SYSTEM

POKORÁDI László; SOMOSI Vilmos

(ORCID: 0000-0003-2857-1887); (ORCID: 0000-0002-4763-2174)

pokoradi.laszlo@bgk.uni-obuda.hu; vilmos.somosi@hungarocontrol.hu

Absztrakt

A 15 év elteltével újra megnyitott Koszovó feletti magas légtér, a HungaroControl Zrt. által nyújtott távoli körzeti légiforgalmi irányítás nagyobb mozgásszabadságot és rövidebb repülési útvonalakat biztosít a térségen átrepülő nemzetközi légi forgalom számára. A közlekedési és kommunikációs hálózatok, hatékony matematikai modellezésének egyik eszköze a gráfelmélet. Egy hálózat vizsgálatának első fontos állomása az elemek közti – sok esetben bonyolult kölcsönhatásokat is jelenthető – kapcsolatok tényének feltárása és gráfban történő ábrázolása. Gráfon csomópontok és élek halmazát értjük melyben csomópontokat élekkel kötünk össze. A tanulmány gráf-modellezésen keresztül ismerteti a térségben üzemelő légtér-felderítési rendszerek, valamint a magyar léginavigációs szolgáltató (HungaroControl Zrt.) közötti adatkapcsolatok sajátosságait.

Kulcsszavak: *gráf-modellezés, radarkapcsolati hálózat, távoli körzeti légiforgalmi irányítás, Koszovó magaslégtér*

Abstract

After 15 years the Kosovo upper airspace was re-opened, and the remore en-route air traffic services by HungaroControl provide more freedom and optimised routes for international air traffic operating through this region. Graph theory is one of the tools of the efficient mathematic modelling of the transport and communication systems. The first significant step in the network analysis is the exploration and visualization of the relationship (dependency) between the elements, which can also represent complex interactions among them. Graph is a conglomeration of edges and junctions where the junctions are connected with edges. This article introduces the special data connectivity of surveillance systems and the Hungarian Air Navigation Service Provider (HungaroControl) by Graph-analysis which is an efficient tool for modelling such a complex transport and communication networks.

Keywords: *Graph modelling, radar data network, remote ATS, Kosovo upper airspace*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.01.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.02.

BEVEZETÉS

Jelentős mértékben átalakította az európai légiközlekedést a 15 év elteltével újra megnyitott Koszovó feletti magas légtér[1], amely így nagyobb mozgásszabadságot és rövidebb repülési útvonalakat biztosít a térségen átrepülő nemzetközi légi forgalom számára. A forgalmi átrendeződés mellett külön iparági előrelépésnek tekinthető, hogy a HungaroControl Magyar Légiforgalmi Szolgálat Zrt. – a NATO-felkérés alapján teljesített – az országhatárokon átívelő légiforgalmi irányításhoz szükséges radaradatokat és levegő-föld kommunikációs kapcsolatot a térségben már telepített és üzemelő rendszereket üzemeltető léginavigációs szolgáltatóktól vásárolja. A világon elsőként megvalósult költséghatékony megoldást az egymással nem szomszédos országok közötti, több határon átnyúló együttműködése, továbbá különleges és innovatív megoldások bevezetése tette lehetővé.

Rendszerszemléletű elemzés esetén a légiforgalmi irányítási rendszer, illetve folyamat hálózati struktúrájúnak tekinthető. A gráfelmélet a matematika, ezen belül a kombinatorika egyik fontos ága. Története a königsbergi hidak híres matematikai problémájával kezdődött, amit Leonhard Euler oldott meg 1736-ban. A gráfelmélet felhasználásával a különböző hálózatokat, hálózati struktúrájú rendszereket és folyamatokat tudunk matematikai modellel hatékonyan leírni és – a kívánt szempont alapján – elemezni.

A gráfelméletnek és mérnöki alkalmazásának kiterjedt matematikai és műszaki szakirodalma található. A technikai folyamatok leírásához szükséges gráfelméleti alapismeretek olvashatók a két Korn [1], illetve Pokorádi [2] könyvében. Alkalmazásukra láthatunk példákat a [3] és [4] publikációkban. Csiszér kutatásainak célja a hálózatkutatás minőségügyi felhasználási lehetőségeinek feltárása, főleg a folyamatfejlesztési szempontokat helyezve az elemzések középpontjába [5], [6]. Zentai a kritikus infrastruktúrák hibatűrését, illetve támadásokkal szembeni ellenálló képességét modellezte gráfelméleti eszközökkel, az infrastruktúrát leíró gráf többszörös összefüggőségét vizsgálva [7].

Tanulmányunk gráfelméleti elemzésen keresztül szemlélteti az országhatároktól és léginavigációs szolgáltatástól függetleníthető úgynevezett távoli (remote) légiforgalmi irányítás technológiai környezetét, a radaradat hálózatok kritikus pontjait és kockázati elemeit. A dolgozat nem terjed ki a levegő-föld kommunikációs, illetve a légiforgalmi szolgálatok közötti hangfrekvenciás koordinációs kapcsolatokra, valamint a jeladatokat biztosító kommunikációs vonalakra, továbbá a légiforgalmi szolgálat adatfeldolgozói rendszereire. Tanulmányunkban a kialakított infrastruktúra elemzését a jelforrástól a jelfeldolgozásig és megjelenítésig (alkalmazói végpontig) végeztük el. A szolgáltatási környezetek és adatkapcsolatok modellezésével a rendszer elemei és a folyamat állomásai közti kapcsolatot szemléltetjük. Az elemek közti kapcsolatok tényének feltárásával, ábrázolásával a diszkrét állapotterű folyamatokat írjuk le gráfok segítségével [2].

A tanulmány az alábbi fejezetekből áll: Az 1. fejezet a történeti előzményeket ismerteti. A 2. fejezet koszovói magaslégtéri irányítási infrastruktúra mutatja be. A 3. fejezet adja meg a gráfelméleti alapokat. A 4. fejezetben a radaradat kapcsolati hálózatok vizsgálata olvasható. Végezetül a Szerzők összegzik tanulmányukat, valamint fogalmazzák meg a további kutatási lehetőségeket.

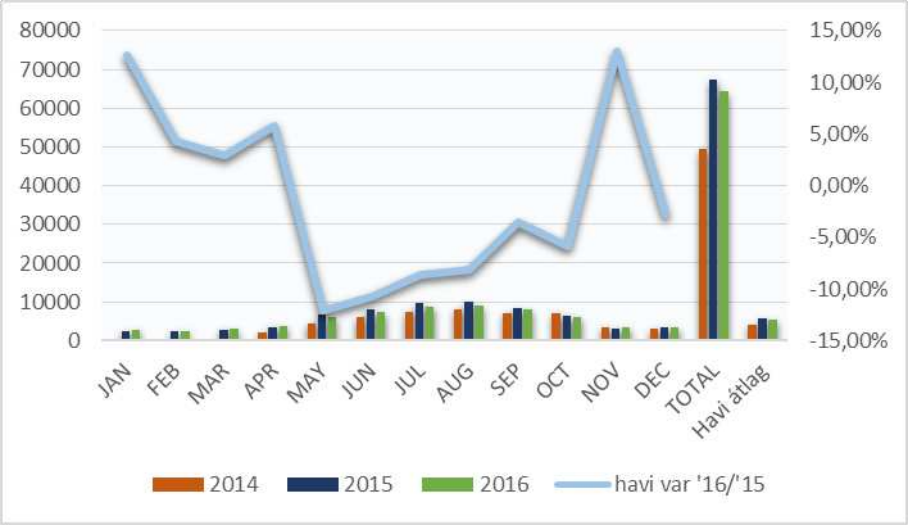
[1] Fligh Level 205-660 (kb. 6200–20 000 méter) közötti repülési magasságtartomány

TÖRTÉNETI ELŐZMÉNYEK

Az ENSZ Biztonsági Tanács 1244. sz. határozatának, valamint az 1999-es Katonai Műszaki Megállapodásnak megfelelően a NATO/KFOR[2] által ellenőrzött Koszovó feletti légtér lezárásra került és 15 éven keresztül elérhetetlen volt a polgári légiforgalom számára [8]. A rendeződő politikai viszonyok eredményeként tárgyalások kezdődtek az úgynevezett magas légtér újranyitásáról, melynek részeként nemzeti léginavigációs szolgáltatók pályázhattak a térség légiforgalmi irányítói szolgáltatásának szerződéses alapon történő biztosítására.

Az eredményes pályázást követően az Észak-atlanti Tanács – a balkáni légiközlekedés normalizációja keretében hozott 2012. április 13-i döntését követően – felkérte Magyarországot, illetve a HungaroControlt a Koszovó feletti magas légtérben a polgári léginavigációs és a kapcsolódó hatósági feladatok ellátására [9]. A magyar kormány felajánlása szerint tehát a HungaroControl technikai lebonyolítóként működik közre a projektben, míg az ENSZ BT fent nevezett határozatának, valamint az 1999-es Katonai Műszaki Megállapodásának megfelelően a légtér továbbra is a NATO/KFOR fennhatósága alatt marad.

A légtér újbóli megnyitásától a repülési útvonalak rövidülése volt várható a térségben, amely jelentősen csökkenti a légtérhasználók üzemeltetési költségeit – az európai légiközlekedési hálózatmenedzserrel (EUROCONTROL Network Manager) közösen végzett előzetes számítások szerint a koszovói légteret igénybe vevő évi 180 ezer légijármű (különösen az Európából a Közel-Keletre és Ázsiába irányuló forgalom) 370 ezer tengeri mérfölddel (kb. 670 ezer kilométerrel) repül majd kevesebbet. A légtér megnyitása így éves szinten 18 millió Euró üzemeltetési költségmegtakarítást eredményezhet a légitársaságoknak, de a környezeti terhelés is jelentősen csökkenhet az évi 24 ezer tonnával kevesebb üzemanyag felhasználásával és a 75 ezer tonnával kevesebb CO_2 károsanyag-kibocsátással [10]. Az európai légtér normalizációja és a technológiai megoldások modellezése-megvalósítása az Európai Bizottság Egységes Európai Égbolt célkitűzéseit is szolgálja, amelynek keretében az európai léginavigációs szolgáltatók magasabb repülésbiztonsági szinten és költséghatékonyabban és a késések csökkentésével biztosítják a légitársaságoknak az optimálisabb repülési útvonalakat [11].



1. ábra Koszovói légiforgalmi statisztika 2014-2016 [13]

[2] Kosovo Force

A HungaroControl jelentése szerint a koszovói légtér igénybevétele egyelőre elmarad az előzetes prognózishoz képest, de lassú, ám folyamatos emelkedési tendenciát mutat: az átrepülő forgalom 2014-ben 49.517 légijármű volt, míg 2015. évben 67.405, 2016. évben pedig 64.405 gépmozgás volt [12]. A forgalom havi alakulását az 1. ábra szemlélteti [13].

A KOSZOVÓI MAGASLÉGTÉRI IRÁNYÍTÁSI INFRASTRUKTÚRA

A HungaroControl 700 kilométeres távolságból, nem közvetlen országhatár-szomszédságban biztosítja az úgynevezett távoli körzeti légiforgalmi irányítást, amelyhez a szükséges adatokat és szolgáltatást a térségben már kialakított infrastruktúrát üzemeltető léginavigációs szolgáltatóktól vásárolja. A magyarországi központból nyújtott légiforgalmi szolgáltatáshoz három szolgáltatási elem tekintetében kellett biztosítani az országhatárokon átívelő folyamatos és redundáns kapcsolatot, a jelforrástól a jelfeldolgozásig és megjelenítésig (alkalmazói végpontig):

- a koszovói légtér lefedettségét biztosító radarok hálózata;
- levegő-föld kommunikációs kapcsolatot biztosító hálózatok;
- légiforgalmi irányító szolgálatok között hangkommunikációs kapcsolatok.

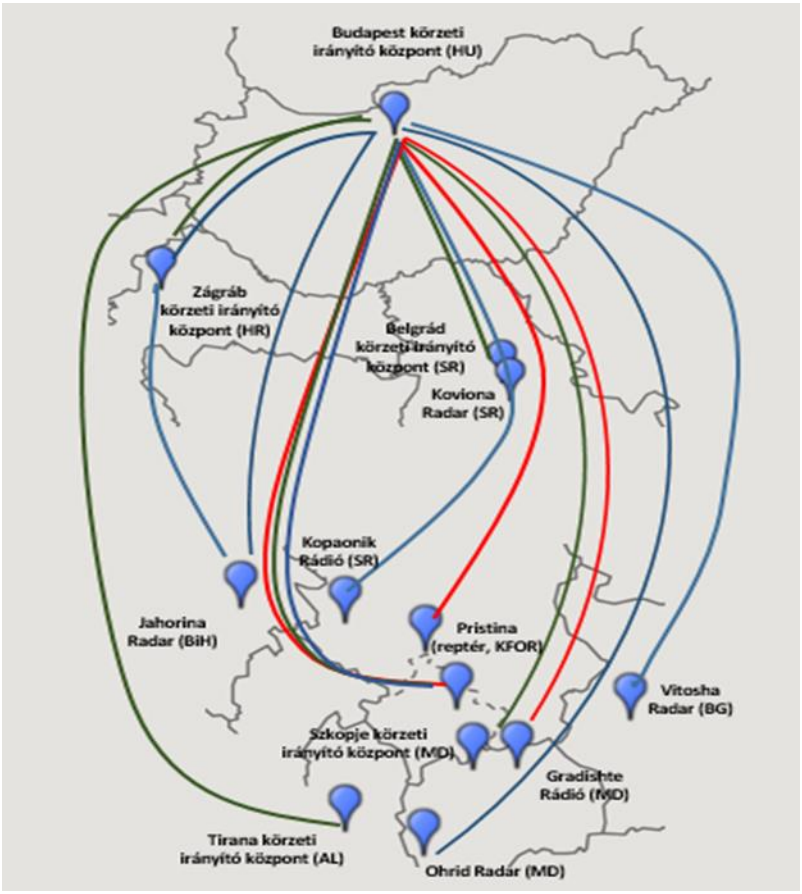
A HungaroControl folyamatos üzemeltetési feltételek teljesülése, illetve az abszolút (99,99%) biztosítottság érdekében megfelelő (két, illetve háromszoros) redundanciát, és hatékony munkatechnológiai eljárásokat alakított ki az adatforrásokra (lokátorok, rádióállomások), az adatkapcsolati hálózatokra, adatfeldolgozásra, és a feldolgozott adat-megjelenítés közötti hálózati elemekre vonatkozóan.

A légiforgalmi irányítói szolgáltatáshoz a térséget megfelelő redundanciával biztosított lefedő levegő-föld hangkommunikációs (rádió) kapcsolatot, radarlefedettséget, illetve a HungaroControl és a koszovói légtérrel szomszédos légiforgalmi irányító szolgálatok közötti kétoldalú földi hangkommunikációs (telefonos) kapcsolatot kellett kiépíteni. Az adatok továbbítását biztosító kereskedelmi szolgáltató szerződésben garantálja a minimum 99,8%-os szolgáltatási folyamatosságot.

A 2. ábra általánosságban szemlélteti a koszovói légtérben történő szolgáltatáshoz kiépített többnemzeti részvételű regionális (levegő-föld, és irányító egységek közötti) kommunikációs, illetve légtér felderítési környezetet. Hangsúlyozandó, hogy az ábrán szereplő adatkapcsolati vonalak nem tükrözik a hálózatok valóságos földrajzi elhelyezkedését, mivel a telekommunikációs szolgáltatók üzleti és védelmi szempontokra hivatkozva általában nem ismertetik a hálózati útvonalakat (nem kötelességük, de megegyezés szerint a közbeszerzés és a szerződéskötés során számukra előírható). Ebből adódóan jelen elemzés nem terjed ki a 4. ábrán e_1-e_7 élekkel jelzett hálózati réteg elemzésére.

Hangsúlyozandó azonban, hogy a távoli körzeti légiforgalmi irányítási infrastruktúra robosztusságának meghatározásában fontos elemet játszik az kommunikációs és adathálózatok, mint kritikus infrastruktúra elemeivel kapcsolatos kockázatok és követelmények feltérképezése is [14].

A kockázatok csökkentése érdekében javasolt a szolgáltatói szerződéseket több féllel is megkötni, illetve kikötni a hálózati útvonalak ismeretét, továbbá azon általános követelmény teljesülését, miszerint legyen mikrohullámú és földfelszín alatti hálózat rendelkezésre állása. A földi hálózat esetében TDM (Time Division Multiplexing) biztosítja az adatok védettségét. A kommunikációs rendszerek fejlődése okán egyre inkább elterjedő IP alapú vonalak alkalmazásakor 256 bites titkosítás a minimum elvárás az ATM iparágban is egyre nagyobb jelentőséggel bíró kiberbiztonság (Cyber Security) érdekében (a kódolás a léginavigációs szolgáltató felelőssége).



2.ábra A koszovói magaslégtéri irányításhoz szükséges adatkapcsolatok [forrás: Szerzők]

A teljes függetlenség szavatolása érdekében, a hálózatokat biztosító szolgáltatók számára javasolt előírni, hogy nem bérelhetnek vonalakat egymástól (ez különösen fontos abban az esetben, ha nem ismertek a szolgáltatók hálózati útvonalai). Az IP alapú adattovábbítási technológia alkalmazása esetében a szerződésekben a szolgáltatás kiesésének kockázatát is kezelni kell. A rendszerbiztonság szempontjából kiemelt jelentőséggel bír, hogy a hálózat minden eleme (áramforrás, nyomvonal, berendezések) rendelkezzen redundanciával.

Amennyiben egy országból több szolgáltatás (például telefonos összeköttetés és radaradatok továbbítása) is biztosított, az adatok egy szerződés keretében biztosított vonalon keresztül érkeznek. A kialakított infrastruktúra alapja a Magyarországgal szomszédos léginavigációs szolgáltatókkal már kialakított hálózatok (Zágráb-Budapest és Belgrád-Budapest interfész), kiegészülve további bérelt vonalakkal[3].

A modellezésben a HungaroControl úgynevezett KATIAS (MRTS adatfeldolgozási) rendszerét – melyet P_7 pontként jelöltünk a radarkapcsolati elemzésben – egy elemként kezelve, annak ellenére, hogy az valójában egymással redundáns (három) feldolgozó egységekből áll: Master és annak tartalékát képező úgynevezett Slave rendszer, illetve mindkettő tartalékát biztosító RFS.

A P_8 pont szintén a HungaroControl összesen négy légiforgalmi irányító munkaállomásának együttes megjelenítése. A koszovói légtérben két szektor üzemeltethető, egyenként 1-1 EC (Executive Controller) és PC (Planning Controller) pozícióval.

[3] lásd e_1 és e_2 vonalak: Jahorina radarjelek közvetlenül és a zágrábi légiforgalmi irányító központtal kialakított vonalon keresztül is beérkeznek a HungaroControlhoz)

GRÁFELMÉLETI ALAPOK

A rendszerelmélet gyakorlati alkalmazásának egyik fontos állomása a rendszerelemek közti – sok esetben bonyolult kölcsönhatásokat is jelenthető – kapcsolatok tényének feltárása és gráfban történő ábrázolása.

Egy nagyméretű, lineáris rendszer gráf-reprezentációjának meghatározása után a gráfot jelképes értelemben „fel kell vágni" kisebb részgráfokra, majd a részgráfok egyenleteinek megoldása után az egyes részek megoldásait „össze kell kapcsolni" (ha szükséges, akár több lépésben is), ami az eredeti rendszer megoldásához vezet. A gráf egyrészt fontos állomás az eredeti, teljes rendszer egyenleteinek felállításában, másrészt a vágási eljárás megtervezéséhez nyújt segítséget [2].

A gráf olyan alakzat, amely pontokból és bizonyos pontpárokat összekötő (nem feltétlenül egyenes) vonaldarabokból áll. Matematikai megfogalmazásban a *G(P;E;f)* gráfon olyan alakzatot értünk, amely a *P* pontokból és bizonyos pontokat összekötő *E* vonaldarabokból áll. A *P* halmaz elemeit pontoknak (esetleg gráf szögpontjainak vagy csúcsainak), az *E* halmaz elemeit pedig a gráf éleinek nevezzük. A fenti jelölésben szereplő *f* függvény az *E* halmazt képezi le a *PxP*-re, azaz bármely *e* élhez hozzárendel egy pontpárt a *P* halmaz elemei közül. Ezért az *f*-t szokás illeszkedési leképezésnek nevezni.

Irányított gráfról akkor beszélünk, ha az élek végpontjainak sorrendjére is tekintettel vagyunk. Irányítatlan gráf esetén a végpontok sorrendje nem releváns.

Irányítatlan gráf esetén, ha P_i és P_j csúcsokat összeköti valamely e_k él, akkor a P_i és P_j szomszédos szögpontok, és az e_k él végpontjai. Irányított gráf esetén, ha az e_k él P_i-ből P_j-be irányul, akkor P_i a kezdőpontja, P_j pedig a végpontja az e_k irányított élnek, illetve P_j szomszédja P_i-nek.

A gráf élei közti kapcsolatokat az úgynevezett csúcs- (szomszédossági-, vagy adjacencia-) mátrixszal lehet táblázatosan megadni.

Irányított gráf esetén az **A** szomszédossági mátrix *i*-edik sor *j*-edik elemének a_{ij} értéke a P_i szögpontból induló és a P_j végpontú élek számát jelöli. Az **A** szomszédossági mátrix *i*-edik hatványa megmutatja, hogy mely szögpontokból mely csúcsok érhetők el pontosan *i* számú lépésben, azaz élen keresztül.

Az elemek közti összetett kapcsolatokat a rendszer vizsgálati gráfjának úgynevezett elérhetőségi mátrixa is jellemzi. Egy *m* szögpontból álló gráf elérhetőségi mátrixán azt az *m* sorból és oszlopból álló $\mathbf{D}_{mxm}$ mátrixot értjük, ahol:

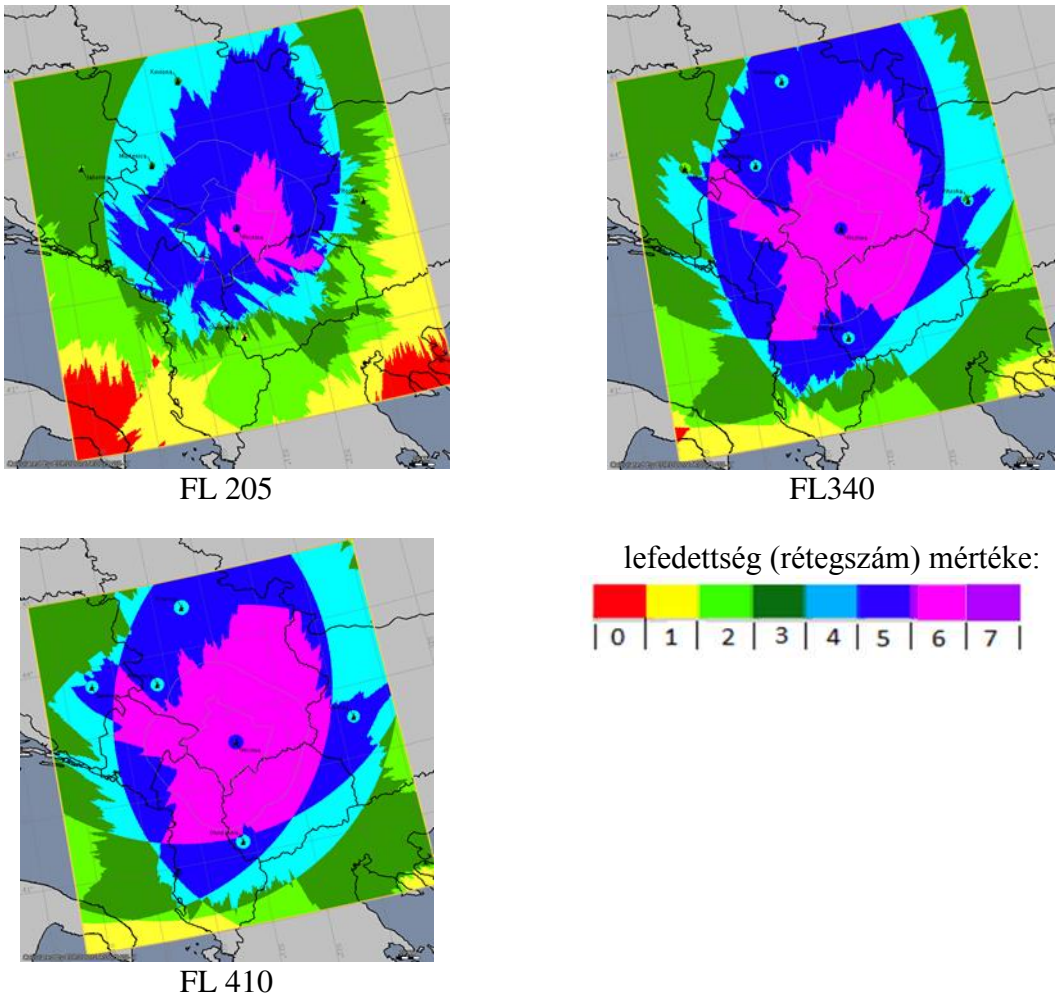
$$d_{ij} = \begin{cases} 1, & \text{ha a } p_i \text{ csúcsból a } p_j \text{ szögpont elérhető} \\ 0, & \text{ha nem} \end{cases} \tag{1}$$

A [2] irodalom alapján könnyen belátható, hogy az elérhetőségi mátrixot a szomszédossági mátrix hatványai segítségével tudjuk felállítani (a módszer részletes leírása a könyvben olvasható).

Fontos itt megjegyeznünk, hogy jelen tanulmányban az utak különbözőségén az általuk érintett szögpontok, vagy azok sorrendjének különbözőségét értjük. Az ugyanazon szögpontokat megegyező sorrendben tartalmazó, de más élekből álló utakat azonosaknak tekintjük. Ilyen eset fordulhat elő, ha a gráfon belül két szögpontot egynél több él köt össze. Ezt az egyszerűsítő feltételt azért vezetjük be, mert végső célunk az elérhetőség vagy el nem érhetőség tényének megállapítása a tényleges utak számától függetlenül (jelen vizsgálatunk során ez különösen azért fontos, mert számunkra nem ismertek a telekommunikációs szolgáltatók hálózati útvonalai). Jelen vizsgálatunk fő célja a gráfok szögpontjai közt meglévő kapcsolatok feltárása.

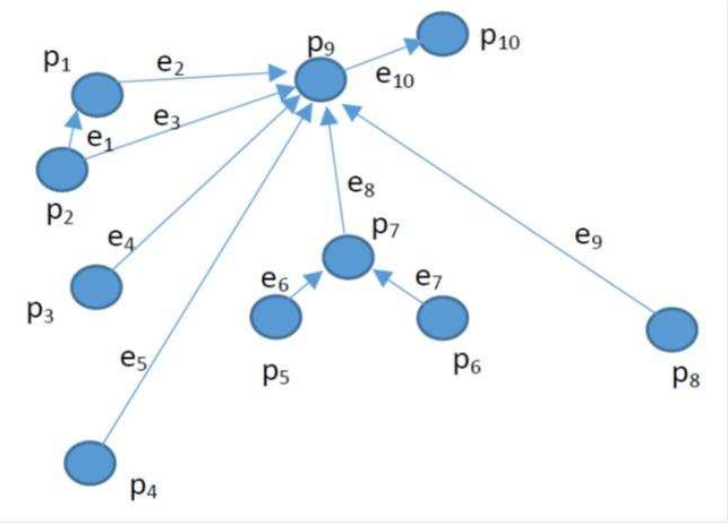
RADARADAT KAPCSOLATI HÁLÓZATOK VIZSGÁLATA

A térség (EUROCONTROL által biztosított szoftverrel számított) abszolút radarlefedettségét a 3. ábra szemlélteti különböző repülési szintek szerint (FL205, FL340, FL410[4]). A cikkben a gráf-modellezést a legnagyobb számú lefedettségi magasságtartományra (rétegszámra) értelmezve végeztük el (tehát azt a helyzetet elemezzük, mikor a térségben repülő azonosított légijárművet 6 radarral detektálják).



3. ábra Radarlefedettség a koszovói térségben [13]

[4] *Flight Level - 205-340-410 (Repülési szintek: 6200m – 10500m – 13000m)*



4. ábra A radarhálózat irányított Gráf-modelleje
P1 – Zágráb ACC (HR); P2 – Jahorina radarállomás (BiH); P3 –Pristina radarállomás (KOS);
P4 – Ohrid radarállomás (MD); P5 – Koviona radarállomás (SRB); P6 – Murtenica radarállomás (SRB) ;
P7 – Belgrád ACC; P8 –Vitosha radarállomás (BG); P9 – HungaroControl adatfeldolgozó rendszer (MRTS és RFS); P10 – HungaroControl légiforgalmi irányítói munkaállomások (2 EC és 2 PC pozíció);
e1 – e10 – adatkapcsolati hálózatok

A 4. ábrán látható irányított gráf szomszédossági mátrixa, illetve annak hatványmátrixai:

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{2}$$

$$\mathbf{A}^2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3}$$

$$\mathbf{A}^3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{4}$$

$$\mathbf{A}^4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{5}$$

Mint az az (5) egyenletből látszik, a vizsgált irányított gráfban a leghosszabb ($P_2 - P_9 - P_{10}$; $P_5 - P_7 - P_{10}$ *és* $P_6 - P_7 - P_{10}$) láncok hosszúsága 3 él. Ebben az esetben a **D** elérhetőségi mátrixot a

$$\mathbf{D} = sign\sum_{i=1}^{3}\mathbf{A}^i = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{6}$$

módon tudjuk meghatározni.

A gráf-modell mátrixalgebrai elemzése alátámasztja a tervezés és kivitelezés során is nagy hangsúlyt kapott szükségletet, miszerint a P_9 (adatfeldolgozási) pont a folyamatban olyan kulcsszerepet játszik, aminek okán elengedhetetlen a többszörös biztosítottság kialakításra. Egy légiforgalmi szolgálat működésében bekövetkező jelentős meghibásodás kockázati

szintje elvileg igen alacsony, de mégsem zárható ki teljes mértékben. A különleges helyzetek kialakulásának egyik példája a 2012. december 7-én a Budapest Liszt Ferenc Nemzetközi Repülőtér irányító tornyában (csőtörés miatt az elektromos rendszer beázása következtében) történt meghibásodás, aminek okán a rádió-kommunikációs, informatikai és az egyéb vezérlő rendszerek működésképtelenné váltak, így a repülőteret ideiglenesen be kellett zárni [15].

A körzeti légiforgalmi szolgálat működésében esetlegesen bekövetkező vis-major helyzetet szemlélteti a térségünkben 2014. július 30-án bekövetkezett esemény, amikor a zágrábi körzeti irányító központ (Zagreb ACC – a 4. ábrán látható gráf P_1 pontja) az extrém nyári időjárási körülmények kialakulása okán a heves esőzés miatti beázás és villámcsapás miatt több órára leállt, a légtér bezárásra került és a forgalmat a környező országok irányába terelték. A gyors ütemű helyreállítási munkálatok ellenére a központ csak 2 nap múlva érte el újból a teljes forgalmi kapacitási értékét [16].

Az irányító központ (egészének vagy kritikus infrastruktúra elemeinek) hirtelen leállása, illetve jelentős mértékű meghibásodása (üzemkiesése), vagy tervezett kapacitás-csökkenése hatásainak csökkentése érdekében a HungaroControl – a hálózatokat, valamint a radarokat üzemeltető szolgáltatókkal közösen – folyamatos (napi, heti rendszerességű) koordinációval tartja számon a radarállomások és vonalak működési státuszát és az egyes javítások várható idejét, időtartamát.

Az elemzés során, a térség redundáns radarlefedettsége vonatkozásában külön kiemelendő annak jelentősége, hogy

- a teljes légtér vertikumára vonatkozóan különböző magasságtartományokban végzett előzetes számítások szükségesek;
- a redundancia mértékének elsődlegesen a repülésbiztonsági kockázatok kezelését kell biztosítaniuk;
- a térség útvonal-egységdíjainak meghatározását jelentősen befolyásolja a redundanciát biztosító szolgáltatói szerződések száma és azok pénzügyi tartalma;
- a redundanciát biztosító rendszerek üzemeltetési és karbantartási ütemtervét javasolt összehangolni, illetve arról előzetesen a szolgáltatást igénybe vevőt előzetesen tájékozatni (a szerződésben vállalt kötelezettségnek megfelelően);
- az adott térségben kialakítani szükséges redundanciát nem csak másodlagos radarokkal javasolt biztosítani, honvédelmi (légtérvédelmi és légtérrendészeti) kötelezettségek fenntartása végett.

KÖVETKEZTETÉSEK

A koszovói légiforgalmi infrastruktúra megmutatta a lehetőségét a távoli körzeti irányítói szolgáltatás szélesebb körű megvalósíthatóságának. A távoli körzeti irányítási környezet (a távoli toronyirányítási technológiához hasonlóan) is intelligens közlekedési rendszernek tekinthető, melyek célja, hogy tényleges intelligencia megtestesítése nélkül innovatív szolgáltatásokat nyújtsanak a különféle közlekedési módokhoz és a forgalomirányításhoz kapcsolódóan [17].

A fejlett alkalmazással – kiépített helyi CNS infrastruktúra, adatkapcsolati és kommunikációs hálózatokon keresztül – elvileg lehetőség nyílik a felelősségi térségtől függetlenül (a világ bármely pontjáról) biztosítható légiforgalmi szolgáltatásra, amely alapvetően megváltoztathatja az európai polgári léginavigációs és légiforgalom-szervezési viszonyokat (technológiai, üzleti, légtér- és kritikus infrastruktúra-védelmi szemszögből egyaránt).

A publikációban bemutatott módszerrel lehetőség nyílik a távoli légiforgalmi szolgáltatási módozatok előzetes elemzésére és a rendszerek, illetve hálózatok gráfokkal történő modellezésére. Az infrastruktúra kritikus elemeinek beazonosításához és a hatások kezelését célzó eljárások kialakításához a nagyméretű és komplex úgynevezett EATMN[5] rendszerek és kapcsolataik reprezentációjához a gráfot részgráfokkal lehet és egyben javasolt modellezni az egyes funkcióknak-témaköröknek megfelelően (például áramforrás-hálózatok és kommunikációs vonalak, radarlefedettség, levegő-föld kommunikáció, adatfeldolgozás és megjelenítés, stb.).

A részgráfok elemzése után az egyes részek eredményeit kell „összekapcsolni" (akár több lépésben is), amely végezetül a teljes rendszer elemzésének eredményéhez vezet. Kijelenthető, hogy a gráf egyfelől fontos állomás az eredeti, teljes rendszer modelljeinek felállításában, másfelől a vágási eljárás megtervezéséhez nyújt segítséget [2].

A kialakításra tervezett távoli (remote) légiforgalmi szolgáltatást biztosító infrastruktúra robosztusságának elemzéséhez segítséget nyújtó gráf-modellezést javasolt a légiforgalmi és léginavigációs rendszerek teljes spektrumára (de legalábbis azon elemekre, amelyek kritikus infrastruktúraként kerülnek beazonosításra) végrehajtani, kiegészítve az épületgépészeti és légiközlekedés-védelmi rendszerekre, elemekre vonatkozó elemzésekkel. A teljes infrastruktúra komplex gráf-modelljét az Európai Légiforgalmi Szolgáltatási Hálózat átjárhatóságáról szóló 552/2004/EK rendelet szerint javasolt felépíteni, a jogszabály szerint az ETAMN vonatkozásában meghatározott alábbi nyolc rendszernek megfelelően [18] [19] [20]:

- légtér-gazdálkodási rendszerek és eljárások;
- a légiforgalmi áramlás szervezésének rendszerei és eljárásai;
- a légiforgalmi szolgálatok rendszerei és eljárásai, különösen a repülési adatokat feldolgozó rendszerek, a légtérellenőrzési adatokat feldolgozó rendszerek és az ember-gép interfészrendszerek;
- távközlési rendszerek és eljárások a földi, a fedélzet és a földi irányítás közötti, valamint a fedélzetek közötti kommunikációhoz;
- navigációs rendszerek és eljárások;
- légtérellenőrző rendszerek és eljárások;
- a légiforgalmi tájékoztató szolgálatok rendszerei és eljárásai;
- a meteorológiai adatok felhasználására szolgáló rendszerek és eljárások.

Tekintettel arra, hogy a telekommunikációs szolgáltató üzleti és védelmi szempontjaira hivatkozva általában nem ismerteti a hálózati útvonalait, az előkészítés és szerződéskötés során javasolt előírni számára annak ismertetését, amely alapján a komplex és mindenre kiterjedő gráf-elemzéshez a hálózati réteg elemzése is szükségszerű. A távoli körzeti légiforgalmi irányítási infrastruktúra robosztusságának meghatározásában fontos elemet játszanak a kommunikációs és adathálózatok is, mint kritikus infrastruktúra elemeivel kapcsolatos kockázatok és követelmények feltérképezése is. [14]

A szolgáltatói szerződéseket javasolt több szolgáltatóval is megkötni, és a hálózati útvonalak bemutatása mellett feltételként megszabni, hogy legyen mikrohullámú[6] és földfelszín [7] alatti hálózat rendelkezésre állása. Az egyre inkább elterjedő IP alapú vonalak alkalmazásakor a 256 bites titkosítást javasolt minimum elvárásként meghatározni az ATM iparágban is egyre nagyobb jelentőséggel bíró kiberbiztonság (Cyber Security) érdekében.

[5] European ATM Network
[6] kockázati szempont: időjárási sérülékenység
[7] kockázati szempont: mechanikai behatás veszélye

A teljes függetlenség szavatolása érdekében, a hálózatokat biztosító szolgáltatók számára javasolt előírni, hogy nem bérelhetnek vonalakat egymástól (ez különösen fontos abban az esetben, ha nem ismertek a szolgáltatók hálózati útvonalai). Az IP alapú adattovábbítási technológia alkalmazása esetében a szerződésekben a szolgáltatás kiesésének kockázatát is kezelni kell. A rendszerbiztonság szempontjából kiemelt jelentőséggel bír, hogy a hálózat minden eleme (áramforrás, nyomvonal, berendezések) rendelkezzen redundanciával.

A teljes értékű modellezés érdekében további elemzés javasolt a HungaroControl úgynevezett KATIAS (MRTS[8] adatfeldolgozási) rendszere vonatkozásában – melyet P_7 pontként jelöltünk az elemzésben – mert az valójában egymással redundáns (három) feldolgozó egységekből áll: Master és annak tartalékát képező úgynevezett Slave rendszer, illetve mindkettő tartalékát biztosító RFS[9].

A (remote) irányítási technológia megvalósíthatóságának megállapításához szintén vizsgálandó a fent említett adatfeldolgozási rendszer, valamint a légiforgalmi irányító munkaállomások kapcsolata. Ez a gráf-modellben szereplő p8 pont, amely a HungaroControl műveleti termében összesen négy pozíciót jelent (a koszovói légtérben két szektor[10] üzemeltethető, egyenként 1-1 EC (Executive Controller) és PC (Planning Controller) pozícióval).

FELHASZNÁLT IRODALOM

[1] KORN, G.A. - KORN, T.M, Mathematical Handbook for Scientists and Engineers, Courier Dover Publications, 1975.

[2] POKORÁDI L.: Rendszerek és folyamatok modellezése. Campus Kiadó Debrecen 2008. ISBN 978-963-9822-06-1

[3] POKORÁDI L.: Rendszerek és folyamatok gráfelméleti vizsgálata, Tudományos Kiképzési Közlemények, MH. SzRTF, Szolnok 1993/2-3, p. 33–44.

[4] POKORÁDI L.: Rendszerek gráfmodellezése. GÉP LIX. 8) pp. 59-62. (2008)

[5] CSISZÉR T.: A hálózatkutatás alkalmazása a folyamatalapú minőségfejlesztésben, Minőség és megbízhatóság, 2011/5, pp. 274-282.

[6] CSISZÉR T.: A kockázati események közötti összefüggések vizsgálata hálózatelemzése, Magyar Minőség 2011/11, pp. 59-61.

[7] ZENTAI D.: Gráfelméleti módszerek a kritikus infrastruktúra védelemben, Hadmérnök, XII. Évfolyam 2. pp. 341-347.

[8] ENSZ 1244 (1999) számú határozat. Forrás: http://epa.oszk.hu/00000/00036/00070/pdf/100-109.pdf (letöltve: 2016.01.10.)

[9] HungaroControl: A NATO/KFOR ismét megnyitotta a Koszovó feletti magas légteret a polgári átrepülő légi forgalom előtt. Forrás: http://www.hungarocontrol.hu/sajtoszoba/hirek/koszovo-magas-legter (letöltve: 2016.01.04.)

[8] Multi Radar Tracking System
[9] Radar Fallback Service
[10] FL205-FL365 és FL365-660 a szektorok magassági tartománya

[10] MTI: Budapestről irányítják Koszovó magas légterét. Forrás: http://www.hirado.hu/2014/06/12/budapestrol-iranyitjak-koszovo-magas-legteret/ (letöltve: 2016.06.12.)

[11] KREUZ M. – SHULTZ M.: Modelling Interactions in Complex Systems – An Air Navigation Service Provider Focussed Approach. 4th SESAR Innovation Days (2014.11.25-27.)

[12] HungaroControl forgalmi statisztika (vállalati adatforrás)

[13] HungaroControl: Éves jelentés 2015. Forrás: http://www.hungarocontrol.hu/download/5b01b0d52ceb14bfa39f401d7beadc31.pdf (letöltve: 2017. 01.10.)

[14] FELLER T. – HÍDVÉGI G. – KÖLLER L.: A nemzetgazdaság és nemzetbiztonság által igényelt „kritikus infrastruktúra" hálózatok komplex szemléletű vizsgálata (Magyar Mérnöki Kamara Közlekedési Tagozat tanulmány). Budapest 2010. november

[15] AIRportal.hu: Ferihegy Tower blackout: Bezárták a repülőteret. Forrás: http://www.airportal.hu/ap/viewtopic.php?t=10877 (letöltve: 2016.01.08.)

[16] Network Manager: Monthly Network Operations Report. Analysis – July 2014. Forrás: https://www.eurocontrol.int/sites/default/files/publication/performance/201407/network-operations-report-july-2014-analysis.pdf (letöltve: 2017.02.01.)

[17] MARKOVITS-SOMOGYI R.: Intelligens közlekedési rendszerek a légiforgalmi irányításban. Repüléstudományi Közlemények 2015/3

[18] 552/2004/EK rendelet az Európai Légiforgalmi Szolgáltatási Hálózat átjárhatóságáról

[19] 68/2011. (XI. 30.) NFM rendelet a léginavigációs és a légiközlekedés biztonságát szolgáló egyéb földi berendezések engedélyezési eljárásáról és hatósági felügyeletéről

[20] 633/2007/EK rendelet az előzetes tájékoztatás, a koordinálás és a légijáratok légiforgalmi irányító egységek közötti átadása céljára szolgáló légiforgalmi üzenettovábbítási protokoll használatára vonatkozó követelmények megállapításáról