HADMÉRNÖK

Kiemelt közlemények

Szabolcs Prisznyák:
The Instruction of Information Technology in the Education of Non-Commissioned Officers in Hungarian Law Enforcement

Ocskay István:
Puma lánctalpas gyalogsági harcjármű és lehetséges megjelenése a magyar honvédség állományában

Rodrigo Guajardo:
Defense Capabilities Development and Defense Industry, U.S. Case Study

15. évf. (2020)
1. szám

ISSN XXXX-XXXX (nyomtatott)
ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

Hadmérnök
Katonai műszaki tudományok online folyóirata
ISSN 1788-1919

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

Kiadó
Ludovika Egyetemi Kiadó Nonprofit Kft.
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu
A kiadásért felel: Koltányi Gergely ügyvezető igazgató
Olvasószerkesztő(k): Resofszki Ágnes, Gergely Zsuzsánna, Orbán Áron

Tartalom

TARTALOM

Fórum

HADMÉRNÖK
BIZTONSÁGTECHNIKA

15. évfolyam (2020) 1. szám 5–17.
DOI: 10.32567/hm.2020.1.1

Forgó Veronika[1]

Az élelmiszer- és gyógyszergyártás biztonsági kérdései és védelmi rendszerei napjainkban

Safety Issues and Defence Systems of Food and Pharmaceutical Manufacturing Nowadays

Az elmúlt években megnőtt az élelmiszerek által okozott megbetegedések kialakulásának száma, emellett még inkább előtérbe kerültek az élelmiszerhamisítások. Ennek korai felismerésére és megelőzésére újabb és újabb technológiai megoldásokat dolgoznak ki a kutatók és az innovátorok abból a célból, hogy növeljék az élelmiszerbiztonságot. A tárgykör vonatkozásában számos tudományos eredmény született a külföldi és a hazai szakirodalomban egyaránt. A szerző az élelmiszerbiztonság biztonságtechnikai módszereit és megoldásait vizsgálja és foglalja össze, illetve következtetéseket és javaslatokat fogalmaz meg a témában.

Kulcsszavak: **élelmiszerbiztonság, védelmi rendszerek, biztonságtechnika, étrendkiegészítő, vízvédelem**

In the last years the number of food-borne diseases has increased, in addition, food counterfeiting has become even more prominent. For early detection and prevention, the researchers and the innovators are developing new and emerging technologies to increase food security. Regarding the subject matter, many scientific results have been achieved both in foreign and domestic literature. The author examines and summarises the safety techniques and solutions of food safety and draws conclusions and suggestions in the subject.

Keywords: **food safety, protection systems, safety, dietary supplement, water protection**

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

Bevezetés

A 19. századtól Magyarországon megjelentek különböző globális problémák, köztük a fogyasztói társadalom megnövekedett igénye, a népességnövekedés, a migráció, az import és export, az ipar és technológia fejlődése, ezáltal az élelmiszerek előállítása, feldolgozása, forgalmazása során változások következtek be. Az 1800-as évek végétől igény volt a feldolgozott élelmiszerre, ebből kifolyólag az 1900-as évek elejére megkétszereződtek az élelmiszeripari gyárak, amelyek a szesz, a kávé, az ásványvíz, a cukor, a liszt, a margarin, a tej és a hús gyártására specializálódtak. Az első világháború után Magyarországon az élelmiszer-előállításban hanyatlás következett be a terület-elcsatolásnak köszönhetően, amely aztán az 1933-as évektől fellendült, például az újonnan kialakított konzervgyártás megjelenésével. A második világháborút követően szintén hanyatlás következett, azonban a kisparaszti gazdaságok által az élelmiszeripar ismét kibontakozhatott. Azonban ez idő alatt a különböző fertőzések, mint a gümőkór, a ragadós száj- és körömfájás, a baromfipestis előfordulási gyakorisága szignifikánsan magasabb volt a korábbinál, amely nem kedvezett sem a mezőgazdaságnak, sem az élelmiszeriparnak. Az 1990-es évektől megszűnt a mezőgazdaság élelmiszer-feldolgozó szerepe, amely megnövelte a háztáji sertés-, baromfi- és tojástermelést. A legfontosabb az állategészségügyben korábbiakban kialakult helyzet normalizálása, a betegségektől mentes állatállomány megteremtése, szigorúbb szabályozások bevezetése volt [1].

Az 1888. évi VII. törvénycikk rendelkezett a ragadós betegségek megelőzéséről. A közfogyasztásra szánt állatok húsát és belsőségeit vagy az állatorvos, vagy a vágatási biztos vizsgálta húsvizsgálat keretén belül. A szabályozások az évek elteltével átalakultak, így a 21/1953. MT sz. rendelet már nemcsak a ragadós betegségek megelőzésére tért ki, hanem a tárolás, feldolgozás, felhasználás, ártalmatlanítás kereteire is. Az első élelmiszertörvénynek a 1958. évi 27. sz. törvényerejű rendelet tekinthető. Emellett nagy hangsúlyt fektettek az élelmiszer-higiéniára és a minőségellenőrzésre is [2]. Napjainkban kiemelt figyelemmel kell kísérni az EU higiéniai rendeletcsomagját, a 178/2002/EK rendeletet az élelmiszerjog általános elveiről és követelményeiről, a 2008. évi XLVI. törvényt az élelmiszerláncról és hatósági felügyeletéről, illetve a *Codex Alimentarius*[2] előírásait és irányelveit a biztonságos és minőségi élelmiszer-előállításhoz.

Felmerül a kérdés, hogy mit is jelent a biztonságos élelmiszer-előállítás, illetve hogyan kapcsolódik ez a biztonságtechnikához?

Célkitűzések

Célom összefoglalni, hogy milyen kockázati tényezők játszhatnak szerepet a biztonságos élelmiszer- és gyógyszeripari termékek gyártásában, illetve melyek azok a védelmi és monitorozórendszerek, amelyek visszaszoríthatják az élelmiszerek közvetítése által befolyásolt reverzibilis és irreverzibilis egészségkárosodások kialakulását. Kitérek

[2] Codex Alimentarius Hungaricus: Magyar Élelmiszerkönyv.

a kritikus behatolási pontok fontosságára, a nyomonkövetési rendszerek hatékonyságára és a szabotázs korai felismerésére.

Berek és munkatársai a biztonságot valamely személy vagy szervezet állapotában és létében határozták meg, mint rendeltetésszerű működést veszélyeztető szándékos jogellenes magatartások vagy azokkal szemben alkalmazott védelmi rendszerelemek szimbiózisa.[3] A 2008. évi XLVI. törvény 14. § (2) értelmében az élelmiszer biztonságosságáért az élelmiszer előállítója vagy az első magyarországi forgalmazó felelős. Ez érinti a teljes élelmiszerláncot, a termőföldtől az asztalig, a minőségmegőrzési vagy a fogyaszthatósági idő lejártáig. A biztonságtechnika egyik tényezője az élelmiszer-biztonság is, amely napjainkban kulcsfontosságú. Berek és munkatársai a biztonságtechnika körébe sorolták a technikai eszközöket, rendszereket és eljárásokat, amelyek alkalmasak a veszélyeztető tényezők csökkentésére és elhárítására [3]. Az élelmiszerbiztonságban megjelennek különböző védelmi, monitorozó-, megfigyelőrendszerek, amelyek által könnyen és gyorsan felismerhetőek a behatolási kísérletek, illetve áttekinthetőek a bekövetkezett események. A HACCP[4] élelmiszerbiztonsági rendszere is egy védelmi rendszernek tekinthető, amely alkalmas a felmerülő veszélyek azonosítására és azok elhárítására, kezelésére és megelőzésére. Figyelembe kell venni, melyek azok a szabályozási pontok, rendszerek, folyamatok, eljárások, amelyek befolyással lehetnek a termék biztonságosságára és minőségére. A rendszerek, folyamatok működése során, szem előtt kell tartani a kémiai, fizikai, biológiai, mikrobiológiai veszélyeket, és előre meghatározott időközönként belső auditok alkalmával elemezni kell azok megfelelőségét, illetve felülvizsgálatkor számolni kell a szabályozó intézkedések sajátosságaival is.

Kutatási módszerek

A téma teljes körű áttanulmányozásához a szakirodalom legaktuálisabb közleményeit térképezem fel a szekunder kutatás során, amelyek különböző technológiai megoldásokkal foglalkoznak az élelmiszerbiztonság témakörében. A külföldi és magyar szakirodalmak, folyóiratok mellett, tanulmányozom a témához kapcsolódó szabványokat, ajánlásokat, magyar jogszabályokat, és EK-rendeleteket. Azonban ahhoz, hogy körültekintően átlássuk a biztonságtechnika és az élelmiszerbiztonság közötti összefüggéseket, átfogóan ismernünk kell a tudomány mai állása szerinti elméleti és gyakorlati eredményeket a tárgykör vonatkozásában. A kvalitatív kutatás által összefoglalt tudományos eredményekből következtetéseket vonok le, majd azokat felhasználva összefoglalom azok élelmiszerbiztonsági hasznosíthatóságát.

[3] Összefonódás.
[4] Hazard Analysis Critical Control Points – Veszélyelemzés és kritikus szabályozási pontok.

A víz mint potenciális biztonsági kockázat az élelmiszer- és gyógyszergyártás során

A biztonságos termék előállításához elengedhetetlen a védelmi vonalak kialakítása. A technológiai folyamatok során víz az alapanyaga mind az élelmiszer-, mind a gyógyszeripari termékeknek. Emellett kritikus behatolási pontként kezelendő a víz, a vízbázisok és a víznyerő helyek, mivel egy esetleges szennyezés vagy mérgezés reverzibilis vagy irreverzibilis kárt okozhat a technológiai folyamatokban, emellett fokozott egészségkockázattal is számolni kell.

A biztonságos termék alapvető feltétele az ivóvíz-minőségű víz biztosítása, amely a 201/2001. (X. 25.) Korm. rendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről előírásainak betartásával és betartatásával foganatosítható.

Berek és Rácz kiemelten fontosnak tartja, hogy rávilágítson a vízbázisok védelmére, amelyek lényegesek a vízminőség biztonságosságának fenntartásában. Ugyanis a vízbázisoknál különböző kockázatokkal kell számolni, amelyek lehetnek természeti eredetű veszélyek, civilizációs és technológiai eredetű veszélyek, illetve szándékos, ártó jellegű cselekmények. A vízbiztonsági terv is hozzájárul a védelem biztosításához, amelynek alapja a veszélyforrások feltárása és a kockázatelemzés. A távfelügyeleti és távvezérlési rendszerek, impulzusátadók hozzájárulnak a vízhozam és a vízveszteség elemzéséhez, valamint a meghibásodások jelzéséhez. Automata mérőberendezések szolgáltatják a mérések adatait, a PH, a vezetőképesség, az ammónium és a zavarosság tekintetében. Emellett nyitás-, mozgásérzékelők és felügyeleti rendszerek biztosítják a szabotázs elkerülését. A mikrobiológiai vizsgálatok végzésére munkaállomások állnak rendelkezésre, amelyek alkalmasak a fertőzések korai felismerésére, azonban a technológia fejlődik, így nap mint nap jelennek meg újabb és újabb gyorstesztek, amelyek mobilapplikációk segítségével képesek lennének azonnal felismerni és kiértékelni egy esetleges fertőzés létrejöttét [4].

Az élelmiszerminőség és -biztonság monitorozórendszerei

Az élelmiszerbiztonságot érintő globális problémák fokozódásával szükségessé vált védelmi, megfigyelő-, jelző- és monitorozórendszerek igénybevétele, amelyekkel gyorsan és hatékonyan felismerhetők a termék biztonságosságának kockázatai. Jelenleg ezek az elektronikus és mechanikus rendszerek azok, amelyek figyelemmel kísérik a termék állapotát az ellátási láncon keresztül. Fontos védvonal a csomagolás, aminek funkciója a termék eltarthatóságának meghosszabbítása, a tápérték megőrzése és a romlás megakadályozása.

Jane Ru Choi és társai tudományos kutatásaik alapján rávilágítottak, hogy a jelenleg alkalmazott analitikai módszerek, mint a HPLC,[5] a GC,[6] a PCR[7] vagy az ELISA[8] időigényesek, ezáltal kevésbé hatékonyak az élelmiszerekből eredő és általuk okozott betegségek

[5] High Pressure Liquid Chromatography – Nagy hatékonyságú folyadékkromatográf.
[6] Gas Chromatography – Gázkromatográf.
[7] Polymerase Chain Reaction – Polimeráz láncreakció.
[8] The Enzyme-Linked Immunosorbent Assay.

korai felismerésére. Ahhoz, hogy gyorsan meg tudjuk határozni, hogy az élelmiszer minőségileg és a biztonságosság szempontjából megfelelő-e, szükséges POC[9]-eszközök alkalmazása. Ezáltal a csomagoláson papír- és chipalapú jelerősítő technikákat alkalmaznak, amelyeket okostelefon-alapú olvasókkal egyesítenek. A papíralapú eszközök eredményessége a kolorimetriás[10] kimutatáson alapul, amely során a tesztcsík az arany nanorészecskék színváltozása révén alkalmas az élelmiszer-szennyeződések és akár egy szabotázs korai azonosítására (kórokozók, vegyi anyagok, élelmiszer-hamisítás). A papíralapú eszközök processzorból, optikai érzékelőből, WIFI-adapterből, újratölthető elemekből és kijelzőből állnak, amelyekhez okostelefon-applikációk szolgáltatják az eredményeket kolorimetriás jelek segítségével. A kolorimetriás kimutatás mellett, a fluoreszcens[11] alapú tesztcsík, a fluoreszcens jeleket, egy miniatürizált fluoreszcens detektorhoz csatlakoztatott iPhone alkalmazás segítségével, képes a pixelintenzitást elemezni, amely a csomagoláson keresztül a baromfiban lévő Salmonella typhimurium[12] kimutatására szolgál. A papíralapú elektrokémiai detektálás alkalmas a sörökben lévő etanol kimutatására nanokompozit segítségével. A chipalapú eszközök lehetővé teszik a kis mennyiségű minták kezelését is. Chipalapú ELISA[13]-ba építettek be nemesfém nanorészecskét, egy ezüstfokozó technikát, amely alkalmas a kukoricában lévő aflatoxin B1 detektálására. Az aflatoxin B1, Aspergillus gombák által termelt mikotoxin, ami megtalálható a mogyoróban, kukoricában, fűszerpaprikában stb. Mérgezés esetén szívgyulladást és májbetegséget okoz. A chipalapú fluoreszcens módszer mellett léteznek elektrokémiai detektálási módszerek, ahol a chip egy elektródából áll és például az E. coli baktérium kimutatását segíti, azonban ezek legnagyobb kihívása a korlátozott funkcionalitás. Tárgyalják, hogy a kulcsfontosságú feldolgozási lépések, köztük a mintavétel, a minta-előkészítés és -detektálás integrálása egy eszközbe továbbra is kihívást jelent a fejlesztők számára. A szerzők javasolják, hogy a jövőben a minták elválasztási technikáit is építsék be a chipekbe [5].

Fatima Mustafa és Silvana Andreescu kísérletének eredménye szerint, a napjainkban alkalmazott hagyományos csomagolási technikák mellett, amelyek alkalmasak a nedvesség- és szagelnyelésre, illetve az antimikrobiális növekedésgátlásra, zsíroxidáció csökkentésére, megjelentek az intelligens csomagolási módszerek is. Intelligens csomagolási módszerek lehetnek frissesség- és nedvességjelzők és az ütésjelzők is. Összefoglalják az intelligens csomagolási technológiákat, köztük a TTI-szenzort,[14] amely a csomagolóanyag külsején elhelyezve, színváltozással megmutatja az expozíció idejét a nem megfelelő tárolási hőmérséklet függvényében. A CoolVu indikátor egy fémből álló címke, amely jelzi a minőségváltozást, hogy minőségromlás nélkül felhasználható-e még a termék vagy sem. Léteznek rádiófrekvenciás (RFID) rendszerek, amelyek az Escherichia coli és a Salmonella-jelenlétet azonosítják a csomagolt élelmiszerekben, immobilizált antitoxinok segítségével. A gyümölcsök érettségének meghatározására

[9] Power over Coaxial.
[10] Fényelnyelésmérésen és az oldatok színének összehasonlításán alapuló módszer.
[11] Az elnyelt fény egy részét kisebb energiájú, más színű fényként visszasugározzák az egyes anyagok, hőkibocsátás mellett.
[12] Hastífusz kórokozója. A vékony és vastagbélben fekélyek alakulnak ki, influenzaszerű tünetekkel, valamint súlyos esetben szív- és idegrendszeri károsodással.
[13] Antigén-antitest-kölcsönhatáson alapuló laboratóriumi módszer.
[14] Time-Temperature Indicators – Idő-hőmérséklet-indikátor.

alkalmas a RipeSense érettségi mutató. A csomagolásra helyezett címke színváltozást eredményez az érettségi foknak megfelelően. A csomagoláson alkalmazott PH-mutatók az illékony aminoknak köszönhetően színváltozást eredményeznek, amelyek a romlott hús és hal kiszűrésére alkalmasak. A glutén kimutatására, ami napjainkban tömeges megbetegedést okoz, elektronikus érzékelőt fejlesztettek ki, az FGT[15]-t, amely képes a glutén mennyiségi meghatározására. A LactoSens-szel a laktóz azonosítása nemcsak a tejben és tejtermékekben, hanem akár a kávé- és csokoládétermékekben is lehetséges. Emellett kitérnek arra, hogy a jelenlegi bioszenzorok fejlesztései még nincsenek teljesen kiforrva, ugyanis minta-előkezelést igényelnek, így a jövőben a kimutatási határ csökkentésére és a minták egyszerűsítésére kell koncentrálni [6].

A számítástechnika fejlődése az élelmiszeripar tevékenységét is befolyásolta. A mobiltelefon-alapú alkalmazások alkalmasak élelmiszerminőség és -biztonság ellenőrzésére. Az IoT,[16] vezeték nélkül vagy kábeles kapcsolat által képes együttműködni tárgyakkal, dolgokkal, miközben szolgáltatásokat, alkalmazásokat hoz létre. A cél, hogy bárhol, bármikor lehessen tárgyakhoz kapcsolódni és információhoz hozzáférést biztosítani a vezetékes és vezeték nélküli szélessávú kapcsolatok segítségével. A felhőalapú technológia képes az intelligens dolgok összekapcsolásával széles körű adatokat tárolni a szolgáltató hálózatán, ezáltal különböző szolgáltatásokat létrehozni. Alexandru Popa és társai vákuum által szárított hagymaszeleteket hasonlítottak össze a hagyományos szárításhoz képest, érzékelők segítségével. Az érzékelők a légkör tartalmát, a lebomló hagymából kibocsátott gázok koncentrációját mérik. A gázérzékelők a VOC[17]-okkal reagálnak, majd feszültségjelet adnak ki, amely elemezhető adatokat generál. Az adatok alapján megállapították, hogy a vákuum alatt szárított hagymaszeletek hosszabb ideig eltarthatók a hagyományos szárításhoz képest. A jövőben hűtött vákuumcsomagolt élelmiszereken is tesztelik a rendszert, amely mobiltelefonnal elérhető lesz, így biztosítja és egyszerűsíti a fogyasztó számára az élelmiszer állapotának ellenőrzését [7].

Az első dolog, amit figyelembe vesz a fogyasztó egy élelmiszeren, az a termék külseje. A termék színét befolyásolja a tárolási hőmérséklet, a páratartalom, a biokémiai változások, és a feldolgozás módszerei. Azonban a mikrobiológiai kockázatokkal és kémiai kockázatokkal nem számol a fogyasztó. A mikrobiológiai kockázatok, amelyek a különböző vírusok, baktériumok, mikotoxinok, paraziták által előidézett súlyos egészségkárosodások okozói lehetnek. Az intelligens csomagolások során alkalmazott nanotechnológiai eljárások alapanyagai a nanokompozit anyagok, amelyek nemkívánatos fizikai és kémiai tulajdonságokat eredményezhetnek, köztük az oldhatóságot vagy toxicitást. A szerző, Vivek és munkatársainak kutatási eredményei megerősítik, hogy nagy kihívás ez az innovátorok számára, mivel ezeket az anyagokat úgy kell elkészíteni, hogy ehetők legyenek, illetve ne tartalmazzanak toxikus oldható részeket, emellett a termék fizikai, kémiai tulajdonságait se befolyásolják. Ilyen anyag lehet például a titán-dioxid, amelyet fotokatalitikus fertőtlenítőanyagként felhasználva, a patogén baktériumok elpusztítását eredményezve alkalmaztak, amely engedélyezett

[15] Floating-Gate Transistor – Lebegőkapu tranzisztor.
[16] Internet of Things –Tárgyak internete.
[17] Illékony szerves vegyületek.

az élelmiszeripari felhasználás során. A közelmúltban a WHO[18] létrehozott egy FOSCOLLAB nevezetű dashboardot, ami képes megjeleníteni a kémiai anyagokat és azok kockázatait, amelyek hozzájárulnak a könnyebb adatelemzéshez, elősegítve veszélyhelyzetben az intézkedések korai meghozatalát. Következtetésképpen ismertetik, hogy a nanoanyagok felhasználásával a jövőben számos potenciális kockázatot és toxicitási problémát fognak feltárni, amelyeket kezelni szükséges [8].

Szabotázs felderítése és megakadályozása az élelmiszer-ellátásban

Az elmúlt években több olyan esemény történt, amely okot ad arra következtetni, hogy mélyebben foglalkozni kell a szabotázs korai felismerésével az élelmiszer-ellátásban, ezzel megakadályozva a fogyasztó egészségkárosodásának kialakulását.

A fenyegetés típusai között kiemelt jelentőségű az élelmiszerhamisítás. 2014-ben Kenyában, egy tejüzem formalin és hidrogén-peroxid hozzáadásával próbálta meg tartósítani a tejet, ezzel meghosszabbítva a termék fogyaszthatósági idejét. 2016-ban Nigériában műanyagból készült rizst foglaltak le a hatóságok. 2017-ben hamis olívaolaj került Olaszországból az Amerikai Egyesült Államokba. Szándékos szennyezés kapcsán 2005-ben Nagy-Britanniában a kenyérben üvegdarabokat és varrótűket találtak. 2016-ban az FBI[19] és a US Department of Agriculture[20] figyelmeztette a gazdákat a kibertámadásokra, köztük a kémkedésre és a hackelésre, amely veszélyeztette a precíziós mezőgazdasági technológiákat. A támadások megelőzéséhez ismerni kell a potenciális és a felmerülő kockázatokat, emellett meg kell érteni a támadót és motivációját, valamint meg kell vizsgálni, hogy van-e lehetősége a támadás végrehajtására és arra, hogy az milyen módszerekkel akadályozható meg. A TACCP[21] alkalmas az élelmiszeripar szélesebb körű kockázatainak értékelésére és kezelésére. A célja, hogy csökkentse a szándékos támadások valószínűségét, a következmények hatásait, védje az élelmiszert és a fogyasztót. A végrehajtásához csapatmunka szükséges, ahol azonosítják a támadót, a módszert, amely veszélyt jelent a termékre és a fogyasztóra, emellett azonosítják a sérülékeny pontokat és azt, hogy hogyan akadályozható meg egy esetleges támadás. A fenyegetés valószínűsége alapján priorizálják a kockázatokat, amelyek veszélyt jelenthetnek a termékre, a fogyasztóra, az objektumra, a vállalatra és a szervezet információs rendszerére is.

A kockázatok csökkentéséhez különböző kritériumokat kell megvizsgálni, mint például a hozzáférési pontok elérhetősége, a szállítási útvonalak, a látogatók összetétele, kamerarendszerhez való hozzáférés stb. A BSI[22] 4 esettanulmányon keresztül mutatja be a TACCP-eljárást, a kockázatértékelési gyakorlatot és annak működtetését. A szabvány célja, hogy az élelmiszeripari vállalkozások számára összefoglalja az ellátási láncok védelmi képességét, a támadási formákat, és a sikeres támadás esetében a következmények csökkentését [9].

[18] World Health Organization.
[19] The Federal Bureau of Investigation.
[20] Egyesült Államok Mezőgazdasági Minisztériuma.
[21] Threat Assessment Critical Control Point – Veszélyértékelés Kritikus Szabályozási Pont.
[22] The British Standards Institution.

Mindez hozzájárul a szabotázs korai felismeréséhez, annak megelőzéséhez és megakadályozásához.

Élelmiszervédelem

A terroristacselekmények megelőzése különböző módszerekkel foganatosítható. A korábbiakban, az egymással szemben álló felek hadászati tevékenysége abban nyilvánult meg, hogy olyan katonai stratégiákkal próbálták elpusztítani az ellenséges felet, mint az állatállomány, a termés megmérgezése és elpusztítása, valamint a kutak és élelmiszerek szennyezése [10].

Ma Magyarországon fennálló probléma az átcímkézés, a fogyaszthatósági és a minőségmegőrzési idő lejártát követően az alapanyagok felhasználása. Szeitzné és munkatársainak a következtetései kiterjednek az élelmiszervédelemre, céljuk, hogy az élelmiszergyártók felelősségteljes odafigyeléssel kezeljék a szándékos károkozás kockázatát és a fenyegetettség mértékét, amellyel a mindennapokban számolni kell. A nemzetközi irodalmakban publikált élelmiszer-biztonság tapasztalatait és gyakorlatait összegzik, céljuk az, hogy ezáltal a hazai gyakorlatban történő megvalósítást segítsék. Megállapításaik kiterjednek a hatékony védelem 10 + 1 aranyszabályára, köztük az élelmiszervédelmi terv készítésére, a beszállítók megbízhatóságára, a beléptetés és az üzemben történő mozgás mivoltára, a csomagolás alkalmazására, a gyanús események kivizsgálására, a válsághelyzeti intézkedési terv gyakorlatára. Kiemelt figyelmet fordítanak a megelőzés lehetőségeinek összefoglalására, ahol a legfontosabbnak a védelmet tituálják. A hatékony védelemhez elengedhetetlen, hogy a gyanús, szokatlan helyzeteket kivizsgáljuk, és azokat dokumentáljuk, valamint a válságkezelési tervnek megfelelően, szabotázs, terrorcselekmény elhárításához együttműködjünk a helyi rendvédelmi szervekkel. Emellett figyelmet kell fordítani a dolgozók szokatlan viselkedésére, a lehetséges rejtekhelyek felderítésére, az informatikai hálózat biztonságosságára. A fizikai védelem megőrzéséhez a be- és kilépési pontokat szabályozni és csökkenteni kell, ugyanakkor fontos, hogy a dolgozók és látogatók csak azonosítás után léphessenek be az objektum területére, mi több, a különösen veszélyeztetett területre történő belépés korlátozottan legyen engedélyezett [11].

Az élelmiszervédelem a gyártón kívül kiterjed az élelmiszer-kereskedelemre is, ahol szintén fontos a forgalmazók körében felmerülő kockázatok kezelése és elhárítása. Kasza és munkatársai értelmezésében a kríziskezelés a bekövetkezett káreseményre fókuszál, szintúgy, mint a helyreállító folyamatokra, a kockázatbecslésre és a -megelőzésre. Hangsúlyt fektetnek a krízismenedzsment-kézikönyv létrehozására, és annak professzionális tagolására, amelynek kidolgozása egy nem kívánt esemény bekövetkezésének megelőzését eredményezheti. Ezáltal súlyosság szerint osztályozzák az incidenseket, majd az egyszerűbb beavatkozás érdekében intézkedési tervben foglalják össze a feladatokat [11].

Az FDA[23] Élelmiszerbiztonsági és Alkalmazott Táplálkozási Központjának 2019. márciusi útmutató-tervezetében összegezték az élelmiszervédelmi tervet és annak

[23] U.S. Food and Drug Administration.

komponenseit, sebezhetőségi értékeléseit, enyhítési stratégiáit és a korrekciós intézkedéseket. Felhívják a figyelmet a biztonsági rések és azok értékelésének fontosságára, amelyek lehetnek például az ömlesztett folyadék ki- és betöltése, a tárolótartályok, silók biztonságossága, a gyártás során a különböző eljárások, mint a hűtés, keverés, homogenizálás, őrlés, töltés. A sebezhetőséget 3 szempont szerint értékelik, az első, hogy a szennyezőanyag hozzáadásával lehetséges-e közegészségügyi hatás kialakulása, a második a fizikai hozzáférhetőség mértéke, a harmadik pedig a támadó képességének eredményessége. Kiemelt jelentőségű a belső támadás, mivel az elkövető, legyen az állandó dolgozó, szezonális munkás, beszállító vagy karbantartó, aki jogosult hozzáférni a termékhez, objektumhoz, mert ezáltal felmerül a szándékos hamisítás lehetősége. A termelőterület kialakítása is meghatározó lehet, például az automatizálás hiánya. Azonban egy zárt csőrendszer vagy egy pneumatikus szállítószalag esetében minimális a kontamináció kialakulása. A termék hozzáférhetőségének minimalizálása, belső támadás esetén, megvalósulhat személyzeti és műveleti alapú csökkentési stratégiával, mint például a kamerarendszer, a fizikai korlátozás, például zárak. A technológiai mérséklési stratégiák között megjelenik a rádiófrekvenciás azonosítókártya, az ujjlenyomat-olvasó, ezáltal csak engedéllyel rendelkező személy léphet egy adott területre, vagy használhatja a védett berendezést, például a be- és kirakodó tömlőt, automatizált számítógépet. A támadóképesség csökkentésére alkalmazott személyzeti és műveleti alapú minimalizálási stratégia, a megfelelő látóvonalak kialakítása, a látogatók azonosítása (beszállító, karbantartó, járművezető), a technológiai mérséklési stratégia, a CCTV,[24] a riasztóberendezések, amelyek figyelmeztetik a biztonsági szolgálatot abban az esetben, ha olyan tartályt nyitnak ki, amely a gyártás során nem megszokott [12].

Az élelmiszer-védelemben azonban a monitorozás nemcsak a védelmi, a megfigyelő-, a monitorozórendszerek alkalmazására terjed ki, hanem magában foglalja a fent nevezett stratégiák nyomonkövetési eljárásait, minőségi, biztonsági, karbantartási eljárásokat, valamint a fizikai védelmi rendszereket, amelyek mind a közegészségügyi hatás kialakulási valószínűségének megakadályozását eredményezik, növelve a biztonságtechnika szakszerűségét. Berek és Horváth kutatási eredményei tükrözik, hogy üzemelő ipari objektumok felújítása közben is felmerülnek új környezeti biztonsági kockázatok. Az objektum- és termékvédelem szempontjából, egy rendszert, egy beruházás alatt, majd azt követően is úgy lehet megfelelően működtetni, ha állapotfelmérést, kockázatelemzést, majd kockázatértékelést végzünk. Az eredményes adatelemzéshez szükséges a kvalitatív és a kvantitatív módszerekkel is megvizsgálni a kockázatokat. Ezt követően fogalmazható meg javaslat az esetleges hibák és kockázatok megelőzésére és elhárítására. A fizikai védelmi rendszerek, mint az élőerős védelem az egyik kulcsfontosságú pontja az élelmiszer-védelemnek. Általuk biztosított a be- és kiléptetés rendje, a gépkocsik átvizsgálása, a belépési pontok és a teljes területet lefedő CCTV-rendszer felügyelete. Azonban már itt felléphetnek a lehetséges biztonsági kockázatok, mint az élőerő tájékozatlansága, szakmai folyamatok és eszközök ismereteinek hiánya. A mechanikai és elektronikai védelem kiépítéséhez és működtetéséhez meg kell állapítani a veszélyeket, azok forrásait, és meg kell

[24] Biztonsági kamera-, megfigyelőrendszer.

határozni a védelem tárgyát, ezáltal üzemeltethetők hatékonyan a védelem rendszerei. A biztonság megőrzéséhez szükséges mind az élőerős védelem, mind a biztonsági-menedzsment-stratégiák és megoldások, mind a fizikai biztonság [13]. Ahogy Kiss Sándor megfogalmazásában megjelenik „a biztonságtechnika különféle objektumok és rendszerek biztonságának növelése, az embert érő káros hatások és a vagyoni kár kockázatának csökkentése, igénybe véve ehhez műszaki, szervezési, egészségügyi, gazdasági intézkedéseket és eszközöket" [14: 25.].

Gyógyszeripari termékek biztonsági kérdései

Az étrend-kiegészítő előállítása választóvonal az élelmiszer- és a gyógyszergyártás között. Ugyanis a 37/2004. (IV. 26.) ESzCsM rendelet az étrend-kiegészítőkről értelmében, az étrend-kiegészítőt élelmiszernek minősítjük, mivel a hagyományos étrend kiegészítését szolgálja, a koncentrált tápanyag-, és élettani hatásokat kedvezően befolyásoló tulajdonságaival [15]. Azonban a csomagolástechnológiáját tekintve granulátum, tabletta, kapszula, ampulla formában értékesítik, amelyek a gyógyszergyártás technológiájának elemei. A granulátumot használják fel a technológiai folyamat közben a tabletta készítésére vagy kapszula töltésére [16]. Dévay megfogalmazásában: „A tabletták préseléssel előállított, meghatározott mennyiségű, egyszeri vagy többszöri hatóanyag-adagot tartalmazó szilárd gyógyszerkészítmények" [17: 427.]. A szerző a kapszulát perorálisan,[25] rektálisan[26] vagy vaginálisan[27] alkalmazandó gyógyszerkészítményként nevesíti, amelynek anyaga zselatin vagy keményítő. Az aszeptikus gyógyszerkészítés alkalmával állítják elő az ampullákat, amelyek injekciós oldatokat tartalmaznak. A jelenleg magyarországi forgalomban lévő ilyen jellegű étrend-kiegészítő termékek a B-vitamin-komplexek, a gyümölcskivonatot tartalmazó készítmények, prebiotikus rostokat tartalmazó készítmények, amelyeket ampullaformában adnak el [16].

Az 1333/2008/EK rendelet I. melléklete az élelmiszerekben található élelmiszer-adalékanyagok funkcionális csoportjaként említi a zselatint és a keményítőt, mint zselésítőanyag és mint módosított keményítő. Az 1333/2008/EK rendelet az élelmiszer-adalékanyagokról 3. cikk (2) bekezdés a) pontja értelmében azonban élelmiszer-adalékanyag az, amit önmagukban nem fogyasztunk, de a gyártás során a technológiai célból való hozzáadása azt eredményezi, hogy önmaga vagy származéka az élelmiszer összetevőjévé válik. Ebben a pontban azonban a rendelet kitér arra, hogy nem minősül élelmiszer-adalékanyagnak a (2) bekezdés a) pontja értelmében az étkezési zselatin és a savasan vagy alkalikusan módosított keményítő. Az ellentmondás miatt a jövőben rendeletmódosításra lesz szükség [18].

A 178/2002/EK rendelet nem minősíti élelmiszernek a gyógyszert, mivel a gyógyszer a 2001/83/EK rendelet az emberi felhasználásra szánt gyógyszerek közösségi kódexéről értelmében, emberi megbetegedések kezelésére vagy megelőzésére szolgál. Az élelmiszer

[25] Szájon át szedhető.
[26] Végbélen keresztül.
[27] Hüvelyen keresztül.

viszont feldolgozott, részben feldolgozott vagy feldolgozatlan anyag vagy termék, amelyet emberi fogyasztásra szánnak, vagy várhatóan emberek fogyasztanak el [19], [20].

Felmerül a kérdés, hogy az étrend-kiegészítő tabletta-, kapszula-, ampullaformában, mint feldolgozott anyag és termék, amelyet emberi fogyasztásra szánnak, mely definíció kérdésköre alá tartozik? Illetve megfogalmazódik az is, hogy a gyártástechnológiák és folyamatok közben fellépő fizikai, kémiai, mikrobiológiai kockázatok között is ekkora az átfedés vagy vannak különbségek, amelyeket eddig nem tártak fel, illetve nem bizonyítottak és veszélyeztethetik a fogyasztót, a termék minőségét és biztonságát.

Következtetések

Az aktuális kutatási eredmények áttanulmányozásával széles körű ismeretekre tettem szert a tárgykör vonatkozásában. Ezáltal arra a következtetésre jutottam, hogy a szerzők átfogóan vizsgálják az élelmiszerbiztonsági rendszerek megbízhatóságát, az élelmiszeripari termékek biztonságosságát. A nemzetközi irodalmak összefoglalásai is bemutatják, hogy a jelenlegi élelmiszerbiztonsági rendszerek nem minden esetben kellő hatékonyságúak. A technológia fejlődésével újabb és újabb módszereket dolgoznak ki annak érdekében, hogy megőrizzék a termékbiztonságot, megakadályozzák a fizikai, kémiai, mikrobiológiai kockázatok bekövetkezését, a szabotázs kialakulását, valamint, hogy a korábban kialakult, élelmiszerek által okozott megbetegedések a jövőben ne ismétlődhessenek meg. Az IoT-rendszerek fejlődésének köszönhetően, a jövőben is fontos az élelmiszervédelmi rendszerek korszerűsítése, amivel nemcsak fenntartható a biztonságosság, hanem növelhető az élelmiszerbiztonsági rendszerek hatékonysága. Ehhez ismerni kell az aktuális kutatási eredményeket, a téma időszerűségeit és innovációit, illetve az újonnan felmerülő technológiai megoldásokat ki kell terjeszteni az élelmiszerellátási láncra is.

Az étrend-kiegészítők szabályozásai ellentmondásosak. Az 1333/2008/EK rendelet az élelmiszer-adalékanyagokról I. melléklete és a 3. cikk (2) bekezdés a) pontja eltérően definiálja az élelmiszer-adalékanyagok fogalmát. Ezáltal javaslom a jövőben rendeletmódosítás megvalósítását, ahhoz, hogy a szabályozás és annak betartása, valamint betartatása is egységessé váljon.

A 178/2002/EK rendelet értelmében, élelmiszer minden olyan anyag vagy termék, amelyet feldolgozatlanul, részben feldolgozva vagy feldolgozott állapotban emberi fogyasztásra szánnak, vagy várhatóan emberek fogyasztanak el. Véleményem szerint, ebben a megfogalmazásban ebbe a kategóriába tartozhatnak a gyógyszerek is, azzal a kiegészítéssel, hogy azok emberi betegségek kezelésére vagy megelőzésére is szolgálnak.

A szabályozások megfogalmazásai országonként eltérőek, azonban az irányelvek azok, amelyekre épülnek az európai nemzetek törvényei, rendeletei, jogszabályai, ezáltal a definíciók kulcsfontosságúak ahhoz, hogy azok megfelelően alkalmazhatók és betarthatók legyenek.

Hivatkozások

[1] K. Szász, „Állategészségügy – Élelmiszer-feldolgozás," in *Magyarország a XX. században,* I. Kollega Tarsoly, szerk., Szekszárd: Babits Kiadó, II. kötet VII. fejezet, II-467., 1996–2000. [Online]. Elérhető: http://mek.niif.hu/02100/02185/html/292.html (Letöltve: 2019. 04. 14.)

[2] G. Bíró, „Élelmiszer-higiénia története és feladatköre," in *Élelmiszer-higiénia,* Budapest: Agroinform Kiadó, 2014. [Online]. Elérhető: www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_533_ElelmiszerHigienia/index.html (Letöltve: 2019. 04. 04.)

[3] L. Berek, T. Berek és L. Berek, „A biztonság, az őrzés és a védelem, valamint a biztonságtechnika értelmezése", in *Személy- és vagyonbiztonság,* Budapest: Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Óbudai Egyetem, ÓE-BGK-3071, 2016, pp. 4–19.

[4] L. I. Rácz és T. Berek, „Vízbázis, mint nemzeti létfontosságú rendszerelem védelme," *Hadmérnök,* 8. évf. 2. sz., 2013., pp. 120–133. [Online]. Elérhető: www.hadmernok.hu/132_11_berekt_rli.pdf (Letöltve: 2019. 05. 11.)

[5] J. R. Choi, K. W. Yong, J. Y. Choi and A. C. Cowie, "Emerging Point-of-care Technologies for Food Safety Analysis," *Waste Coffee Ground Biochar: A Material for Humidity Sensors, Sensors,* vol. 19, no. 4, pp. 1–31, 17 February 2019. DOI: https://doi.org/10.3390/s19040817

[6] F. Mustafa and S. Andreescu, "Chemical and Biological Sensors for Food-Quality Monitoring and Smart Packaging," *Foods,* vol. 7, no. 10, pp. 1–20, 16 October 2018. DOI: https://doi.org/10.3390/foods7100168

[7] A. Popa, M. Hnatiuc, M. Paun, O. Geman, D. J. Hemanth, D. Dorcea, L. H. Son and S. Ghita, "An Intelligent IoT-Based Food Quality Monitoring Approach Using Low-Cost Sensors," *Symmetry,* vol. 11, no. 3, pp. 1–18, 13 March 2019. DOI: https://doi.org/10.3390/sym11030374

[8] V. K. Bajpai, M. Kamle, S. Shukla, D. K. Mahato, P. Chandra, S. K. Hwang, P. Kumar, Y. S. Huh and Y-K. Han, "Prospects of using nanotechnology for food preservation, safety, and security," *Journal of Food and Drug Analysis,* vol. 26, no. 4, pp. 1201–1214, October 2018. DOI: https://doi.org/10.1016/j.jfda.2018.06.011

[9] The British Standards Institution, "PAS 96:2017 – Guide to protecting and defending food and drink from deliberate attack," November 2017. [Online]. Elérhető: www.food.gov.uk/sites/default/files/media/document/pas962017.pdf (Letöltve: 2019. 04. 30.)

[10] S. M. Szeitzné, J. Cseh, I. Ficzere és A. Hámos, *Élelmiszervédelmi útmutató vállalkozásoknak A Magyar Élelmiszer-biztonsági Hivatal javaslatai élelmiszereink védelme, egészségünk, valamint a vállalkozások jó hírnevének megőrzése érdekében.* Budapest: Agroinform Kiadó és Nyomda, 2010.

[11] G. Kasza, J. Surányi, Z. Lakner, B. Bódi, F. Deák, G. Faludi, A. Horváth, L. Mészáros, A. Szántó és I. Danczák, „Rendkívüli helyzetek és kezelésük az élelmiszer- kereskedelemben – irányelvek és tapasztalatok," *Élelmiszervizsgálati Közlemények,* 68. évf. 3–4. füzet, 2012., pp. 101–117.

[12] U.S. Department of Health and Human Services Food and Drug Administration Center for Food Safety and Applied Nutrition, "Mitigation Strategies to Protect Food Against Intentional Adulteration: Guidance for Industry – Revised Draft Guidance," March 2019. [Online]. Elérhető: www.fda.gov/media/113684/download (Letöltve: 2019. 05. 05.)
[13] T. Berek és T. Horváth, „Fizikai védelmi rendszerek dinamikusan változó környezetben," *Hadmérnök,* 9. évf. 2. sz., pp. 16–24., 2014.
[14] S. Kiss, „A biztonságtechnika kialakulásának történetéről," *Hadmérnök,* 10. évf. 4. sz., p. 25., 2015.
[15] 37/2004. (IV. 26.) ESzCsM rendelet az étrend-kiegészítőkről
[16] A. Dévay, *A gyógyszertechnológia alapjai.* Pécs: Pécsi Tudományegyetem Gyógyszertechnológiai és Biofarmáciai Intézet, 2013., pp. 1–159.
[17] A. Dévay, „Tablettázás," in *A gyógyszertechnológia alapjai,* Pécs: Pécsi Tudományegyetem Gyógyszertechnológiai és Biofarmáciai Intézet, 2013., p. 427.
[18] 1333/2008/EK rendelete az élelmiszer-adalékanyagokról
[19] 178/2002/EK európai parlamenti és tanácsi rendelete az élelmiszerjog általános elveiről és követelményeiről, az Európai Élelmiszerbiztonsági Hatóság létrehozásáról és az élelmiszerbiztonságra vonatkozó eljárások megállapításáról
[20] 2001/83/EK európai parlamenti és tanácsi irányelve az emberi felhasználásra szánt gyógyszerek közösségi kódexéről

HADMÉRNÖK
BIZTONSÁGTECHNIKA

15. évfolyam (2020) 1. szám 19–29.
DOI: 10.32567/hm.2020.1.2

Zólyomi Zsolt[1]

A biztonság és a biztonságmenedzsment vizsgálata vállalati nézőpontból

Inspection of Security and Security Management from a Company Point of View

Mi a biztonság, mit értünk alatta, amikor szóba hozzuk, megfogalmazzuk? Mit értünk ma Magyarországon vállalati biztonságmenedzsment alatt, valamint milyen fejlettségi szintre pozícionálhatjuk napjainkban a nemzetközi biztonságmenedzsment jelenlegi vezető tudományos, szakmai iránymutatásaihoz viszonyítva?
A hazai szakirodalomban többféle, többrétegű és a biztonságot különbözőképpen értelmező meghatározásokkal találkozhatunk, ezek összefoglalása nem célja az értekezésnek, sokkal inkább annak az iránynak a felvázolása, ami a legközelebb áll a vállalati biztonságmenedzsmenthez.
A biztonság megszervezéséről született szakvélemények, akár egy objektum esetében, akár egy rendszer felépítéséről értekeznek, a vagyonvédelmet egy piramisformával ábrázolják. Ezt a piramist általában három részre osztják fel, mechanikai, elektronikus és élőerős védelemre.
Ezzel szemben én egy átfogóbb, komplex megközelítést javaslok, ami véleményem szerint jobban lefedi a biztonsági rendszert. Kiemelem a biztonságmenedzsment elengedhetetlen és vezető szerepét. A biztonságmenedzsment a biztonsági rendszer vezető része/eleme, amely megtervezi, létrehozza, működteti és folyamatosan tökéletesíti a teljes biztonsági vagy védelmi rendszert, ami nélkül nem beszélhetünk megfelelő, hatékony védelemről.

Kulcsszavak: **biztonság, biztonságmenedzsment, védelem, mechanikai, elektronikus, élőerős, komplex biztonságmenedzsment**

What is security, what does it mean when we talk about it and formulate it? What do we mean by corporate security management in Hungary today, and what level of development can we position today in relation to the current leading scientific and professional guidelines of international security management?

[1] Flex, biztonsági főigazgató, Európa, Közel-Kelet, Afrika, e-mail: zszolyomi1@gmail.com, ORCID: https://orcid.org/0000-0002-2800-1430

In the Hungarian security literature we can find several, multi-layered and differently interpreted definitions, the summary of which is not the aim of the article, but rather to establish the direction that is closest to corporate security management. Experts on the setup of security system, either in the case of a single object or in the design of a system, depict security system as a pyramid. This pyramid is usually divided into three parts, mechanical, electronic and human guarding forces.
In contrast, I suggest a more comprehensive, complex approach, which in my opinion covers the security system more completely. I highlight the essential leading role of security management. Security management is the leading component of a security system that designs, creates, operates and continually improves a complete security or defence system, without which we cannot talk about adequate, effective protection.

Keywords: **security, security management, protection, mechanical, electronic, human guarding, complex security management**

A biztonság és annak értelmezése

Mi a biztonság, mit értünk alatta, amikor szóba hozzuk, megfogalmazzuk? A mai angol nyelvhasználatban a „security" a latin „securitas" (biztonság, gondtalanság, lelki nyugalom) [1] szó többlépcsős módosulásával került be. Ez az átvétel és átalakulás az 1100-as évek elejétől az 1400-as évek végéig tartott (Sikernesse, Sikerhede, Sikerte, majd Security) [2]. A magyar nyelvben a biztonság szó „biztonlét" jelentéssel került be az 1862-ben kiadott Czuczor Gergely féle szótárba [3], ahol még új szóként jelölik: „Divatba nem régen jött szó, a régi és helyesebb biztosság értelmében" [3: 680.]. A jelenleg is használatos magyar értelmező szótár szerint a biztonság jelentése a következő: „A dolgoknak, életviszonyoknak olyan rendje, olyan állapot, amelyben kellemetlen meglepetésnek, zavarnak, veszélynek nincs v. alig van lehetősége, amelyben ilyentől nem kell félni"[4].

A hazai szakirodalomban többféle, többrétegű és a biztonságot különbözőképpen értelmező meghatározásokkal találkozhatunk, ezek összefoglalása nem célja az értekezésnek, sokkal inkább annak az iránynak a felvázolása, ami a legközelebb áll a biztonságmenedzsmenthez.

Számomra a legjellemzőbb módon határozza meg a biztonság fogalmát: Dr. Berek Lajos, Dr. Berek Tamás és Berek László 2016-ban az Óbudai Egyetemen megjelent, *Személy és vagyonbiztonság* című kiadványa, amelynek az első fejezetében foglalkoznak a szerzők a biztonság fogalmának értelmezésével.

„A biztonság személyek és szervezetek azon állapota, melyet, a létüket, illetve rendeltetésszerű működésüket veszélyeztető szándékos jogellenes magatartások és az azokkal szemben alkalmazott védelmi erőforrások együtthatása határoz meg"[5: 6.].

Ezzel a megfogalmazással tudok a leginkább egyetérteni, hiszen, ha nagyon leegyszerűsítjük a biztonság értelmezését, akkor az veszélymentességet, a veszély, vagy a fenyegetettség hiányát jelenti, amit tökéletesen lefed a fenti definíció. Még a biztonság alapértelmezésén kívül szükségesnek tartom megemlíteni a biztonság fontosságát. A biztonságot Maslow piramisa [6] alapvető fontosságúnak tartja, mindjárt a második szinten említi a létszükségletek kielégítése után, vagyis a biztonságra

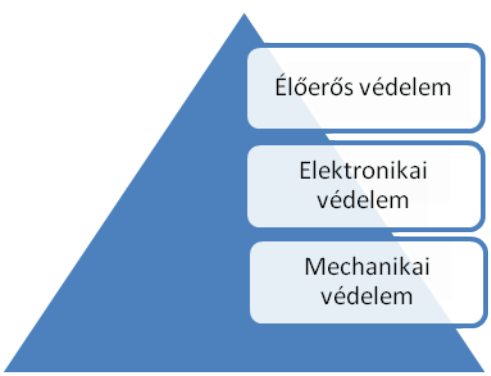
igény van, a biztonság az ember alapvető szükséglete. (Szükséglet: a bennünk támadt hiányérzet megnyilvánulása [saját megfogalmazás].)

Összefoglalhatjuk, hogy a biztonság olyan személy vagy szervezet állapota, amelynek léte és rendeltetése van. Ezt a létet, illetve rendeltetést veszélyeztetheti valami, amely veszély kivédésére és elhárítására az ember létrehozza, elkészíti a védelmet. Például a személy vagy szervezet értékeit, vagyonát veszélyeztetheti több tényező is, tűz, természeti vagy ember által okozott katasztrófa, támadás, lopás stb. A lopás példájánál maradva ezt a veszélyeztetést vagy más szóval kockázati tényezőt az ember úgy tudja elhárítani, ha védelmi berendezéseket telepít, őrséget szervez és működtet, kapcsolatban van a bűnüldöző hatóságokkal.

A fentiekből jól nyomon követhető, hogy értekezésemben nem a nagy egésszel, a mindenre kiterjedő általános biztonsági kérdésekkel, hanem annak egy szeletével, a multinacionális és/vagy nagyvállalatok, gazdálkodó szervezetek biztonságával kívánok foglalkozni.

„A biztonságot közvetlenül két tényező határozza meg. Az egyik a veszélyeztetés, azaz a szándékos jogellenes magatartások, melyek negatívan befolyásolják a biztonságot. A másik az alkalmazott védelmi erőforrások mennyisége és minősége. Minél több erőt és hatékonyabb őrzést és védelmet alkalmazunk, annál magasabb szintű lesz a biztonság. Ugyanis az alkalmazott védelmi erőforrások a szándékos jogellenes magatartásokkal szemben hatnak, azt akadályozzák, a legjobb esetben megakadályozzák" [6].

A biztonság megszervezéséről született szakvélemények, akár egy objektum esetében, akár egy rendszer felépítéséről értekeznek, a vagyonvédelmet egy piramisformával ábrázolják. Ezt a piramist általában három részre osztják fel, mechanikai, elektronikus és élőerős védelemre.

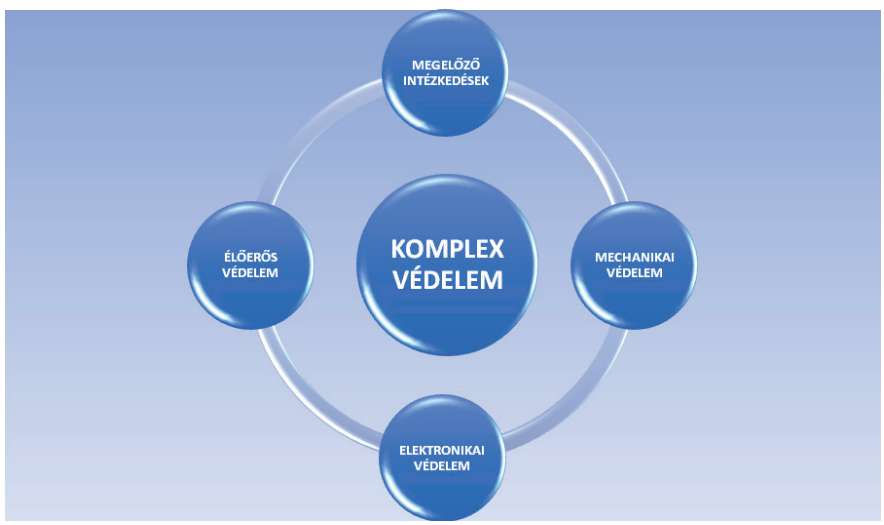


1. ábra
A vagyonvédelem [a szerző szerkesztése]

Ennek a háromszintű piramisnak a kibővített formáját használják sokan, hivatkozva Utassy Sándor *Komplex villamos rendszerek biztonságtechnikai kérdései* című doktori (PhD) értekezésére. Ebben a piramisban már megjelennek védelmi intézkedések, biztosítás és a kockázat is, de a biztonságmenedzsmentet senki sem említi [7].

2. ábra
Utassy-féle vagyonvédelem [17]

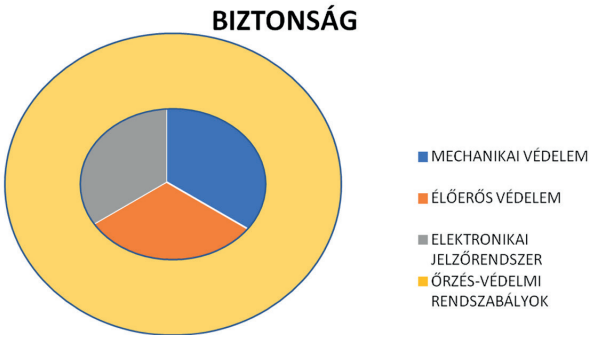
A kérdést az „integrált fizikai védelem" kialakítása szemszögéből megközelítő szemlélet [8] a komplex vagyonvédelem egymáshoz kapcsolódó összetevőiként azonosítja a mechanikai, az elektronikai, valamint az élőerős védelmet, amelyek együttese kiegészítve a megelőző intézkedésekkel csökkenti a kockázatok előfordulási valószínűségét és a bekövetkező események káros hatását [8].



3. ábra
A komplex vagyonvédelem főbb komponensei [8]

A fenti csoportosítás komponenseit egyenként vagy akár egyszerre is alkalmazhatják, azonban a magas szintű biztonság a fentiek összehangolt, optimális, arányos alkalmazásával érhető el, ez a komplex őrzés-védelem [9].

Az őrzés és védelem komplexitását vizsgáló szakemberek szerint ez az egyik meghatározó problémája a vagyonvédelemnek, ugyanis kapcsolatukat az alapján lehet vizsgálni, hogy melyik milyen mértékben járul hozzá a biztonsághoz, amit nehéz megállapítani [5].



4. ábra

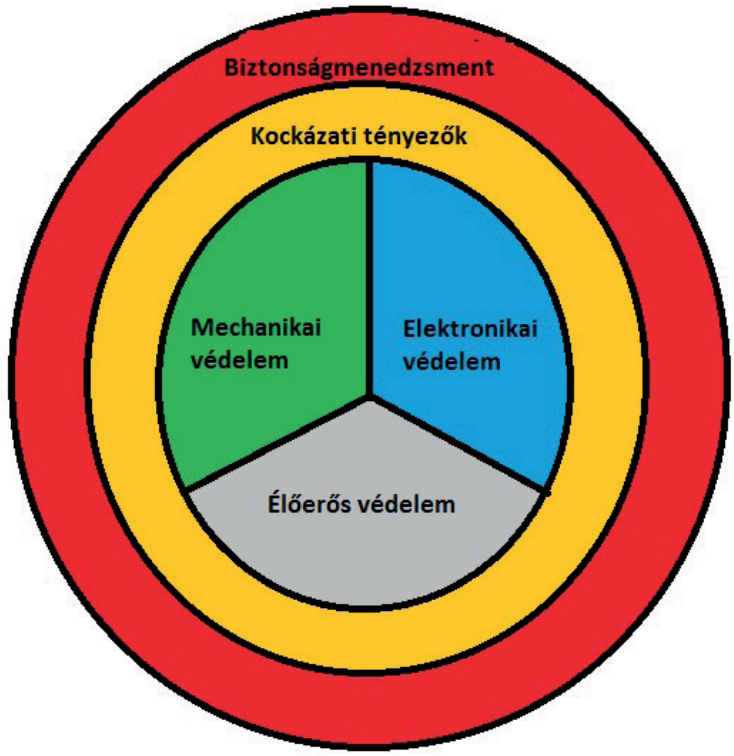
A védelmi erőforrások és az alkalmazott rendszabályok kapcsolata [9]

Ezek arányának kialakítását gondos tervezőmunka kell hogy megalapozza. A már üzemelő objektumok területén végzett átalakítások, kivitelezések azonban kihívások elé állítják a biztonsági szervezeteket, mivel kényszerűen változtatni szükséges a már kialakított arányokon. A kivitelezési munkák dinamikusan változó környezetet generálnak, a biztonsági kockázatok kezelésére a tervezői szakaszban kell felkészülni. Az alaprendeltetésének megfelelően a gazdasági társaság biztonsági szervezetének feladata, hogy működésével támogassa a szóban forgó társaság gazdasági érdekeinek megvalósulását [10].

Olyan speciális eset is előfordulhat, amikor a komplex védelmi rendszer üzemeltetését biztosító villamos hálózat hiánya korlátozza például az elektronikai alrendszer megfelelő arányának kialakítását [11].

A fentiek fényében egy gazdasági társaság biztonsági szervezetének szemszögéből vizsgálva a kérdést, én egy átfogóbb megközelítést javaslok, ami véleményem szerint jobban lefedi a biztonsági rendszert. A lenti grafikus ábrázolás (5. ábra) alapján látható, hogy a három fő elem a mechanikai, elektronikus és élőerős védelem van a centrumban, ahol azonos arányban szerepelnek, hiszen minden egyes szervezet/vállalat esetében annak sajátosságai, szükségletei alapján határozzák meg az arányait. Például egy hulladékgyűjtő állomás elektronikai védelmi rendszere nem hasonlítható egy IT-vállalat szerverfarmjának elektronikai védelmi rendszeréhez, vagy egy multinacionális óriásvállalat beléptető-rendszere sem említhető együtt egy körülbelül tízszemélyes iroda beléptetési rendszerével. Mindezekre a fő védelmi elemekre hatnak a kockázati tényezők, amelyeket számításba kell venni, ezek előzetes elemzésének eredményei alapján szükséges kialakítani a fő védelmi rendszereket. Ezt az egész rendszert pedig körbefonja a biztonságmenedzsment. A biztonságmenedzsment a biztonsági rendszer vezető része/eleme, amely megtervezi, létrehozza, működteti,

és folyamatosan tökéletesíti a teljes biztonsági vagy védelmi rendszert, ami nélkül nem beszélhetünk megfelelő, hatékony védelemről.



5. ábra
A biztonsági rendszer [a szerző szerkesztése]

A biztonságot befolyásolják közvetlen és közvetett tényezők, a közvetett tényezők, mint a jogi környezet, biztosítási intézményrendszer, gazdasági tényezők, közbiztonság, munkanélküliség stb. [5: 6.]. A közvetlen tényezőkről már volt szó, ezek a kockázati tényezők és a védelmi erőforrások [5: 6.]. Ebbe én még beleértem a biztonságmenedzsmentet is, mert a biztonságmenedzsment a lehető legközvetlenebbül befolyásolja a biztonságot mint védelmi erőforrás. Egy szint felett, ami lehet árbevétel vagy dolgozói létszám, vagy a termék vagy tevékenység értékessége, bizalmassága, egyértelműen kötelezően kellene biztonságmenedzsmentet alkalmazni a biztonsági rendszer kialakítására és működtetésére. Sajnálatos módon elterjedt az a nézet, hogy a biztonság egy improduktív szervezet, mert nem hoz létre bevételt. Ezt az álláspontot a felkészületlen vezetők vallják, akik nem képesek átfogó rendszerekben gondolkozni, ezért ezek a vezetők és az általuk vezetett szervezet/vállalat hosszú távon nem lehet sikeres, mert nem tudják a rájuk bízott szervezetet a leghatékonyabban működtetni. Ez a hozzáállás helytelen. A biztonsági szervezet egy felkészült és hatékony biztonságmenedzsmenttel a szervezet/vállalat veszteségeinek minimalizálásával

vagy megszüntetésével jelentős financiális bevételt tud teremteni (nem engedi, hogy a dolgozók, illetve külsősök ellopják a vállalat értékeit). Egy lehetséges másik útja a biztonságmenedzsment vállalati értékteremtésének, amikor bevonják a leltárhiányok feltárásába, illetve azok megszüntetése érdekében bevezetendő leltárfolyamatok megtervezésébe, ellenőrzési pontok kialakításába.

Összefoglalva megállapíthatjuk, hogy egy felkészült biztonságmenedzsment a szervezet bevételeit növelheti, hatékony tevékenységével produktív ágazatként növelheti a vállalat pénzügyi hatékonyságát.

A biztonságmenedzsment

Mit értünk ma Magyarországon vállalati biztonságmenedzsment alatt, valamint milyen fejlettségi szintre pozícionálhatjuk napjainkban a nemzetközi biztonságmenedzsment jelenlegi vezető tudományos, szakmai iránymutatásaihoz viszonyítva?

A vállalati biztonságmenedzsment hazai kialakulásának előzményei, gyökerei, lényegének értelmezése, jelenlegi szintjének a gyakorlatban megvalósuló irányai különböző mértékben eltérnek a nemzetközi vezető eljárásmódoktól, vagy nem teljes egészében fedik le a vállalati biztonságmenedzsment teljes spektrumát, ezért szükséges és kívánatos az átfogó komplex biztonságmenedzsment-eljárás mielőbbi általános gyakorlattá válása.

A rendszerváltás vagy rendszerváltozásig hazánkban nem létezett vállalati biztonságmenedzsment. Az akkori társadalmi és gazdasági rendszer vagyon-, és személybiztonsági kérdésekben kizárólag az állami rendészeti, tűz-, katasztrófa-, polgárvédelmi (és titkosszolgálati) szervekre támaszkodott. Ezen kívül, helyenként, főleg veszélyes ipari üzemekben létrehozott üzembiztonsági rendészet tevékenykedett, amely inkább munkabiztonsági feladatokat látott el, de foglalkozott vagyonvédelemmel is. Még megemlíthetjük a különböző őröket a rendszerváltozás előtti időszakból, mint akik szintén a biztonsággal foglalkoztak a 20. század nagyobbik részében Magyarországon, például éjjeliőr, vadőr, mezőőr, halőr stb. Az állami és a társadalmi tulajdon kollektív tulajdon volt, egyéni értelemben csak személyi tulajdonról beszélhettünk. Ebben a korszakban magántulajdon gyakorlatilag nem létezett, az össztulajdon 2%-át sem érte el, így annak védelmével sem kellett foglalkozni.

Ilyen biztonsági háttér mellett ért el minket a szabad piacgazdaság minden biztonsági kockázati tényezőjével együtt. Erre nem voltunk felkészülve, mint ahogy az elbizonytalanított rendészeti szervek sem. Az alapfeladatuk ellátására igyekeztek erőiket átcsoportosítani, miközben régebbi szerepükhöz képest kivonultak a gazdasági területről. Ekkor szembesültek az immár tulajdonossá vált vezetők is azzal, hogy már maguknak kell gondoskodniuk az értékeik védelméről. Mivel vállalatibiztonságmenedzsment-képzés egyáltalán nem létezett, illetve még ma sem nagyon létezik, ezért különböző vezetési irányok alakultak ki, amelyek még ma is tartják magukat, bár már a kívánatos komplex biztonságmenedzsment is kialakulóban van.

Biztonságmenedzsment szemléleti irányai:

- rendőri-katonai,
- őrzésvédelmi,
- munkavédelmi,
- biztonságtechnikai,
- informatikusi,
- komplex biztonságmenedzsment.

A rendőri-katonai irány: volt rendőri és katonai vezetők által bevezetett irányzat, amely az objektumok fizikai védelmére, illetve a nyomozásokra koncentrál. Ez a legdominánsabb biztonságvédelmi irányzat jelenleg hazánkban.

Az őrzésvédelmi irány: vagyonvédelmi szolgáltatók szemléletéből alakult ki, fő súlypont az emberi (őrök általi) őrzésre helyeződik, általában „külsős" szemszögből ítélik meg a szükséges védelmi szintet.

A munkavédelmi irány: (safety) munkavédelmi mérnökök által képviselt elgondolás, ahol a munka-, tűz- és egészségvédelemre helyeződik a fókusz. A vészhelyzetmenedzsmenten belül a vészhelyzeti reagáláson van a fő hangsúly.

A biztonságtechnikai irány: biztonságtechnikai mérnökök általi megközelítés, ami a biztonságtechnikai rendszeren és elemein alapul, mint a kamerarendszer, beléptetőrendszer vagy riasztórendszerek.

Az informatikusi irány: informatikus mérnökök által gyakorolt eljárásrend, jellemzője az informatikus, analitikus rendszerszemlélet, amelyben majdnem kizárólagos prioritása a számítástechnikai rendszernek, elemeinek, illetve a hálózatvédelmi rendszereknek van.

Mind az öt előzőleg felsorolt biztonságmenedzsment-irányzat a lehető legszűkebben értelmezi a biztonságmenedzsmentet, kizárólag a saját szakmai elméletének és gyakorlatának megvalósítását tartja feladatának, a biztonságmenedzsment egyéb feladatait igyekszik kizárni a felelősségi területéből, illetve áthárítani más szervezeti egységekre, lemondva ezáltal az átfogó szintű kontroll kialakításáról.

Példaképpen a rendőri-katonai, illetve az őrzésvédelmi irányzat számára megfelelő megoldás az, ha nem kell részt venniük az információbiztonság megvalósításában (e-mail-ellenőrzés, internethasználat-figyelés, vállalat kárára történő információáramlás stb.), azt teljes mértékben ráhagyják az IT-szervezetre. Ez egy kényelmes felállási mód véleményük szerint, de ezzel át is adják a teljes ellenőrzést az IT-szervezetnek a terület felett, vagyis a szükséges adatok nem állnak azonnal a rendelkezésükre majd egy jövőbeni visszaélés kivizsgálásához, vagy ezekhez az adatokhoz csak körülményesen és késedelemmel juthatnak hozzá [12].

Egy középkori latin szólást szeretnék idézni, ami úgy szól, hogy: „Extra Hungariam non est vita, si est vita, non est ita." Ami magyarul így szól: Magyarországon kívül nincs élet, ha van élet, nem ilyen [13]. Ezt én úgy értelmezem, hogy minden általános szabályt valamilyen mértékben az adott hely/ország szokásai szerint módosítani kell, vagyis a helyi sajátosságokat figyelembe kell venni, hogy a szabály megfelelően tudjon megvalósulni.

A komplex biztonságmenedzsment: (security) nemzetközi, elsősorban angolszász alapú megközelítés, betelepült multinacionális vállalatok által hozott szigorú biztonsági

kultúra és eljárásrend. A magántulajdon védelme megkövetelte és kialakította saját védelmi rendszerét, ami a 20. század utolsó harmadában indult lendületes fejlődésnek. Jellemzője, hogy átfogó módon áll a biztonsághoz, annak minden elemét igyekszik integrálni a rendszerébe [12].

Szakirodalmunk szempontjából szintén megfigyelhetjük ugyanezt a tagozódást. Legszélesebb a paletta a biztonságtechnikával foglalkozó kiadványok tekintetében, nevükből kifolyólag ezekre a művekre alapvetően jellemző az egyes témák részletes, mélységekbe menő mérnöki feldolgozása, sem itt, sem a többi területen nem találunk átfogó, komplex szemléletű tanulmányt, ami a biztonságmenedzsmentről szólna. Komplexitásra való törekvés nézőpontjából mindenképpen meg kell említeni az 1999-ben megjelent *Hivatása a védelem* [14] című kiemelkedő munkát, amely 14 író és négy szerkesztő közös munkájának eredménye. Ebben a műben a szerzők sorra veszik az objektumvédelem, személyvédelem, kivonuló szolgálat, rendezvénybiztosítás, pénz- és értékszállítás kérdéseit, őrök által használt technikai eszközöket stb. Szemléletére jellemző a komplexitásra való törekvés, de érezhető a végrehajtói vagy szolgáltatói nézőpont. Főleg az őrzésvédelmi szemlélet tapasztalható benne némi rendőri-katonai befolyással. Kitűnő példa az informatikai megközelítésre Vasvári György *Vállalati biztonságirányítás* [15] című munkája, amelynek az alcíméből már láthatjuk is, hogy az „Informatikai biztonságmenedzsment"-ről szól. Szövényi György *Biztonságszervezői menedzsment* [16] című értekezésében még többségében megtalálható a rendőri-katonai szemlélet, nagyon erős jogi háttérrel, de már a komplex biztonságmenedzsment is megnyilvánul egyes elemeiben. Ilyen például az *A biztonságszervező menedzser eszköztára* (84–93. oldal), ahol a humán biztonság nélkülözhetetlen elemeit fejti ki a szerző. Szintén figyelemreméltó, hogy a szerző már használja *A komplex biztonságvédelmi rendszer kialakítása* (98–107. oldal) című fejezetében a komplex kifejezést, de még nem érti alatta az átfogó komplex biztonságmenedzsmentet teljes egészében. Sajnos a témánkat teljes mértékben lefedő, magyar, összefoglaló mű még nem készült el, ezt pótolni kell.

Nem szabad elfeledkezni arról, hogy jelentős számban jelennek meg hazai publikációk a biztonsággal foglalkozó lapokban, mint a *Detektor Plusz* magazin, az *Árgus,* vagy a *Biztonság.* Több hazai egyesület, például a Magyarországi Biztonsági Vezetők Egyesülete, a Magyar Biztonsági Fórum (MBVE, MBF) vagy a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara igen aktívan tevékenykedik annak érdekében, hogy a biztonság a megfelelő szintre kerüljön. Még sok a teendő ebben az irányban, hogy amikor a biztonságmenedzsmentről beszélünk, akkor ugyanazt is értsük alatta mindannyian. Ezt akkor érhetjük el, ha van megfelelő oktatás, tananyag és rendszer. Ennek a célnak az eléréséért mi, a jelenkori biztonsági szakemberek vagyunk a felelősök, nekünk kell tenni azért, hogy mindez megvalósulhasson.

Összefoglalás

A hazai viszonyokat közelebbről érezzük, de ha kitekintünk Európába, vagy még távolabb a világ bármelyik régiójába, akkor sem éppen megnyugtató érzéseink keletkeznek. Számos problémát, krízishelyzetet, érdekellentétet, konfliktust tapasztalhatunk.

Elegendő azonban a közelmúltbeli 2008-as gazdasági válságra, a 2011-gyel kezdődött „arab tavaszra," a mostanában is pengeélen táncoló, európai uniós adósságválság megoldásának kísérleteire, a migrációs nyomásra és a globális felmelegedés hatásaira, a világ népességének növekedési ütemére, valamint az atomhatalmak szemben álló politikai és gazdasági érdekeire gondolni. Ezek a tendenciák mind azt mutatják, hogy pillanatok alatt romolhat az általános biztonság, több lesz az anyagi javak elleni támadás, lopás, betörés, szállítmányok eltulajdonítása, fosztogatása. Vagyis jóval több feladatunk lesz és sokkal mostohább körülmények között kell mindezeket elvégeznünk. Mindezekre fel kell készülnünk, mert csak akkor leszünk képesek megvédeni a ránk bízott értékeket, ha egy hatékonyan működő, a biztonság teljes spektrumát átfogó, komplex biztonsági rendszert tudunk működtetni. A szerencsésebbeknek közülünk ehhez rendelkezésére is fognak állni a szükséges anyagi alapok, a kevésbé szerencséseknek, pedig még sokkal hatékonyabban kell majd felhasználniuk szellemi kapacitásaikat.

Összegezve megállapítható, hogy a rendszerváltozástól eltelt majdnem három évtized alatt a hazai biztonságmenedzsment több irányban is jelentős eredményeket tud felmutatni, határozott fejlődésen ment keresztül, de az összefogó, rendszerező, standardizáló feladatok még előttünk vannak. Kívánatossá vált egy egységes, komplex biztonságmenedzsment-rendszer kialakítása, amely a nemzetközi eljárások mentén a hazai viszonyok figyelembevételével képes átfogó, hatékony, jól működő rendszerként üzemelni.

Hivatkozások

[1] Dictzone, Latin-magyar szótár, „securitas," *Dictzone,* [Online]. Elérhető: https://dictzone.com/latin-magyar-szotar/securitas (Letöltve: 2019. 09. 01.)

[2] Online Etymology Dictionary, "security," *Online Etimology Dictionary,* [Online]. Elérhető: www.etymonline.com/word/security (Letöltve: 2019. 09. 01.)

[3] G. Czucor, *A Magyar Nyelv Szótára I.* Pest: Emich Gusztáv, 1862, [Online]. Elérhető: https://mek.oszk.hu/cgi-bin9/czuczor2.cgi?kezdobetu=B&szo=BIZTONS%C3%81G&offset=108 (Letöltve: 2019. 09. 01.)

[4] Arcanum, A magyar nyelv értelmező szótára, „biztonság," *Arcanum,* [Online]. Elérhető: www.arcanum.hu/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/b-1EF8E/biztonsag-2119D/ (Letöltve: 2019. 09. 01.)

[5] L. Berek, T. Berek és L. Berek, *Személy- és vagyonbiztonság.* ÓE-BGK 3071, Budapest: Óbudai Egyetem, 2016., p. 6.

[6] K. Papp és A. Ujváriné Siket, *Az egészségügy és az ápolás általános alapelvei.* Debreceni Egyetem Egészségügyi Kar, 2014., p. 5. Az alapvető emberi szükségletek és kielégítésük, 19. kép, Maslow szükségleti piramisa, [Online]. Elérhető: www.tankonyvtar.hu/hu/tartalom/tamop412A/2010_0020_apolas_magyar/5_az_alapvet_emberi_szksgletek_s_kielgtsk.html (Letöltve: 2019. 09. 01.)

[7] S. Utassy, „Komplex villamos rendszerek biztonságtechnikai kérdései," Doktori (PhD) értekezés, 2009, [Online]. Elérhető: https://adoc.tips/komplex-villamos-rendszerek-biztonsagtechnikai-kerdesei.html (Letöltve: 2019. 09. 01.)

[8] T. Berek, „Vészhelyzeti víztermelő létesítmények integrált fizikai védelme," *Műszaki Katonai Közlöny,* 27. évf. 4. sz., pp. 227–236., 2017.
[9] L. Berek és A. Vass, „Gázturbinás erőműi objektum védelme," *Hadmérnök,* 9. évf. 2. sz., pp. 5–15., 2014.
[10] T. Berek és T. Horváth, „Fizikai védelmi rendszerek dinamikusan változó környezetben," *Hadmérnök,* 9. évf. 2. sz., pp. 16–24., 2014.
[11] A. Vass és L. Berek, „Napenergia és az elektronikai jelzőrendszer, villamos energia hálózattól távol lévő objektumok védelmének lehetőségei," *Hadmérnök,* 10. évf. 2. sz., pp. 41–57., 2015.
[12] Zs. Zólyomi, „Biztonságmenedzsment itthon, napjainkban," *Detektor Plusz,* 5. sz., pp. 14–15., 2011.
[13] Idegen szavak szótára, „Extra hungariam non est vita, si est vita, non est ita," *Idegen szavak szótára,* [Online]. Elérhető: http://idegen-szavak-szotara.hu/extra-hungariam-non-est-vita,-si-est-vita,-non-est-ita.-jelent%C3%A9se (Letöltve: 2017. 11. 19.)
[14] J. Devecsai, J. Nán, M. Varga és L. Gábor, *Hivatása a védelem.* Budapest: CEDIT Kft., 1999.
[15] Gy. Vasvári, *Vállalati biztonságirányítás*. Kiskunlacháza: Time-Clock Kft., 2007.
[16] Gy. Szövényi, *Biztonságvédelmi kézikönyv.* Budapest: KJK-Kerszöv, 2000.
[17] A. D. Kovács, „Objektumvédelem," *Detektor Plusz,* 4. sz., 2018. [Online]. Elérhető: http://detektorplusz.hu/index.php?m=23998 (Letöltve: 2019. 09. 01.)

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

15. évfolyam (2020) 1. szám 31–44.
DOI: 10.32567/hm.2020.1.3

Ocskay István[1]

Puma lánctalpas gyalogsági harcjármű és lehetséges megjelenése a magyar honvédség állományában

The PUMA Tracked Infantry Fighting Vehicle and its Possible Appearance in the Inventory of the HDF

A Puma harcjármű a Bundeswehr legkorszerűbb, a 21. századi elvek alapján épített lánctalpas harcjárműve. De hogy jutott el a német harcjárműfejlesztés a Marder 2 lövészpáncélostól a jelenlegi Puma IFV lánctalpas harcjárműig, annak rendszeresítéséig. Melyek voltak az eszköz kifejlesztésének főbb fázisai, lépései, akadályai. Melyek a harcjármű főbb technikai paraméterei, jellemző technikai megoldásai, újdonságai? Vajon ez a harcjármű képes-e betölteni a Magyar Honvédség eszközállományában a 2005-ben, a BMP-1 lánctalpas harcjárművek kivonásával keletkezett űrt, és képes-e a jelenlegi magyar hadműveleti és technikai követelményeknek megfelelni? A cikk mondanivalójával szeretném meggyőzni az olvasót arról, hogy ez az eszköz jelenlegi tulajdonságaival miért csak korlátozásokkal alkalmas ennek a feladatnak az elvégzésére.

Kulcsszavak: **lánctalpas harcjármű, harcjárműfejlesztés, hadműveleti követelmény, Magyar Honvédség, Puma, Marder**

The PUMA Infantry Fighting Vehicle is the ultimate, most modern tracked IFV among the IFV inventory of Bundeswehr and it was designed to fulfil all requirements that an IFV should provide in our century. How the German fighting vehicle development has reached this status from MARDER 2 APC to PUMA IFV? What have been the main phases, obstacles and successes of this development? What are the main technical descriptions and technical solutions of PUMA IFV? Could this be the vehicle to fulfil all the given operational and technical requirements posed by the Hungarian Defence Forces, to replace the BMP-1 IFVs of Soviet origin, withdrawn almost 15 years ago? I hope that reading this article you will agree with me in that

[1] MH Modernizációs Intézet, kutatás és fejlesztési igazgató, e-mail: ocsysteve@gmail.com, ORCID: https://orcid.org/0000-0003-0279-8215

this IFV with its current configuration is not fully capable to fulfil the previously mentioned post.

Keywords: **IFV, fighting vehicle development, operational requirements, Hungarian Defence Forces, PUMA, MARDER**

Bevezetés

A Puma lánctalpas harcjármű születése, hasonlóan a többi társához, nem volt problémamentes, és hasonlóan kortársaihoz jelentősen el is húzódott, köszönhetően annak, hogy a jármű részegységei, főbb elemei, de még a kisebb alrendszerek elemeit újra, és újként kellett kialakítani, majd később integrálni egy amúgy forradalmi kialakítású járműbe.

A Magyar Honvédség (a továbbiakban: MH) Zrínyi 2026 haderő- és hadfelszerelés-fejlesztési program keretében, a NATO-elvárásoknak megfelelően, egy könnyű-, egy közepes- és egy nehézdandár-képesség megteremtését tűzte ki célul, 2026-os határidővel. A nehézdandár-képesség keretében 2018 decemberében szerződés aláírására került sor a német KMW[2] hadiipari vállalattal Leopard harckocsik és PzH 2000 (Panzerhaubitze 2000) önjáró tarackok beszerzésére. Azonban a nehézdandár-képesség nem létezhet harcjárművek, azon belül is lánctalpas harcjárművek nélkül. 2019 februárjában felreppent hírek alapján az MH, a nehézharcjármű-képesség kialakítása érdekében 200 db Puma lánctalpas harcjárművet vásárol majd Németországból.

A Puma lánctalpas harcjárművek**,** ezek alapján több mint 15 évnyi szünetet követően hoznák vissza a lánctalpasharcjármű**-**képességet az MH-ba, hiszen 2004-ben, miniszteri döntést követően, a BMP-1 lánctalpas harcjárműveket kivonták az MH állománytáblájából. Ezzel egy olyan képességhiány keletkezett a harcjárművek terén az országban, amelyet az akkor már meglévő majd 700 darabos BTR-80 és BTR-80A kerekesharcjármű**-**flotta sem volt képes betölteni. A megváltozott geopolitikai helyzetre való tekintettel, a NATO 2016-os varsói ülésén megfogalmazták, hogy a NATO keleti határainak magasabb szintű védelme érdekében a tagországoknak nehézdandárokkal kell rendelkeznie. A nehézdandár**-**képességet a NATO szakemberei a harckocsik és a lánctalpas harcjárművek rendszeresítésében és alkalmazásában látják.

Ebben a cikkben arra szeretnék választ adni, hogy vajon a Bundeswehr igényeinek megfelelően kifejlesztett, napjainkban még csak a német haderőben rendszeresített lánctalpas harcjármű alkalmas-e az MH hadműveleti, valamint technikai követelményeinek megfelelni?

A lánctalpas gyalogsági harcjármű

A nemzetközi és a hazai szakirodalomban megjelenő eltérő értelmezések miatt szükségünk van annak tisztázására, hogy mit is nevezünk lánctalpas gyalogsági harcjárműnek. A Magyar Katonai Szabvány idevonatkozó megállapítása szerint a lánctalpas harcjármű fogalma: „Katonai lánctalpas gépjármű, mely fegyverrendszerrel (komplexummal)

[2] Krauss-Maffei Weigmann.

van ellátva, és az ellenség élőerejének, technikájának és létesítményeinek megsemmisítésére és lefogására szolgál" [1: 3.]. Ezt kiegészíti, illetve pontosítja a lánctalpas gyalogsági harcjármű fogalmánál: „Páncélozott gyalogsági harcjármű, mely a gépesített lövészalegységek szállítására szolgál, továbbá a harc harcjárműből történő megvívására és a gyalogos lövészek tűztámogatására szolgál" [1: 4.].

Ez a meghatározás az 1980-as évek felfogását tükrözi, de egyvalamire nem ad választ: milyen fegyverzettel kell, hogy az eszköz rendelkezzen, hogy gyalogsági harcjármű és ne páncélozott szállító harcjármű legyen. A fent idézett szabvány szerint a lánctalpas páncélozott szállító harcjármű: „Páncélozott lánctalpas harcjármű, melynek rendeltetése a gépesített lövészcsapatok személyi állományának az elszállítása a harcmezőre, azok tűztámogatása, valamint a katonai felszerelések szállítása, és pótkocsik vontatása" [1].

Pontosabb képet ad a lánctalpas harcjármű fogalmáról az 1990. november 19-ei az Európai Hagyományos Fegyveres Erőkről szóló Szerződés, a köznyelvben *CFE Szerződésnek* emlegetett memorandum, amely pontosan meghatározza mi minősül még napjainkban is lánctalpas gyalogsági harcjárműnek. Ezek alapján a páncélozott gyalogsági harcjármű fogalma: „Olyan, elsődlegesen lövészraj szállítására tervezett és felszerelt páncélozott harcjárművet jelent, amely rendszerint lehetővé teszi a csapatok számára, hogy a jármű belsejéből páncélvédettség alatt tüzelhessenek, és amelyet legalább 20 mm-es űrméterű felszerelt vagy szervezetszerű gépágyúval és esetenként páncélelhárító rakétával láttak el" [2].

A *Hadtudományi Lexikon,* a fenti meghatározásokon túl megemlíti, hogy „a gyalogsági harcjárművek általában 10-40 mm vastag acélpáncélzattal, vagy ennek a védőképességnek megfelelő védőképességű más anyagokból készült páncélzattal borított, kerekes vagy lánctalpas futóműves, 8-25 tonna harci tömegű, 9-12 fő szállítására alkalmas, rendszerint úszóképes járművek. Fegyverzetük körforgó toronyba épített géppuska, valamint gépágyú vagy löveg, esetenként páncéltörő rakéták" [3].

Hasonlóan jellemzi az eszközfajtát a *Katonai Terminológiai Értelmező Szótár,* amely szerint „a gyalogsági harcjármű páncélvédelemmel és fegyverzettel ellátott kerekes vagy lánctalpas harcjármű. Kezelőszemélyzete általában 2-3 fő, emellett 6-10 felfegyverzett katona szállítására alkalmas" [4].

Az MH-ban a gyalogsági harcjárművekkel szemben támasztott hadműveleti követelményeket a Honvéd Vezérkar Hadműveleti Csoportfőnöksége határozta meg legutóbb 2017-ben, amely alapján: „A gépesített lövész lánctalpas gyalogsági harcjármű rendeltetése: az összfegyvernemi kötelék részeként fokozott tűzerővel, mozgékonysággal és páncélvédettséggel gyors manőverek végrehajtása, az ellenséges erők megsemmisítése a siker kifejlesztése érdekében. A harcjármű képes hatékonyan pusztítani közepes távolságon az ellenséges páncélozott eszközöket és az élőerőt, továbbá képes az egységes műveleti helyzetkép kialakításához szükséges adatok továbbítására és fogadására" [5].

A fenti fogalommeghatározások közül a CFE-ben megfogalmazott változatot tekintem a legpontosabbnak, a legjobban körülírtnak, és ismerve a Puma főbb technikai jellemzőit, előzetesen kijelenthetem, hogy a Puma lánctalpas gyalogsági harcjármű megfeleltethető a fenti feltételeknek, de azért ismerjük meg részleteiben, hogyan is fejlődött ki ez a harcjármű, és melyek annak leglényegesebb jellemzői.

A Marder 2 harcjármű

Az 1980-as évek közepétől, az akkori Nyugat-Németország hadserege megkezdte a rendszerben lévő Marder 1 lánctalpas harcjárművek leváltását egy új, Marder 2-nek nevezett eszközzel. A Bundeswehr akkori követelménytámasztása olyan járműre vonatkozott, amely mobilitás tekintetében képes a Leopard 2 harckocsikkal együtt mozogni a harcmezőn, biztosítja hétfős lövészraj szállítását, emelt szintű páncélvédelemmel rendelkezik, és ellenáll a szovjet BMP-2 harcjármű 30 mm-es lőszereinek, valamint stabilizált, nagy hatékonyságú, 35-50 mm közötti űrméretű toronyfegyverzettel rendelkezik. A német Krauss-Maffei, a későbbi KMW vállalat, kapta a megrendelést ezen jármű prototípusának megalkotására, ami az 1. ábrán látható, és amelynek a gyári munkakódja a „VT 001" volt [6].

1. ábra
A Marder 2 harcjármű prototípusa [19]

A prototípusjárműbe több kísérleti berendezést, fődarabot is beépítettek mint például az MTU[3] dízelmotor, vagy a különleges kialakítású 35 és 50 mm-es lőszereket egyaránt tüzelni képes MK 35/50 Rh 503 típusú gépágyú [7].

A harcjármű alvázát a Krauss-Maffei vállalat tervezte, és a követelményeknek megfelelően a hegesztett páncéllemezekből készített test szemből ellenállt az abban az időben gyártott valamennyi típusú 30 mm-es lövedéknek. A páncéltest a 155 mm-es

[3] Motoren- und Turbinen-Union GmbH.

repeszgránátok repeszei ellen is hatékony védelmet biztosított. A kiegészítő páncélok rögzítése oldható csavarkötéssel volt megoldható. Ezeknek a tulajdonságoknak azonban ára volt, mégpedig a tömegnövekedés: a jármű össztömege *16 tonnával haladta meg* a leváltásra tervezett Marder 1 lánctalpas harcjármű össztömegét, így 42,5 tonna lett.

Annak érdekében, hogy a jármű mégis kimagasló manőverezőképességgel rendelkezzen egy 18,3 literes V8 hengerelrendezésű turbófeltöltős dízelmotorral szerelték fel, amelyet az MTU gyár fejlesztett ki direkt a program részére MTU 881 Ka-500[4] névvel. Az 1000 lóerő leadására képes erőforrás segítségével a jármű teljesítmény–tömeg aránya 22,62 Le/tonna lett. A motor egy Renk HSWL-284-C típusú automata (hidromechanikus) sebességváltón keresztül hajtja meg a mellső láncmeghajtó kerekeket, és biztosít a harcjárműnek maximálisan 62 km/órás végsebességet.

A gépágyút – 10 és + 45 fok között lehetett függőlegesen mozgatni, a gépágyúhoz rendszeresített 177 + 110 db lőszert a toronyba málházták be.

A Marder 2 harcjármű legfontosabb technikai adatai:

- Tömege: 44,3 tonna;
- Teljes hossza: 7,31 m;
- Szélessége: 3,48 m;
- Magassága: 3,05 m;
- Személyzet: 3 (vezető, parancsnok, irányzó) + 8 deszantolható katona;
- Fő fegyverzet: 35/50 mm MK Rh503 gépágyú;
- Párhuzamosított géppuska: 7,62 mm HK MG3 géppuska;
- Motor típusa: MTU V8 881 dízel, 760 kW (1,030 Le);
- Fajlagos teljesítmény: 16.6 kW/tonna;
- Hatótáv: 500 km szilárd felszínű úton;
- Sebesség (e/h[5]): 60/27 km/h szilárd felszínű úton [8].

Összegzésképpen kijelenthetem, hogy a Marder 2 harcjármű egy nagyszerű fejlesztés volt, amely bár megelőzte korát, viszont két nagy hibával is rendelkezett, amelyek egyike sem technikai, technológiai probléma: nagyon drága volt a beépített kísérleti elemek, felszerelések kifejlesztése, és rossz időben, a hidegháború végével jelent meg a színpadon, amikor a szemben álló felek már inkább a haderejük csökkentésében gondolkodtak, és a társadalmi viszonyok is inkább a katonai kiadások csökkentését szorgalmazták.

A Puma harcjármű

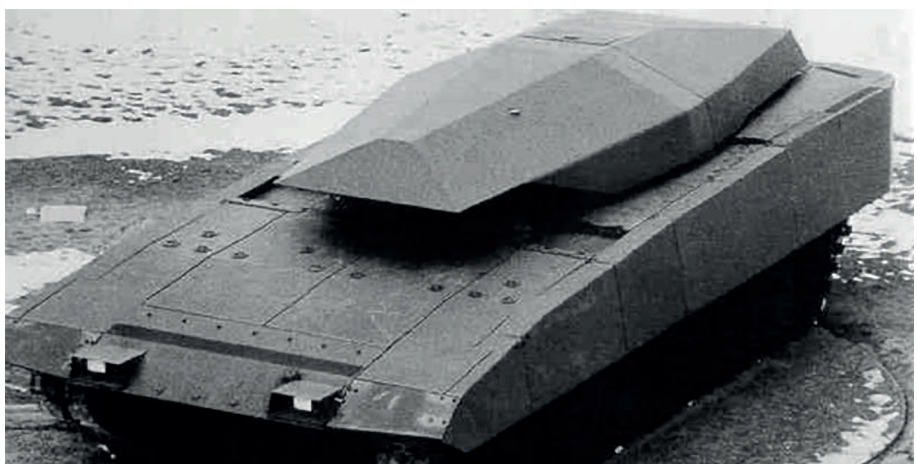
A politikai és gazdasági átrendeződéseket követően az 1990-es évek közepén felvetődött ismételten az igénye annak, hogy a meglévő Marder 1A3 harcjárművek kiváltásának a tervezése végett kezdjék meg, felhasználva a Marder 2 kifejlesztése során nyert egyes tapasztalatokat, egy új, a legmodernebb felszerelésekkel felszerelt gyalogsági harcjármű

[4] A program törlésével ez a motor lesz a PzH 2000 típusú önjáró tarack erőforrása.
[5] Előre – hátra.

kifejlesztését, amely a „Neue Gepanzerte Plattformen"[6] (a továbbiakban: NGP) nevet kapta. A program célja egy olyan járműplatform kifejlesztése volt, amely alkalmas más és más feladatú, páncélozott eszközhöz egy közös hordozóalvázat biztosítani. Az így összegyűjtött tapasztalatok biztosították volna a lánctalpas gyalogsági harcjármű, vagy páncélozott szállító harcjármű, légvédelmi páncélos vagy akár egy harckocsi közös alvázának a kifejlesztését is, ami jól látszik az egyetlen megmaradt prototípus kialakításán a 2. ábrán [9].

A Bundeswehr által támasztott követelmények között szerepelt:

- a jármű legyen 55–60 tonna közötti tömegű nehéz gyalogsági harcjármű és 60–70 tonna közötti harckocsi konfiguráció esetében;
- ennek megfelelően kialakítása legyen moduláris, hogy biztosítsa különböző feladatú járművek kialakítását;
- legyen ezenfelül minél kompaktabb kialakítású, biztosítva a legnagyobb elérhető szállító/rakteret;
- legalább 1000 LE teljesítményű dízelmotorral rendelkezzen;
- a feladatrendszerének megfelelően rendelkezzen moduláris páncélzattal;
- a légi szállíthatóság biztosítása [10].



2. ábra
Az NGP egyetlen fennmaradt prototípusa [9]

A Puma lánctalpas harcjármű születése

Az ígéretes NGP-program vizsgálatai 2001-ben fejeződtek be alapvetően sikeresen, és egyben táptalajt biztosítottak az 1998-ban elindult, de csak 2001-ben felgyorsuló

[6] NGP Új (generációs) Páncélozott Platform (németül).

„neuer Schützenpanzer"[7] megalkotásához. A program először „Igel,"[8] majd „Panther,"[9] de végül „Puma" néven vált ismertté.

A munka végrehajtására a Krauss-Maffei Wegmann és a Rheinmetall Landsysteme PSM néven egy konzorciumot hozott létre a németországi Kasselben. A Bundeswehr megalakításának 50. évfordulójára, 2006. május 5-én, egy a nagyközönségnek Munsterben megtartott nyilvános bemutató keretében adták át tesztelésre az eszközt. A tesztek végeztével 2010. december 6-val a Védelmi Technológia és Beszerzési Szövetségi Hivatal[10] átvette a végleges kialakítású járművet, így hivatalosan innen számítják a Puma harcjárművek sorozatgyártását [10].

A Puma harcjármű legfontosabb technikai adatai [10]:

- Tömege: 31,45 t „level A" és 43 t „level C" fokozatokkal szerelve;
- Teljes hossza: 7,6 m;
- Szélessége: 3,0 m „level A" és 3,9 m „level C" fokozattal szerelve;
- Magassága: 3,6 m;
- Személyzet: 3 (vezető, parancsnok, irányzó) + 6 deszantkatona;
- Páncélzat: AMAP11 moduláris kompozit páncél;
- Fő fegyverzet: 30 mm MK30-2/ABM gépágyú 400 db lőszerrel;
- Párhuzamosított fegyver: 5,56 mm HK MG4 géppuska, 2000 lőszerrel;
- Páncéltörő rakéta: RAFAEL Spike LR 2 + 2 db rakéta;
- Ködgránátvetők: 6 db 76 mm-es gránátvető a tornyon;
- Motor: MTU V10 892 dízel 800 kW (1100 LE);
- Fajlagos teljesítmény: 18.6 kW/tonna, a „level C" védelmi szinttel szerelve;
- Hatótáv: 460 km szilárd felszínű úton;
- Végsebesség (e/h): 70/30 km/h szilárd felszínű úton.

A Puma lánctalpas harcjármű kialakítása

A Puma lánctalpas harcjármű a világ egyik legjobb védelemmel rendelkező, nagy mobilitású és nagy tűzerővel rendelkező harcjárműve, amely sok tekintetben teljesíti a mozgékonyság–páncélvédelem–tűzerő hármas legjobb kiegyensúlyozottságát. A valóságot tekintve a Puma jelentős mértékben nem tér el a kor többi lánctalpas harcjárműveitől, azonban pár olyan jelentős újítás található benne, amelyek együttes hatása teszi ezt a járművet a 21. század egyik meghatározó járművévé.

Vegyük sorra ezeket az újításokat, amelyek: a moduláris páncélzat, a nagy tűzerejű, hatékony lőszereket tüzelő gépágyú és a lánctalpas harcjármű kategóriában egyedülálló teljesítményű erőforrás.

[7] Új harcjármű (németül).
[8] Sündisznó.
[9] Párduc.
[10] Bundesamt für Wehrtechnik und Beschaffung.
[11] Advanced Modular Armor Protection – Fejlett Moduláris Páncélvédelem.

Páncéltest – Páncélvédelem

A Puma harcjármű kifejlesztésénél elsődleges szempontok közé tartozott a páncélvédelem kérdése, de nemcsak annak mennyisége és minősége, de modularitása, feladatra szabhatósága is. A harcjárműre három páncélvédelmi szintet terveztek, amelyeket „Level „A", „B" és „C" szinteknek neveztek el. Ebből a „B" szint nem valósult meg, csak az „A", azaz légi szállítható,[12] alap, pótpáncélozás nélküli verzió, illetve a „C" szint, azaz a harci[13] szint, amely a legnagyobb páncélvédelmet adja a járműnek. Ez utóbbi szint képes a NATO STANAG 4569/AEP-55 KE 5 védelmi szint alapján körkörös védelmet biztosítani a 30 mm-es nyíllövedékek ellen, amely moduláris páncélzat kialakítása jól látszik a 3. ábrán lévő harcjármű esetében is. A „C" szintű modulelemek felszerelését a harcjárművek kezelőszemélyzete 1 óra alatt végre tudja hajtani [11].

A harcjármű tüzérségi lőszerek repeszeinek, illetve azok résztöltetei, valamit a kumulatív töltetek elleni védelem területén úgynevezett CLARA[14] kompozit/reaktív páncélt kapott. Ahol a kompozit páncél valami oknál fogva nem alkalmazható, ott védőrácsot kaphat az eszköz.

3. ábra

A Puma részlegesen megbontott moduláris páncélzata [11]

[12] A mint Air transportable.
[13] C mint Combat.
[14] Composite Lightweight Adaptable Reactive Armor, Kompozit Könnyű Adaptálható Reaktív Páncél.

További korszerű megoldások felelnek azért, hogy a küzdőtérben helyet foglaló személyzet minél kisebb sérülési kockázattal rendelkezzen, aminek megfelelően például az üzemanyag-mennyiség több mint 80%-a a harcjármű páncéltestén kívül helyezkedik el. A német mérnökök egy szellemes megoldással a jármű hidropneumatikus futóművét olyanná alakították ki, hogy a jobb- és baloldali lengőkarok és rugóelemek oldalanként egy-egy egységet képezzenek, és emellett alkalmasak legyenek üzemanyag tárolására is [12].

Természetesen a küzdőtér rendelkezik mindazokkal a felszerelésekkel és berendezésekkel, amelyekkel egy korszerű harcjárműnek a 21. században rendelkeznie kell. Így a járműben megtalálható a teljes légkondicionáló rendszer, hűtő-fűtő elemekkel, és természetesen szennyezett terepszakasz leküzdésekor az ABV-szűrővel kombinálva, megtisztított levegővel látja el a kezelőszemélyzetet.

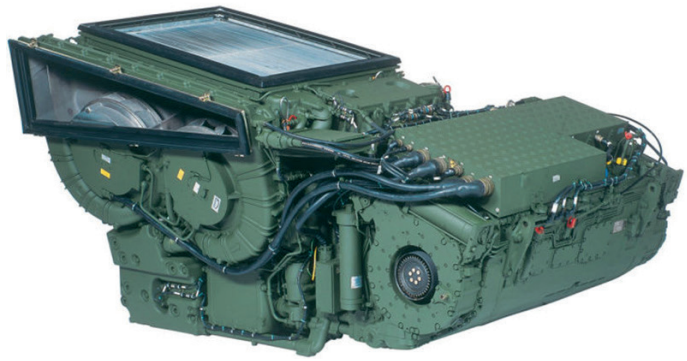
A megnövelt aknavédelem miatt megemelt padlólemez, az energiaelnyelő lövészkatona-ülések, a különféle kényelmet és biztonságot fokozó berendezések és kommunikációs eszközök elhelyezése miatt, a távirányított torony adta belső térnövekedés ellenére is a lövészpáncélos küzdőtere elég szűkös, holott nagyságát tekintve meghaladja az amerikai Bradley M2A2 lövészpáncélos hasonló értékeit.

Erőátvitel – Mozgékonyság

A harcjárművek mozgékonyságának, általános feladatrendszerüknél fogva, meg kell egyeznie vagy jobbnak kell lennie, mint azoknak a harckocsiknak, amelyeket kísérniük, támogatniuk kell. A Puma harcjármű ebben a tekintetben is élen jár, ugyanis a lánctalpas harcjárművek közül egyedülállóan, több mint 1000 lóerős dízelmotorral rendelkezik. Az MTU V10 892 típusú turbófeltöltős dízelmotornak névlegesen 800 KW (1088 LE) a teljesítménye. A leadott teljesítménye még „C szintű" moduláris páncélzat esetében is magasabb fajlagos teljesítményt biztosít, mint a Leopard 2A7 harckocsi, amelynek a majd 20 tonnával nagyobb tömegére kevesebb, mint 500 lóerővel több teljesítmény jut [13].

Az MTU gyár ezt a motort kifejezetten a Puma harcjármű részére fejlesztette ki, ahol a kompaktság, a nagy teljesítménysűrűség volt a mérvadó tervezési elv. A mérnökök munkáját dicséri, hogy a hasonló teljesítményű harckocsi/harcjármű-erőforrásokhoz képest a motor tömege és térfogata közel 60%-kal kisebb. A motor egy kilogrammjára több mint egy kilowatt teljesítmény jut, ami egyedülálló ebben a kategóriában.

Az erőátviteli egységben a motoron kívül egy RENK HSWL 256 típusú, 6 előre és 6 hátrameneti fokozattal rendelkező hidrosztatikus/hidrodinamikus kormányberendezéssel ellátott automata nyomatékváltó is helyet kapott, amely mellett egy starter-generátor és a közös hűtőegység is található, ahogy az 4. ábrán is látható. A jelentős teljesítményigényű fedélzeti elektromos berendezések ellátását a lendkerékbe szerelt generátor biztosítja.



4. ábra
Az MTU V10 892 motor és a RENK HSWL 256 nyomatékváltó alkotta „erőmű” [14]

Fegyverzet – Tűzerő

A torony tervezésénél a mérnökök szakítottak a korábbi harcjárműépítési általános gyakorlattal, és a Marder harcjárművekkel ellentétben távirányított, kezelő személyzet nélküli tornyot álmodtak meg az eszköz részére. Az alumíniumból készült, de páncélelemekkel fedett torony és benne a fegyver elhelyezkedését kettős aszimmetriával oldották meg, így tartva meg a fegyvert a jármű hossztengelyében, ami jól kivehető az 5. ábrán.

5. ábra
A Puma legelső prototípusán jól kivehető a torony és a fegyver aszimmetrikus elhelyezése [15]

Maga a torony kialakítása hasonló alapokon nyugszik, mint a Leopard 2 harckocsié, azaz a löveg/gépágyú elöl, a lőszerkészlet hátul helyezkedik el. A Puma harcjárműnél ez még azzal az előnnyel is jár, hogy a teljes lőszerkészlet a kezelőszemélyzettől elszeparáltan tárolható. A harcjármű tornyának kifejlesztésénél több alapvető szempontot is figyelembe vettek a tervezők, köztük, hogy a parancsnok tudjon az irányzótól függetlenül megfigyelést végezni és alkalmas legyen önálló tűzvezetésre, valamint át tudja venni a fő fegyverzet kezelését, az irányzótól.[15] A gépágyút a távirányított toronyban úgy építették be, hogy a harcjármű közelében és a levegőből érkező fenyegetések ellen is kiválóan lehessen használni, így függőlegesen – 10° és + 45° között lehet irányozni vele [10].

A Puma esetében szakítottak a bonyolult és drága, és a csapatpróbák tapasztalatai alapján műszaki kockázatot jelentő MK35/50 Rh 503 típusú fegyver alkalmazásával, hanem a Rheinmetall vállalattól rendelték meg az MK 30-2/ABM[16] típusú 30 mm-es gépágyút. A gépágyú alapja az MK 30-2 típusú gépágyú volt, ami az úgynevezett AHEAD[17]-technológiával rendelkezik. A gépágyúcső végére egy olyan csőszájféket szereltek fel, amely egyben tartalmazza a lövedék torkolati sebességét mérő, valamint annak detonálási idejét beállító rendszerét is.

A gépágyúhoz alapvetően kétfajta lőszert rendszeresítettek, amelyekből a csigavonal alakú tárban 80: 120 arányban hevederezik be a kétféle lőszertípust. A lőszerek közül az APFSDS-T[18] lőszer hivatott a kisebb páncélvédelemmel rendelkező célok leküzdésére, míg a másik, általános rendeltetésű lőszer a KETF[19] rövidítést kapta. Ez egy olyan időzítőgyújtóval szerelt lövedék, amelynek a detonálási idejét az irányzó tudja meghatározni. A lőszer felrobbanásakor, a lövedék forgása miatt egy forgó repeszkúp jön létre, amely 179 db apró, 2-3 mm hosszú wolframhengert tartalmaz, amelyről a 6. ábrán lehet látni egy szemléletes metszeti képet. Ez a fajta lőszer alkalmas kisebb célok rongálására is, így az ellenséges felderítőeszközök, nem páncélozott célok megsemmisítésére, de akár drónok ellen is bevethető. A Puma esetében a szokásosan 7,62 mm-es kaliber helyett a párhuzamosított géppuska űrméretét 5,56 mm-re csökkentették le, így azonos lőszertömeg mellett nagyobb mennyiségű lőszer, jelen esetben járművenként 2000 db-os lőszerkészlet jár [16].

Harckocsik ellen a Puma leghatékonyabb fegyvere a torony bal oldalára integrált MELLS[20]-rendszer, ami kettő, az Eurospike[21] által gyártott SPIKE LR tandem robbanófejes páncéltörő-rakétát tartalmazza, 4.000 méteres maximális lőtávolsággal és 700 mm páncélátütési képességgel (RHA-egyenérték). A harcjármű önvédelmét vannak hivatva biztosítani a torony végébe szerelt 6 db, 76 mm-es ködgránátvetők is, amelyeknek a leváltása a Rheinmetall által kifejlesztett ROSSY ködgránátvetőkre hamarosan várható [17].

15 Ez az úgynevezett hunter-killer-lehetőség.
16 Air Burst Munitions, azaz levegőben detonáló lőszer.
17 Advanced Hit Efficiency and Destruction, azaz Fejlett Találati és Megsemmisítési Hatékonyság.
18 Armor-Piercing Fin-Stabilized Discarding Sabot Tracer – Űrméret alatti leválóköpenyes páncéltörő nyíllövedék nyomjelzővel.
19 Kinetic Energy-Timed Fuse – Kinetikus energiájú lövedék időzítővel ellátva.
20 Mehrrollenfähige Leichte Lenkflugkörpersystem – Többfunkciós, könnyű páncéltörő rakétarendszer.
21 40%-ban a Rheinmetall tulajdona.

6. ábra
A KETF-lőszer, annak metszete és repeszeinek szórásképe [18]

Az MH által támasztott főbb követelmények

Az MH a nehézdandárba tervezett lánctalpas gyalogsági harcjárművek beszerzésére megalkotta a hadműveleti követelményrendszerét, amely dokumentumnak a Puma jármű értékelésének szempontjából legfontosabb megállapításai, hogy a jármű:

- tegye lehetővé egy (lövész) raj teljes körű harci alkalmazását Magyarország éghajlati viszonyai és azok szélsőségei között, évszaktól és napszaktól függetlenül, korlátozások nélkül;
- biztosítsa a kezelőszemélyzet (2-3 fő – vezető, parancsnok és/vagy irányzó,) valamint a raj állományának (6-8 fő) és felszerelésének málházását;
- a szakági járművek kialakításához a konstrukció – a kialakítás és a szükséges mértékű átalakítás révén – bázisjárműként legyen felhasználható;
- egy feltöltéssel hatótávolsága legalább 500 km legyen [5].

A többi részletezett technikai és hadműveleti követelményeken túl ajánlásként szerepel, hogy a jármű:

- legyen (vízi átkelésre történő felkészítést követően) úszóképes;
- rendelkezzen kiegészítő – fő tűzfegyver irányzásától független – fegyverrendszerrel a harcjárműparancsnok részére.[22]

[22] un. hunter – hunter képesség.

Következtetések

A fenti információk, és a rendelkezésre álló követelmények tekintetében, irodalomvizsgálat és összehasonlító elemzések alapján kijelenthetem, hogy a jármű, a főbb paraméterek szempontjából megfelel az MH által támasztott előírásoknak, követelményeknek. Azonban a Zrínyi 2026-ban is megjelenő digitáliskatona-program eredményeivel felszerelt 21. századi katona, akár a teljes fegyverzettel és felszereléssel ellátott német katona is, aki használja az IdZ,[23] jövő katonája felszerelését, éppen csak, hogy be tudja magát „préselni" a harcjármű üléseibe, ami a hasonló paraméterekkel rendelkező magyar katona esetében is gondot fog okozni. A tervezők kijelentése alapján az az ideális lövészkatona a Puma szempontjából, akinek a magassága nem haladja meg a 184 cm-t, mert ellenkező esetben az nem képes normaidő alatt elhagyni a járművét [17].

Ezenfelül a jármű hatótávja kisebb, mint azt az MH követelményei előírják, és az eszköz, harci tömegénél fogva nem úszóképes. Mivel Magyarország területén hozzávetőlegesen 30 km-enként található egy legalább 10 méter szélességű vízfolyás, így a mozgásképesség fenntartása érdekében a műszaki mozgástámogatás rendszerét kell ehhez igazítva, összehangoltan fejleszteni.

A harcjármű ezenkívül nem rendelkezik a parancsnok által külön kezelhető fegyverrel, csak az irányzótól képes a feladat átvételére, a fő fegyverzet használatára.

Megállapításom szerint jelenleg a legnagyobb hátránya a Puma harcjárműnek, ami alapján ebben a kialakításában *nem, vagy csak korlátozásokkal alkalmas* az MH lánctalpas harcjárművel szemben támasztott követelményeknek megfelelni, az az, hogy a harcjárműből csak lövészpáncélos verzió készült, és nem is tervezik rövid távon ennek a rendszernek a megváltoztatását. Ez köszönhető annak, hogy a Bundeswehr a többi feladatot (mentés-vontatás, hídvetés, logisztikai, műszaki biztosítás stb.) a már meglévő lánctalpas vagy kerekes technikai eszközökre bízza, mint a Boxer kerekes harcjármű, vagy a Leopard 1 harckocsi alvázára épített szakjárművek.

A fenti megállapításaim alapján bizton állíthatom, hogy a Puma gyalogsági harcjármű ebben a formájában nem vagy csak kompromisszumokkal felel meg a Honvéd Vezérkar Hadműveleti Csoportfőnökség által támasztott követelményeknek, ami csak az eszközök átalakításával vagy másfajta, hasonló képességekkel rendelkező lánctalpas harcjármű alkalmazásával lenne kiváltható, mint például amilyen a Rheinmetall által gyártott Lynx lánctalpas harcjármű.

Hivatkozások

[1] Katonai lánctalpas gépjárművek. Típusok, szakkifejezések és meghatározások, Magyar katonai szabvány MSZ-K 0143, Magyar Szabványügyi Testület, 2006.

[2] Arcanum, „Az európai hagyományos fegyveres erőkről (CFE) szóló szerződés," *Arcanum,* [Online]. Elérhető: www.arcanum.hu/hu/online-kiadvanyok/Tenyek-Konyve-tenyek-konyve-1/nato-16647/fegyverzetkorlatozas-leszereles-17791/

[23] Infanterist der Zukunft.

fegyverzetkorlatozas-17853/a-fobb-fegyverzetkorlatozasi-egyezmenyek-es-szerzodesek-kronologiaja-19631994-17882/1990-az-europai-hagyomanyos-fegyveres-erokrol-cfe-szolo-szerzodes-178AB/ (Letöltve: 2019. 02. 26.)
[3] J. Szabó szerk., *Hadtudományi Lexikon A-L.* Budapest: Magyar Hadtudományi Társaság, 1995.
[4] M. Berkáné Danesch szerk., *Katonai terminológiai értelmező szótár.* Budapest: Zrínyi Kiadó, 2015.
[5] A gépesített (nehéz) lövész lánctalpas gyalogsági harcjármű hadműveleti követelmények, 1717/136-3/2017. HVK HDMCSF, HVK Hadműveleti Csoportfőnökség ügydarab.
[6] „SPz Marder 2 (Bw) – Prototyp," *panzerbaer.de,* [Online]. Elérhető: www.panzerbaer.de/types/bw_spz_marder_2-a.htm (Letöltve: 2019. 02. 26.)
[7] "Marder 2 Infantry Fighting Vehicle," *fighting-vehicles.com,* [Online]. Elérhető: http://fighting-vehicles.com/marder-2-infantry-fighting-vehicle/ (Letöltve: 2019. 02. 26.)
[8] "Marder 2 Infantry Fighting Vehicle," *military-today.com,* [Online]. Elérhető: www.military-today.com/apc/marder_2.htm (Letöltve: 2019. 03. 20.)
[9] "Brand new armored platform NGP (Neue Gepanzerte Plattformen), which is not built," *survincity.com,* [Online]. Elérhető: http://survincity.com/2013/05/brand-new-armored-platform-ngp-neue-gepanzerte/ (Letöltve: 2019. 03. 20.)
[10] "Armoured Infantry Fighting Vehicle (AIFV) Puma", *Defence Technology Review,* no. 4, 2014. [Online]. Elérhető: www.mittler-report-shop.de/product_info.php?language=en&products_id=65 (Letöltve: 2019. 03. 20.)
[11] "Puma IFV SPz," *fighting-vehicles.com,* [Online]. Elérhető: http://fighting-vehicles.com/puma-ifv-spz/ (Letöltve: 2019. 03. 20.)
[12] N.R.P., "Schützenpanzer Puma: Germany's deadly new Infantry Fighting Vehicle," *defencyclopedia.com,* [Online]. Elérhető: https://defencyclopedia.com/2015/06/26/schutzpanzer-puma-germanys-deadly-new-infantry-fighting-vehicle/ (Letöltve: 2019. 03. 20.)
[13] "New Puma infantry fighting vehicle to successively replace predecessor Marder," *defence.com,* [Online]. Elérhető: www.rheinmetall-defence.com/en/rheinmetall_defence/public_relations/themen_im_fokus/puma_ersetzt_marder/index.php (Letöltve: 2019. 03. 21.)
[14] Autobild, "Alle infos zum SPZ Puma," *Autobild,* [Online]. Elérhető: www.autobild.de/bilder/alle-infos-zum-spz-puma-3545265.html#bild28 (Letöltve: 2019. 03. 21.)
[15] "Puma Infantry Fighting Vehicle Enters Bundeswehr Service," *defencetalk.com,* June 2015, [Online]. Elérhető: www.defencetalk.com/puma-infantry-fighting-vehicle-enters-bundeswehr-service-64656/ (Letöltve: 2019. 03. 21.)
[16] "The German Puma Infantry Fighting Vehicle," *tanknutdave.com,* [Online]. Elérhető: http://tanknutdave.com/the-german-puma-ifv/ (Letöltve: 2019. 03. 21.)
[17] *Defence Technology Review,* no. 3, 2018, [Online]. Elérhető: www.mittler-report-shop.de/product_info.php?language=en&products_id=299 (Letöltve: 2019. 03. 21.)
[18] „Rheinmetall gyári előadás," nyilvánosan közzétehető ábra, 2017. 12. 15.
[19] „Rheinmetall GmbH. felvétel," Deutsches Panzermuseum, Munster, 2018. 01. 18.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
15. évfolyam (2020) 1. szám 45–61.
DOI: 10.32567/hm.2020.1.4

Bodnár László[1]

Lakott területet érintő erdőtüzek vizsgálata, és a védekezés egyes lehetőségei

Examination of Forest Fires at Inhabited Areas and Certain Possibilities of Protection

Az erdő- és vegetációtüzek az egyik legnagyobb kihívást jelentő természeti katasztrófák. A globális éghajlatváltozás következményeként ma már olyan területeken is kialakulnak szabadtéri tüzek, ahol erre korábban nem volt példa. Ez további kutatási igényt jelent. A cikk megírásában fontos szerepet kapott a témakörrel kapcsolatos hazai és nemzetközi szakirodalom tanulmányozása és elemzése, valamint egy nemzetközileg elismert erdőtüzes konferencián való részvétel, ami rámutatott a hazai hiányosságokra és fejlesztési lehetőségekre. Emellett a szerző műszaki rajzokat készített, és számításokat végzett a kutatás során. A cikkben a szerző a WUI (Wildland–Urban Interface) területen keletkező tűzesetek megelőző tűzvédelmét vizsgálja, különös tekintettel a védelmi zónák létrehozására. A vizsgálatból levont következtetések lehetőséget adnak egyes nemzetközi tűzvédelmi módszerek továbbfejlesztésére, és azok jogszabályi alapú javaslattételére. A cikkben bemutatott védőzóna-tervezés hasznosítható a vegetációtűz megelőzésében, valamint a lakóépületek műszaki tervezésében.

Kulcsszavak: **Wildland-Urban Interface (WUI), tűzterjedés, belső zóna, valós zóna, optimális zóna**

Forest and vegetation fires are natural disasters with major challenges in most countries all over the world. As a result of the global climate change, a large number of outdoor fires are generated in areas where this type of disaster has not been typical so far. This requires further research in the related branch of science. When writing the paper, it was important to analyse the relevant Hungarian and international literature in the topic. It was also important to participate in an

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: bodnar.laszlo@uni-nke.hu, ORCID: https://orcid.org/0000-0001-9196-8030

international forest fire conference, which highlighted the shortcomings and the development opportunities in Hungary. In addition, the author made technical drawings and calculations during the research. As a result of the paper, the author examines some of the options of the fire prevention in case of fires at the WUI (Wildland Urban Interface). The conclusions drawn from the study provide an opportunity to improve some international fire protection methods, and opportunity for legislative proposals. The plan of the protection zone presented in the paper can be used in the prevention of the vegetation fires and in the technical design of the residential buildings.

Keywords: **Wildland Urban Interface (WUI), fire propagation, internal zone, real zone, optimal zone**

Bevezetés

Számos publikáció következtetése alapján megállapítható, hogy vannak olyan rendkívüli események, (természeti katasztrófák) amelyek a globális felmelegedés számlájára írhatók. Nyáron több forró nappal, és elhúzódó szélsőséges időjárási tényezővel kell számolni, mint korábban [1], [2]. Ez több lehetőséget ad az erdő- és vegetációtüzek kialakulására. 2018-ban a tűzesetek súlyosan érintették Svédországot, az Egyesült Királyságot, Írországot, Finnországot és Lettországot is, olyan államokat, ahol eddig az erdőtüzek nem jelentettek komolyabb kihívást a védelmi szférának. Az európai erdőtüzek információs rendszere (EFFIS[2]) mintegy 10 milliárd eurós veszteséget becsült tűzesetek miatt. 2017-ben az erdőtüzek több mint 1,2 millió hektárnyi területet pusztítottak el. Emellett az Európai Unióban a természetes földterületek kárértékén túl a tüzek 127 ember életét követelték [3]. A cikkben a 2017-es adatokat mutatom be, mivel a kutatás befejezésekor a 2018-as adatok még nem álltak teljeskörűen rendelkezésre. A statisztikai adatok megismerése után felmerül a kérdés, hogy az erdőtüzek ellen milyen állampolgári megelőzési módszerek vannak, illetve hogy ezek mennyire hatékonyak a megelőző tűzvédelem szempontjából.

Az erdőtüzek oltásának hatékonyságát ma már számos publikáció vizsgálta. Ezek a tanulmányok elsősorban a tűzoltói beavatkozást érintették részletesebben [4], [5]. A vegetációtüzek megelőzéséről kevesebb publikációt lehet találni [6], azt is elsősorban a nemzetközi szakirodalmak között [7], [8]. A cikkben a természetes erdőterület peremvidékén lévő lakott területek, WUI[3] (Wildland-urban Interface – a továbbiakban: WUI) tűzveszélyének elemzését mutatom be. Az USA-ban és a mediterrán országokban már találtak összefüggést a WUI-területek és a tűzesetek között. Ennek köszönhetően, ezekben az országokban már folynak vizsgálatok az úgynevezett WUI-térképezésre [9]. A WUI-területen keletkezett tűzesetek veszélye azért nagy, mert egyrészt az éghető biomassza veszélyt jelent a lakosságra nézve, másrészt pedig az emberi gondatlanságból vagy szándékosságból okozott tüzek is jelentős veszélyt jelentenek

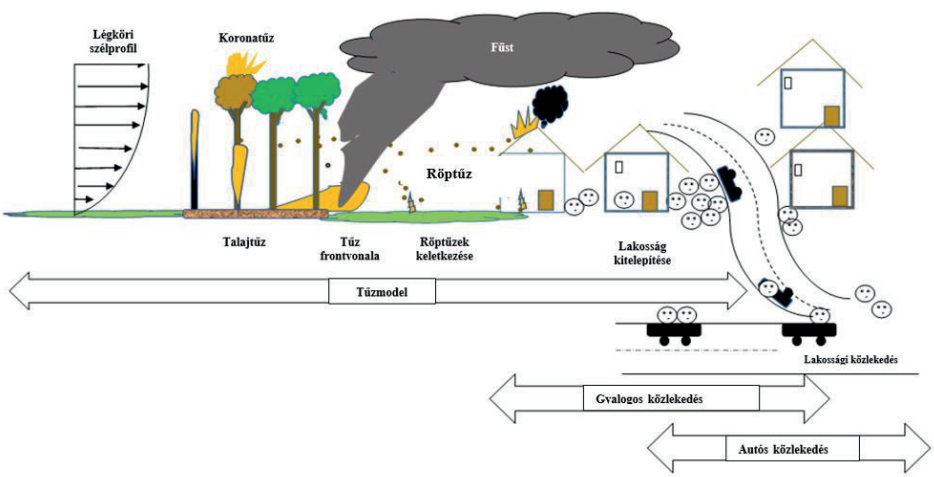
[2] European Forest Fire Information System.

[3] WUI (Wildland-Urban Interface) olyan terület, ahol az épített környezet a természetes környezet határán, peremén található. Ezeknek a területeknek a tűzveszélye igen nagy.

a természetes növényzetre. Ennek következtében felmerül a kérdés, hogy az erdőtüzek tulajdonképpen természeti vagy civilizációs katasztrófák? A válasz nem egyértelmű, viszont az, hogy e két tényező jelentős hatással van az erdőtüzek kialakulására vitathatatlan. Ahhoz, hogy a WUI-területen keletkezett tűzkárokat megelőzzük, vagy adott esetben csökkentsük, tűzmegelőzési megoldásokra, irányelvekre van szükség. A cikkben ezért a nemzetközi szinten ismert és elfogadott erdőtűzmegelőzési módszereket mutatom be és elemzem, elsősorban az úgynevezett védelmi zónák létrehozásának vizsgálatával. Feltételezésem szerint a védelmi zónák létrehozásával csökkenthető vagy akár meg is előzhető az erdőről a lakóépületre történő tűzátterjedés. Ennek eredményeként megnő az erdő peremvidékén élők biztonsága.

WUI-tüzek kialakulása és terjedése

A hazai [10], [11] és nemzetközi szakirodalom [12] tekintetében már számos szerző foglalkozott az erdő- és vegetációtüzek kialakulásával. A különböző kutatások és elemzések eredménye, hogy az erdőtűz kialakulásának legfőbb oka az emberi gondatlanság, feltétele pedig a kedvező időjárás és az éghető biomassza jelenléte [13]. Az éghető biomassza már önmagában veszélyt jelent a lakosságra nézve. Ez különösen igaz akkor, ha az időjárás meleg, száraz, illetve esetenként erős széllökések lépnek fel. Ezeket az időszakokat nevezzük tűzszezonnak. Magyarországon ez a kora tavaszi, illetve a nyári időszak. Amikor már a tűz kialakult, rendkívül fontos a tűzterjedés megakadályozása, különösen azokon a területeken, ahol a lakosság közvetlenül az erdő peremvidékén él [14]. Ezek a már fent említett WUI-területek. Itt az erdőtűz az emberi életet és az anyagi javakat is veszélyeztetheti, ennek következtében pedig szükségessé válhat akár a lakosság kitelepítése is. Ezt a folyamatot mutatja be az 1. ábra.



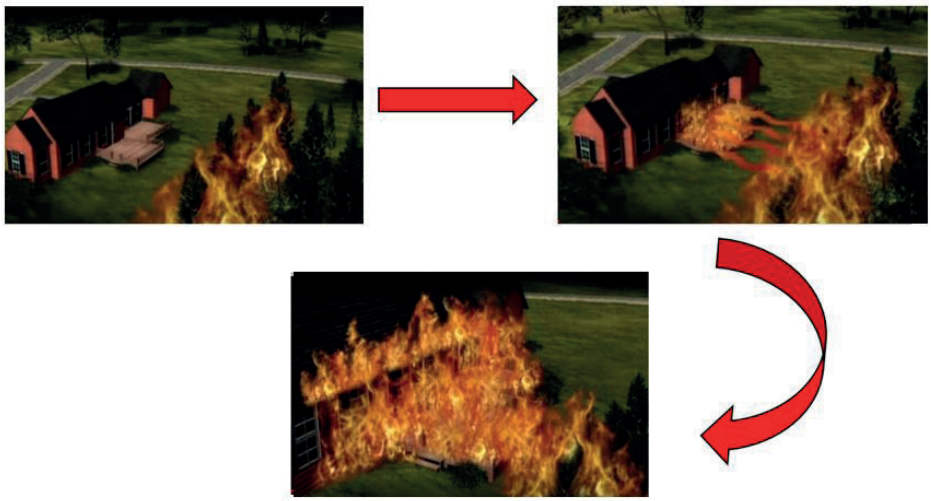
1. ábra
Tűzterjedés WUI-területen. (a szerző szerkesztése [15] alapján)

Nemcsak a mediterrán régióban, de Magyarországon is nagyszámú erdőtűz keletkezik a tűzveszélyes időszakokban [16]. Ekkor a tüzek kialakulása és terjedése is gyors, különösen erős légköri mozgás esetén. Egy erdőterület kapcsán fontos a vegetáció tekintetében a kialakulni képes lángmagasság, illetve lánghossz vizsgálata, hiszen ez lehetőséget ad koronatűz kialakulására [10]. Bár ennek megelőzésére nemzetközi szinten találunk erdészeti megoldásokat, azonban ez teljes mértékben nem megoldott, így számos esetben a koronatüzek kialakulása nem előzhető meg [17]. Az erős intenzitású, gyorsan terjedő tüzek jelenségei közé sorolható a lángképződés, a füstképződés, valamint a röptűz kialakulása (firebrand[4]). Ez utóbbi komoly kihívást jelent, hiszen a légköri mozgás okozta röptűz keletkezése megváltoztatja a tűzoltás taktikáját, valamint hatással van az erdőhöz közeli lakóépületek veszélyeztetésére is. A röptüzek nagyon könnyen lángra gyújtják az éghető anyagokat, ami lakóövezetben az épület tetőzetét is jelentheti. Ettől kezdve dominóhatás-szerűen már az erdőterület közelében lévő valamennyi lakóépületet veszélyezteti a tűz, aminek egyik következménye lehet a veszélyben lévő lakosság kitelepítése. A lakosság kitelepítése, kimenekítése polgári védelmi feladat, ezért egy ilyen típusú katasztrófa-elhárítást a hivatásos katasztrófavédelmi szervezet polgári védelmi és tűzoltósági szakterülete közösen együttműködve hajt végre [18]. Ez azonban csak akkor fordul elő, ha a tűz a lakóépületek felé terjed, ezzel veszélyeztetve az emberi életet [19], [20]. Ez WUI-területen különösen nagy veszélyt jelent. A tűz épített környezetre történő terjedését a következő fejezet mutatja be.

Tűzterjedés WUI-területen

A tűz számos esetben veszélyeztetheti az emberi életet és az anyagi javakat, különösen WUI-területen. Ahhoz, hogy a tűz lakóépületre történő terjedését vizsgáljuk, elengedhetetlen a röptűz jelenségének a vizsgálata, ugyanis ez okozza a WUI-tüzek nagyrészét. Ahogyan az előző fejezet is említi, a röptüzek a tűzterjedés során a levegőbe kerülő olyan égő fadarabok, amelyek légköri mozgás hatására a tűz frontvonalától távolabbi területeken az éghető biomasszát meggyújtva további tüzeket eredményeznek. Ilyen röptüzek keletkezhetnek a lakóingatlanok épületszerkezetén vagy akár az azt körülvevő gyúlékony építményeken is [21]. Ahogy a WUI kapcsán megkülönböztetünk közvetlen és közvetett WUI-t, úgy a tűzterjedés során is megkülönböztethetünk közvetlen és közvetett lakóépületre történő tűzterjedést. Erre mutat példát a 2. ábra.

[4] A „firebrand" a tűz frontvonalában keletkező, még égő fadarab, amely a tűz frontvonalától távolabb a földre hullva újabb tüzek (spotfire) kialakulását okozhatja.



2. ábra

Közvetlen tűzterjedés lakóépületre (a szerző szerkesztése [22] alapján)

Lakóépületre történő közvetlen tűzterjedés esetén a tűz frontvonala tulajdonképpen eléri az épített környezetet és meggyújt mindent, ami éghető. Ebben az esetben a röptüzek (firebrands) közvetlenül felülről hullanak rá az épületre, ezzel tüzet okozva. Ez a legtöbb esetben lombkoronáról történik, nem pedig talajtűz következményeként. Az ilyen típusú tüzek ellen lakossági módszerekkel szinte lehetetlen védekezni, a tüzet a legtöbb esetben a kiérkező, elsődlegesen beavatkozó tűzoltó erők oltják el. A 2. ábrán jól látható, hogy ha a tűz eléri a lakóépületet és azon tűz keletkezik, rövid idő alatt az egész épületszerkezet meggyullad, ez pedig már a többi közelben lévő lakóépületekre is komoly veszélyt jelent. Viszont abban az esetben, amikor a lakóépület távolabb helyezkedik el a tűz frontvonalától, akkor elsősorban a röptüzek (spot fire[5]) talajtüzeket létrehozva oldalról érik el a lakóépületet. Ezt mutatja be a 3. ábra.

[5] A „spot fire" a röptűz azon fajtája, amikor az égő fadarabok (firebrands) a tűz frontvonalától távolabbi helyeken egy másik, új tűz kialakulását idézték elő. Míg a firebrand a még hulló, égő fadarabot jelenti, addig a „spot fire" a már földre érkezett kialakult új tűzfészket. A két fogalom között a magyar nyelv nem tesz különbséget, mindkettőt egyaránt röptűznek nevezi a szakirodalom.

3. ábra
Közvetett tűzterjedés lakóépületre (a szerző szerkesztése [22] alapján)

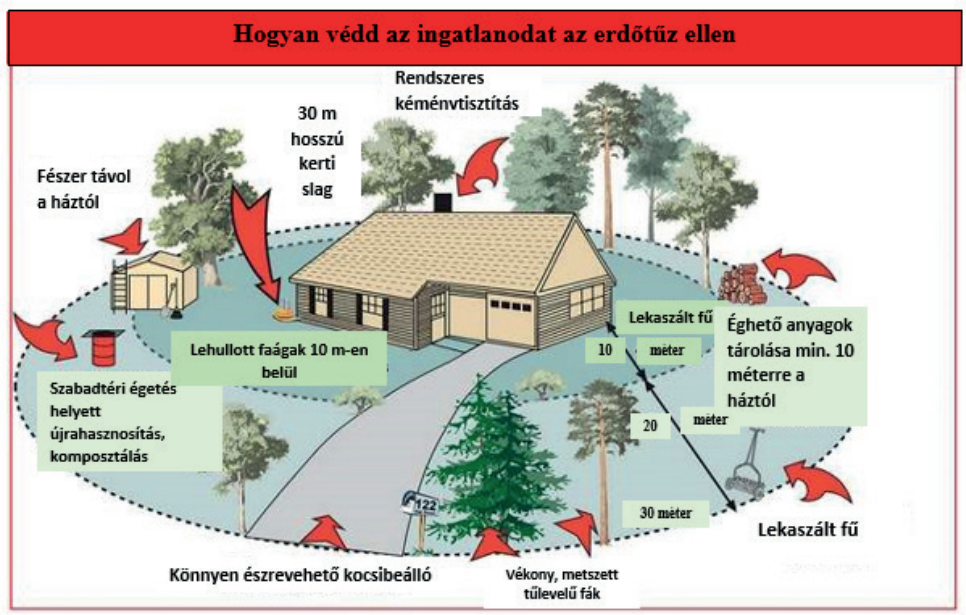
A 3. ábra bal felső sarkában megjelennek az első röptüzek, amelyek a talaj gyúlékony növényzete miatt könnyen meggyulladnak, majd megkezdődik a talajszintű tűzterjedés. A röptüzek az intenzív feláramlás következtében folyamatosan keletkeznek. Emiatt az első röptüzek megjelenése után továbbiakra kell számítani (3. ábra jobb felső kép). Ezután rövid időn belül a röptüzek elérik a lakóépület valamely éghető részét (3. ábra bal alsó kép), a képen jelen esetben egy verandát, ahol a legtöbbször számos gyúlékony anyag található. Innen már csak egy lépés az épületszerkezetre történő tűzterjedés. Ez akár az egész épület leégéséhez, valamint további lakóépületre történő terjedéséhez vezethet (3. ábra bal alsó kép). Az épületek közötti tűzterjedés a WUI-tüzek esetében ott jelenti a legnagyobb kihívást, ahol a lakosság az erdő peremvidékén, tömbösítve (nagy laksűrűség) él.

Az erdőről az épített környezetre terjedő tüzek kapcsán fontos vizsgálni, hogy az ilyen jellegű tüzek ellen milyen megelőzési, illetve védekezési lehetőségek vannak. A következő fejezetben a lakóépületek védelmére szolgáló lakossági megoldásokra vonatkozó javaslatokat mutatom be.

Javaslatok lakossági tűzmegelőzési módszerekre WUI-területen

Mivel Magyarországon a WUI eddig kevésbé ismert fogalom, ezért az azokkal kapcsolatos védekezési lehetőségek sem ismertek. Azonban egyes országokban ez van

a tűzvédelmi politika középpontjában (Portugália, USA). Az erdőről a lakóövezetbe terjedő tűzesetek vizsgálata alapján rendkívül fontos különböző lakossági irányelvek betartása, a lakóépületek tűz elleni védelme érdekében. Nemzetközi szinten erre már találunk olyan irányelveket, amelyek betartásával nagymértékben hozzájárulhatunk egy-egy lakóépület megmentéséhez WUI-területen. Ezek a közvetlen tűzterjedést megelőző módszerek elsősorban az állampolgároknak szólnak, betartásuk nem igényel sem jelentős időt, sem pedig jelentős többletköltséget, ezért betartásuk javasolt és a világ bármely országában alkalmazhatók. Ezt mutatja be a 4. ábra.



4. ábra

Megoldások WUI-tüzek elleni védekezésre (a szerző szerkesztése [23] alapján)

Ahogyan az ábrán is látszik, a következő egyszerű lakossági módszerek megvalósítása segítheti a WUI-n lévő ingatlanok tűzvédelmét [23]:

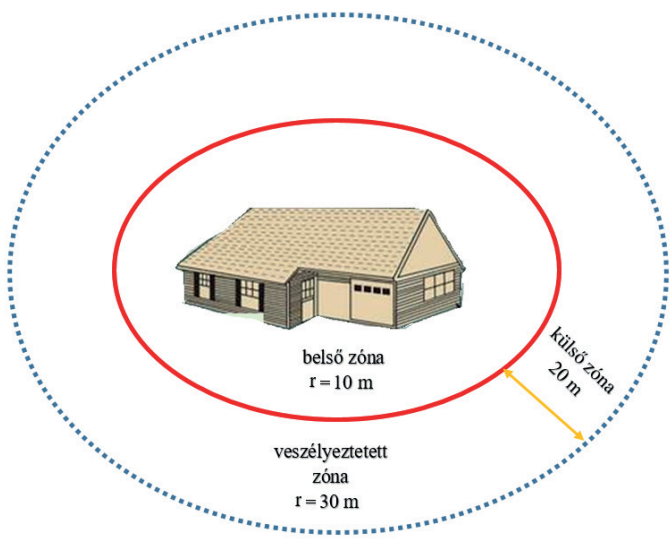
- Növényzet csökkentése az ingatlanhoz vezető út/járda mentén. Ezáltal a járda mint biomasszamentes sáv tűzpásztaként szolgál, megelőzve a talajtüzek terjedését.
- A lakóépületet körülvevő gyepterületen fontos a rendszeres fűnyírás, úgy, hogy a fűszálak mérete lehetőleg ne haladja meg a 10 cm-t. Ez a módszer lassítja a tűzterjedést.
- Az elszáradt leveleket, faágakat el kell távolítani, mivel ezek rendkívül könnyen meggyulladnak.
- A kémény rendszeres tisztítása, valamint a lakóépület közelében lévő fák kinyúló koronarészének távolsága minimum 3 méterre legyen a kéménytől.

- Az ingatlanhoz tartozó egyéb gyúlékony építmények (például fészer, garázs) távolsága a lakóépülettől legyen legalább 10 méter (belső zónahatár).
- Folyamatos vegetációtisztítás a lakóépülettől számított 10 méteren belül. (belső zóna)
- Szabadtéri égetés helyett komposztálás vagy újrahasznosítás.
- Közvetlenül a ház közelében legyen egy legalább 30 méter hosszú locsolótömlő a kezdetleges röptüzek oltása érdekében.

Ezek a módszerek hatékonyan hozzájárulhatnak a megelőző tűzvédelem, valamint a különböző katasztrófák építésügyi vonatkozásaihoz is [24].

A lakóépület belső védelmi zónájának vizsgálata

Az előző fejezetek alapján látható, hogy a lakossági intézkedéseknek számos formája van. Ezek elsősorban a 4. ábrán feltüntetett 30 méter sugarú kör területén belül alkalmazhatók hatékonyan. Ezt a területet, amely tulajdonképpen a lakóépületet, valamint annak közvetlen környezetét lefedi, a nemzetközi szakirodalom „Home Ignition Zone"-nak (HIZ) nevezi [25]. Az ehhez hasonló területeken a tűzoltói beavatkozás veszélyes, ezért figyelembe kell venni a beavatkozás biztonsági követelményeit is [26], [27].



5. ábra
Lakóépület veszélyeztetett zónái WUI-területen (a szerző szerkesztése [22] alapján)

Az 5. ábra segítségével megvizsgáljuk a fent említett területet a WUI-n. A 30 méter sugarú kör területét két részre lehet osztani úgy, mint külső zóna (közvetett kockázat) és belső zóna (közvetlen kockázat). A belső zóna a lakóingatlan körüli 10 méter sugarú

kör területe, a külső zóna pedig a belső zóna határától számított 20 méter sugarú kört foglalja magában. Így összesen a veszélyezetetett terület nagysága egy 30 méter sugarú kör (HIZ) területe. Az elemzés szempontjából a továbbiakban a lakóépületet körülvevő belső zónát vizsgáljuk, mivel ez az a terület, amely a tűzterjedés szempontjából fontosabb az emberi élet és az anyagi javak védelme érdekében.

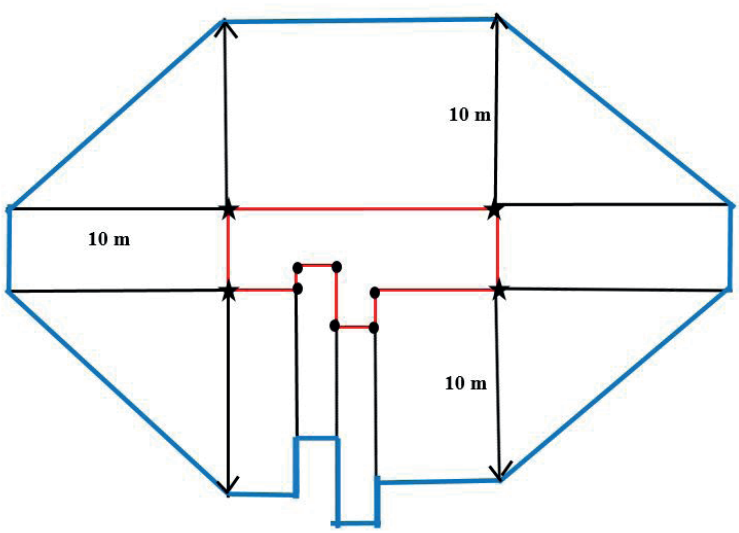
A belső és külső zóna szemléltetése után fontos elsősorban a belső zóna méretének (T_{bz}) meghatározása. Mivel a vizsgált terület kör alakú, ezért a kör területének számítását veszem alapul ami:

$$T = r^2\pi$$

azaz jelen esetben

$$T_{bz} = r^2\pi = (10\ m)^2\ 3{,}14 = 314\ m^2$$

A belső zóna mérete tehát jelen esetben 314 m^2. Ahogyan az 5. ábrán is látszik, a lakóépületet körülvevő belső zóna határa (10 m – piros kör) az épület mértani középpontjától lett mérve. Ennek előnye, hogy a zóna így egy jól szemléltethető kör alakú síkidom, amivel könnyű számolni. Ezt nevezhetjük mértani belső zónának. Hátránya viszont, hogy ennek a zónának a valós nagysága hibás, hiszen egy lakóépületnek jelentős hossza, szélessége és magassága is van a középponthoz képest. Ez azt jelenti, hogy a 10 méteres határ az épület és a zóna széle között számos helyen valójában nem éri el a 10 métert, a kiugró épületrészek miatt. Így a belső zóna valós formája nem lehet kör alakú! A valós alak formája sokszögalak. Ezt nevezhetjük valós belső zónának. Így a feltételezett belső zóna mérete sem 314 m^2, hanem jelentősen több. Ezt az alábbi módon vizsgáltam:

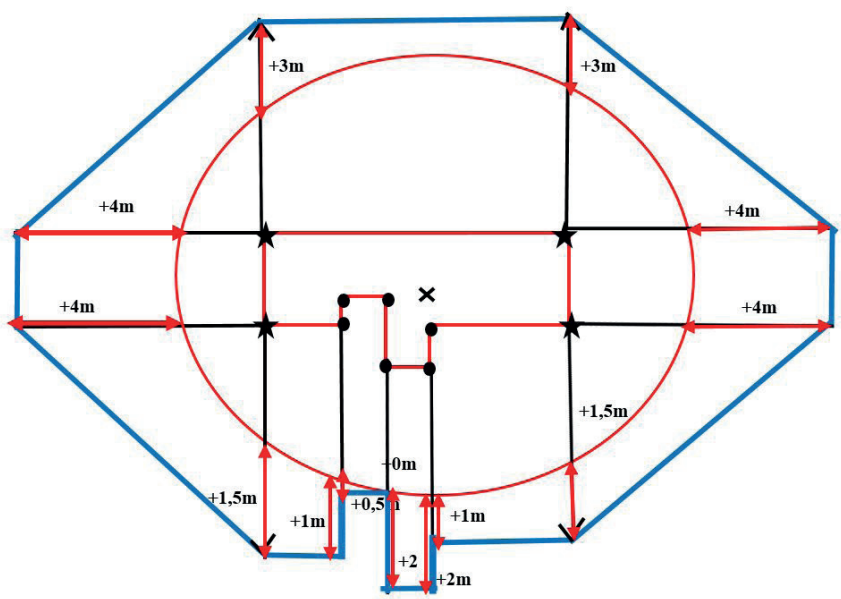


6. ábra

A belső zóna valós mérete [a szerző szerkesztése]

Az ábra műszaki rajzának elkészítéséhez, valamint a valós belső zóna meghatározásához az 5. ábrán feltüntetett épület alaprajzát használom. Ennek eredménye a 6. ábrán szemléltetett valós belső zóna kialakítása. Itt a zóna 10 méteres határa nem az épület középpontjától lett mérve, hanem a lakóépület alaprajzának kiugró, szélső részeitől. Ezek úgynevezett csúcspontokban végződnek, amelyeket az ábrán fekete pontokkal, illetve csillagokkal jelöltem (10 db). A csúcspontoktól mért 10 méteres távolságokat összekötő vonal pedig kiad egy sokszögalakot. A fekete pontokkal jelölt csúcspontokból egy, míg a csillaggal jelölt csúcspontokból két irányba húztam meg a távolságokat, így összesen 14 mért pont keletkezett. Ennek a zónának a területe szemmel láthatóan is nagyobb, mint a lakóépület mértani középpontjától mért 10 méter sugarú kör területe. A kiugró és benyúló épületrészek miatt a csúcspontoktól mért távolságok az eredeti kör alakú zónán kívül esnek.

Így tehát a valós belső zóna sokszögalakja már relevánsabbnak tekinthető, mint a kör, hiszen ebben az esetben az épület kialakítása is figyelembe lett véve a zónahatárok létrehozásakor. Hátránya azonban az, hogy nehéz vele számolni, illetve jogszabályi alkalmazás esetén a kör alakú zónameghatározás egyszerűbb, érthetőbb és megvalósíthatóbb. A megoldás tehát a két zónatípus összefésülésében rejlik, egy optimális zóna kialakításának lehetőségével. Ez úgy valósítható meg, ha a sokszögalakú síkidom területének nagyságához közel azonos területű kör alakú síkidomot hozunk létre.



7. ábra

10 méteres távolság közti különbség a mértani és a valós belső zóna között [a szerző szerkesztése]

Az ábrán piros körrel lett jelölve a mértani, a lakóépület középpontjától mért 10 méter sugarú kör. A 6. ábrához hasonlóan a lakóépület csúcspontjaitól mért 10 méteres határvonalakat összekötő görbét is ábrázoltam kék színnel, amely egy valós, sokszögalak

síkidomot formál. A 7. ábra bemutatja a két zóna határpontjai közötti távolságot (piros nyilak) a 14 mért ponton. Láthatjuk, hogy az épület kialakítása miatt a csúcspontok közötti távolsága változó, attól függően, hogy az épület adott csúcspontja milyen távolságra helyezkedik el a lakóépület mértani középpontjától. Ez lehet akár 4 méter is. Ahhoz, hogy egy új, optimális kör alakú zónát rajzolhassunk, meg kell határozni, hogy a két zónahatár közötti különbség átlagosan hány méter ($S_{átl}$). Ezt az értéket úgy kapjuk meg, ha a két zóna határpontjai közötti távolságokat összeadjuk, majd elosztjuk a mért pontok (csúcspontok) számával. Ez jelen esetben a következőképpen alakul:

$$S_{átl} = \frac{3m + 3m + 4m + 4m + 1{,}5m + 1m + 2m + 2m + 0m + 0{,}5m + 1{,}5m + 4m + 4m + 1m}{14} = \frac{31{,}5\ m}{14} = 2{,}25\ \text{m}$$

A rövid számolás eredménye jelentős. A sokszögalak alakú valós belső zóna határai átlagosan 2,25 méterrel távolabb esnek, mint a kör alakú mértani belső zóna határai. Ez a 10 méter sugarú kör esetén több mint 20%-os eltérés. Ez is azt bizonyítja, hogy a valós belső zóna értékei relevánsak, ám az értékek gyakorlati felhasználásához köralakra van szükség. Ezt egy optimális belső zóna létrehozásával érhetjük el a következőképpen:

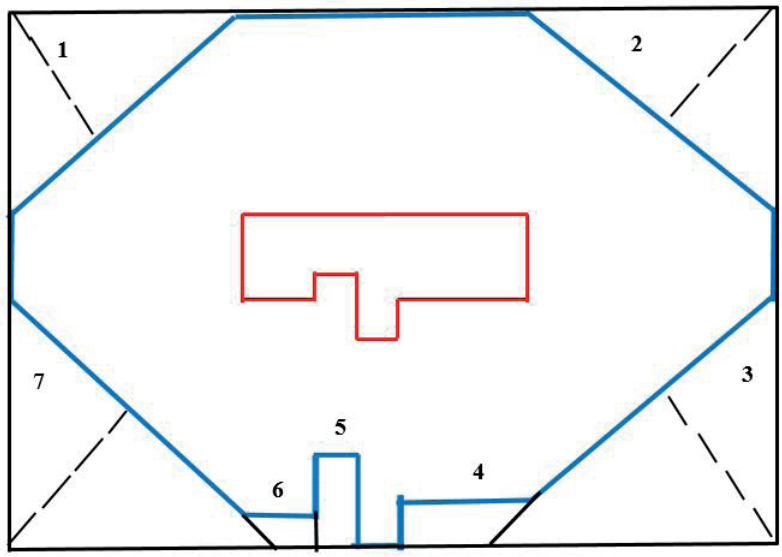
Az eddig bemutatott két zónát összevetve, a 10 méteres zónahatár értékét megtoldjuk a fent kiszámított 2,25 méterrel, (2 m-rel az egyszerűbb számolás miatt) ezzel létrehozva egy 12 méter sugarú kört. Ennek köszönhetően átlagos távolságot kapunk a lakóépület valamennyi csúcspontjától egy kör alakú síkidom formájában. Ez tulajdonképpen a két zóna eredményének összevetése, amelynek eredménye egy kör alakú síkidom. Ennek a területe feltételezhetően megközelíti a valós belső zóna területének nagyságát. Minél kisebb a két zóna területének különbsége, az optimális kör alakú belső zóna kialakításának lehetősége annál jobb.

A következőkben e két síkidom területének kiszámítása következik. Első lépésként a 12 méter sugarú kör ($T_{kör\_optimális}$) területét számolom ki, ami:

$$T_{kör\_optimális} = r^2\pi = (12\ m)^2 x\ 3{,}14 = 452{,}16\ m^2$$

Az optimális kör alakú zóna területének nagysága tehát 452,16 m^2. Feltételezésem szerint ez az érték megközelíti majd a valós belső zóna területének nagyságát.

Második lépésként következik a sokszögalakú síkidom területének kiszámítása. Mivel erre nincsen külön képlet, ezért a terület kiszámítása úgy lehetséges, hogy a sokszögalakú síkidom legszélső pontjait (határértékeit) négy irányban összekötöm, ezzel létrehozva egy téglalapot. Ezt szemlélteti a 8. ábra.



8. ábra
A valós belső zóna kiszámítása [a szerző szerkesztése]

Azzal, hogy létrehoztam egy téglalapot a sokszögalak körül, úgy további síkidomok keletkeztek. 4 db háromszög, 2 db trapéz és 1 db téglalap. A valós belső zóna sokszögalakú területét tehát úgy számolhatjuk ki, ha a nagy téglalap területéből kivonjuk az összes újonnan létrehozott síkidom területét. A számítás során először a nagy téglalap területének kiszámítását kezdem.

A téglalap területe: A téglalap vízszintes oldalának – a) oldal – mérete 28,5 méter, b) oldala pedig 24,5 méter. A téglalap területe tehát:

$$\mathrm{T} = axb = 28{,}5mx\ 24{,}5 = 698{,}25\ \mathrm{m}^2$$

Ezután következik a háromszögek ($T_{háromszög}$) területének számítása:

$$T_{háromszög} = \frac{a\ ma}{2}$$

A számolást részletesen nem fejtem ki, a képlet használatával valamennyi háromszög területe kiszámítható, az egyes eredményeket pedig az 1. táblázat mutatja be.

1. táblázat

A létrehozott síkidomok területnagyságai a 8. ábra alapján [a szerző szerkesztése]

Síkidom száma a 8. ábrán	Síkidom területének nagysága
1	49 m^2
2	49 m^2
3	64 m^2
4	3,5 m^2
5	2 m^2
6	1,5 m^2
7	64 m^2

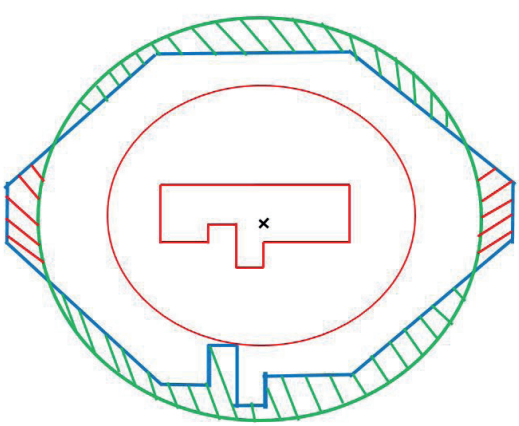
Összeadva az összes síkidom területét ($T_{összes\_síkidom}$) a következő értéket kapjuk:

$$T_{összes\_síkidom} = (49\ m)^2 + (49\ m)^2 + (64\ m)^2 + (3{,}5\ m)^2 + (2\ m)^2 + (1{,}5\ m)^2 + 64\ m)^2 = 233\ m^2$$

Viszont ahhoz, hogy a sokszögalak formájú valós belső zóna területét ($T_{valós\_zóna}$) meghatározzuk, a most kapott értéket ki kell vonni a téglalap területének nagyságából, ami:

$$T_{valós\_zóna} = (698{,}25\ m)^2 - (233\ m)^2 = 465{,}25\ m^2$$

A szerző által meghatározott kör alakú optimális zóna akkor hatékony, ha területének nagysága a lehető legjobban megközelíti a most kapott értéket. A kör alakú optimális belső zóna mérete a kiszámoltak alapján 452,16 m^2, a most kapott valós terület pedig 465,25 m^2. Ez jelen esetben 97%-os pontosságot jelent. Természetesen a különböző lakóépületek kialakítása miatt a sokszögalak is minden esetben változik, ez pedig olyan kieső vagy ki nem számítható területeket jelenthet, amelyek megváltoztathatják ezt a pontosságot. Ez azonban olyan minimális, hogy a hatékonyság függvényében eltekinthetünk tőle. Összességében megállapítható, hogy három egymástól eltérő belső zónát alakíthatunk ki. Ezt szemlélteti a 9. ábra.



9. ábra

A mértani, a valós és az optimális belső zóna [a szerző szerkesztése]

A három belső zóna tehát a következő:

- *Mértani belső zóna:* Az épület mértani középpontjától mért 10 méter sugarú kör területe (piros kör területe).
- *Valós belső zóna:* Az épület szélétől mért 10 méter hosszúságú területeket összekötő zóna, amelynek formája sokszögalak. Mivel tűz esetén a lángok kezdetben az épület szélét érik el, ezért ennek a zónának a mérete és területe a leghitelesebb. Ehhez viszonyítjuk a többi zónát (kék sokszögalakú síkidom területe).
- *Optimális belső zóna:* Az egyszerűbb számítás és jogszabályi alkalmazás érdekében létrehozott zóna, amelynek területe szinte teljesen megegyezik a sokszögalakú zóna területével (zöld kör területe).

Az optimális belső zóna kapcsán azonban fontos megemlíteni, hogy a zóna szélső értéke, egyes helyeken meghaladja a valós belső zóna határvonalát, ebben az esetben a terület „túlbiztosított" (zöld vonalak). Más helyeken azonban éppen a valós belső zóna területén belül található, ezek a területek pedig így „alulbiztosítottak" (piros vonalak) lesznek. Ennek elemzésével, számításával, valamint kiértékelésével a szerző egy későbbi cikkben kíván foglalkozni.

Következtetések

Összességében tehát megállapítható, hogy a WUI-területek megelőző tűzvédelme komplex. Magyarországon eddig a WUI-területek megelőző tűzvédelmével kevesen foglalkoztak, azonban a nemzetközi szakirodalomban már találni erre egyes irányelveket. Ennek eredményeként a WUI-n található lakóingatlanok közelében lévő területek belső és külső zónára oszthatók. A belső zóna a lakóépület körüli 10 méter sugarú kör területe. Ez a 10 méteres határérték azonban csak akkor releváns, ha a kör középpontja a lakóépület mértani közepe. Minden más esetben a belső zóna valós alakja sokszögalak. Ennek oka az épületek kiugró részei. A cikkben e kérdéskör problémáit és nehézségeit elemeztem, műszaki rajzok, valamint számítások segítségével.

A cikk eredménye, hogy egy WUI-n lévő lakóépület valós belső zónája csak sokszögalakú lehet, köszönhetően az épület kiugró részeinek (valós belső zóna). A sokszögalakú síkidommal azonban nehéz számolni, ezért a szerző javaslatot tett egy a valós zóna területének nagyságához hasonló méretű kör alakú belső zóna létrehozására (optimális belső zóna), a jogszabályi adaptációs lehetőségekre való tekintettel. Figyelembe véve az épület kiugró részeit, megállapítottam, hogy ha az eredeti 10 méter sugarú kör nagyságát megemeljük közel 20%-kal (jelen esetben 2 méterrel), akkor a valós sokszögalakú zónához közel azonos nagyságú (97%) belső zónát kapunk. A feltételezést, miszerint a valós zóna kiváltható egy optimális zónával igazoltuk, hiszen a két zóna területe közötti különbség csupán 3%.

A WUI-területek megelőző tűzvédelme tehát hangsúlyos feladatkör, ezért fontos meghatározni azt is, hogy a hazai viszonyok között mely országrészekben van most is aktualitása a problémának. Ilyen terület Pest megye déli része, Bács-Kiskun és Csongrád

megyék tanyás térségei, Heves, Borsod-Abaúj-Zemplén és Somogy megyék zártkerti övezetei, valamint Budapest vonzáskörzetének erdő-lakott terület határai.

Hivatkozások

[1] M. Van Aalst, "The Impacts of Climate Change on the Risk of Natural Disasters," *Disasters,* vol. 30, no. 1, pp. 5–18, 2006. DOI: https://doi.org/10.1111/j. 1467-9523.2006.00303.x

[2] L. Teknős, „A globális klímaváltozás és a katasztrófavédelem kapcsolata, avagy a katasztrófavédelem reagálása az új kihívásokra Magyarországon," *Hadmérnök*, 4. évf. 2. sz., pp. 80–94., 2009.

[3] "Advance EFFIS Report on Forest Fires in Europe, Middle East and North Africa 2017," European Forest Fire Information System, European Commission, European Union, 2018. DOI: https://doi.org/10.1111/10.2760/476964

[4] Á. Restás, "Developing the effectiveness of aerial firefighting using instant foam based on Hungarian–Slovakian cooperation," In Proceedings of 5th International Scientific Conference on Fire Protection and Rescue Services 2018 Zilina, Slovakia, M. Monosi and J. Müllerová, Eds. Zilina: University of Zilina, 2018, pp. 1–9.

[5] S. Shwababa and Á. Restás, "Veld fire mitigation strategy: a vision for an innovative and integrated approach to managing risks in land reform farms, a case of land reform beneficiaries in South Africa" in *Advances in forest fire research 2018,* Coimbra, Portugal, D.X. Viegas Ed. Coimbra: Imprensa da Universidade de Coimbra, 2018, pp. 183–191. DOI: https://doi.org/10.14195/978-989-26-16-506_18

[6] D. Nagy, „FIRELIFE Erdőtűz megelőzési Program – Innováció és kommunikáció nyertes pályázatának előkészítésének és végrehajtásának tapasztalatai," [Online]. Elérhető: www.termeszetvedelem.hu/_user/browser/File/LIFE/LIFE_Termeszetvedelmi_trening/Kommunikacios_terning_20170406/K%C3%B6rnyezetv%C3%A9delmi%20Ir%C3%A1ny%C3%ADt%C3%A1s%20tr%C3%A9ning_2017_04_06_Dr_Nagy%20D%C3%A1niel.pdf (Letöltve: 2019. 05. 04.)

[7] K. Kalabokidis, A. Ager, M. Finney, N. Athanasis, P. Palaiologou and C. Vasilakos, "AEGIS: a wildfire prevention and management information system," *Natural Hazards and Earth System Sciences,* vol. 16, no. 3, pp. 643–661, 2016. DOI: https://doi.org/10.5194/nhess-16-643-2016

[8] D. X. Viegas, *Advances in forest fire research.* Coimbra: Imprensa da Universidade de Coimbra, Portugal, 2014. DOI: http://dx.doi.org/10.14195/978-989-26-0884-6

[9] C. Lampin-Maillet, M. Jappiot, M. Long, C. Bouillon, D. Morge and J-P. Ferrier, "Mapping wildland-urban interfaces at large scales integrating housing density and vegetation aggregation for fire prevention in the South of France," *Journal of Environmental Management,* vol. 91, no. 3, pp. 732–741, 2010. DOI: https://doi.org/10.1016/j.jenvman.2009.10.001

[10] P. Debreceni, L. Bodnár és R. Pellérdi, „Az erdőtűz kockázatának csökkentési lehetőségei Magyarországon," *Védelem Tudomány,* 2. évf. 2. sz., pp. 1–11., 2017.

[11] Á. Restás, „A hivatásos katasztrófavédelmi szervek beavatkozói tevékenysége az éghajlatváltozás okozta károk felszámolásánál," in *Adaptációs lehetőségek az éghajlatváltozás következményeihez a közszolgálat területén,* T. Berek, szerk. Budapest: Nemzeti Közszolgálati Egyetem, 2019., pp. 584–614.
[12] B. Homchaudhuri, M. Kumar and J. Cohen: "Optimal Fireline Generation for Wildfire Fighting in Uncertain and Heterogeneous Environment," In Proceedings of the American Control Conference, Baltimore: USA ACC2010-1472 (Art. No. 5531049) pp. 5638–5643. DOI: https://doi.org/10.1109/ACC.2010.5531049
[13] P. Debreceni és P. Pántya, „A fokozottan tűzveszélyes időszakok meghatározásának lehetőségei". *Műszaki Katonai Közlöny,* 29. évf. 1. sz., pp. 243–260., 2019. DOI: https://doi.org/10.32562/mkk.2019.1.20
[14] M. Tonini, F. Amato and J. Parente, "Wildland Urban Interface assessment and prediction in relation to land use and land cover changes. The Portuguese case study," in *Advances in Forest Fire Research 2018,* X.D Viegas Ed., Coimbra: Imprensa da Universidade de Coimbra, 2018, pp. 870–877. DOI: https://doi.org/10.14195/978-989-26-16-506_96
[15] R. Wadhwani, "Fire management research at Imperial College, London," *bnhcrc.com.au,* [Online]. Elérhető: www.bnhcrc.com.au/news/blogpost/rahul-wadhwani/2018/fire-management-research-imperial-college-london (Letöltve: 2019. 03. 12.)
[16] E. Plana, M. Font, M. Serra, M. Borràs and O. Vilalta, *Fire and Forest Fires in the Mediterranean; A Relationship Story between Forests and Society.* Freiburg: Forest Sciences Centre of Catalonia, 2016, [Online]. Elérhető: http://efirecom.ctfc.cat/docs/revistaefirecom_en.pdf (Letöltve: 2019. 07. 31.)
[17] L. Bodnár és L. Komjáthy, „Erdőtűz megelőzési módszerek erdészeti megoldásai," *Hadmérnök,* 13. évf. 2. sz., pp. 117–125., 2018.
[18] Á. Muhoray, „A polgári védelem helye a modern katasztrófavédelemben," *Hadmérnök,* 12. évf. 2. sz., pp. 188–200., 2017.
[19] International Federation of Red Cross, "Information bulletin, Portugal: Forest Fires," *International Federation of Red Cross,* [Online]. Elérhető: www.ifrc.org/docs/Appeals/17/IB1_Portugal_forest_fires_19062017.pdf (Letöltve: 2019. 05. 04.)
[20] A. Barberopoulou and T. Tsiropoulos, "The fire of July 23rd, 2018 Mati, Attiki Greece: Lessons learned in the face of lacking crisis management," Poster, American Association of Geographers, 2019. DOI: https://doi.org/10.13140/RG.2.2.21913.88167
[21] J. Cohen, *A site-specific approach for assessing the fire risk to structures at the wildland/urban interface.* Ashville: USDA Forest Service SEGTR-69, 1991.
[22] YouTube, "Understanding Fire Behavior in the Wildland/Urban Interface," National Fire Protection Association, *YouTube,* [Online]. Elérhető: www.youtube.com/watch?v=pPQpgSXG1n0 (Letöltve: 2019. 03. 06.)
[23] YouTube, "Cordelia Fire Protection District: Fire Safety," *YouTube,* [Online]. Elérhető: www.youtube.com/watch?v=pPQpgSXG1n0 (Letöltve: 2019. 03. 06.)
[24] G. Érces és J. Ambrusz, „A katasztrófák építésügyi vonatkozásai Magyarországon," *Védelem Tudomány,* 4. évf. 2. sz., pp. 45–83., 2019.

[25] J. Cohen, "An analysis of Wildland-Urban Fire with Implications for preventing Structure Ignitions," in *V. Short Course on Fire Safety.* Coimbra, Portugal, US Forest Service, Missoula Fire Sciences Laboratory, 2018, pp. 23–36.
[26] P. Pántya, „A katasztrófavédelem és a tűzoltóságok hazai és nemzetközi tevékenysége, a beavatkozások keretei, a biztonság és a hatékonyság megjelenése," *Hadmérnök,* 12. évf. 2. sz., pp. 201–213., 2017.
[27] Á. Restás, P. Pántya és S. Rácz, „A tűzvédelem komplexitása a korszerű megelőzéstől a hatékony beavatkozásig," in *Katasztrófavédelem 2015 Tudományos Konferencia,* Szentendre, Á. Restás, A. Urbán szerk., Budapest: BM Országos Katasztrófavédelmi Főigazgatóság, 2015., pp. 161–165.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
15. évfolyam (2020) 1. szám 63–78.
DOI: 10.32567/hm.2020.1.5

Fekete Árpád[1]

A földrengéskockázat elemzése valószínűségi módszerrel

The Analysis of Seismic Hazard with the Probabilistic Method

A földrengéskockázat mérnöki szempontból való elemzésének célja, hogy a tervezett építmények ellen tudjanak állni adott mértékű talajmozgásnak. Egy jövőben bekövetkező földrengésnek nagy a bizonytalansága a helyet, a méretet és az ebből eredő talajmozgás-intenzitást illetően. A valószínűségi földrengéskockázat-analízis (Probabilistic Seismic Hazard Analysis – a továbbiakban: PSHA) megpróbálja ezeket a bizonytalanságokat számszerűsíteni és kombinálni, hogy egy adott hely jövőbeli rengésveszélyeztetettsége explicit módon leírható legyen. A cikk konkrét számítási példán is demonstrálja a módszer alkalmazását. Magyarország földrengés szempontjából legveszélyeztetettebb zónájának környékén számítjuk ki a talajgyorsulás átlagos értékét meghaladó valószínűséget a PSHA-egyenletek segítségével.
Magyar nyelvű folyóiratokban vagy könyvekben a PSHA-módszer matematikai hátteréről csak keveset olvashatunk. E cikk célja, hogy az olvasó a valószínűségszámítás segítségével megértse a PSHA alkalmazását, illetve annak korlátait.

Kulcsszavak: földrengéskockázat, PSHA-módszer, talajmozgás-intenzitás, Cornell-modell

The goal of seismic hazard engineering analyses is to ensure that the planned structures can withstand a given level of ground shaking. There is a great deal of uncertainty about the location, size and resulting ground motion intensity of future earthquakes. Probabilistic Seismic Hazard Analysis (PSHA) tries to quantify these uncertainties, and combine them to produce an explicit description of the future shaking that may occur at a site.
This work demonstrates the application of the method by specific calculative example. The probability (that is more than the average) of ground motion intensity

[1] Nemzeti Közszolgálati Egyetem Víztudományi Kar, főiskolai docens, e-mail: fekete.arpad@uni-nke.hu, ORCID: https://orcid.org/0000-0002-1435-8658

is calculated by PSHA equations in the most dangerous zone of Hungary regarding earthquakes.
We can read only a little about the mathematical background of the PSHA method in Hungarian journals or books. The aim of this work is to help the reader understand the application and the limitations of PSHA with the help of the probability theory.

Keywords: **seismic hazard, PSHA method, ground motion intensity, Cornell model**

Bevezetés

A földrengés előrejelzésének legfontosabb stratégiai feladata annak meghatározása, hogy egy adott térségben mekkora erősségű földrengésre kell számítanunk egy bizonyos időszakban. A mérnökök ennek az információnak az ismeretében képesek a különböző létesítményeket a várható földrengésekkel szemben ellenállónak tervezni. A földrengéskockázat meghatározásánál alapvető feladat az, hogy kiszámítsuk a földrengés által okozott talajmozgás mértékét (általában a gyorsulást) és különböző spektrális jellemzőit a vizsgált helyszínen.

A földrengéskockázat elemzésére kétféle eljárás ismeretes: a determinisztikus és a valószínűségi módszer. A determinisztikus módszer (DSHA – Deterministic Seismic Hazard Assessment) hátránya, hogy erősen függ a környék múltbeli szeizmikus tevékenységének ismertségétől, és elsősorban szeizmikusan erősen aktív területeken (lemezhatárokon) alkalmazható. E módszer alapfeltevése az, hogy a vizsgált terület közelében a szeizmikus aktivitás a jövőben ugyanolyan lesz, mint a múltban, és tudjuk, mekkora rengések várhatók a térségben [1].

Sokkal megbízhatóbb eredményeket kapunk a statisztikus, valószínűségi becslésen alapuló eljárással, amely PSHA (Probabilistic Seismic Hazard Assessment) módszerként ismeretes. Célja, hogy a végeredményt jelentő veszélyeztetettségi szint mértékét a vízszintes irányú PGA (Peak Ground Acceleration), maximális talajgyorsulással jellemezze.

A PSHA-módszer

A módszer alkalmazásához, azaz a földrengéskockázat statisztikus becslése céljából egy földrengés-előfordulási eloszlást kell feltételeznünk [2]. Ez az általánosan használt eloszlási modell a Poisson-modell. Legyen ξ az a valószínűségi változó, amely azoknak a földrengéseknek a száma egy t időintervallumban, amelyeknek erőssége legalább M magnitúdójú. Ha τ jelöli a legalább M magnitúdójú földrengés átlagos ismétlődési idejét, akkor a Poisson-eloszlás szerint

$$P(\xi < 1) = F(1) = 1 - e^{-t/\tau}, \tag{1}$$

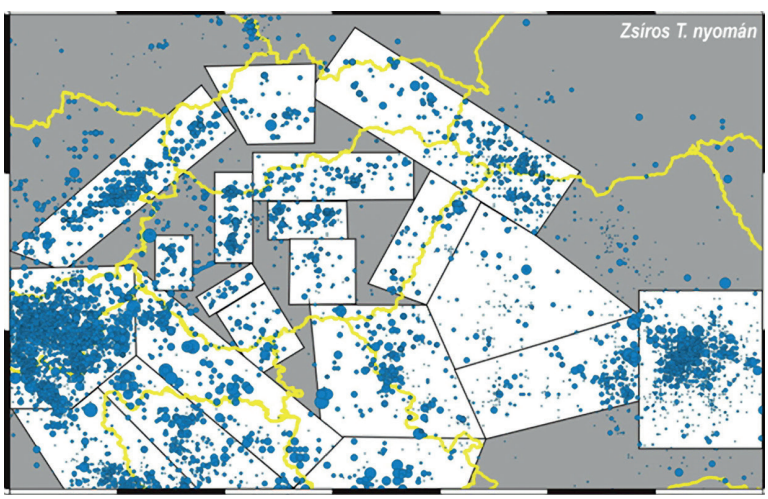
ami annak a valószínűsége, hogy egy adott t időintervallumban nem fordul elő M méretűnél nagyobb földrengés (F az eloszlásfüggvényt jelöli).

A PSHA alkalmazása során még feltesszük, hogy a földrengések egymástól függetlenek, valamint azt, hogy a tapasztalt földrengés-gyakoriság stacionárius. A PSHA eredménye általában egy adott időintervallumban és helyen várható maximális vízszintes irányú PGA-érték meghatározása. (Közönséges épületek tervezésénél százéves időszakon belüli csúcsgyorsulás-értéket határoznak meg. A legnagyobb kockázatot jelentő atomerőművek és völgyzáró gátak tervezésekor egy tízezer éves időintervallumon belül várható legnagyobb PGA-értéket kell figyelembe venni [2].) A PGA egysége a g, 1g = 9,817 ms^{-2}. 0,001 g gyorsulás már érezhető, a 0,2 g esetén az emberek egyensúlyukat vesztik, míg a 0,5 g gyorsulásértéket csak az erre tervezett épületek bírják ki.

A PSHA-analízis öt lépésből áll. Az alábbi öt alfejezet ezeket tárgyalja.

A vizsgált területre ható forrászónák kijelölése

A forrászóna azt jelenti, hogy ezen belül hasonló tulajdonságokkal, hasonló valószínűséggel és gyakorisággal bíró földrengések keletkeznek véletlenszerűen. A forrászónák kijelölésének alapja a múltbeli szeizmicitás eloszlása, valamint a geológiai és a tektonikai ismeretek. A forrásterület lehet egy folt, azaz ténylegesen területgeometriájú, de lehet vonal is, amely egy vetőt reprezentál. Érdemes megnézni a Pannon-medence lehetséges forrászónáit az 1. ábrán [3]. Ilyen térkép megszerkesztéséhez nagy segítség a földrengés-katalógus, amiben a vizsgált területen a múltban kipattant földrengések időpontját, földrajzi helyét és becsült erősségét sorolják fel.



1. ábra

A Pannon-medence forrászónáinak egy lehetséges kijelölése [3]

Magyarországon eddig 6 Richter-magnitúdónál vagy 9 fokos Mercalli-intenzitásnál nagyobb földrengést még alig észleltek, ezért definíció szerint Magyarország területét aszeizmikus területnek tekinthetjük, bár jelentősebb földmozgások nálunk is

előfordulhatnak. Ennek oka a Balkán-félszigeten húzódó Vardar-törésvonal (gyakorlatilag a Vardar-folyó völgye), amely Magyarország területén végződik, így aktivitása néha ránk is hatással van. Egy Richter-skála szerinti 5-ös erősségű rengés körülbelül 20 évente következhet be. A legutóbbi ilyen esemény az 1985-ös berhidai földrengés volt, 4,9-es értékkel. Magyarországon az eddigi legnagyobb rengés 1763. június 28-án következett be Komáromban, amely becslés szerint 6,3-as erősségű volt. A város egyharmada elpusztult és több mint hatvanan meghaltak [4].

Tapasztalati összefüggés meghatározása a földrengések magnitúdója és ezek egységnyi időtartam alatt várható száma között

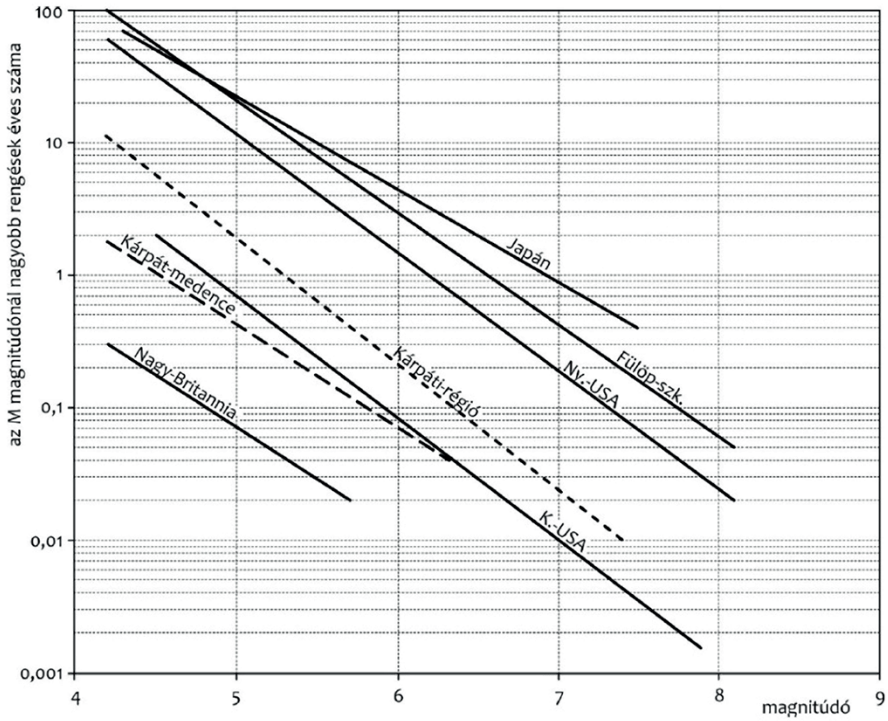
Beno Gutenberg és Charles Francis Richter 1956-ban közösen publikálták nevezetes egyenletüket:

$$\lg\lambda_m = a - bm, \tag{2}$$

ahol λ_m azon rengések gyakorisága, amelyek mérete legalább *m* magnitúdójú, *a* és *b* a területre jellemző állandók [5]. Az *a* és *b* konstansnak döntő befolyása van a végeredményre. Az *a* és *b* értékek meghatározásának alapja a regisztrált földrengés-tevékenység. A *b* együttható pozitív értékéből következik, hogy a kisebb méretű rengés gyakoribb, vagyis minél kisebb földrengésekről van ismeret, az együtthatók értéke annál több adatból számítható ki. Tehát érzékeny földrengés-megfigyelő rendszerrel *a* és *b* értéke még viszonylag rövid idő alatt is megbízhatóbbá tehető [1].

Érdemes a (2) egyenlet alapján megvizsgálni a földrengések éves számát a Föld különböző szeizmikus aktivitással jellemezhető részein.

Az egyes földrengésrégiók esetében az egyenes meredekségét meghatározó *b* érték csak kisebb eltéréseket mutat, ezért az egyenesek közel párhuzamosak. A földrengéses zónák aktivitása közti eltérést az *a* mutatja. A 2. ábráról látható, hogy Magyarország szeizmikus aktivitása nagyjából megegyezik az USA keleti részére jellemzővel, és messze elmarad az aktív területekétől (Japán, Fülöp-szigetek).



2. ábra

A földrengések éves száma a Föld különböző részein [2]

A (2) egyenlet segítségével megadható a rengések magnitúdójának kumulatív eloszlásfüggvénye (CDF – Cumulative Distribution Function), ami azt mutatja meg, hogy a rengések mekkora része kisebb egy adott *m* magnitúdójú rengésnél, feltéve, hogy a rengések egy m_{min} minimális magnitúdónál nagyobbak [ezt a (3) képletben a feltételes valószínűség fejezi ki] [6]. Ezt azért érdemes bevonni a számításokba, mert az m_{min}-nél kisebb magnitúdók hatástalanságuk miatt nem játszanak szerepet a mérnöki tervezésnél. Ha $F_M(m)$ jelöli az *M* valószínűségi változó kumulatív eloszlásfüggvényét, akkor

$$F_M(m) = P(M \le m | M > m_{min}) = \frac{\lambda(m_{min} < M \le m)}{\lambda(m_{min} < M)} = \frac{\lambda_{m_{min}} - \lambda_m}{\lambda_{m_{min}}} = \frac{10^{a-bm_{min}} - 10^{a-bm}}{10^{a-bm_{min}}} = 1 - 10^{-b(m-m_{min})}, \quad m > m_{min}. \tag{3}$$

Ha $f_M(m)$ jelöli az *M* sűrűségfüggvényét, akkor deriválva a kumulatív eloszlásfüggvényt kapjuk, hogy

$$f_M(m) = \frac{d}{dm} F_M(m) = \frac{d}{dm}\left[1 - 10^{-b(m-m_{min})}\right] = b\ln(10) 10^{-b(m-m_{min})}, \quad m > m_{min}. \tag{4}$$

A (4) egyenletet úgy kaptuk, hogy abban nincs meghatározva felső határ a magnitúdóra. Ha azonban megadunk egy maximális magnitúdót (m_{max}), feltételezve, hogy annál nagyobb erősségű földrengés kizárható egy adott területen, akkor a (3) és (4) a következőképpen módosul [6]:

$$F_M(m) = \frac{1-10^{-b(m-m_{min})}}{1-10^{-b(m_{max}-m_{min})}}, \quad m_{min} < m < m_{max}\,, \tag{5}$$

$$f_M(m) = \frac{bln(10)10^{-b(m-m_{min})}}{1-10^{-b(m_{max}-m_{min})}}, \quad m_{min} < m < m_{max}\,. \tag{6}$$

A későbbi PSHA-egyenletekhez a magnitúdók folytonos eloszlását érdemes átalakítani magnitúdók diszkrét halmazává. Tekintsük az alábbi táblázatot:

1. táblázat

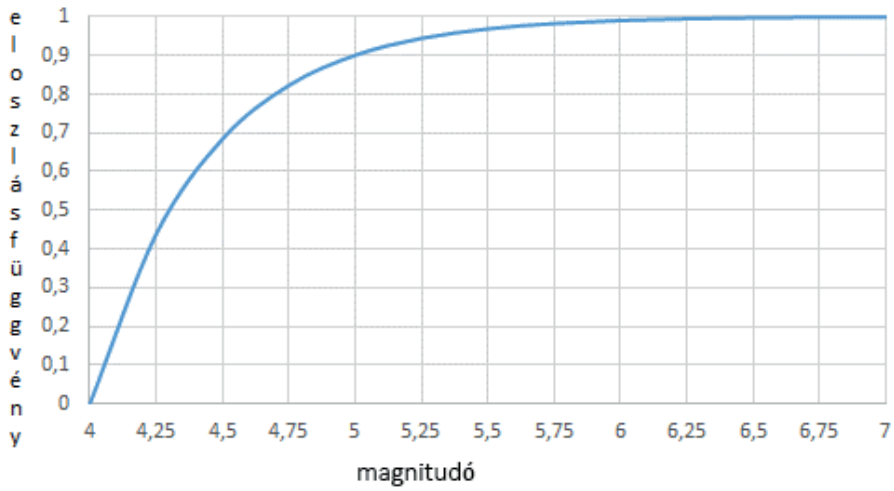
A magnitúdók valószínűségei [a szerző szerkesztése]

m_j	$FM(m_j)$	P(M=m_j)
4,00	0,0000	0,4381
4,25	0,4381	0,2464
4,50	0,6845	0,1385
4,75	0,8230	0,0779
5,00	0,9009	0,0438
5,25	0,9447	0,0246
5,50	0,9693	0,0139
5,75	0,9832	0,0078
6,00	0,9910	0,0044
6,25	0,9954	0,0024
6,50	0,9978	0,0014
6,75	0,9992	0,0008
7,00	1,0000	0,0000

Az első oszlopban az m_{min} = 4 és m_{max} = 7 és közötti magnitúdók vannak feltüntetve 0,25 közökkel. A második oszlopban az (5) képlettel számított kumulatív eloszlásfüggvény szerepel, b = 1 választással. A harmadik oszlop adja meg a magnitúdók diszkrét értékeinek valószínűségeit a

$$P(M = mj) = FM(mj + 1) - FM(mj) \tag{7}$$

összefüggéssel számolva. A kumulatív eloszlásfüggvényt mutatja a 3. ábra:



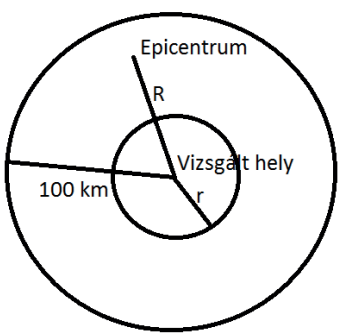
3. ábra

Az 1. táblázat alapján szerkesztett kumulatív eloszlásfüggvény [saját szerkesztés]

Távolságeloszlás meghatározása az epicentrumtól a vizsgált területig

A PSHA-egyenletekben szerepet játszik a vizsgált terület és az epicentrum távolságának eloszlása is. Feltesszük, hogy a vizsgált terület környezetében a földrengés kipattanásának valószínűsége azonos. A távolságeloszlás számítása az alábbi két példa segítségével könnyebben megérthető [6].

Az első példában a vizsgált helyünknek egy 100 km-es kör alakú környezetét vesszük, amelyben a földrengés kipattanásának helye bárhol fennállhat azonos valószínűséggel. Jelölje az *R* valószínűségi változó a helyünk és az epicentrum távolságát. Ezeket foglalja össze a 4. ábra:



4. ábra

Az 1. példa vázlatos illusztrációja [a szerző szerkesztése]

Annak valószínűségét, hogy az epicentrum a vizsgált helyünktől egy *r* távolságnál közelebb van, egyszerű geometriai valószínűséggel megadhatjuk:

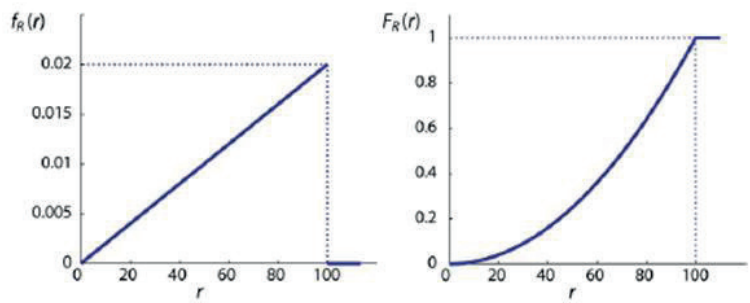
$$P(R \le r) = F_R(r) = \frac{r^2\pi}{10000\pi}. \tag{8}$$

Ez alapján felírható az eloszlásfüggvény és a sűrűségfüggvény:

$$F_R(r) = \begin{cases} 0 & ,ha\ r < 0 \\ \frac{r^2}{10000}, & ha\ 0 \le r < 100, \\ 1 & ,ha\ r \ge 100 \end{cases} \tag{9}$$

$$f_R(r) = \begin{cases} \frac{r}{5000}, & ha\ 0 \le r < 100 \\ 0, & különben. \end{cases} \tag{10}$$

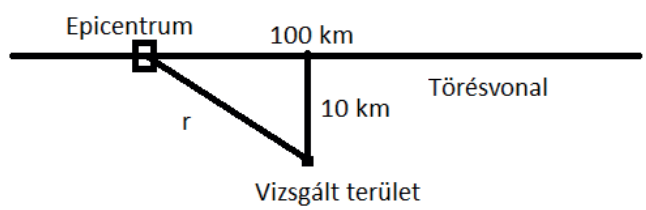
Az 5. ábra a (9) és (10) grafikonjait mutatja:



5. ábra

A vizsgált terület és az epicentrum távolságának sűrűség- és eloszlásfüggvénye [6]

A második példában az epicentrum egy 100 km hosszú törésvonalon bárhol kialakulhat és a vizsgált helyünk 10 km-re fekszik a törésvonaltól (6. ábra).



6. ábra

A 2. példa vázlatos illusztrációja [a szerző szerkesztése]

Ha az *R* valószínűségi változó jelöli a vizsgált terület és az epicentrum távolságát, akkor annak valószínűsége, hogy ez valamely *r*-nél kisebb (felhasználva a Pitagorasz-tételt

és azt a meggondolást, hogy az epicentrum a vizsgált hely jobb oldalán is lehet a 6. ábrán):

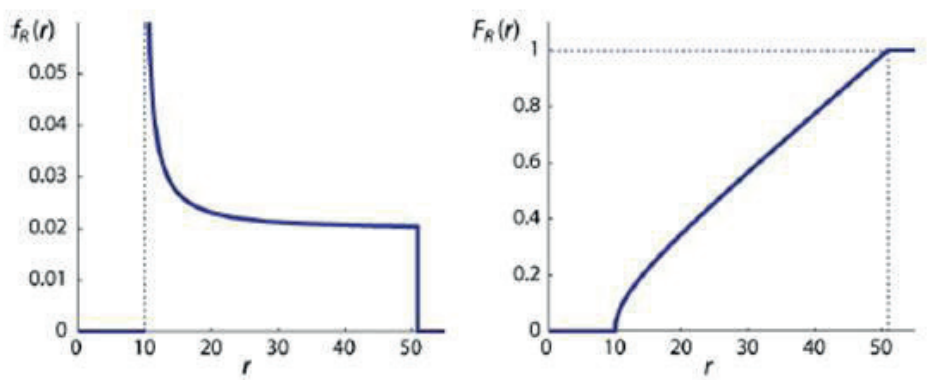
$$P(R \le r) = F_R(r) = \frac{\text{a törésvonal hossza r távolságon belül}}{\text{törésvonal hossza}} = \frac{2\sqrt{r^2-100}}{100}. \qquad (11)$$

Ez alapján felírható az *R* valószínűségi változó eloszlásfüggvénye és sűrűségfüggvénye:

$$F_R(r) = \begin{cases} 0 & , \ ha\ r < 10 \\ \frac{2\sqrt{r^2-100}}{100} & , ha\ 10 \le r < 51 \\ 1 & , ha\ r \ge 51 \end{cases} \qquad (12)$$

$$f_R(r) = \begin{cases} \frac{r}{50\sqrt{r^2-100}}, & ha\ 10 \le r < 51 \\ 0 & , \ különben. \end{cases} \qquad (13)$$

A (12) és (13) összefüggéseket szemlélteti grafikonnal a 7. ábra:



7. ábra
A vizsgált terület és az epicentrum távolságának sűrűség- és eloszlásfüggvénye [6]

A talajmozgás intenzitásának vizsgálata

Megvizsgáljuk, hogy a forrászónától a vizsgált területig hogyan csökken a földrengés által keltett maximális vízszintes PGA[2] értéke. Ennek elemzésére tekintsük az alábbi

[2] PGA (Peak Ground Acceleration) maximális talajgyorsulás.

talajmozgás-intenzitás előrejelző modellt, amely valószínűségi eloszlást ad az intenzitásra [7]:

$$\ln IM = \overline{\ln IM}\,(M, R, \theta) + \sigma(M, R, \theta) \cdot \varepsilon, \tag{14}$$

ahol $\ln IM$ a talajmozgás-intenzitás mérték (általában PGA) természetes alapú logaritmusa (IM – Intensity Measure). Az $\ln IM$ valószínűségi változó és normális eloszlással jól prezentálható. Az $\overline{\ln IM}\,(M, R, \theta)$ és a $\sigma(M, R, \theta)$ tagok a modell kimenetelei, amelyek az $\ln IM$ feltételezett közepét, illetve szórását jelölik. Ezek a magnitúdó, a távolság és θ (egyéb paraméterek) függvényei. Az ε standard normális valószínűségi változó, amely $\ln IM$-ben a megfigyelt variabilitást jellemzi.

A (14) egyenlet igen általános, ezt jobban megérthetjük, ha Carl Allin Cornell számítását figyelembe vesszük a PGA logaritmusának feltételezett közepére vonatkozóan [7]:

$$\overline{\ln PGA} = -0{,}152 + 0{,}859M - 1{,}803 \ln(R + 25). \tag{15}$$

Cornell az $\ln PGA$ szórását 0,57-nek veszi és a modelljében minden magnitúdó és távolság konstans. A PGA természetes alapú logaritmusa normális eloszlású valószínűségi változó, így könnyen kiszámítható annak valószínűsége, hogy egy bizonyos szintet meghalad a PGA:

$$P(PGA > x|m, r) = 1 - P(PGA \leq x|m, r) = 1 - \phi\left(\frac{\ln x - \overline{\ln PGA}}{\sigma_{\ln PGA}}\right). \tag{16}$$

A (16) egyenlet bal oldalán szereplő valószínűség a PGA sűrűségfüggvényének segítségével is felírható:

$$P(PGA > x|m, r) = \int_x^{\infty} f_{PGA}(u)du. \tag{17}$$

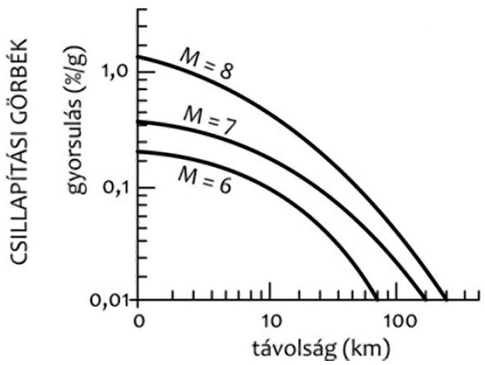
Tekintsünk a (16) egyenletre konkrét számítási példát. Legyen adott egy 6-os erősségű földrengés, és azt vizsgáljuk, hogy az epicentrumtól 3, 10 és 30 km távolságra hogyan változik annak valószínűsége, hogy a PGA meghaladja a 0,5 g-t. Ez a gyorsulásérték kritikus, mert ezt, mint említettük, csak az erre tervezett épületek bírják ki.

Először a (15) egyenlettel kiszámítjuk az $\ln PGA$ feltételezett közepeit, amelyek 3, 10, 30 km távolságok esetén rendre –1,006, –1,408, –2,223. Az $\ln PGA$ szórása 0,57, ez változatlan. Így

$$\begin{aligned} P(PGA > 0{,}5|6, 3) &= 1 - \phi\left(\frac{\ln 0{,}5 - (-1{,}006)}{0{,}57}\right) = 1 - \phi(0{,}55) = 0{,}2912 \\ P(PGA > 0{,}5|6, 10) &= 1 - \phi\left(\frac{\ln 0{,}5 - (-1{,}408)}{0{,}57}\right) = 1 - \phi(1{,}25) = 0{,}1056 \\ P(PGA > 0{,}5|6, 30) &= 1 - \phi\left(\frac{\ln 0{,}5 - (-2{,}223)}{0{,}57}\right) = 1 - \phi(2{,}68) = 0{,}0037 \end{aligned} \tag{18}$$

Látható, hogy 3 km-es távolságban a 0,2912 komoly valószínűség, így ezt a tervezésnél kötelező figyelembe venni, de még 10 km-es távolságban a körülbelül 10%-os

valószínűség is figyelemreméltó. A 7. ábra a 6, 7, 8 magnitúdójú rengések PGA-jának csillapodásait mutatja a távolság függvényében.



8. ábra
Csillapítási görbék a távolság függvényében [2]

A PSHA-egyenletek felírása az eddigi információk segítségével

A (14) összefüggésben már szerepelt az intenzitási mérték (*IM*) mint valószínűségi változó. Most már fel tudjuk írni azt az egyenletet, amely megadja azt a valószínűséget, hogy az intenzitási szint meghalad egy bizonyos *x* szintet [6]:

$$P(IM > x) = \int_{m_{min}}^{m_{max}} \int_{0}^{r_{max}} P(IM > x|m,r) f_M(m) f_R(r) dr dm\,, \qquad (19)$$

ahol $P(IM > x|m,r)$ a (16), $f_M(m)$ a (6), míg $f_R(r)$ a (10) vagy (13) formulákból számolható ki. Ez az egyenlet azonban nem ad tájékoztatást a földrengések gyakoriságáról a vizsgált területen. A (19) egyenletben a $P(IM > x)$ valószínűség helyett azonban vizsgálhatjuk annak $\lambda(IM > x)$ gyakorisági rátáját. A $\lambda(M > m_{min})$ jelölje annak gyakorisági rátáját, hogy a földrengés erőssége nagyobb, mint m_{min}. Mivel $P(IM > x) = \frac{\lambda(IM>x)}{\lambda(M>m_{min})}$, ezért annak gyakorisága, hogy a földrengés intenzitása meghalad egy bizonyos *x* szintet [6]:

$$\lambda(IM > x) = \lambda(M > m_{min}) \int_{m_{min}}^{m_{max}} \int_{0}^{r_{max}} P(IM > x|m,r) f_M(m) f_R(r) dr dm \qquad (20)$$

Az előbbi egyenlet csak egy lehetséges kipattanási hellyel számol a vizsgált terület közelében, de előfordulhat, hogy a közelben több forrászóna lehet. Ekkor a (20) egyenlet tovább általánosítható. Legyen *n* db forrászónánk, ekkor felírható, hogy

$$\lambda(IM > x) =$$

$$= \sum_{i=1}^{n} \lambda(M_i > m_{min}) \int_{m_{min}}^{m_{max}} \int_{0}^{r_{max}} P(IM > x|m,r) f_{M_i}(m) f_{R_i}(r) dr dm. \tag{21}$$

Praktikusabb azonban a számításokhoz a (21) egyenlet diszkretizált változatát használni [6]:

$$\lambda(IM > x) =$$

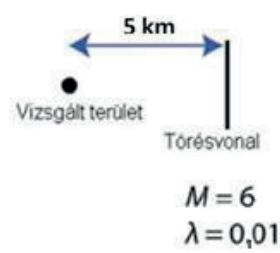
$$= \sum_{i=1}^{n} \lambda(M_i > m_{min}) \sum_{j=1}^{n_M} \sum_{k=1}^{n_R} P\left(IM > x \middle| m_j, r_k\right) P\left(M_i = m_j\right) P(R_i = r_k), \tag{22}$$

amiben a $P(M_i{=}m_j)$ kiszámításához a (7) összefüggést alkalmazzuk.

A (21) és (22) egyenleteket *PSHA-egyenleteknek* nevezzük. Az eredmény, azaz egy bizonyos intenzitási szint meghaladási rátája nagyon hasznos mérnöki döntések meghozatalakor, rengésbiztos építmények tervezése kapcsán. A következő fejezet példát ad ezen egyenletek gyakorlati alkalmazására, megértésére.

PSHA-számítás Magyarország legveszélyeztetettebb területére

Példánkban azt elemezzük, hogy Magyarországon a legveszélyeztetettebb zónában, azaz a Balaton északi csücskétől Komáromig húzható széles sávban, az úgynevezett Móri-árok környékén milyen valószínűséggel haladja meg a talajgyorsulás a 0,4 g értéket, ami már komoly károkat is okoz. Magyarországon, mint már említettük, 6 Richter-magnitúdónál nagyobb földrengést csak keveset észleltek (ezek is körülbelül 100 évente egyszer fordulnak elő a földrengéskatalógusok történelmi megfigyelései alapján). Tekintsük tehát az említett vonalat, ahol M = 6 erősségű földrengés pattan ki, λ = 0,01 éves gyakorisággal. A vizsgált helyünk legyen 5 km-re a törésvonaltól (9. ábra):



9. ábra
A számítás adatai [a szerző szerkesztése]

A Cornell-modell alapján, azaz (15)-be behelyettesítve az adatokat $\overline{\ln PGA} = -1{,}1303$, amiből a talajgyorsulás átlagos értékére, azaz $\overline{PGA}$-ra 0,3229 adódik és $\sigma_{\ln PGA} = 0{,}57$ a standard érték. Használjuk a (22) egyenletet:

$$\lambda(PGA > x) = \lambda(M > m_{min})P(PGA > x|6;5)P(M = 6)P(R = 5) = 0{,}01P(PGA > x|6;5). \quad (23)$$

Az egyenlet jobb oldalát kiszámítva:

$$P(PGA > x|6;5) = 1 - \phi\left(\frac{\ln x - (-1{,}1303)}{0{,}57}\right). \quad (24)$$

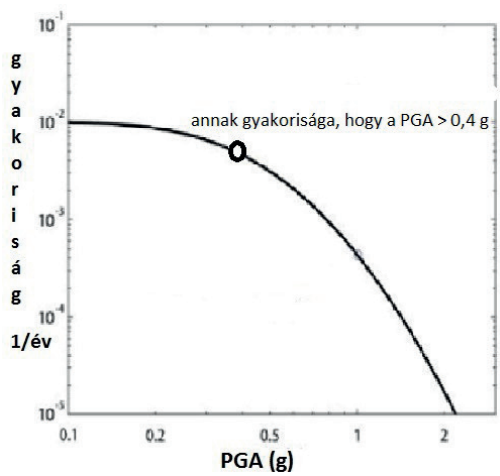
Ebből bármely *x* értékre ki tudjuk számítani a valószínűséget. Nézzük meg azt a valószínűséget, hogy a talajgyorsulás meghaladja a 0,4 g értéket:

$$P(PGA > 0{,}4|6;5) = 1 - \phi(0{,}3754) = 0{,}352. \quad (25)$$

Ezt (23)-ba helyettesítve megkapjuk a gyakoriságot is:

$$\lambda(PGA > 0{,}4) = 0{,}01 \cdot 0{,}352 = 0{,}00352. \quad (26)$$

Ez azt jelenti, hogy körülbelül 284 évente fordulhat elő a vizsgált zónánkban nagyon komoly károkat okozó, 0,4 g-nél nagyobb földrengés (A földrengéstörténeti katalógus alá is támasztja ennek a számításnak a megbízhatóságát). Ha a számításokat kellően sok PGA-szintre kiszámítjuk, akkor kirajzolódik a veszélyeztetettségi görbe, amely megadja annak gyakoriságát, hogy egy bizonyos mértéknél nagyobb talajgyorsulásra hány évente kell számítanunk. Ezt a görbét szemlélteti a 10. ábra:



10. ábra
A veszélyeztetettségi görbe [a szerző szerkesztése]

A módszerről levont következtetések, hiányosságok

A PSHA-eljárás, mint láttuk valószínűségi becslést ad a földrengések által egy adott helyen keltett maximális vízszintes gyorsulás értékének meghatározására. A tervezés szempontjából azonban van egy másik kulcsfontosságú paraméter, a ***rengések frekvenciája***.

A felszíni mozgás egy adott helyen különböző frekvenciájú hullámkomponensek szuperpozíciójaként áll elő. Ezen komponensek frekvenciája általában 0 és 15 Hz között van, ezt nevezik frekvenciatartalomnak. A mozgás frekvenciatartalmát a mérnöki gyakorlatban használatos válaszspektrummal jellemzik.

Ugyanazon rengésre ugyanazon a helyen a különböző épületek is eltérően reagálnak. Először igen összetett módon kezdenek el mozogni, majd rezgésük frekvenciája fokozatosan egy adott érték felé tolódik el, ezt az épület ***sajátfrekvenciájának*** nevezik. Gyakran használják a ***sajátperiódus*** kifejezést is, ami a sajátfrekvencia reciproka, és azt adja meg, hogy az mennyi idő alatt tesz meg egy teljes lengést [8]. Általában minél magasabb egy épület, annál alacsonyabb a sajátfrekvenciája, vagyis hosszabb a sajátperiódusa. Az alábbi (2.) táblázat néhány építményre jellemző sajátperiódusról ad tájékoztatást:

2. táblázat

Építmények sajátperiódusa/frekvenciája [8]

Építmény típusa	Tipikus sajátperiódus/frekvencia
egyszerű tartószerkezetek	0,1 s / 10 Hz
2 szintes épületek	0,2 s / 5 Hz
5 szintes épületek	0,5 s / 2 Hz
10–20 szintes épületek	1–2 s / 0,5–1 Hz
felhőkarcolók, függőhidak	2–6 s / 0,16–0,5 Hz

Az épületek akkor szenvedik el a legnagyobb kárt, amikor a talajmozgással rezonanciába kerülnek, vagyis amikor a földrengéshullámok legnagyobb energiájú összetevőinek frekvenciája és az épület sajátfrekvenciája megegyezik [8].

Az utóbbi évek tapasztalata azt mutatja, hogy a földrengésveszély mértékét sokszor nem maga a földrengés, hanem az általa generált természeti jelenség határozza meg. Például a 2001. január 13-án a Csendes-óceán alatt, Salvadortól mintegy 100 km-re kipattant $M = 7{,}6$ erősségű földrengés tragikus következményeit az általa kiváltott földcsuszamlások okozták [2]. A szeizmológiai szakirodalomból jól ismertek a *rengések okozta földcsuszamlások*. Ezek oka az, hogy a talajviszonyok a szeizmikus hullámok erős rázó hatása miatt megváltoznak. Így a rengés hegyvidéki területeken az erózió miatt már eleve meglazult kőzetek leomlását vagy az esővízzel átitatott, átázott talajrétegek lecsúszását eredményezi.

Nehezen kiszámítható még a földcsuszamlásokon kívül a *talajfolyósodás* jelenségének következménye. A hosszan tartó erős mozgások előidézhetik a vizes, laza szemcsés talajok szilárdságának elvesztését és folyadékszerű viselkedését, azaz a talajfolyósodást. A jelenség oka az, hogy az erős rázkódás hatására a laza szemcsés anyag

tömörödni kezd. Ekkor a benne lévő hézagok térfogata lecsökken, ami miatt a benne lévő víz nyomása – ha nem tud valahová elfolyni – megnő. Ha a pórusvíz nyomása eléri a fölötte lévő talajrétegek nyomását, akkor ez az anyag úgy kezd el viselkedni, mint egy viszkózus folyadék, elveszíti teherhordó-szilárdságát, és korlátlanul deformálódhat [9]. Lejtős terepen már néhány fokos lejtőnél is előfordulhat, hogy ha egy felszín alatti talajrétegben következik be az elfolyósodás, akkor a gravitációs erő miatt a felszíni, nem elfolyósodott rétegek elmozdulnak lefelé, a lejtő irányába, akár több tíz métert is megtéve. A mozgás már nagyon enyhe (egy fok alatti) lejtőknél is megindulhat, károsítva a csővezetékeket, közműveket, sekély alapozású szerkezeteket. Elfolyósodás bekövetkezésekor, ha egy épület alapozása ilyen rétegben található, a rengés annak kiemelkedését, süllyedését vagy felborulását okozhatja.

A 2004. december 26-án kipattant szumátra–andamáni (M = 9,1) és a tóhokui 2011. március 11-ei (M = 9,0) gigantikus földrengések okozta hatalmas veszteségek nem magának a földrengésnek, hanem az általa keltett *szökőárnak* a következményei. Hiába volt meglehetősen pontosan meghatározva Tóhokunál a vízszintes PGA, ha a károkat döntő mértékben előidéző szökőárral kapcsolatos veszélyeztetésre vonatkozóan nem történt megfelelő prognózis [2].

A földrengésveszély számításának eljárásai nem terjednek ki az *utórengések* lehetséges hatására sem. A legnagyobb utórengések igen jelentős szeizmológiai terhelést jelentenek, s ezek sokszor hosszú idő elteltével következnek be. Például Chilében 2010. február 27-én M = 8,8 erősségű földrengés pattant ki, és ez 2011 februárjában több nagy utórengést produkált, amelyek közül a legnagyobb M = 6,8 erősségű volt [2].

Földrengések intenzitását alapvetően határozza még meg a vizsgált hely geológiája, *talajviszonya*. Nagyon sok földrengésnél megfigyelték, hogy azokon a helyeken, ahol a felszín közelében fiatal, laza, homokos és agyagos üledékek találhatók, sokkal nagyobb károk keletkeztek, mint ott, ahol keményebb kőzetek bukkannak a felszínre. Az intenzitás növekedése még erőteljesebben jelentkezik mesterségesen feltöltött területeken. Egy M = 6,0 méretű földrengés esetén például a maximális vízszintes gyorsulás értéke 0,2 és 0,3 g között változik, ha a felszíni kőzet kemény, sziklás; 0,3-0,5 g, ha ez átlagos üledék, és végül 0,5-1,0 g laza üledék vagy feltöltés esetén [2]. Ugyanazon földrengés epicentrumától ugyanolyan távol fekvő helyek között akár 2 intenzitáskülönbség is előfordulhat. Szűkebb területen, településen belül is igen változatosak lehetnek a talajviszonyok, aminek következtében különböző súlyosságú károk keletkeznek.

Összefoglalás

Összegzésképpen elmondható, hogy a földrengéskockázat-elemzésnek sok hiányossága van. Sajnos mind a mai napig nem sikerült megbízható módszert találni az előrejelzés megoldására, sőt egyes vélemények szerint a földrengés kipattanása olyan sok tényezőtől függ, a folyamat olyan kaotikus, hogy pontos előrejelzésre sohasem lesz mód. Lehetőség van azonban a földrengéskockázat valószínűségi alapú meghatározására, vagyis annak kiszámítására, hogy valamely területen megadott méretű talajrázkódás adott időszak alatt milyen valószínűséggel várható. Kiszámítottuk ilyen

módon a PSHA-egyenletek segítségével Magyarország földrengés szempontjából legveszélyeztetettebb területén a talajgyorsulás 0,4 g értékét meghaladó valószínűségét.

A földrengéskockázat ismeretében történő előzetes felkészüléssel a földrengés által okozott károk és veszteségek csökkenthetők. Az előzetesen végrehajtott kárenyhítő intézkedések körébe tartozik egyebek mellett az építmények telephelyének megfelelő kiválasztása, az épület- és gépészeti szerkezetek földrengésálló tervezése, kivitelezése.

Hivatkozások

[1] P. Mónus, L. Tóth és K. Gribovszki, „A földrengéskockázat fogalma és meghatározási módszerei," *georisk.hu,* 2002, [Online]. Elérhető: http://georisk.hu/Tothetal/2002_gykonf_mptlgk.pdf (Letöltve: 2019. 05. 31.)

[2] P. Varga, „Földrengések előrejelzése," *Magyar Tudomány,* 172. évf. 7. sz., pp. 843–860., 2011.

[3] T. Zsíros, „A Kárpát-medence szeizmicitása és földrengés veszélyessége," in *Magyar Földrengés Katalógus 456-1995.* MTA GGKI, 2000.

[4] P. Varga, „Földrengések a történelemben. Komárom katasztrófája 1763-ban," *História,* 20. évf. 8. sz., pp. 22–25., 1998.

[5] B. Gutenberg and C. F. Richter, „Magnitude and energy of Earthquakes," *Annali di Geofisica,* vol 9, no. 1. pp. 1–15, 1956. DOI: https://doi.org/10.1038/176795a0

[6] J. Baker, "An Introduction to Probabilistic Seismic Hazard Analysis (PSHA)," *web.stanford.edu,* 2008, [Online]. Elérhető: https://web.stanford.edu/~bakerjw/Publications/Baker_(2008)_Intro_to_PSHA_v1_3.pdf (Letöltve: 2019. 05. 04.)

[7] C. A. Cornell, "Engineering Seismic Risk Analysis," *Bulletin of the Seismological Society of America,* vol. 58, no. 5, pp. 1583–1606, 1968.

[8] L. Tóth, P. Mónus és T. Zsíros, „Földrengések hatása épületekre," *foldrenges.hu,* [Online]. Elérhető: www.foldrenges.hu/index.php?option=com_content&view=article&id=20:foeldrengesek-hatasa-epueletekre&catid=19&Itemid=23 (Letöltve: 2019. 04. 28.)

[9] L. Tóth, „A lokális geológiai viszonyok hatása a telephelyen várható gyorsulásokra (A felső laza rétegek intenzitás módosító hatása, spektrális karakterisztikái)," *Magyar Geofizika,* 31. évf. 5–6. sz., pp. 143–161., 1990.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

15. évfolyam (2020) 1. szám 79–90.
DOI: 10.32567/hm.2020.1.6

Horváth Lajos[1]

A közép-tiszai árvízvédelmi fővédvonalba épített vízépítési műtárgyak életkor- és állapotelemzése

Age and Status Analysis of Hydraulic Structures Built in the Middle-Tisza Flood Defence Dike

Az elmúlt évtizedek sorozatosan rekordokat döntő tiszai árhullámai rávilágítottak arra, hogy az érintett árvízvédelmi létesítmények (földgátak, vízépítési műtárgyak, támfalak stb.) a magas víznyomásból származó többlet-igénybevétellel szemben ellenállóak, amennyiben a teherbírásuk és a műszaki állapotuk megfelelő. Jelen cikkben a szerző a közép-tiszai árvízvédelmi fővédvonalba épült vízépítési műtárgyak életkora alapján korfát készít, amelyről átfogó elemzést végez. A korfa és a műszaki állapot viszonylatában összefüggéseket tár fel, valamint javaslatot fogalmaz meg a fenntartási és felújítási munkák, mint műszakiállapot-javító elemek elvégzésének hatékonyabbá tételére.

Kulcsszavak: **árvízvédelem, vízépítési műtárgy, zsilip, árvíz, árvízvédelmi töltés**

During the past decades, the record-breaking flood waves of the Tisza have highlighted that the affected flood protection facilities (earth dams, water construction structures, bulkheads, etc.) are resistant to excess pressure from high water pressure, if their load capacity and technical conditions are adequate. In this article, the author prepares an age pyramid based on the age of the hydraulic structures built in the main line of the Middle Tisza flood defence, about which a comprehensive analysis has been carried out. It reveals the relationship between the age pyramid and the technical conditions, and makes proposals for making maintenance and renovation works more efficient and for improving the technical state of elements.

Keywords: **flood protection, hydraulic structures, levee, flood, dike**

[1] Közép-Tisza-vidéki Vízügyi Igazgatóság, műszaki igazgatóhelyettes, e-mail: horvath.lajos@kotivizig.hu, ORCID: https://orcid.org/0000-0003-1499-503X

Bevezetés

Az 1998-as évet követően többször vonult le a mértékadó árvízszintet[2] (a továbbiakban: MÁSZ) meghaladó árhullám a Közép-Tiszán, amely jelentős többletterhelést rótt az érintett árvízvédelmi létesítményekre. Ezek az árvizek komoly pénzügyi forrásokat, gépi és emberi munkaerőt igényeltek a védekezési és a helyreállítási munkák végzése során a vízügyi ágazattól, valamint a társszervezetektől. A 2000. évi rendkívüli árhullámot követően – vizsgálva és bizonyítva a MÁSZ emelkedő tendenciáját – megindultak az előzetes tervezési folyamatok, amelyek az árvízi veszélyeztetettség csökkentésére tett intézkedéseket tűzték ki célul. Megalkották a törvényi szintre emelt Vásárhelyi Terv Továbbfejlesztésének [1] alapkoncepcióját (a továbbiakban: VTT). A terv legfőbb alappillére az árvízvédelmi létesítmények előírás szerinti kiépítése, a kapcsolódó infrastrukturális fejlesztések, az árvízi tározás és a folyó vízszállító képességének növelése mellett.

A magasabb árhullámszintek miatt felül kellett vizsgálni az érvényben lévő MÁSZ-tervezési alapértékeket is. 2014-ben a vízügyi ágazat részéről ezek kiszámítása megtörtént, az új szintek jogszabályba történő rögzítése és kiadása megtörtént [2]. Az új értékek a megelőző értékekhez képest jellemzően emelkedők, de változó eltérést is mutatnak. (Például a Tiszán Szolnoknál 88,39 mBf[3]-ről 89,63 mBf-re változott.) Az árhullámok emelkedésével a védelmi létesítmények víznyomásból adódó terhelése is jelentősen megnövekedett, amelyet minden esetben figyelembe kell venni a létesítmények vízjogi engedély megszerzéséhez kötött felújításánál, fejlesztésénél, átalakításánál vagy újak építésénél.

A védelmi létesítmények többségében árvízvédelmi földgátak, amelyeken a különböző keresztezőlétesítmények (például belvízcsatorna, öntözőcsatorna, közút, vasút) átvezetésénél vízépítési műtárgyakat építenek be. Ezek a műtárgyak a töltésépítések előrehaladásával a Közép-Tiszán 1880-tól kezdődően létesültek, de nagy számban főként 1930 és 1989 között építették őket, az akkori tervezési előírások figyelembevételével.

Az építéstől napjainkig eltelt idő alatt megemelkedtek a tervezési magassági szintek, így feltételezem, hogy a műtárgyak nem minden esetben felelnek meg az előírt biztonsági előírásoknak, ezért fejlesztési beavatkozások végzése indokolt lehet.

Az árvízvédelmi művek egyes elemei a kritikus műszakiinfrastruktúra-elemek körébe tartoznak – amelyek esetében jogszabály szerinti azonosítási eljárást folytattak le –, mivel védelmi képességük miatt jelentős hatással vannak az érintett területen élő lakosság biztonságára és az odatelepült gazdasági, ipari értékekre.

A vizsgált téma aktualitását az is bizonyítja, hogy az árhullámok szintjének megemelkedésével egyenes arányban nő a műtárgyakat érő víznyomásterhelés, valamint a műtárgyak folyamatosan öregednek az elmaradó fejlesztési munkák következményeként. E két befolyásoló elem hatása összeadódva hatványozottan emeli a rongálódás, tönkremenetel bekövetkezésének valószínűségét, egy rendkívüli vízterhelés megjelenésekor. A vizsgálat alá vont vízépítési műtárgyak kora – a felújításokat is

[2] Mértékadó árvízszint: a jégmentes árvíznek az 1%-os valószínűségű vízhozamából származtatott vízszint.
[3] mBf – a Balti-tenger (kronstadti) közepes vízszintjéhez viszonyított tenger feletti magasság méterben.

figyelembe véve – a tervezéskori élettartamukból adódóan elöregedettnek mondható. Feltételezem, hogy nem történtek meg olyan ütemben azok a szükséges felújítások, amelyek biztosították volna a megfelelő műszaki állapot folyamatos szinten tartását.

Számos szakirodalom és publikáció foglalkozik az árvízvédelmi földanyagú töltések tönkremenetelével, valamint azok kísérőjelenségeivel, de a vízépítési műtárgyak rongálódásának, tönkremenetelének kutatási témájával kapcsolatban csak kis számban jelentek meg tudományos jellegű cikkek és publikációk a hazai szakirodalomban (bemutatásukra lentebb kerül sor a releváns hazai publikációk fejezetben).

A Közép-Tisza-vidéki Vízügyi Igazgatóságnál (a továbbiakban: KÖTIVIZIG) mindvégig felelős beosztásban töltött, 15 év alatt szerzett gyakorlati tapasztalataim és a feltárható nyilvántartási adatok alapján megvizsgáltam a KÖTIVIZIG területén lévő fővédvonali vízépítési műtárgyak jellemző műszaki állapotát, a korfa elöregedését és az elmaradt felújítások mértékét.

Célom a tudományos közlemény megírásával, hogy műszaki szakmai érvek alátámasztásával felhívjam a figyelmet arra, hogy az árvízvédelmi földművek fejlesztésével párhuzamosan a műtárgyak állapotjavítására is szükséges kellő figyelmet fordítani. A tervszerű felújításokat és fejlesztéseket ütemezetten, a rendelkezésre álló erőforrások figyelembevételével kell végezni, hogy a jövőben bekövetkező magasabb árhullámok kivédhetővé váljanak. Védelmi vonalaink műszakilag alkalmasak és teherbírók kell hogy legyenek feladatuk elvégzésére, ezzel megelőzve egy árvízkatasztrófa bekövetkezését.

A tiszai árvízvédelmi fővédvonalak rendszere, a töltések műtárgyai, az árvízcsúcsok jellemzői

Árvízvédelmi töltések építésének története

Az ármentesítés és vízszabályozás megindulása előtt a magyar Alföldet a folyók kiöntései, árvizek borították az év legnagyobb részében. Hatalmas nádrengetegek és járhatatlan mocsarak tarkították az Alföld felszínét. Emberi települések leginkább az árvizek fölé emelkedő dombhátakon alakultak ki, és lakóik élete minden vonatkozásban szorosan hozzá volt kötve a vizek életéhez. Igazi „vízivilág" volt, amely szükség esetén élelmet és védelmet biztosított számukra [3].

A törökök kiűzése után, amikor az ország politikai, gazdasági és társadalmi viszonyai kezdtek megszilárdulni és állandósulni, a népesség száma is megnövekedett, a lakosság életviszonyai is megváltoztak. Az addigi állattartás mellett már egyre több lett a megművelt földterület, és az árvizek kiöntései után egyre nagyobb lett az elszenvedett kár is. A falvak, települések lakói eleinte elszigetelten, magukra hagyva küzdöttek a pusztító árvizek ellen. Ez a küzdelem teljesen hiábavaló és meddő fáradozás volt.

A 19. század első felében levonult nagy árvizek mérhetetlen pusztításai után következő ínséges idők hatása alatt a folyók menti községek lakói mind egységesebben követelték a kormányzattól az állandóan megismétlődő árvizek elleni megfelelő intézkedések megtételét. Különösen az 1845. évi tiszai árvíz pusztítása után vált sürgős követeléssé a Tisza árvizeinek megfékezése és szabályozása [3].

Széchenyi István buzdítására és felhívására az érdekeltek egyletekbe tömörültek a vízszabályozás megoldása céljából és 1846. január havában már megalakították az ármentesítő társulatok központi szervét, a Tisza-völgyi Társulatot. Ettől kezdve a Tisza-völgyében egymás után alakultak a különböző Tisza-szabályozó és ármentesítő társulatok, azzal a céllal, hogy érdekeltségeik területén közös erővel védekezzenek az árvizek pusztításai ellen. Tervek készültek, amelyek nyomán a folyó kanyarulatait átmetszésekkel rövidítették meg, és gátak emelkedtek partjain.

Ezzel megkezdődött egy olyan heroikus küzdelem, amelyben nincs megállás egy pillanatra sem. A gátak közé szorított folyó igyekszik lerázni bilincseit. Az egykori kiöntések, mocsarak helyén falvak, városok, gyártelepek, utak, vasutak létesültek, élnek, virágoznak.

Az ármentesítő töltések véglegesnek tekinthető szelvénye az 1919. és 1932. évi nagy árvizek után alakult ki. Az akkori társulatok saját biztonságuk érdekében, általában sürgősen végrehajtották a szükséges töltéserősítési munkákat. Napjainkban, ahol az árvédelmi biztonság nincs meg, a fejlesztési feladatok elsősorban a töltések keresztszelvényeinek szélességi és magassági hiányainak pótlásával kapcsolatban jelennek meg [3].

A töltéseket keresztező műtárgyak, létesítmények

Az árvízvédelmi töltések jelentős hosszúságú – esetenként több száz kilométeres egybefüggő – vonalas létesítmények. Elkerülhetetlen (a jelentős hossz miatt) a keresztezések szükségessége más, főként szintén vonalas jellegű infrastruktúra-elemmel. A hazai árvízvédelmi fővédvonalakban jelentős számú és sokféle típusú kereszteződésű létesítmény található (zsilipek, nyomócsövek, szivornyák, ivóvíz-, szennyvíz-, termékvezetékek, erősáramú és hírközlő kábelek, út-, vasútátvezetések, valamint egyéb létesítmények). Ezeknek a szerkezeteknek eltérő az állapota, kora, nem ritkák köztük az évszázados létesítmények sem. Állaguk, műszaki jellemzőik folyamatos, naprakész ismerete fontos a védekezés-irányítás számára [4].

A tiszai árvízvédelmi töltést keresztező létesítmények több kategóriába sorolhatók az alábbi funkciók szerint:

- zsilip;
- nyomócső, szivornya;
- keresztező út/vasút;
- közműátvezetés (csőszerű, vezetékjellegű);
- bújtató;
- híd;
- egyéb műtárgy (aluljáró, árvízkapu, kulisszanyílás, egyéb létesítmény).

A műtárgyak és létesítmények, magassági elhelyezkedésük szerint, három kategóriába sorolhatók:

- térszín alatti;
- térszíni;
- térszín feletti.

A jelen tanulmányban kifejezetten az árvízvédelmi fővédvonalba épített térszín alatti vasbeton vízépítési zsilipek körét vizsgáltam, amelyek az árvízi veszélyeztetettség terén a legnagyobb halmazt teszik ki.

Árvízcsúcsok szintjének emelkedő tendenciája

A Közép-Tiszán az 1880. évtől napjainkig vizsgált időszakban az árvízcsúcsok növekedése és egyben a valaha mért legnagyobb vízszint[4] (a továbbiakban: LNV) rekordjának meghaladása számos esetben fordult elő. Az 1. táblázatban láthatók azon tiszai vízrajzi mérőállomáson mért vízállásadatok, amelyek esetében LNV-meghaladás történt. Az adatokat értelmezve megállapítható, hogy tízszer vonult le rekordszinten árhullám a vizsgált időszakban, és ezek közül a szintemelkedések 132 cm-től (tiszaugi vízmérce esetében) a 223 cm-ig (szolnoki vízmérce esetében) szórnak. Az adatok elemzéséből az is megállapítható, hogy az emelkedések üteme az eltelt idő függvényében nem egyenletes, hanem az utóbbi időszakban az emelkedés mértéke felgyorsult. Például a szolnoki vízmércén mért vízállások tekintetében 1888-tól 1970-ig (82 év alatt) 117 cm-t, míg 1970-től 2000-ig (30 év alatt) 106 cm-t emelkedett. Előbbi esetben 1,4 cm/év, második esetben 3,5 cm/év az átlagos emelkedés.

1. táblázat

Vízmérce állomásokon mért LNV-vízállások növekedése
(a szerző szerkesztése a KÖTIVIZIG Vízrajzi Adatok Gyűjteménye[5] alapján [5])

Év	Vízmérce-állomás	Vízállás [cm]	Vízmérce-állomás	Vízállás [cm]	Vízmérce-állomás	Vízállás [cm]	Vízmérce-állomás	Vízállás [cm]
1888	Tiszafüred	742			Szolnok	818		
1895			Tiszabő	866	Szolnok	827		
1919			Tiszabő	919	Szolnok	882	Tiszaug	814
1932	Tiszafüred	750	Tiszabő	921	Szolnok	894	Tiszaug	840
1967	Tiszafüred	765						
1970	Tiszafüred	773	Tiszabő	935	Szolnok	935	Tiszaug	843
1979	Tiszafüred	788	Tiszabő	949				
1999	Tiszafüred	835	Tiszabő	1023	Szolnok	974	Tiszaug	844
2000	Tiszafüred	881	Tiszabő	1080	Szolnok	1041	Tiszaug	932
2006							Tiszaug	946

Az árvízcsúcsok meghaladása mellett figyelembe kell venni, hogy a MÁSZ első jogszabályi előírásának megjelenését követően az LNV-rekordot döntő szintek mellett

[4] Legnagyobb víz (LNV): A vízmércén a vizsgált évig bezárólag előfordult legmagasabb vízállás.
[5] Vízrajzi Adatok Gyűjteménye: A KÖTIVIZIG napi rendszerességgel észlelt vagy mért vízrajzi adatait tartalmazó gyűjtemény, amely nyilvános online felületen vagy írásos kiadványként nem hozzáférhető, azonban hivatalos adatszolgáltatás keretében elérhető.

további 4 esetben fordult elő (1999., 2000., 2006. és 2010. években), hogy a levonuló árhullám ezen érték felett tetőzött a Tisza KÖTIVIZIG működési területére eső szakaszán.

Kijelenthető, hogy az elmúlt évek emelkedő bekövetkezési gyakoriságú árhullámai és azok magasságai jelentős növekedést mutatnak, így várhatóan egy jövőbeli rekordot döntő árvíz bekövetkezésének valószínűsége magasabb az azt megelőzőnél. Az árvízvédelmi létesítmények vízépítési műtárgyai, mint fokozott kockázatú infrastruktúra-elemek víznyomásterhelésnek való kitettségei az árhullámok szintjének emelkedésével együtt nőnek.

A releváns hazai publikációk

Az árvízvédelmi létesítményeket érintően számos leíró és elemző tanulmány jelent már meg, elsődlegesen vízügyi ágazati folyóiratokban,[6] főként földanyagú gátak építése, töltés-tönkremenetelek (szakadások) [6], árvízi jelenségek, árvízvédekezési beavatkozások kapcsán. Ezek közül célzottan kevés ágazati szakirodalom foglalkozik az árvízvédelmi műtárgyak állapotával, korával vagy esetleges tönkremenetelével.

Az árvízi katasztrófák bekövetkezése a világban főként rendkívüli árhullámokból és az azt követő töltésszakadásból valósul meg, ritkán fordul elő, hogy műtárgy-tönkremenetelre vagy azzal szorosan összefüggő műszaki problémára vezethető vissza. Magyarországon is ismert árvíz alatti műtárgyon bekövetkező károsodás nem történt, mert a védelmi beavatkozások megtétele stabilizálta azok állapotát és nem következett be tönkremenetel, és ebből adódó árvízi elöntés.

Egy ilyen kiemelkedő eset volt a 2000. évi árhullám során végbement Kurca-toroki zsilip és szivattyútelep jelentős károsodása, meghibásodása, amelyről két leíró publikáció is megjelent [8]. A cikkek teljeskörűen bemutatják a károsodáshoz vezető körülmények kialakulását, a meghibásodás folyamatát, a kárelhárítás érdekében tett beavatkozásokat, valamint a hiba helyreállításának elvégzését. A publikációkban utalás történt arra is, hogy a kialakult károsodás összefüggésbe hozható (nem elsődleges kiváltó okként) a műtárgy korával (az építés éve 1885.), annak eredeti műszaki állapotával (téglaboltozatos zsilipcsatorna), annak ellenére, hogy korábban egy kisebb javításon esett át.

Az árvédelmi létesítmények (műtárgyak) építésére, fejlesztésére, felújítására jelentős pénzügyi finanszírozás szükséges és időigényes folyamat. Ezért, azok állapotromlásának javítása vagy megállítása csak ütemezett tervezéssel és kivitelezéssel valósítható meg. Egy 1977-ben megjelent közlemény is foglalkozott az árvízvédelmi fejlesztési beruházások optimális elosztásának dinamikus tervezésével [9], amelyben megoldásokat mutattak be arra, hogy a beruházások megvalósítása több évre tervezhetően megtörténhessen. Sajnos, ez továbbra is jelentős probléma, az akkor vázolt helyzet jelenleg is megoldásra vár.

Egy kutatás eredményeit bemutató szakmai cikkben összegyűjtötték azokat a dokumentált, a Kárpát-medencében az árvízvédelmi fővédvonalak tönkremenetelével és a gátszakadások kialakulásával járó eseményeket, valamint azok bekövetkezésének

[6] Vízügyi ágazati folyóiratok: *Hidrológiai Közlöny, Hidrológiai Tájékoztató, Vízügyi Közlemények.*

okait, amelyek között néhány esetben található műtárgyrongálódásból származó gátszakadás is [6].

A vízépítési műtárgyak tervezési élettartama, korfája

Vizsgált műtárgyak köre

A KÖTIVIZIG vagyonkezelésében lévő 707 km árvízvédelmi fővédvonalon 722 db keresztezés található, amelyek közül kifejezetten az árvízkockázati kitettség szempontjából legfontosabb, térszín alatti zsilipes vízépítési műtárgyakat vizsgáltam. Ezen műtárgyak száma 143 db, amelyek közül 11 db-nak hiányosak az alapadatai, többek közt az építés éve.

Az árvízvédelmi fővédvonalakban lévő, keresztező műtárgyak országos adatbázisának első verzióját 1996-ban hozták létre, míg a második 1998-ban készült el. Az adatbázis tartalmazza az elsőrendű árvízvédelmi vonalakban lévő műtárgyak adatait az árvízvédelmi nyilvántartási tervek alapján, valamint a fővédvonalakat keresztező létesítményekre vonatkozó legfontosabb információkat. Összesen több mint 2300 műtárgyról, egyenként csaknem 40 alfanumerikus és szöveges adatot, valamint csatolt fényképet, műszaki rajzot tartalmaz [4]. A jelen tanulmányban vizsgált műtárgyak esetében, ezen adatbázis hiányos volta miatt a KÖTIVIZIG saját nyilvántartási adataiból dolgoztam. A továbbiakban mindenképpen szükséges az országos adatbázisban szereplő területi hiányosságok feltárása és teljes körű feltöltése.

Tervezési élettartam

A jelenlegi hazai szabályozás a vasbeton műtárgyak tervezési élettartamára vonatkozóan teljes körű. A tervezési élettartam meghatározása minden esetben a beruházó felelőssége. Ezzel kapcsolatos részletes előírást az érvényben lévő MSZ EN 1990:2005[7] számú magyar szabvány ad. A szabvány szerkezeti és környezeti osztályba rendeli az előírható tervezési élettartam függvényében a vasbeton tartószerkezeti létesítményeket, és közé sorolhatók be az árvízvédelmi műtárgyak is. A tervezési élettartam a cserélhető tartószerkezeti részek esetében 10-25 év (például zsilip elzárószerkezetei), míg az épületek tartószerkezetei és egyéb szokásos tartószerkezetek esetében 50 év. Figyelembe vehető még a legmagasabb osztály előírása a monumentális épületek tartószerkezeteire és hidakra vonatkoztatva, ami 100 évet határoz meg tervezési élettartamnak. A már megépített árvízvédelmi zsilipek tervezése és kivitelezése idején – a 2005-ös év előtt – még nem ezen előírás volt követendő a betonminőségek figyelembevétele tekintetében.

Az 1940-es évek előtt épült műtárgyak egy része vegyes szerkezetű betonból, terméskőből és téglából készült, nem pedig az 1950-es évektől elterjedő, korszerűnek számító vasbeton technológiával. Általánosságban ágazati tervezői szinten elfogadott,

[7] MSZ EN 1990:2005: Eurocode: A tartószerkezetek tervezésének alapjai.

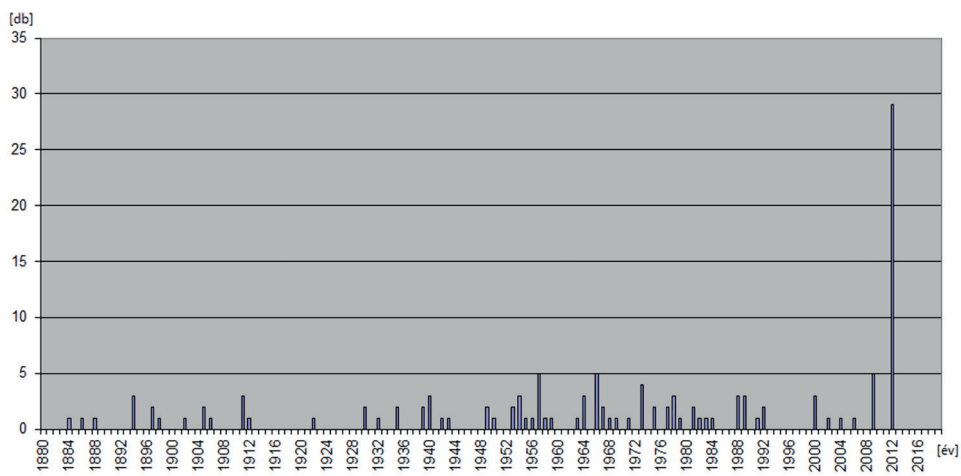
hogy a nem speciális célt szolgáló vízépítési műtárgyak tervezési élettartama a jelenlegi és a régi szabályozást is tekintve 50 év.

Korfa

A KÖTIVIZIG nyilvántartási adataiból előállítottam az árvízvédelmi fővédvonalban létesített műtárgyak számának diagramjait az építés éve szerinti bontásban, amelyeket az 1. és 2. ábra szemléltet.

A diagramok alapján megállapítható, hogy az egyes években létesített műtárgyak száma jelentős összefüggésben áll a múltbeli történelmi és árvízi eseményekkel. Az első világháború idején építés nem történt, de azt követően jelentős munkálatok indultak meg. Megfigyelhető az is, hogy a második világháború idején, ha kis számban is, de voltak építési munkálatok, de azt követően az építési intenzitás sokszorosa lett az azt megelőző időszakhoz képest. A harmadik, nagyobb törést a műtárgyépítésekre a rendszerváltás hozta, amikor teljesen abbamaradtak az építési beruházások.

A 2009-es és 2012-es évek magasabb, kiemelkedő értékei a már ismertetett VTT-program keretében megvalósult, 3 db közép-tiszai árvízi tározó[8] építése során létesített új árvízvédelmi zsilipekből adódnak.



7. ábra

Műtárgyak évenkénti építésének kimutatása (a szerző szerkesztése [10] adatainak alapján[9])

A történelmi események mellett jelentős összefüggés figyelhető meg az LNV-szintet meghaladó árhullámot követő években is. Jellemzően abban az évben vagy az azt követő

[8] Közép-Tiszai árvízi tározók: Tiszaroffi (2009.), Nagykunsági (2010.), Hanyi-Tiszasülyi (2012.)

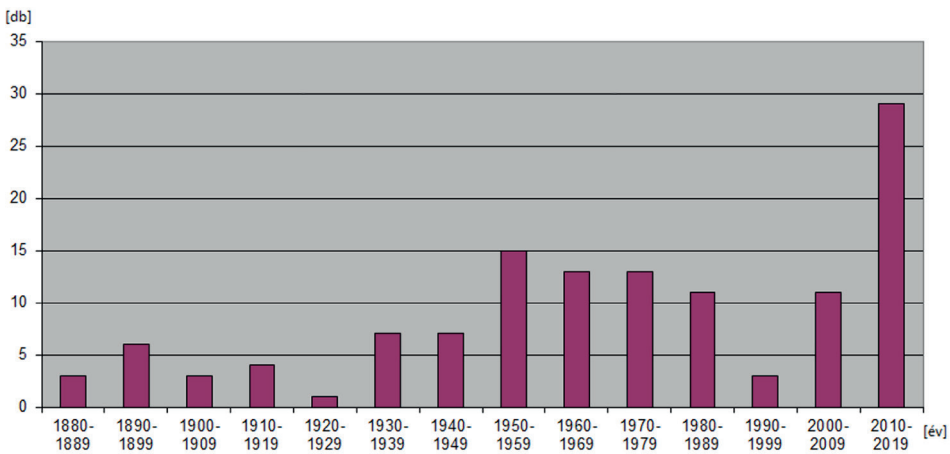
[9] Árvízvédekezési Terv: 10/1997. (VII. 17.) KHVM rendelet az árvíz- és belvízvédekezésről előírása alapján a KÖTIVIZIG által készített árvízvédekezési terv, amely nyilvános online felületen vagy írásos kiadványként nem hozzáférhető, azonban engedélyhez kötött adatszolgáltatás keretében elérhető.

években, mikor LNV-t meghaladó árhullám vonult le, az árvízvédelmi fejlesztések és egyben műtárgyépítések jelentős szerepet kaptak a hazai építési beruházások között.

Az 1970. évi MÁSZ-érték meghatározását megelőzően a tervezési és egyben kiépítési szinteket az LNV-szinthez mért 1,5 méteres magassági biztonsági szinttel jelölték ki (például az 1895. évi és 1932. évi árhullámok).

Az 1900-tól 1970-ig terjedő időszakban az árhullámokat követően meghatározott kiépítési szintnek megfelelő fejlesztések tervezésének megkezdése rövid idő alatt megindult. A mai gyakorlatra jellemző a fejlesztések időbeli elhúzódása. Például a 2014-es év előtti MÁSZ-előírásra történő kiépítettség a 2000-es években 50% körüli volt, míg jelenleg a 2014. évi MÁSZ-előírások figyelembevételével 10% alatti.

Megállapítható az is, hogy a vizsgált időszakon belül (1884–2019) átlagosan 1,06 db műtárgy épült évente. Amennyiben csak azokat az éveket vizsgáljuk, amelyekben tényleges műtárgyépítés történt, úgy 2,65 db műtárgyépítés/év az átlag.



8. ábra

Műtárgyak évtizedenkénti építésének kimutatása (a szerző szerkesztése[10] [10] alapján)

Az évtizedenkénti vízépítési műtárgyak koreloszlásából (2. ábra) az is megállapítható, hogy a műtárgyak jelentős része a tervezési élettartamon túl van és a VTT-beruházásokat érintő adatokat leszámítva a korfa elöregedett.

A műtárgyak átlagéletkora 44,8 év, ami megközelíti a tervezési élettartam 50 évét. (Amennyiben a VTT-beruházásból származó, 2012-ben létesített 29 db új műtárgyat kivesszük az átlagszámításból, úgy az átlagéletkor 56 évre adódik.)

[10] Árvízvédekezési Terv: 10/1997. (VII. 17.) KHVM rendelet az árvíz- és belvízvédekezésről jogszabály előírása alapján a KÖTIVIZIG által készített árvízvédekezési terv, amely nyilvános online felületen vagy írásos kiadványként nem hozzáférhető, azonban engedélyhez kötött adatszolgáltatás keretében elérhető.

A közép-tiszai vasbeton műtárgyak állapota

A 2. táblázatban a 143 db vizsgált műtárgy állapotát soroltam 5 kategóriába az éves őszi szakágazati bizottság felülvizsgálatai és megállapításai alapján. A vizsgálat főként szemrevételezés alapján történt. Megállapítható, hogy a kategóriák alapján a műtárgyak kétharmada megfelelő, azonban egyharmaduk valamilyen beavatkozást igényel. Feltárható az a változás is, ami a beavatkozást igénylő műtárgyak 2011-ről 2018-ra történő átrendeződését mutatja, miszerint a megfigyelendő kategóriából átsoroltak bizonyos műtárgyakat a javítandó kategóriába. Ez alapvetően a műtárgyak állapotromlását jelzi. A vizsgált 143 db műtárgy esetében 11 alkalommal került sor felújításra, ebből 9 esetben elhasználódásból származó állapotromlás miatt, 3 esetben pedig még garanciális beavatkozás történt. A felújítással érintett műtárgyak mértéke 8% alatti. A tervezési élettartamot meghaladó korú műtárgy, azaz 1969 előtt épített és felújításon át nem esett zsilip a KÖTIVIZIG területén 54 darab, ami jelentős felújítási elmaradást és egyben árvízi kockázatot mutat.

2. táblázat

Árvízvédelmi töltésben lévő műtárgyak állapota (a szerző szerkesztése [11] adatainak alapján[11])

Év	Megfelelő [db]	Megfigyelendő [db]	Megszüntetésre javasolt [db]	Javítandó [db]	Átépítendő [db]	Összesen [db]
2011	68	28	3	5	10	114
2017	97	18	3	18	7	143
2018	96	19	4	17	7	143

Mivel a tervezési élettartamon túl van a vízépítési műtárgyak jelentős része, és a tervezéskori méretezés óta kimagasló terhelésváltozás állt be, így a műtárgyak ellenőrző méretezési számítását feltétlen szükséges elvégezni. Vízzárásra, süllyedésre, elcsúszásra, billenésre és teherbírásra vizsgálva megállapítható, hogy szükség van-e egy azonnali építési (felújítási) beavatkozásra, vagy sem.

Következtetések

Megállapítható, hogy a KÖTIVIZIG működési területén vizsgált vízépítési műtárgyak korfája jelentősen elöregedett, a feltárt építési évük és az elvégzett felújítási munkák figyelembevétele alapján. Az állapotuk egyharmada a szakágazati felülvizsgálatok megállapításai szerint nem megfelelő, ami a tervezési élettartamot meghaladó korú műtárgyak arányával összhangban van.

[11] Szakbizottsági felülvizsgálati jegyzőkönyv: a 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól előírása alapján a KÖTIVIZIG vagyonkezelésében lévő védműveken évenkénti rendszerességgel felülvizsgálatot kell tartani, amiről szakbizottsági felülvizsgálati jegyzőkönyv készül, amely nyilvános online felületen vagy írásos kiadványként nem hozzáférhető, azonban engedélyhez kötött adatszolgáltatás keretében elérhető.

Kijelenthető, hogy a vizsgált 143 darab vízépítési műtárgy esetében a felújítási munkák végzése elmaradt a szükséges mértéktől, annak ellenére, hogy a beavatkozást igénylő esetekben az állapotromlás is kimutatható volt. Ez a tendencia folyamatosan jellemzi a műtárgyak állományát. A műszaki állapot minimálisan elvárható szinten tartásához elengedhetetlen a felújítási munkák ütemezett elvégzése a pénzügyi keretek figyelembevétele mellett.

Az elmúlt évek árvízvédelmi beruházásai során alkalmazott korlátozott finanszírozási konstrukciókat figyelembe véve, a vízépítési műtárgyak esetében is szükséges a beavatkozási munkák prioritási sorrendjének meghatározása. A műtárgyak állapot- és állékonysági vizsgálata során figyelembe kell venni a jelenleg érvényben lévő MÁSZ-értékeket, valamint alkalmazni kell a tervezéskori és jelenlegi előírásokat, valamint biztonsági tényezőket. A műtárgyak szemrevételezéses vizsgálatát javasolt kiegészíteni roncsolásmentes műszaki diagnosztikai mérésekkel és az acél anyagú elzárószerkezetek esetében korrózióvizsgálattal is.

Szükséges az országos műtárgynyilvántartási adatbázisba a meglévő és még felkutatható nyilvántartási adatokat is feltölteni, azért, hogy az ilyen célból készült komplex adatbázisrendszerben a műtárgyak adatai elérhetők és funkcióik alapján kereshetők legyenek. Ez nagyban segíti az árvízvédelmi feladatok tervezését, és képet ad a műtárgyak állapotáról vagy azok elvárható műszaki szinttől való elmaradásáról.

A cikk megírásával az volt a célom, hogy műszaki szakmai érvekkel felhívjam a figyelmet az árvízvédelmi földművek fejlesztésével párhuzamosan végzendő, keresztező műtárgyak állapotjavításának szükségességére is. A tervszerű felújításokat és fejlesztéseket ütemezetten, a rendelkezésre álló erőforrások figyelembevételével kell elvégezni azért, hogy a jövőben bekövetkező magasabb árhullámok kivédésére műszakilag alkalmasak legyenek, megelőzve ezzel egy árvízkatasztrófa bekövetkezését.

Tervezem, hogy a jövőben a vizsgált műtárgyak körét kiterjesztem a teljes hazai területre, azzal a céllal, hogy a KÖTIVIZIG területén feltárt adatok összehasonlíthatóvá váljanak az országos adatokkal is.

Hivatkozások

[1] 2004. évi LXVII. törvény a Tisza-völgy árvízi biztonságának növelését, valamint az érintett térség terület és vidékfejlesztését szolgáló program (a Vásárhelyi-terv továbbfejlesztése) közérdekűségéről és megvalósításáról
[2] 74/2014. (XII. 23.) BM rendelet a folyók mértékadó árvízszintjeiről
[3] Z. Károlyi és G. Nemes, *A Közép-Tiszavidék vízügyi múltja II.* Budapest: Vízügyi Dokumentációs és Tájékoztató Iroda, 1975., p. 125.
[4] S. Bara, „Az árvízvédelmi műtárgyak adatbázisa," *Vízügyi Közlemények,* 81. évf. 3. sz., pp. 391–404., 1999.
[5] KÖTIVIZIG, *Vízrajzi adatok gyűjteménye.* Szolnok, 2006.
[6] L. Nagy, *Gátszakadások a Kárpát medencében.* Budapest: Országos Vízügyi Főigazgatóság, 2017.

[7] Á. Jászné Gyovai, „A Kurca-toroki zsilip és a Mindszent II. szivattyútelep egyidejű meghibásodása és a hibák elhárítása a 2000. évi tiszai árvíz során," *Hidrológiai Közlöny,* 85. évf. 1. sz., pp. 51–52., 2005.
[8] I. Gy. Török, „A Kurca-toroki zsilip," *Vízügyi Közlemények,* 85. évf. 4. sz., pp. 600–608., 2003.
[9] Gy. Meszéna, „Árvízvédelmi fejlesztési beruházások optimális elosztásának dinamikus tervezése," *Vízügyi Közlemények,* 59. évf. 1. sz., pp. 7–21., 1977.
[10] KÖTIVIZIG, *Árvízvédekezési terv.* Szolnok, 2019.
[11] KÖTIVIZIG, *Szakbizottsági felülvizsgálati jegyzőkönyv.* Szolnok, 2019.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

15. évfolyam (2020) 1. szám 91–105.
DOI: 10.32567/hm.2020.1.7

Legárd Ildikó[1]

Célpont vagy! – a közszolgálat felkészítése a kiberfenyegetésekre

You Are a Target! – The Preparation of the Public Administration against Cyber Security Threats

Napjainkban a közigazgatás megszervezése elképzelhetetlen infokommunikációs technológiák alkalmazása nélkül. Azonban bármennyire is védjük rendszereinket és a bennük tárolt adatokat a legmodernebb fizikai és logikai intézkedésekkel, még mindig a humán faktor jelenti a legnagyobb kockázatot. A fenyegetésekkel szembeni hatékony védelmet a felhasználók biztonságtudatossága tudja biztosítani, amely egy jól megszervezett és sikeres biztonságtudatosító program segítségével alakítható ki. A tanulmány bemutatja a humán alapú és a számítógép-alapú social engineering típusú támadás technikáit, áttekinti a biztonságtudatosság és az információbiztonság-tudatosító program fogalmát és ez utóbbi megvalósításának öt lépését, valamint megvizsgálja egy hatékony tudatosítóprogramhoz szükséges módszerek, kommunikációs csatornák és belső PR-eszközök alkalmazási lehetőségeit.

Kulcsszavak: információbiztonság, biztonságtudatosság, információbiztonság-tudatosító program, social engineering, belső PR-eszközök

Nowadays, the organisation of public administration is unimaginable without infocommunication technologies. Although the physical and logical protection of the system and the stored data may be well developed, the human factor will be a risk of security. The effective protection against the threats is to provide security awareness through implementing a well-developed and successful Information Security Awareness program.
This study presents the methods of human-based and IT-based social engineering attacks, reviews the category of security awareness and security awareness programs, determines five steps of the implementation and examines the different methods, the potential communication channels and internal PR tools of an effective program.

[1] Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola, doktorandusz, e-mail: ildiko.legard@gmail.com, ORCID: https://orcid.org/0000-0002-1469-8679

Keywords: **information security, security awareness, security awareness program, social engineering, internal PR tools**

Bevezetés

Az utóbbi bő három évtizedben bekövetkező technológiai fejlődés, a digitalizáció ugrásszerű megnövekedése, az infokommunikációs eszközök és szolgáltatások rendkívüli fejlődése, az internet széles körű elterjedése, a gyors hozzáférés visszavonhatatlanul megváltoztatta az emberek életét, a vállalkozások működését és a közigazgatás szervezését.

Magyarországon a 2015-ben indított *Digitális Jólét Program* már alapvető célként határozza meg a digitális állam megteremtését és annak részeként a teljes közigazgatás digitális átalakítását [1].

A közigazgatás által döntően elektronikus információs rendszerekben[2] tárolt, feldolgozott és továbbított adatok és információk mennyiségének, illetve mibenlétének köszönhetően, napjainkban a magyar állami és önkormányzati szervek egyre több, a kibertér[3] felől érkező fenyegetésnek vannak kitéve, amelyek egyaránt érinthetik mind magukat a szerveket, mind pedig a munkavállalókat.

„Napjainkban jól elkülöníthető a kiberfenyegetések négy fajtája. Ezek a kiberbűnözés, a hacktivizmus és kiberterrorizmus, a kiberkémkedés és a kiberhadviselés" [2: 143–144.]. A közigazgatást érintő fenyegetések esetében mind a négy relevanciával bír.

Az NTT Security által 2019-ben közzétett *Global Threat Intelligence Report* alapján a közigazgatás a kiberfenyegetések 5 legnépszerűbb célpontja között van [3].

A közszférában dolgozók a támadók számára értékes és kiemelt célpontnak számítanak, hiszen általuk a nemzeti adatvagyon részét képző adatokhoz, információkhoz is hozzáférhetnek, vagy megbéníthatják egy egész szervezet és végső soron akár az egész ország működését is.

Ahogy Beláz Annamária fogalmaz tanulmányában, „Ahhoz, hogy a közigazgatási rendszer hosszútávon működőképes maradjon, valamint a rendszerekben előállított, tárolt, feldolgozott és továbbított adatok védelme biztosított legyen, az államnak elsőrendű feladata az információbiztonság szervezése és az információbiztonsági szemléletmód kialakítása, fenntartása" [4: 93.].

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1 § (1) 14. b „elektronikus információs rendszer:
a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy
c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;"

[3] A kibertér egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszereket, valamint beágyazott processzorokat és vezérlőket [9: 30.].

Social engineering

Az elmúlt évtizedekben az információs rendszerek védelme egyre kifinomultabbá vált, ugyanakkor a rendszereket használók biztonságtudatossága nem tartott lépést a technikai fejlődés ütemével. Így nem meglepő, hogy a kiberbűnözők egy új és nagyon hamar népszerűvé vált támadási formát kezdtek el alkalmazni, az úgynevezett social engineering-et.

A social engineering az emberi hiszékenységre, együttműködő-képességre építő támadási forma. A támadók olyan alapvető emberi tulajdonságokat használnak ki, mint a segítőkészség, a hiszékenység, a befolyásolhatóság, a naivság vagy a kíváncsiság, amely jó eséllyel minden emberben ott lakozik, amelyekhez hozzáadódhat a biztonságtudatosság különböző okokból (alulképzettség, hanyagság stb.) bekövetkező hiánya, valamint a támadó általi szándékos megfélemlítés, zsarolás vagy megvesztegetés. Ezek kihasználásával már a támadó könnyen vagy mindenesetre könnyebben megkerülheti a rendszerek fizikai és logikai védelmi vonalát, például tűzfalakat vagy behatolás-detektáló rendszereket [5: 117.].

A social engineering típusú támadásokat, aszerint, hogy a támadó milyen módszereket használ, két csoportba lehet sorolni:

1. Humán alapú támadások [6], [7]

A humán alapú technikák alkalmazásához nem feltétlenül szükséges szaktudás, a támadó nem használ informatikai eszközöket, bárki által kivitelezhetők, azonban előzetes megfigyelést és felkészülést igényelnek. A támadó és áldozata között közvetlen kontaktust feltételez, így a lebukás veszélye is nagyobb [6: 4.].

Típusai:

- segítség kérése;
- segítség nyújtása (fordított social engineering);
- megszemélyesítés, vagyis az identitáslopás;
- thombstone theft, azaz a sírkőlopás, amely a megszemélyesítés egy speciális fajtája;
- shoulder surfing (képernyő lelesése);
- az irodai hulladék átvizsgálása, azaz a dumpster diving;
- tailgating, vagyis a szoros követés módszere a bejáraton történő bejutáshoz;
- piggybacking: a támadó az áldozat segítségével és tudtával jut át a bejáraton.

2. Számítógép-alapú támadások [8], [7]

A közvetett kapcsolattartást preferáló, számítógép-alapú támadások sokkal elterjedtebbek, mivel a támadó valamilyen informatikai eszközön keresztül lép kapcsolatba az áldozattal, így kisebb a lebukás veszélye.

Típusai:

- adathalászat – phishing: olyan üzenet, jellemzően e-mail, küldése az áldozatnak, amely megtéveszti őt és olyan hamis weboldalra „irányítja át", ahol kiadja személyes adatait, felhasználónevét, jelszavát. Több vállfaja ismert:
  - hamisított e-mailek és hamisított weboldalak (scam); vishing (VOIP-csalás), vagyis telefonos adathalászat; smishing, amelynek során az adathalász üzenet sms-ben érkezik; pharming, azaz az eltérítéses adathalászat; whaling, vagyis „bálnavadászat", amelyek esetében a célpontok köre a vezetői réteg; nyereményjátékokat, ajándékokat vagy ingyenes szolgáltatásokat hirdető áloldalak.
- kártékony programok: a támadás során olyan rosszindulatú kódok vannak elrejtve az eszközön vagy a fájlon, amelyeknek segítségével megszerezhetik a célszemély vagy egy szervezet adatait, például:
  - keylogger, azaz billentyűzetnaplózó; baiting: fertőzött, kártékony kódokat tartalmazó adathordozó eszköz (pendrive, CD, DVD, SD-kártya) „elvesztése" a kiszemelt szervezetnél vagy annak közelében, amit a gyanútlan és óvatlan alkalmazott csatlakoztat a saját gépéhez, így megfertőzve a saját, sőt jó eséllyel az egész szervezet rendszerét; javítás, frissítés felajánlása; trójai programok; veszélyes csatolmányok.
- Wi-Fi-hálózat veszélyei:
  - A hálózat üzemeltetője képes monitorozni a hálózaton zajló adatforgalmat, így elsősorban a nyílt hozzáférésű Wi-Fi-hálózatok rejtenek magukban veszélyeket, hiszen gyakran adathalász célokat szolgálnak, bár előfordulhat jelszóval védett hálózatok esetében is.
- okostelefon-alkalmazások általi hozzáférés – alkalmazásengedélyekből fakadó kockázatok: az okostelefonra telepített alkalmazások nemcsak a készülék alapvető funkcióihoz, hanem használatukért cserébe egyéb adatokhoz és információkhoz is kérnek és általában kapnak hozzáférést, mint például a felhasználó személyes adataihoz, névjegyeihez, fényképeihez, üzeneteihez.

A social engineering típusú támadás forgatókönyve – bár céljától függően más és más környezetben hajtják végre – általában állandó, és leggyakrabban négy lépésből áll, amelyeket egymásra épülve hajtanak végre. A lépések a következők [9: 52–54.]:

1. információszerzés: tipikusan internetről szerzett információk: közösségi hálózatok, keresőoldalak, a szervezet saját honlapja, telefonon keresztüli vagy írásban történő információszerzés, esetleg személyes felkeresés;
2. kapcsolat kiépítése a cél szempontjából legalkalmasabbnak ítélt és kiválasztott személlyel, aki akár egy vezető is lehet;
3. kapcsolat kihasználása;
4. támadás végrehajtása.

A social engineering típusú támadás alapja a támadás sikeres végrehajtásához szükséges információk megszerzése. Napjainkban az esetek döntő többségében a támadók az internet segítségével, online és elsősorban a közösségi oldalakról (például Facebook,

Twitter, LinkedIn) gyűjtik a szükséges információkat, mivel ezeken az oldalakon kis költséggel, gyorsan, nagy mennyiségű adat érhető el [10: 396.].

A személyre utaló információk megszerzése elősegíti a tökéletes célpont, a leggyengébb láncszem kiválasztását a szervezetnél, akin keresztül majd a támadók sikeresen férhetnek hozzá a kívánt rendszerhez.

„A social engineering típusú támadások sikeres végrehajtása két tényezőn múlik, egyrészt az informatikai eszközök és rendszerek sebezhetőségén, másrészt a felhasználók biztonságtudatossági ismeretein és azok megfelelő alkalmazásán, hiszen ha az alkalmazottak ismerik a lehetséges támadási és védekezési alternatívákat, akkor a különféle bizalmas információk megszerzésére irányuló támadások bekövetkezésének valószínűsége csökkenthető" [11: 269.].

Biztonságtudatosság (security awareness) és a biztonságtudatosító programok

Biztonságtudatosság

A biztonságtudatosságnak, pontosabban az információbiztonság-tudatosságnak (information security awareness) nincs egy általánosan elfogadott fogalma, annak összetevőit több magyar és nemzetközi kutatás is megkísérelte meghatározni.

Egyes szerzők a fogalom egyéni aspektusait hangsúlyozzák, minthogy a biztonságtudatos személy nemcsak a megfelelő szintű tudással rendelkezik az információbiztonság területén, hanem megérti és elfogadja annak jelentőségét, és képes az elsajátított ismereteknek megfelelően cselekedni és viselkedni [12], [13]. Aldawood és Skinner a felhasználó azon képességeit emeli ki, hogy képes felismerni, beazonosítani, elkerülni vagy megbénítani egy rosszindulatú támadási kísérletet [14: 6.].

Nemeslaki András és Sasvári Péter a definíció szervezeti aspektusait emeli ki, mint hogy „az információbiztonság-tudatosság a szervezet kultúrájának része, olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a szervezetek alkalmazottai elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják azokat, és másokkal is megismertetik, illetve betartatják ezeket" [15: 169.]. Bulgurcu és társai úgy határozzák meg az információbiztonság-tudatosságot, mint a munkavállaló általános ismereteinek és attitűdjének halmazát az információrendszerek használatával kapcsolatban úgy, ahogy azt a szervezeti környezetben értelmezik [16: 532.]. Az információbiztonság-tudatosság ebben a vonatkozásban két fő területből áll, egyrészt az általános szintű információbiztonsággal kapcsolatos tájékozottságból, másrészt az információbiztonsági szabályozások és stratégiák ismeretéből [17: 54.].

Az információbiztonság-tudatosság fogalmának alábbi, általános meghatározására teszek javaslatot:

Az információbiztonság-tudatosság a tudás, a képességek és a viselkedés olyan hármasa, amely biztosítja az egyén számára a megfelelő szintű informatikai és információbiztonsági ismereteket, az ezekre épülő és alkalmazásukat biztosító képességeket, valamint e két elemnek megfelelő, belső igényként megjelenő, az információbiztonság jelentőségét elismerő viselkedést.

Információbiztonság-tudatosító programok

A biztonságtudatosság fejlesztése kiemelt feladat az egyéneknél és szervezeteknél egyaránt, amelynek legfontosabb eszköze az információbiztonság-tudatosító programok kialakítása.

Számos nemzetközi informatikai biztonsági szabvány utal a tudatosítási programra, mint a minősítés megszerzésének előfeltételére, úgy mint az ISO 27001, COBIT, vagy az ISO 9001:2000 [12: 6.].

Szabályozás

A kiberbiztonságra vonatkozó magyarországi dokumentumokban, szabályozásban kiemelt figyelmet fordítanak a tudatosítás jelentőségének hangsúlyozására.

A 2013-ban elfogadott *Nemzeti Kiberbiztonsági Stratégia* a kiberbiztonság fogalmi elemeként határozza meg a tudatosságnövelő eszközök folyamatos és tervszerű alkalmazását [18].

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) kimondja, hogy az elektronikus információs rendszerek védelme érdekében a szervezet vezetője köteles gondoskodni „az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról" [19: 11. § (1) g)].

Az Ibtv. hatálya alá tartozó szervek számára a biztonságtudatosság képzésekkel kapcsolatban további feladatokat állapít meg a 41/2015. (VII. 15.) BM rendelet [20: 3.1.7.].

Az információbiztonság-tudatosító programok eredményessége

Számos hazai és külföldi kutatás megerősíti azt a tényt, hogy az alkalmazottak hiába vesznek részt egy tudatosító képzésen, hiába vannak birtokában a szükséges információbiztonsági tudásnak, szándékosan vagy nem szándékosan mellőzik vagy nem veszik figyelembe a biztonsági folyamatokat, előírásokat [17], [21], [22], [5]. Nemeslaki András és Sasvári Péter 2014-ben a magyar üzleti és közszféra információbiztonság-tudatosságát vizsgálta, és arra a megállapításra jutottak, hogy az információbiztonság-tudatosság fejlettnek mondható a közszférában az állami intézményeknél, valamint az állami tulajdonú szervezeteknél, mégis az alkalmazottak kisebb részénél még mindig fejlesztésre szorul [15].

Ezért a legfontosabb, hogy nem elegendő pusztán egy tudatosító programot megszervezni, hatékony és sikeres program szükséges ahhoz, hogy az alkalmazottak viselkedése pozitív irányban változzon.

A szakértők többsége egyetért abban, hogy a hatékonyság azt jelenti, hogy a biztonságtudatosító program képes a résztvevők tudását, attitűdjeit és viselkedését pozitív irányban változtatni az információbiztonság szempontjából, ezáltal csökkentve és megelőzve a szervezetre ható biztonsági fenyegetéseket és kockázatokat [23], [24: 63–64.].

Hogyan fejlesszünk hatékony és sikeres tudatosítási programot?

A következő öt lépésben bemutatom, hogyan lehet egy szervezeti igényekhez igazodó, ugyanakkor a felhasználóknak nemcsak a tudásbővítésre, hanem a képességeik fejlesztésére és viselkedésük megváltoztatására fókuszáló tudatosítási programot kialakítani.

1. A tervezéshez szükséges információk megszerzése:
   - a szervezet jellemzői: köz- vagy magánszféra, milyen típusú adatokat kezel, a szervezet stratégiája milyen hosszú- és rövidtávú célokat fogalmaz meg;
   - az információbiztonság szempontjából a kulcsterületek beazonosítása, ahol a biztonsági problémák jelentkeztek, a fenyegetések, kockázatok és incidensek tipizálása és ezek gyökereinek elemzése, valamint a szükséges helyreállító intézkedések beazonosítása;
   - a szervezet humán jellemzői: hány fős a szervezet, mekkora a fluktuáció; mely munkavállalói körnek szeretnénk a programot szervezni, az érintetti kör kor szerinti összetétele, munkaköreik és biztonságtudatosságuk szintjének meghatározása.
2. Felsővezetői támogatás biztosítása: kutatások igazolják, hogy a támogatás nélkülözhetetlen eleme a sikeres programnak [25].
3. A tudatosító program megtervezése:
   - a célcsoportnak megfelelő tudatosítóanyag összeállítása,
   - a szervezeti és humánpolitikai jellemzőkhöz igazodó módszerek és kommunikációs csatornák kiválasztása, valamint
   - az időzítés megtervezése.
4. A tudatosító program megvalósítása.
5. A program megvalósítása közben és végén a visszacsatolások alapján a program korrekciója.

A program sikeressége és hatékonysága szempontjából a 3. pont, tehát a tudatosító program megtervezése kulcsfontosságú tényező. Ahhoz, hogy a program képes legyen a résztvevők tudását, attitűdjeit és viselkedését megváltoztatni, szükséges, hogy a megfelelő embernek, a megfelelő információt, a megfelelő formában adjuk át.

A célcsoportnak megfelelő tudatosítóanyag összeállítása

A tananyag összeállítása szempontjából nagyon fontos tényező, mondjuk úgy, az „érzékenyítés". Egy szervezeten belül az egyik leggyakoribb probléma a veszélyérzet hiánya, amely a fenyegetettség fel nem ismerésén, valamint a munkatársak biztonsággal és a kapcsolódó védelmi intézkedésekkel való passzív viszonyán alapszik, ami kiegészül a biztonsággal kapcsolatos belső szabályozók nem megfelelő alkalmazásával vagy mellőzésével.

A tananyag összeállítása során a legfontosabb átadandó üzenetre kell koncentrálnunk, arra, hogy bárki áldozattá válhat ebben infokommunikációs technológiák és elektronikus információs rendszerek által átszőtt világban, viszont néhány nagyon

fontos tanács és trükk segítségével időben elkerülhetjük, hogy potenciális célponttá váljunk.

Tehát a program alapvető célja, hogy felhívja a figyelmet a potenciális fenyegetésekre, segítséget nyújtson a támadások időben történő felismeréséhez és elhárításához, valamint összességében hozzásegítse a résztvevőket elsősorban a munkahelyi, ugyanakkor a személyes és az otthoni biztonsághoz is. A cél elérése érdekében egyszerű, rövid, a napi gyakorlatban és a munkavégzés során jól alkalmazható tudást szükséges közvetíteni a résztvevők felé érdekes, újszerű formában.

A szervezeti és humánpolitikai jellemzőkhöz igazodó módszerek és kommunikációs csatornák kiválasztása

Az információbiztonsági tréningeknek számos formája ismert, amelyek különféle kommunikációs eszközökre építenek.

Aldawood és Skinner a tudatosítási programokról írt tanulmányukban, módszereit tekintve különbséget tesznek a tradicionális és a modern social engineering tréning és tudatosító program között. Meglátásuk szerint a hagyományos tréningek eszköztára – a belső vagy külső képzések, tréningek, poszterek, emlékeztetők és az online kurzusok – általában unalmas, fárasztó, nem tartják fenn a figyelmet, túl általánosak, formálisak és a tartalmat túl komoly környezetben közvetítik, valamint a módszerek egyáltalán nem alkalmazkodnak a résztvevők egyéni tanulási képességeihez. Ezek a tréningek egyszerűen csak elmondják a tudnivalókat a támadásokról, ugyanakkor nem mutatnak be valódi, megtörtént eseteket és nem adnak praktikus tanácsokat, hogy hogyan ismerjenek fel, illetve kezeljenek a résztvevők egy ilyen támadást. Tehát a tradicionális formák egyedüli alkalmazása nem biztosítja a megfelelő biztonsági kultúra kialakulását a résztvevőknél.

Ezzel szemben a modern tudatosító programok szimulációs technikákat, interaktív játékokat, virtuális laboratóriumokat, valamint tematikus videókat és modulokat alkalmaznak. A szimulációs technika például segít a social engineering módszerek tudatosításában, az interaktív játékok és virtuális laboratóriumok közreműködésével kipróbálható, hogy egy támadás azonosításától a kárenyhítésig milyen lépcsőkön keresztül vezet az út. Ezek a modern módszerek segítenek az alkalmazottaknak felismerni, hogy vajon egy üzenet támadás-e vagy sem. Ráadásul ezeket a gyakorlatokat az alkalmazottak a munkájuk mellett is egyszerűen elvégezhetik, így nem jelentenek plusz terhet számukra [14: 6–8.].

Szász Antónia és Kiss Gábor tanulmánya a jelszóvisszafejtő programok oktatási célú felhasználásáról alátámasztja a hagyományos és a modern eszközök közötti különbségtételt [26].

A legfrissebb nemzetközi kutatási eredmények mind kiemelik a tudatosítás szempontjából a megfelelő kommunikáció jelentőségét. A SANS Intézet által évente összeállított „Security Awareness Report" már 2017-ben a tudatosítási program sikerességének kritikus pontjaként emelte ki a megfelelő kommunikációt [27].

Ezért is nagyon fontos, hogy beazonosítsuk a célközönséget és igényeit, hogy a megfelelő kontextusban és megfelelő nyelvezettel tudjunk hozzájuk szólni.

E feladat megoldásában segítségül hívom a marketing, a marketingkommunikáció, valamint a PR fogalmát, és megvizsgálom e fogalmak és eszközrendszereik alkalmazási lehetőségeit az információbiztonság területén.

A marketing fogalmát sokan, sokféleképpen definiálták már, mégis a legelfogadottabb és leginkább idézett meghatározását Bauer András és Berács József közölték *Marketing* című könyvükben [28]. Eszerint szűkebb értelemben „a marketing olyan vállalati tevékenység, amely a vevők/felhasználók igényeinek kielégítése érdekében értelmezi a piacot, meghatározza az eladni kívánt termékeket és szolgáltatásokat, megismerteti azokat a fogyasztókkal, kialakítja az árakat, megszervezi az értékesítést és befolyásolja a vásárlókat". Kiterjesztett értelemben azonban „a marketing minden értékkel rendelkező jószág (termék, szolgáltatás, eszme, ötlet, érzés stb.) cseréje. Az üzleti, vállalati szférán túl kiterjed az olyan nem nyereségorientált területekre is, mint például az oktatás, a kultúra, a vallás, a politika stb." [28: 1.1.1., 1.1.3.].

Mint látható, a marketing nem csupán termékek és szolgáltatások, hanem lényegében bármilyen gondolat, eszme, sőt akár személy megismertetését, elfogadtatását és népszerűsítését is szolgálhatja. Ebben az értelemben a biztonságtudatosítás területén is alkalmazható a marketing fogalma, ahol a szervezet a biztonságtudatosság értékét közvetíti a „vevők", azaz az alkalmazottak felé, és sikeres „értékesítés" esetén a munkatársak megfelelő biztonságtudatossága lesz az eredmény.

A marketing egyik legfontosabb eszköze a marketingkommunikáció, ami olyan tervezett cselekvéssorozat, amely a vállalat marketingrendszerébe illeszkedik, célja egy termék (szolgáltatás), márka vagy vállalat (intézmény) megismertetése, népszerűsítése, a fogyasztó figyelmének felkeltése, vásárlásra ösztönzése, illetve érdeklődésének megtartása kommunikáció segítségével [29: 12.]. Az ismertetett célrendszer teljes egészében megfeleltethető a biztonságtudatosítási program céljainak, sőt, a jelenleg alkalmazott programok alapvető célkitűzéseit meg is haladja, amennyiben beépíti új elemként az érdeklődés folyamatos fenntartását kommunikációs eszközök segítségével. Ezért érdemes áttekinteni, hogy a marketingkommunikáció eszközei közül melyik adoptálható és alkalmazható a biztonságtudatosítási programok megvalósítása során.

A marketingkommunikáció eszközei közül van egy kifejezetten olyan terület, amely dedikáltan a vállalaton belüli kommunikációval foglalkozik, ez pedig a belső PR (public relations). „A belső, vagy más néven vállalati PR esetében a vállalat beosztottjai és vezetői között zajlik a kommunikáció, az információáramlás. Ennek az a fő célja, hogy a dolgozók minél jobban megismerjék a cégük (munkahelyük) céljait, azzal tudjanak azonosulni, és azokat a saját maguk által alkalmazható megfelelő eszközökkel tudják elősegíteni" [30: 36.].

A tudatosítási program sikere szempontjából kiemelkedő jelentőséggel bír, hogy a résztvevők el tudják-e fogadni és elismerik-e az információbiztonság szervezeti jelentőségét, képesek-e a magatartásukat, mindennapi tevékenységüket ennek megfelelően alakítani és ezzel a szervezet hosszú távú célját, a biztonságtudatos szervezeti kultúra kialakítását támogatni.

Éppen ezért vizsgáljuk meg, hogy a belső PR eszközei alkalmazhatók-e, és ha igen, milyen formában a biztonságtudatosítási programban.

A könnyebb áttekinthetőség érdekében a belső PR három csoportba sorolt [30: 39–40.], azaz a személyes, a csoportkommunikációs és a tömegkommunikációs eszközei közül

a számunkra releváns elemeket és azok lehetséges alkalmazási területeit az alábbi táblázatban foglaltam össze.

1. táblázat

A belső PR eszközeinek lehetséges alkalmazási területei a biztonságtudatosító programban
[a szerző szerkesztése]

Belső PR eszközei	Biztonságtudatosító program
1. A személyes kommunikáció eszközei	*1. A személyes kommunikáció eszközei*
Párbeszéd, megbeszélés	Az információbiztonsági incidens által érintett vagy érintettek személyes megkeresése, a problémák okának feltárása, megoldási javaslatok közös kidolgozása, visszaellenőrzés.
Előadás	Előadások tartása a felhasználók számára az információbiztonság egy-egy, ugyanakkor mindenkit érintő kérdéséről.
Telefonbeszélgetés	Az információbiztonsági problémával, kérdéssel a szakterülethez fordulók telefonon történő tájékoztatása a teendőkről, a felmerülő kérdések átbeszélése, visszaellenőrzés.
Levelezés, e-mailek	Az információbiztonsági problémával, kérdéssel a szakterülethez fordulók e-mail útján történő tájékoztatása a teendőkről, a felmerülő kérdések átbeszélése, visszaellenőrzés.
Meghívók	Meghívók küldése akár nyomtatva, akár online egy-egy rendezvényre, megbeszélésre, előadásra, amelynek célja a figyelem felkeltése a program iránt.
Oklevelek	Motivációs eszközként, például interaktív játékban történő részvételért, egy incidens kezelésében nyújtott segítő közreműködésért, információbiztonsági kvízek eredményes kitöltéséért.
2. A csoportkommunikáció eszközei	*2. A csoportkommunikáció eszközei*
Konferencia típusú rendezvények [31: 17.]	Például: • **tájékoztatók** egy-egy, a legtöbb munkatársat érintő incidens esetén; • **tematikus konferenciák/fórumok**, például szakértők meghívása social engineering témában; • **értekezletek** egy incidens kapcsán az érintetti körrel; • **képzések, továbbképzések** szervezése például vezetői körnek, átlagfelhasználóknak; • több telephellyel rendelkező szervezetek esetén **road-show** alkalmazása.
Audiovizuális PR-eszközök, mint • Diaképek, írásvetítő fóliák, szemléltetőeszközök • PR-filmek, videók • Multimédia • Számítógépes prezentáció • Computer-animáció	**Audiovizuális eszközöket** szemléltetés céljából nagyon fontos alkalmazni a konferenciatípusú rendezvényeken, de személyes megbeszélések vagy értekezletek alkalmával is, akár prezentáció, akár képek, videóanyagok vagy egyéb eszközök formájában. A **PR-filmek és -videók** nemcsak konferenciatípusú rendezvényen alkalmazhatók, hanem például az intraneten is közzé lehet tenni, vagy körlevélben elküldeni. Ezek a figyelemfelhívó videók általában 1-5 perc hosszú, dramatizált filmanyagok, amelyek egy biztonsági kockázatot vagy annak helyes kezelését mutatják be [32], vagy például a saferinternet.hu weboldalon számos a gyermekeknek, fiataloknak és szülőknek, pedagógusoknak szóló videó található [33].

Belső PR eszközei	Biztonságtudatosító program
Hagyományos nyomtatványok	Bár egyre kevésbé használatos, de még mindig találkozhatunk a hagyományos nyomtatványokkal, mint például • a **vállalati/szervezeti újság**, amelybe egy-egy az információbiztonsággal kapcsolatos érdekesség, fontos hír is helyet kaphat, • konferencia, szakmai fórum **meghívók,** • **tájékoztató kiadványok** az információbiztonság egy-egy kérdéséről, • **szervezeti éves/féléves/negyedéves beszámolóban** az információbiztonságot érintő statisztikák, tapasztalatok bemutatása, • faliújságon figyelemfelkeltő **poszterek, plakátok** elhelyezése, vagy egy-egy **program hirdetése.**
Hírlevelek, (News Release)	**Hírlevelek**, vagy **professzionálisan megírt cikkek nyomtatott vagy online verzióban.** Lényege, hogy könnyen áttekinthető és könnyen olvasható legyen. Hírlevél keretében tájékoztatni tudjuk a munkatársakat **egy rendkívüli esemény kiértékelését követően a következtetésekről.**
Aktuális cikkajánlások	**Magyar vagy a nemzetközi sajtóból egy-egy érdekes cikk** ajánlása tipikusan online formában.
Faliújságok, hirdetések	A **belső intranethálózaton** figyelemfelkeltő **poszterek** elhelyezése, egy-egy program **hirdetése**, vagy **tudatosító kiadványok** népszerűsítése, **tájékoztató honlapok** elérési útvonalának megosztása (például EU, ENISA aktuális döntései, kiadványai).
3. A tömegkommunikáció eszközei	*3. A tömegkommunikáció eszközei*
Online magazinok, portáloldalak	Körlevélben vagy az intraneten érdemes megosztani azon oldalak elérhetőségét, amelyek naprakész információkat, figyelemfelhívó módon, röviden összefoglalva osztanak meg az érdeklődőkkel (például a Nemzeti Kibervédelmi Intézet hírlevele [34]).
Online kapcsolatok: fórum, hírlevél, levelezőlista	**Internetes csevegőfórumok, közösségi felületek**

Az internetes csevegőfórumok, közösségi felületek kapcsán külön szeretnék kitérni néhány mondat erejéig a Nemzeti Közszolgálati Egyetem (NKE) várhatóan 2019 decemberében induló pilot programjára. Az NKE által üzemeltetett Továbbképzési és Vizsgaportálon, az úgynevezett Probono oldalon egy olyan információbiztonság-tudatosító tesztcsatornát fejlesztettek ki, amely egy Facebookhoz hasonló közösségi oldal, amelynek célja, hogy egyszerű, rövid, a napi gyakorlatban és a munkavégzés során jól alkalmazható tudást közvetítsen az érdeklődők felé érdekes, újszerű formában. Három, az IT és információbiztonság terén jártas szakértő közreműködésével a hét minden napján új tartalommal jelentkezik a portál hol hosszabb, tartalmasabb cikkek, hol pedig rövidebb bejegyzések, képek/poszterek, a nemzetközi, illetve a magyar sajtóban megjelent, általuk kommentált hírek formájában.

A csatornára feliratkozóknak lehetőségük van hozzászólni a közzétett bejegyzésekhez, kérdezni és segítséget kérni a szakértőktől, vagy esetleg egy általuk fontosnak tartott témát javasolni későbbi feldolgozásra.

A csatorna jelenleg tesztelés alatt áll, de reményeink szerint az információbiztonság-tudatosítás egy teljesen újszerű és minden eddiginél hatékonyabb, a résztvevők saját belső motivációjára építő önfejlesztési formát biztosít a közszolgálatban dolgozóknak.

A táblázatban felsorolt eszközök, módszerek kiválóan alkalmazhatók a tudatosítási programok megvalósítása során, sőt, egy részüket jelenleg is alkalmazzák a szervezetek, ugyan nem tudatosan és kimondottan marketingkommunikációs eszközként.

Az összehasonlítással azonosítottam azokat a belső PR-eszközöket, amelyek adaptálhatók egy tudatosítási programba, és meghatároztam az adott eszközök alkalmazási területeit és formáit is, példákkal alátámasztva. Célom egy olyan módszertani gyűjtemény létrehozása volt, amelynek segítségével egyrészt hatékonyabban tudja a vezetés az információbiztonság értékét eljuttatni a munkatársakhoz, másrészt a szervezetek – figyelembe véve a sajátosságaikat, a célcsoportot és az átadni kívánt ismereteket –, össze tudnak állítani egy hatékony tudatosítási programot.

Tehát a felsorolt eszközök csupán egy összefoglalása az alkalmazható módszerek sokszínűségének, minden szervezetnek magának kell az eszközök megfelelő kombinációjával biztosítania a tudatosítási programjuk sikerességét.

3.3. Az időzítés megtervezése

Nagyon fontos, hogy a tudatosítási program keretében a munkavállalók ne csak egyetlen egyszer találkozzanak az információbiztonsággal, például egy hagyományos frontális képzés keretében, amikor belépnek a szervezethez, hanem gondosan megtervezett tudatosító program keretében, meghatározott időközönként valamilyen formában találkozzanak az információbiztonsággal. Ahogy a mondás is tartja, „ismétlés a tudás anyja." A tapasztalatok azt mutatják, hogy ha abbahagyjuk a tanulást, akkor a megszerzett ismeretanyag és tudás szintje exponenciálisan elkezd csökkenni, éppen ezért nagyon fontos az élethosszig tartó tanulás. Minél többet olvasunk és tanulunk, minél nagyobb a tudásunk, annál nagyobb eséllyel hívjuk elő az adott helyzetben szükséges információkat. És ez igaz az információbiztonság-tudatosító programokra is. Egyrészt ezért is nagyon fontos, hogy rendszeresen közvetítsünk új és ismételt információkat, illetve tudásanyagot a munkatársak felé, másrészt azért is, mert a támadók folyamatosan újabb és újabb típusú támadás megvalósításán kísérleteznek, ezért nagyon fontos az információbiztonsággal kapcsolatos ismeretek naprakészen tartása.

Következtetések

A közigazgatás digitális átalakításának, az e-közigazgatás megteremtésének köszönhetően, mára már a nemzeti adatvagyon jelentős részét elektronikus információs rendszerekben tárolják, amelyeket az arra kötelezett szervek a legmodernebb fizikai és logikai védelmi intézkedésekkel és technológiai megoldásokkal védik az illetéktelen személyekkel és a lehetséges támadásokkal szemben. Éppen ezért a támadók azt a pontját támadják egy rendszernek, amely a leggyengébbnek bizonyul, ez pedig nem más, mint az ember. Bárhogy is védjük rendszereinket, mind hiábavaló, ha munkatársaink figyelmetlenségből, hanyagságból vagy netán rosszindulatból, vagy egyszerűen csak az alapvető informatikai és elektronikus információbiztonsági ismeretek hiányából

fakadóan nem tudnak, vagy nem akarnak biztonságtudatosan és felelősségteljesen viselkedni rendszereik és eszközeik (például okostelefon, pendrive) használatakor.

A hatékony és eredményes kiberbiztonság és a biztonságtudatos szervezeti kultúra megteremtésének az egyik legfontosabb eleme a közszférában dolgozók megfelelő felkészültsége, a biztonságtudatosság, aminek kialakításához sikeres és hatékony biztonságtudatosítási program megszervezése és folyamatos fenntartása, menedzselése szükséges.

Tanulmányommal segítséget kívánok nyújtani egy olyan tudatosítási program kidolgozásához, amely képes a felhasználók biztonságtudatosságát növelni. Ennek érdekében megvizsgáltam a biztonságtudatosság fogalmi összetevőit és megállapítottam, hogy ez nemcsak az informatikai és információbiztonsági ismeretekre épül, hanem nélkülözhetetlen elemei a fenyegetések korai felismerését és a reagálást biztosító képességek és az információbiztonság jelentőségét hangsúlyozó magatartás is. E három fontos területet fejlesztő tudatosítási program kidolgozása érdekében tanulmányoztam a programok lényegi elemeit, a cél- és eszközrendszerét vizsgáló nemzetközi kutatásokat, és arra a következtetésre jutottam, hogy csak akkor biztosítható a sikeresség, ha beazonosítjuk a program célcsoportját és annak biztonságtudatossági szintjét (Kinek?), specifikusan meghatározzuk a nekik megfelelő ismereteket (Mit?), és ezeket a célcsoporthoz, valamint a szervezethez illeszkedő kommunikációs csatornák és eszközök segítségével közvetítjük feléjük (Hogyan?). A megfelelő közvetítő közeg biztosítása érdekében megvizsgáltam, hogy a marketingkommunikáció és azon belül a belső PR fogalma és eszközrendszere alkalmazható-e a biztonságtudatossági programra. Arra a megállapításra jutottam, hogy a belső PR-nak számos olyan személyes, csoportos és tömegkommunikációs eszköze, módszere van, amely sikeresen alkalmazható a tudatosítási programok során, sőt, néhányat már a szervezetek alkalmaznak is.

Tanulmányom legfontosabb következtetése, hogy a tudatosítási programok tekintetében nem határozható meg egy minden szervezetre érvényes megoldási javaslat, amely hatékonysághoz és sikerességhez vezet, minden szervezetnek a maga sajátosságaihoz és igényeihez igazodó, valamint változatos kommunikációs csatornákat és eszközöket alkalmazó tudatosítási programot kell kidolgoznia és megvalósítania.

Hivatkozások

[1] „A Digitális Jólét Program 2.0," *digitalisjoletprogram.hu,* 2017. július. [Online]. Elérhető: https://digitalisjoletprogram.hu/files/57/1c/571c60381c274901733f8a2fc8a1cca5.pdf (Letöltve: 2019. 10. 27.)

[2] Cs. Krasznay, „A polgárok védelme egy kiberkonfliktusban," *Hadmérnök,* 7. évf. 4. sz., pp. 142–151., 2012.

[3] NTT Security, "Global Threat Intelligence Report." *NTT Security,* 2019, [Online]. Elérhető: www.nttsecurity.com/docs/librariesprovider3/resources/2019-gtir/2019_gtir_report_2019_uea_v2.pdf (Letöltve: 2019. 11. 15.)

[4] A. Beláz, „A közigazgatás információbiztonsága: megjósolhatók az incidensek?," *Hadtudomány: A magyar Hadtudományi Társaság folyóirata,* 29. évf. 3. sz., pp. 92–104., 2019. DOI: https://doi.org/10.17047/HADTUD.2019.29.3.92
[5] I. Legárdné Nagy, A biztonságos számítógép-használat jogi és szabályozási háttere – Az elektronikus információbiztonság-tudatosság és tudatosítás jelenlegi helyzete, lehetőségei és kihívásai a közszolgálatban, Diplomamunka, Nemzeti Közszolgálati Egyetem, Budapest, 2018.
[6] V. Deák, „A social engineering humán alapú támadási technikái," *Biztonságpolitika.hu,* p. 11, 2017. április 10.
[7] P. Bányász, „Social engineering and social media," *Nemzetbiztonsági Szemle,* 6. évf. 1. sz., pp. 59–77., 2018.
[8] V. Deák, „A számítógép alapú social engineer támadási technikák," *Biztonságpolitika.hu,* 2017. április 28.
[9] L. Muha és Cs. Krasznay, *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, 2014.
[10] V. Deák, „A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során," *Hadmérnök,* 13. évf. *3. sz.,* pp. 391–402., 2018.
[11] V. Deák, „Kártékony programok terjedése social engineering technikákon keresztül," *Hadmérnök,* 14. évf. 2. sz., pp. 256–271., 2019.
[12] I. Veseli, *Measuring the Effectiveness of Information Security Awereness Program.* M. S. thesis, Gjøvik University College, Gjøvik, 2011, p. 87.
[13] R. S. Shaw, C. C. Chen, A. L. Harris and H.-J. Huang, "The impact of information richness on information security awareness training effectiveness," *Computers & Education,* vol. 52, no. 1, pp. 92–100, Jan. 2009. DOI: https://doi.org/10.1016/j.compedu.2008.06.011
[14] H. Aldawood and G. Skinner, "Reviewing Cyber Security Social Engineering Training and Awareness Programs – Pitfalls and Ongoing Issues," *Future Internet,* vol. 11, no. 3. p. 73, 2019. DOI: https://doi.org/10.3390/fi11030073
[15] A. Nemeslaki és P. Sasvári, „Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában," *Infokommunikáció és Jog,* 60. sz., pp. 169–177., 2014.
[16] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "2010: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly,* vol. 34, no. 3, pp. 523–548, 2010. DOI: https://doi.org/10.2307/25750690
[17] M. Illésy, A. Nemeslaki és Z. Som, „Elektronikus információbiztonság-tudatosság a magyar közigazgatásban," *Információs Társadalom,* 14. évf. 1. sz., pp. 52–73., 2014.
[18] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
[19] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
[20] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott techno-

lógiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
[21] L. Nagy, „Az informatikai kultúra – különös tekintettel a felhasználói tudatosságra – a Magyar Honvédség szervezetében a generációk viszonyrendszerében," *Hadtudományi Szemle,* 8. évf. 4. sz., pp. 393–431., 2015.
[22] A. Schüller, „Az Y generáció és az információbiztonság," *Hadmérnök,* 6. évf. 2. sz., pp. 339–347., 2011.
[23] M. Bada, A. M. Sasse and J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," Jan. 2015. [Online]. Elérhető: https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf (Letöltve: 2019. 10. 29.)
[24] A. N. W Prah, A. A. Otchere and K. E. Opan, "The perceived effectiveness of information security awareness," *Information and Knowledge Management,* vol. 6, no. 7, p. 62, 2016.
[25] Cs. Kollár, „Az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében coaching és tanácsadás módszerével," *Magyar Coachszemle,* 5. évf. 3. sz., pp. 35–50., 2016.
[26] A. Szász és G. Kiss, „Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra," *Információs Társadalom,* 18. évf. 3–4. sz., pp. 82–104., 2018. DOI: https://doi.org/10.22503/inftars.XVIII.2018.3-4.4
[27] „Security Awareness Report," *naganresearchgroup.com,* 2017, [Online]. Elérhető: www.naganresearchgroup.com/SANSSAR2017.pdf (Letöltve: 2019. 11. 02.)
[28] A. Bauer és J. Berács, *Marketing.* Budapest: Akadémia Kiadó, 2016. DOI: https://doi.org/10.1556/9789634540076
[29] I. Fazekas és D. Harsányi, *Marketingkommunikáció érthetően.* Budapest: Szókratész Külgazdasági Akadémia, 2011.
[30] E. Lendvai és J. Gál, *Marketingkommunikáció 1.* Budapest: TÁMOP-4.1.2-08/1/A, Új Magyarország Fejlesztési Terv, 2011. [Online]. Elérhető: https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0034_marketingkomm_1/adatok.html (Letöltve: 2019. 10. 28.)
[31] H. Csáfor, *Vállalatok külső és belső kommunikációja (PR).* Eger: Eszterházy Károly Főiskola, 2012.
[32] Youtube, „60 másodperc biztonság – Az internet veszélyei," *Youtube,* [Online]. Elérhető: www.youtube.com/watch?v=ISPAFbkh424. (Letöltve: 2019. 11. 03.)
[33] Safer internet, „Biztonságosabb internet pedagógusoknak," *Safer internet,* [Online]. Elérhető: http://saferinternet.hu/tippek-videok/szuloknek-pedagogusoknak (Letöltve: 2019. 11. 03.)
[34] „eGov hírlevél," [Online]. Elérhető: https://hirlevel.egov.hu/tag/nemzeti-kibervedelmi-intezet/ (Letöltve: 2019. 11. 03.)

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

15. évfolyam (2020) 1. szám 107–119.
DOI: 10.32567/hm.2020.1.8

Tímár Attila[1]

Árvízvédelmi töltések potenciális veszélyforrásai a Körösök vidékén

Potential Sources of Danger of Flood Protection Dams in the Körös River Area

Az árvízvédekezések óta az árvízvédelmi rendszerek fejlesztése mellett a védekezési módszerek is állandó fejlődésen mentek át. A fejlődés a védekezés szinte minden területére kiterjedt a kor technikai színvonalához alkalmazkodva. A védekezési rendszer kiépítése óta a védekezések legnagyobb veszélyforrásai az árvízi jelenségek, amelyek ellen a védekezés alapeszköze még mindig a homokzsák. Ezen jelenségek elleni védekezés mindig reflektorfénybe helyezi egy időre a védekezés fokát és a töltések szerkezeti állapotának kérdését. A publikáció célja az olvasó számára bemutatni a Körösök vidékén lévő árvízvédelmi rendszerek fejlődésének történetét, valamint világos képet mutatni a veszélyforrások kialakulásának okaira.

Kulcsszavak: árvíz, árvízvédelem, árvízvédekezés, árvízvédelmi töltés, jelenségek, holt meder

Since flood protection has been practiced, in addition to the development of flood protection systems the methods of flood protection underwent constant development. The development covered almost all areas of flood protection and adapted to the technical standard of the age. Since the development of the flood protection system, the biggest sources of danger are flood phenomena, against which the basic means of protection are still sandbags. The protection against these phenomena calls attention to the seriousness of flood protection and the question of the structural condition of the dykes for a while. The aim of this paper is to present the development history of the flood protection systems in the Körös river area as well as to give a clear description about the reasons for the emergence of safety hazards.

[1] Körös-vidéki Vízügyi Igazgatóság, Vízrajzi Monitoring Osztály, csoportirányító, e-mail: timar.attila@kovizig.hu, ORCID: https://orcid.org/0000-0001-8637-4887

Keywords: **flood, flood control, flood protection, flood protection dam, flood phenomena, cut-off channel**

Bevezetés

Az éghajlatváltozás egyik következménye a csapadékeloszlás intenzitásának változása. Ez egyúttal azt is jelenti, hogy az árvizek kialakulásának a veszélye fokozottan jelentkezik a Kárpát-medencében. Így nem lehet kérdéses az, hogy hazánkban minden olyan szervezetnek és szervnek kiemelt feladata az árvízvédekezésben való részvétel, amely rendelkezik különleges eszközökkel vagy különleges felkészültségű szakemberekkel. A Magyar Honvédség az egyik meghatározó szereplője ennek a rendszernek, így a haditudományi és katonai műszaki kutatásoknak kiemelt figyelmet kell fordítania erre a területre. A kérdéssel foglalkozó szakemberek közül érdemes megemlíteni Pataky Iván nevét, aki elsőként vizsgálta a honvédség alkalmazásának lehetőségeit ezen a területen, az 1990-es évek elején [1]. Padányi József mind kandidátusi (1994) [2], mind MTA-doktori munkájában (2007) [3] kiemelt feladatként kezelte a kérdést. Védelmi igazgatási szempontból Hornyacsek Júlia kutatásait kell említenünk [4], de Földi László munkássága is meghatározó ezen a területen [5].

Az árvízi védekezés kritikus pontja az árvízvédelmi töltések védelme. A töltéseken történő védekezés elsősorban a magassági hiány pótlásával történik, de tartós árvizek esetén a legnagyobb problémát – a magassági hiány után – az árvízvédelmi jelenségek okozzák. Ezek azok a munkálatok, amelyekkel egy tartós árvíz vagy esetleg egy nem megfelelő (szerkezetű) töltésnél kialakuló jelenségek ellen kell fellépni. Az árvízvédelmi töltések egyik legfontosabb tulajdonsága az állékonyság, amelyet nagymértékben befolyásol a töltések vízzel való áztatása. Az áztatóhatás következtében különböző árvizes jelenségek, szivárgások jelentkeznek, amelyek nagymértékben gyengítik az árvízvédelmi töltések állékonyságát.

Dél-Alföld mint a síkvidéki vízgazdálkodás bölcsője

Magyarország a Kárpát-medence legalacsonyabb területe, így ezeknek a topográfiai adottságoknak és az éghajlati viszonyoknak köszönhetően a Duna vízgyűjtőjére lehullott csapadékok ide folynak le. Ezek a tényezők tették Közép-Európán belül Magyarországot mind felszíni, mind felszín alatti vízkészletekben egyedülállóan gazdag térséggé, ugyanakkor e sajátosságok okozták, hogy a 19. századig az ország mai területének 30%-a állandó vízjárta vidék volt.

A 19–20. század során ezeket a vízjárta területeket az akkori polgári fejlődési igényeknek megfelelően lecsapolták, és igyekeztek minél gyorsabban árvízmentesíteni [6].

Az árvízvédekezés és ármentesítés esetén illendő megemlíteni a Dél-Alföldet mint a síkvidék vízgazdálkodás bölcsőjét, ahol a 19–20. században számos jelentős árvíz pusztított, és e pusztítások, valamint a térség igen jó termőföldi adottságai hozzájárultak a vízrendezések mihamarabbi elvégzéséhez.

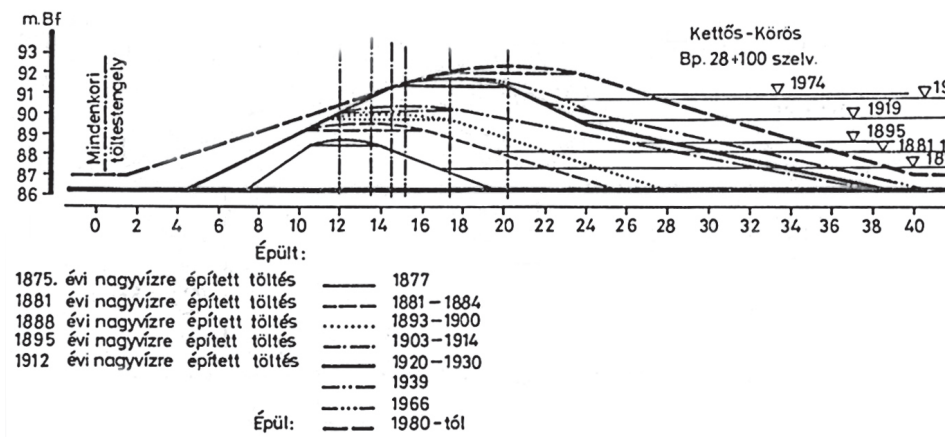
A Körös-vidék ármentesítésének fejlődése

A vidék alföldi területeinek ármentesítése volt hazánkban az első, amelynél a mederrendezések és azokhoz szorosan kapcsolódó töltésépítési munkák már részletes magassági adatokat is tartalmazó felvétel alapján indultak el. A javaslat és tervek fő célkitűzése a Körösök árvizeinek leérkezésének meggyorsítása úgy, hogy azok a Csongrád alatti Tisza-szakaszon még a Tisza árvizeinek odaérkezése előtt levonuljanak. Ennek érdekében a folyókon a mederhosszakat jelentős számú átvágással rövidítették le, esésüket növelték, az árvizek levonulási idejét csökkentették, de a szűkre szabott hullámtérrel az árvizek levonási szintjét jelentősen emelték [7].

Ármentesítés, árvízvédelmi rendszer

A korábban lecsapolt folyóktól elhódított területeket, amelyek az idő elteltével mezőgazdasági területekké váltak, időnként a folyók vízjátékából adódóan egy-egy árvizes időszakban ismét elöntötte a víz. Ezen területek ármentesítésének biztosítása érdekében a folyókkal párhuzamosan gátakat emeltek, hogy az elöntéseket töltésekkel gátolják.

A gátak építésével a folyók lefolyási és esésviszonyai megváltoztak, vízjátékuk megnövekedett, így az újabban kialakuló árvizek gát között tartását a gátak magassági, valamint keresztmetszeti növelésével tudták megoldani, az 1. ábrán látható módon.

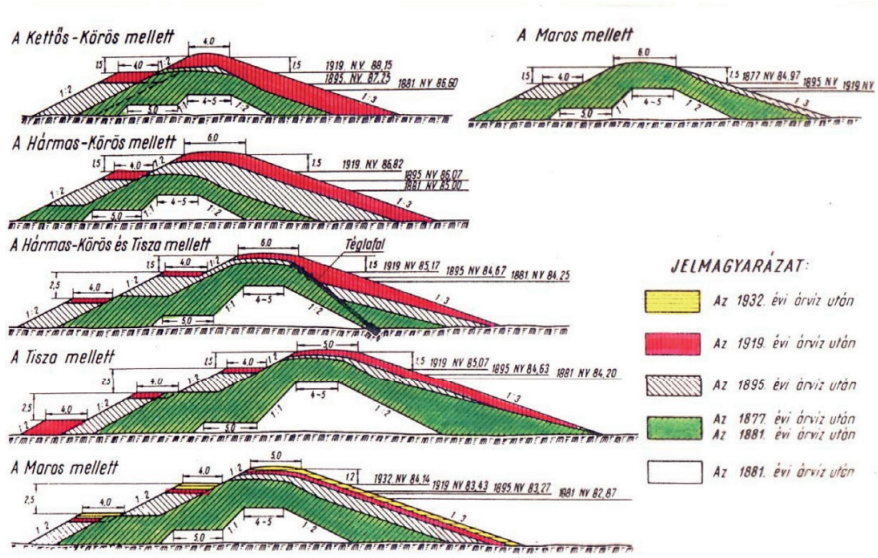


1. ábra

Az árvízvédelmi töltések kiépítésének szakaszai a Kettős-Körösön [8]

Ezekben az időkben a gátak építésénél még nem használtak modern elgondolásokat, elveket, a talajmechanika jelenlegi módszereit. A gátak méreteit legtöbbször tapasztalati úton állapították meg, és ezek a gátak szolgáltak példaként az árvizek elleni védekezésben. A fejlődést követően az árvizek biztonságos levonulása érdekében a töltések

szabályozása, magasítása történt egymásra halmozás során. Az így kialakult töltéseket inhomogén, „hagymaszerkezetű" töltésekké építették át, amit a 2. ábra szemléltet.



2. ábra

Az árvízvédelmi töltések fejlesztése [9]

A töltések akkori fejlesztéseinek építési metszeteit tanulmányozva megállapítható, hogy a töltések keresztmetszetét nemcsak a mentett oldal irányába, hanem a vízoldal irányába is növelték. Ezzel az építéssel sajnálatos módon hozzájárultak a hullámtér területének csökkentéséhez, amellyel, mint tudjuk az árvizek levonási szintjét emelték.

Feltételezhetőleg a mezőgazdasági területek megóvása vezethetett ehhez az építési megoldáshoz, amely akkoriban elfogadhatóbb volt mint jelenleg. Természetesen a települések közelsége (például Békés, Gyomaendrőd) is befolyásolta a töltések fejlesztési lehetőségeit.

A gátak magasításával párhuzamosan az akkori folyószabályozási munkálatok részét képezte a folyókanyarulatok átvágása, illetve egy-egy új meder ásása is ahová a folyót átterelték, ezzel is növelve a termőterületek nagyságát, valamint biztosítva az élet és gazdálkodás biztonságát a gyorsabb vízlevezetéssel. Ezeket a munkákat szemlélteti a 3. ábra, ami a Gyula város környéki munkálatokat ábrázolja a Magyar Királyság (1819–1869) – Második katonai felmérés térképén.

3. ábra

Gyula város környékének folyószabályozási munkái [10]

E munkálatok nem csupán az átvágások megfelelő szelvényű kiépítését jelentette, hanem ezzel párhuzamosan a mederrendezési, fenntartási és partvédelmi munkákat is, ahol a feladatok körébe tartozott a nagyvízi szabályozás (átvágások anyamederré fejlesztése és a töltések vonalazásának javítása), a középvízi szabályozás (mederelfajulás és medervándorlás megakadályozása) és a kisvízi szabályozás (hajózás érdekében történő munkálatok) [11].

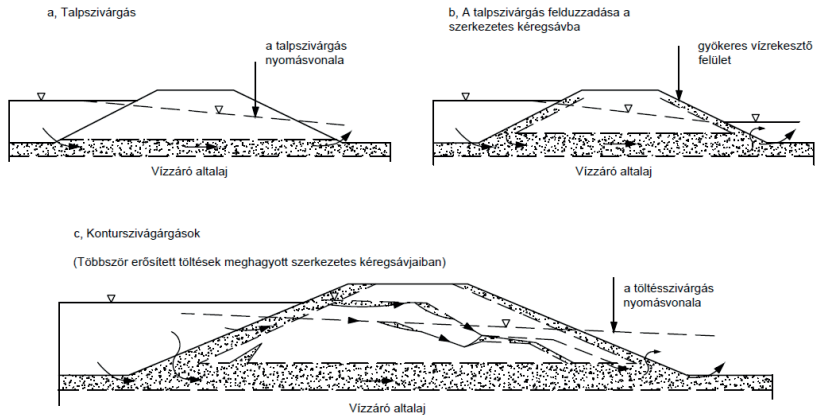
A Körös-völgyének árvízvédelmi kiépítését a fent említett folyószabályozási munkálatok határozták meg a 18. századtól és műtárgyaival biztosították a jelenlegi védekezés alapjait.

E kiépített védelmi rendszer fontosságát és méreteit igazolja az a tény, hogy a Körösök rendszerét alkotó vízfolyások igen heves vízjárásúak, valamint a vízgyűjtőt érő jelentősebb csapadékot követően 28-36 órán belül a Körösök magyarországi határszelvényeinél 8-10 méteres vízszintemelkedést is okozhatnak. Továbbá a kialakuló árvizek tartósságát tekintve a folyók felső szakaszain 5-10 néha 20 napig, az alsó szakaszon zömmel 10-30, nem ritkán 40 napig, de szélsőséges esetben 60-70 napig áztatja az árvíz a töltéseket [12].

Árvizes jelenségek kialakulása

A Körösök árvízvédelmi töltései kivétel nélkül anyagárokból, a kötött fedőrétegek anyagának válogatás nélküli felhasználásával épültek. Továbbá ugyanígy történtek a töltések többszörös megerősítései is. Ebből az építési eljárásból következik, hogy a töltések belseje majdnem kivétel nélkül heterogén.

Az árvizek alatt végzett vizsgálatok szerint a töltések heterogenitása a szivárgások szempontjából három formában jelentkezhet: szerkezetes „talprétegként", áteresztő „kontúrsávok" és áteresztő „járatok" formájában, a 4. ábrán látható módon.



4. ábra

Az árvízvédelmi töltések fejlesztése [13: 50.]

A növényzettel benőtt területeken a fedőréteg felső része hasonló módon, mint a töltésrézsűk szerkezetes kéregsávja, gyökérnyomos, féregjáratos és morzsalékos szerkezetű, tehát erősen áteresztő még akkor is, ha a réteg anyaga önmagában vízzáró.

A töltések építésénél és erősítésénél ez a szerkezetes áteresztőréteg kisebb-nagyobb vastagságban rendszerint a töltés alatt maradt. Ennek anyagát építették be a töltésbe az anyagárok felső részéből is, és foltokban vagy lencsékben ilyen anyagok maradtak a töltéserősítéseknél az új töltésrész alatt. Árvízkor tehát ebben a „szerkezetes talpsávban" jelentős mértékű talpszivárgások, a töltés belsejében megmaradt szerkezetes „kontúrsávokban" pedig kontúrszivárgások tudnak kialakulni még akkor is, ha az altalaj fedőrétege és a töltés anyaga különben vízzáró.

A fedőréteg anyagából épült töltésekben változik az anyagok kötöttsége és változik természetesen a beépítés tömörsége is. Ezek a minőség- és tömörségváltozások pedig azt jelentik, hogy árvízkor a töltésben az egyik anyag gyorsabban, a másik lassabban, az egyik gyengébben, a másik erősebben duzzad. Az árvíz utáni kiszáradáskor pedig az egyik anyag már zsugorodni kezd, amikor a másik még megtartja megduzzadt térfogatát. A töltésben tehát már az első árvízi telítődés és az utána következő kiszáradás hatására anyagsűrűsödéseknek és lazulásoknak kell bekövetkeznie, másodlagos hézagoknak, hajszálrepedéseknek kell kialakulnia. A következő árvizeknél természetesen a telítődés folyamatát és a duzzadások mértékét már ezek a másodlagos jelenségek is erősen befolyásolják, tovább növelik a töltés belsejének feldarabolódását és ezzel a töltés áteresztőképességét is. Akkor pedig, ha a töltésben valamilyen formában már határozottabb keresztszivárgások is ki tudnak alakulni, megindulhat a kilúgozódás és ezzel az egyes részek morzsalékos szerkezettűvé alakulása is. A töltés belseje tehát „járatossá" alakulhat, elöregedhet [13: 49–50.].

A töltés és az altalajszivárgások – leszámítva a fakadó vizek esetleges károkozásait – önmagukban még nem feltétlenül káros jelenségek. Akármilyen foltokban vagy

már összefüggő felületeken jelentkező ázalgás vagy szivárgás, csurgás jelentkezik is tehát a rézsün, vagy felületi nedvesedés, szivárgás a biztonsági sávon, azok csak akkor veszélyeztethetik a védvonal állékonyságát, ha a töltésben vagy az altalajban olyan talajmechanikai folyamatokat indítanak meg, amelyek a védvonal átszakadásához vezethetnek. A védvonalak állékonyságát és az árvízvédelmi beavatkozások, esetleg a védvonalak későbbi megerősítésének a szükségességét tehát nem a szivárgások, hanem minden esetben a szivárgások várható következményei alapján kell megítélni.

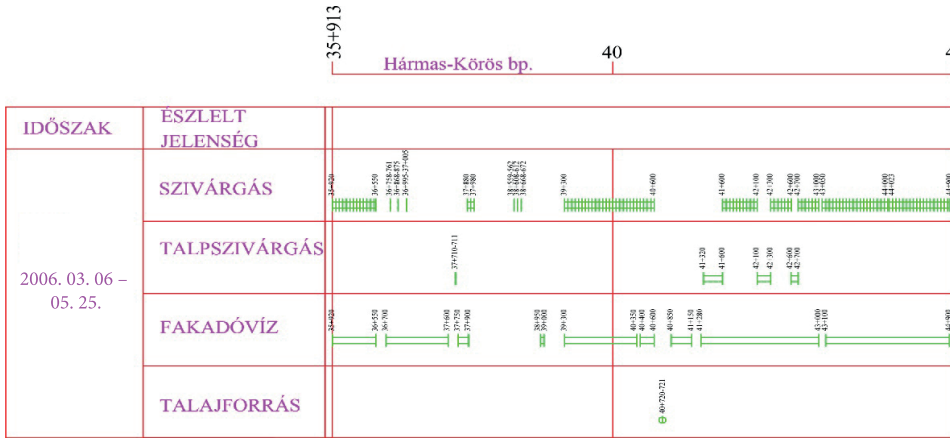
A töltés és az altalajszivárgásoknak három következménye befolyásolhatja károsan a védvonalak állékonyságát, a talajok szilárdságának telítődés miatti csökkenése, a szivárgási nyomás és a felhajtóerő [13: 59.].

5. ábra

Védekezés a Hármas-Körös fűzfászugi rámpájánál szivárgás ellen [14]

Az árvíz idején az állékonyságot veszélyeztető káros jelenségeket a 10/1997 KHVM rendeletben előírtaknak megfelelően jelzőzászlóval kell megjelölni. Ha a jelenség fokozott megfigyelést igényel, akkor sárga, ha azonnali beavatkozást igényel, akkor piros zászlóval kell ellátni az észlelt jelenség helyét.

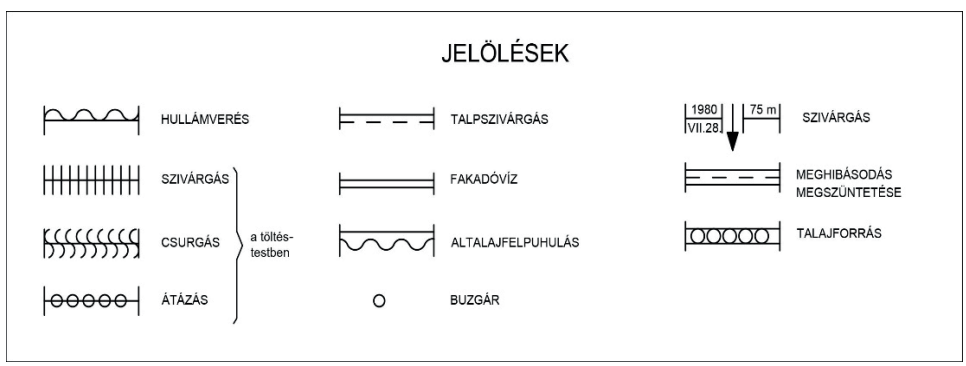
Az észlelt jelenségek minden árvíz után az aktualizált árvízvédelmi tervbe nyilvántartásba kerülnek, a vízfolyás szelvényszámával és az észlelés időpontjával a 6. ábrán látható módon.



6. ábra

Metszet a 12. 01 árvízvédelmi terv észlelt jelenségeiből [15]

Az észlelt jelenségeket megkülönböztetés céljából a 7. ábrán látható jelzésekkel ábrázolják.



7. ábra

Észlelt árvízvédelmi jelenségek ábrázolásának jelei [16]

Holtmeder-keresztezések

Az árvízvédelmi töltések holtmeder-keresztezésére irányuló kutatások az 1980. évi Körös-völgyében történt hosszúfoki töltésszakadást (8. ábra) követően kezdődtek el az árvízvédelmi töltések védőképességének fokozása érdekében.

8. ábra
Kettős-Körös hosszúfoki töltésszakadás légi felvétele, 1980 [16]

A holt medrek keresztezése országos program keretén belül 1983-ra a Körösök fővédvonalait teljes egészében felderítették. A felderítést követően a Körös-vidéki Vízügyi Igazgatóság területén 423 darab holtmeder-keresztezést lokalizáltak. Példaként a holt meder kereszteződését a 9. ábra szemlélteti a Magyar Királyság (1819–1869) Második katonai felmérés és a Google műholdképének 50–50%-os egymásra halmozott térképe alapján.

9. ábra
A Sebes-Körös és holtmeder-keresztezéseinek egymásra halmozott térképe [17]

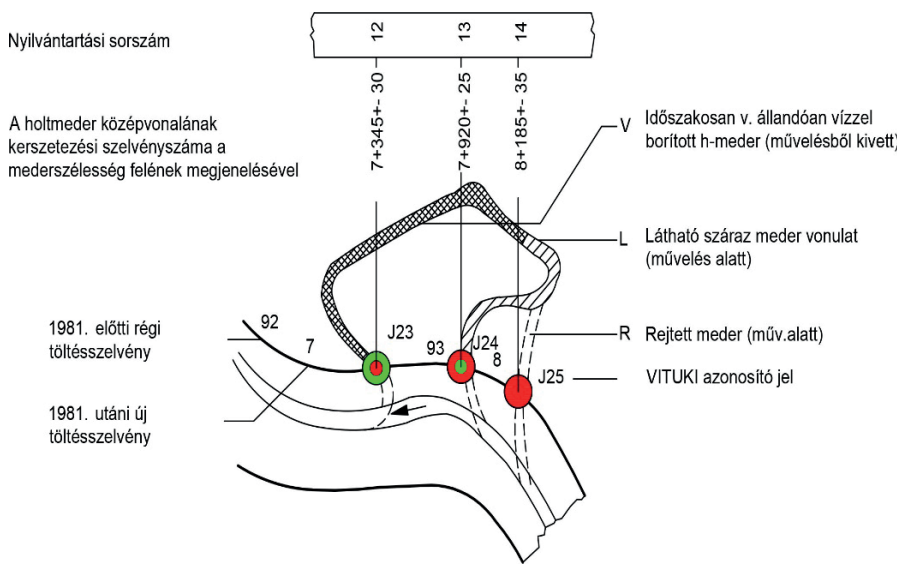
A holt medrek keresztezési helyeinek lokalizálására és rendszerezésére, különböző évszakokban készült légi fotókat készítettek, valamint topográfiai térképeket használtak fel.

A mezőgazdasági területeken a vegetációs időszakon kívül, valamint csapadékosabb időjárások során lokalizálhatóbbak voltak a holt medrek helyei.

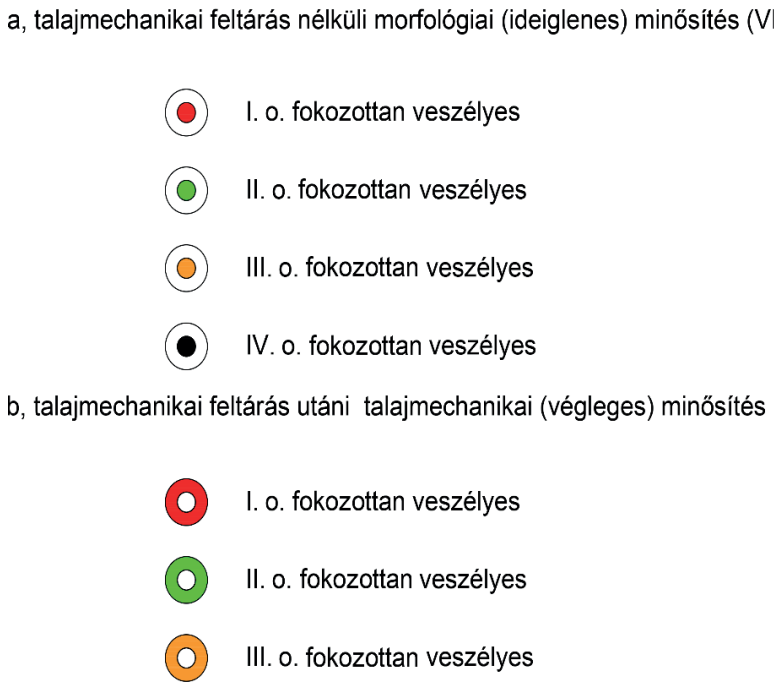
A keresztezések helyeit légi felvételek értékelése alapján lokalizálták, majd veszélyességi szempontok szerint rangsorolták őket:

1. Talajmechanikai feltárás nélkül morfológiai (ideiglenes) minősítés alapján:
   A minősítés pontozással történt, ahol a töltés és az ősmeder keresztezését vizsgálták az alapján, hogy a töltés az ősmeder homorú, domború vagy esetleg egyenes partját metszi, valamint ellenőrizték a beszivárgási hely és a töltéstengely közötti távolságot is.
   A pontozások kiértékelése alapján négy különböző osztályba sorolták ideiglenesen a keresztezéseket.
2. Talajmechanikai feltárás utáni talajmechanikai (végleges) minősítés:
   Ahol a talajmechanikai fúrások szerint lett értékelve I.-től III. fokozatig, hogy mely keresztezések veszélyesek.

A keresztezések minősítését a 10. ábra, a pontozások kiértékelésének minősítését a 11. ábra mutatja be.



10. ábra
Holt medrek minősítése [18: 1]



11. ábra
Kereszteződések minősítése [18: 1]

A holtmeder-keresztezések az árvízvédelmi jelenségek kialakulásának egyik gyakori veszélyforrása. Ezek a medrek rendszerint valamilyen terepmélyedéssel kapcsolatosak, azonban nem minden terepi mélyvonulat jelenthet holt medret, valamint nem csak kizárólag holt medreknél alakulhat ki árvizes jelenség.

A Vízügyi Tudományos Kutató Intézet (VITUKI) 1980-as altalajokra vonatkozó kutatásai alapján a holt medrektől függetlenül számos nem kellő biztonsági tényezőjű (NKBT) töltésszakadásokat határoztak meg geoelektromos mérés/szondázás és talajmechanikai fúrások alapján.

Ezen szakaszok sajátossága, hogy a töltés altalajhibái túlzott vízáteresztő képességgel rendelkeznek, így állékonynak tekinthetők egy-egy árvíz esetén.

Árvízvédelmi töltésekbe az elmúlt időszakban számos beavatkozás történt (drénszivárgók, megcsapoló kutak, fóliaszigetelések, résfalak, szádlemezverések) az árvizes jelenségek megakadályozására és egyben a töltések állékonyságának növelése érdekében.

Következtetések

A leiratban áttekintést adtam a Körös-vidék vízügyi múltjáról, ármentesítéséről, folyószabályozásairól és a jelenlegi árvízvédelmi rendszerek kiépítéséről.

Bemutattam az árvizek időszakában a védelmi képességet leginkább befolyásoló tényezőket, mind árvízvédelmi töltések szerkezeti hibáiból adódóan, mind holtmederkeresztezések, valamint NKBT-s szakaszok esetében.

Véleményem szerint az árvizes jelenségek jelentik a legnagyobb problémát egy-egy levonuló árvíz esetében, hiszen akár egy jelenségből adódó töltésszakadás a nem várható események között tartható számon, és éppen emiatt okozhatják a legnagyobb pusztítást egy-egy árvíz esetén. Ezért úgy gondolom, hogy a jövőben további kutatást igényel a jelenségek várható megjelenésének meghatározása, különösen a holt medrek területének további részletes vizsgálatát tartom fontosnak talajmechanikai és geofizikai mérésekkel, szivárgáshidraulikai modellezési vizsgálatokkal egybekötve.

Hivatkozások

[1] I. Pataky, „Katasztrófavédelem és honvédelem," *Hadtudomány,* 15. évf. 4. sz., 2005. [Online]. Elérhető: http://mhtt.eu/hadtudomany/2005/4/2005_4_12.html (Letöltve: 2019. 10. 11.)

[2] J. Padányi, „A Magyar Honvédség műszaki csapatainak lehetőségei és feladatai békeidőben a természeti- és civilizációs katasztrófák megelőzésében és a következmények felszámolásában," Kandidátusi értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 1994., p. 130.

[3] J. Padányi, „A NATO-tagság hatása a Magyar Honvédség szárazföldi csapatai műszaki támogatásának elméletére és gyakorlatára," Doktori értekezés, Magyar Tudományos Akadémia, Budapest, 2007., p. 204.

[4] J. Hornyacsek és L. Keszely, „A katonai erők, képességek alkalmazása katasztrófák esetén," *Hadmérnök,* 8. évf. 2. sz., pp. 191–209., 2013. [Online]. Elérhető: www.hadmernok.hu/132_18_hornyacsekj_kl.pdf (Letöltve: 2019. 10. 11.)

[5] L. Földi és L. Halász, „New tendencies in global climate change and their effects on the climate of Hungary," *Hadmérnök,* 14. évf. 1. sz., pp. 99–107., 2019.

[6] F. Glatz, „A víz a Kárpát-medencében," *Ezredforduló,* 11. évf. 1. sz., p. 18–21., 2007.

[7] L. Polgár, Z. Szappanos, Z. Kováts, M. Andó, J. Dabolczi, D. Kovács, I. Vágás, L. Ligeti, J. Szilágyi, J. Major, M. Szabó és I. Balló, *Árvízvédelem, folyó- és tószabályozás, víziutak Magyarországon.* Budapest: Országos Vízügyi Hivatal, 1979. pp. 150–151.

[8] Z. Zorkóczy, *Árvízvédelem.* Budapest: Országos Vízügyi Hivatal, 1987.

[9] L. Nagy, *Árvízvédekezés a településeken.* Budapest: Innova Print, 2010.

[10] „Magyar Királyság (1819–1869) Második katonai felmérés térképe, Gyula Város és környéke," *mapire.eu,* [Online]. Elérhető: https://mapire.eu/hu/map/second-survey-hungary/?layers=5&bbox=2318912.966664928%2C5866857.93854328%2C2422026.5178216305%2C5897432.74985735 (Letöltve: 2019. 10. 11.)

[11] *A Közép-Tiszavidék Vízügyi múltja II.* Budapest: Vízügyi Történeti Füzetek, 1979. p. 40.
[12] L. Szlávik, „A Tisza-völgy árvízvédelme és fejlesztése," Földrajzi Konferencia, Szeged, 2001., p. 15.
[13] L. Galli, *Az árvízvédelmi földművek állékonyságának vizsgálata.* Budapest: Országos Vízügyi Hivatal, 1976.
[14] „Árvíz 2006. 04. 27. Gyoma – Kisörvető – Mezőtúr jelenségek," Körös-vidéki Vízügyi Igazgatóság, 2006.
[15] Árvízvédelmi tervek, Észlelt árvízi jelenségek 1970-től napjainkig, JEL-1201-III, Körös-vidéki Vízügyi Igazgatóság.
[16] L. Szlávik, „Az 1980. évi Körös-völgyi árvíz és következményei," *Körös-vidéki Hírlevél,* 20. évf. Ksz., p. 11., 2010.
[17] „Magyar Királyság (1819–1869) Második katonai felmérés térkép és műholdas térkép 50–50%-os átlátszósággal egymásra halmozott térképe," *mapire.eu,* [Online]. Elérhető: www.mapire.eu (Letöltve: 2019. 10. 11.)
[18] Árvízvédelmi tervek, „Holtmeder keresztezések nyilvántartási terve, jelmagyarázat," Körös-vidéki Vízügyi Igazgatóság.

HADMÉRNÖK
VÉDELEMGAZDASÁG

15. évfolyam (2020) 1. szám 121–131.
DOI: 10.32567/hm.2020.1.9

Rodrigo Guajardo[1]

Defense Capabilities Development and Defense Industry, U.S. Case Study

Védelmi képességfejlesztés és védelmi ipar, USA esettanulmány

New product development is a very complex process independent of the domain, and defense industry is not an exception, being an especially challenging process that involves interactions between industrial suppliers of goods and services with multiple government offices often trying to balance competing objectives. The big dilemma is: How governments acquire the equipment, goods, and services needed for their armed forces at a reasonable price, appropriate quality, and with a reasonable time frame? Complex weapon systems are developed by the Ministry of Defense (MoD) through the defense acquisition system, which must provide more affordable systems as a matter of national security. Yet the defense acquisition system is in a perpetual state of reform, the fact is there is no evidence of improved acquisition outcomes. In this research, U.S. MoD defense acquisition system will be analyzed and the reforms that had to be made to improve the current acquisition outcomes.

Keywords: acquisition process, capabilities development, systems engineering, new product development, defense industry

Az új eszközök fejlesztése, területtől függetlenül mindig nagyon komplex folyamatot jelent, természetesen a védelmi ipar sem kivétel ez alól, hiszen ez egy olyan kihívásokkal teli ágazat, amely az ipari termékek és szolgáltatások beszállítói és a kormányhivatalok közötti kapcsolatot foglalja magában, és gyakran az egymással versengő célkitűzések kiegyenlítésére van szükség. A nagy kérdés a következő: az egyes országok kormányai hogyan vásárolják meg a fegyveres erők számára szükséges felszereléseket, eszközöket és szolgáltatásokat elfogadható áron, megfelelő minőségben és észszerű határidőn belül? A bonyolult fegyverrendszereket a Honvédelmi

[1] National University of Public Service, PhD Student, Doctoral School of Military Engineering, e-mail: rodrigoguajardosantana@gmail.com, ORCID: https://orcid.org/0000-0002-3141-7410

Minisztérium a védelmi beszerzési rendszerén keresztül dolgozza ki, amely nemzetbiztonsági szempontból megfizethetőbb rendszert kell, hogy biztosítson. Azonban a védelmi beszerzési rendszer jelenleg úgynevezett reformállapotban van, hiszen a javuló eredmények még váratnak magukra. Ebben a tanulmányban az Amerikai Védelmi Minisztérium beszerzési rendszerét elemezzük és azokat a megvalósításra váró reformokat, amelyek a jelenlegi beszerzési folyamat eredményeinek a javításához elengedhetetlenek.

Kulcsszavak: **beszerzési folyamat, képességek fejlesztése, rendszerfejlesztés, új eszközök fejlesztése, védelmi ipar**

Introduction

Decisions associated with how to balance the competing objectives of delivering new military equipment at a reasonable price, with the appropriate quality, and with a reasonable time frame are normally taken under an environment defined by high stakes, high accountability, and high uncertainty. New product development at a high level at the Ministry of Defense (MoD) is achieved through a complex defense acquisition system, with also many opportunities for improvement. Despite its limitations, the defense acquisition system is proved to be an effective way to produce weapons that have performed well in battle [1].

Military planning is loaded with uncertainties, which demands an in-depth analysis of the scenarios where our troops will operate and the threats to which they will be exposed and, of course, imaginative solutions (scenarios). Military planning should not focus only on determining the means necessary for a specific type of conflict or mission, but it should be much more general and aimed at obtaining capabilities that allow covering a broad spectrum from them. Now, it must take into consideration that to obtain the most accurate results, the most likely scenarios will have to be included and the most demanding operational environments. In military terms, capabilities are "the set of factors (systems of weapons, infrastructure, personnel and logistical support) settled on the basis of doctrinal principles and procedures, that they seek to achieve a certain military effect at a strategic, operational or tactical level to fulfil the assigned missions" [2]. That is to say, a military capability is not only a weapon or a weapon system, but also a set of factors, more or less critical, but all equally important for achieving the desired effect.

New military equipment or more complex weapon system development are developed by the MoD through the defense acquisition system, which must provide more affordable systems as a matter of national security. The defense acquisition system is perceived to be in a perpetual state of reform in many countries without any evidence of improved acquisition outcomes, but indeed the reality regarding product development process all around the world is not different from the defense situation.

Global Performance Assessment for New Product Developments

Many new products' development fails; the Product Development and Management Association (PDMA[2]) led an international comparative research and multi-industry performance analysis in 2012 and determined that approximately 39% of all new developments had failed to reach the market with a minimum level of failure, even more, the failure rates grew by over 54% in the case when the development of new products required high levels of innovation [3].

According to the studies carried out by the PDMA dating from 1990 and shown in Table 1, the failure rate for the development of new products would be around 40%, which is consistent with the empirical studies conducted by [4] that analyses studies and reports since 1977 to 2010 and that estimate a failure rate for new products of 40%, thus demonstrating that the failure rate has been constant over time.

Table 1.

History and results of comparative performance assessment study CPAS [Made by the author.]

N° Study	Year	Sample (Bussiness Units)	Fail Rate (%)
1st Study	1990	189	42
2nd Study	1995	383	41
3rd Study	2004	416	41
4th Study	2012	453	39

As can be seen in Figure 1 and analyzing data report from PDMA 2012, only 44% of the new products with moderate innovation met the development schedule on time and 49% of them met the initial budget restrictions. The situation is not better in relation with new products with radical innovation, only 29% of the new products with a high level of innovation met development on time and only 32% of them met the initial budget restrictions. These poor records of new product achievements are shared all across the world without any distinction of industry, revealing that product development tasks are highly difficult.

[2] PDMA – U.S. organization created in 1976 that focuses on the unique set of integrated activities involved in the full lifecycle of product development and management, including innovation.

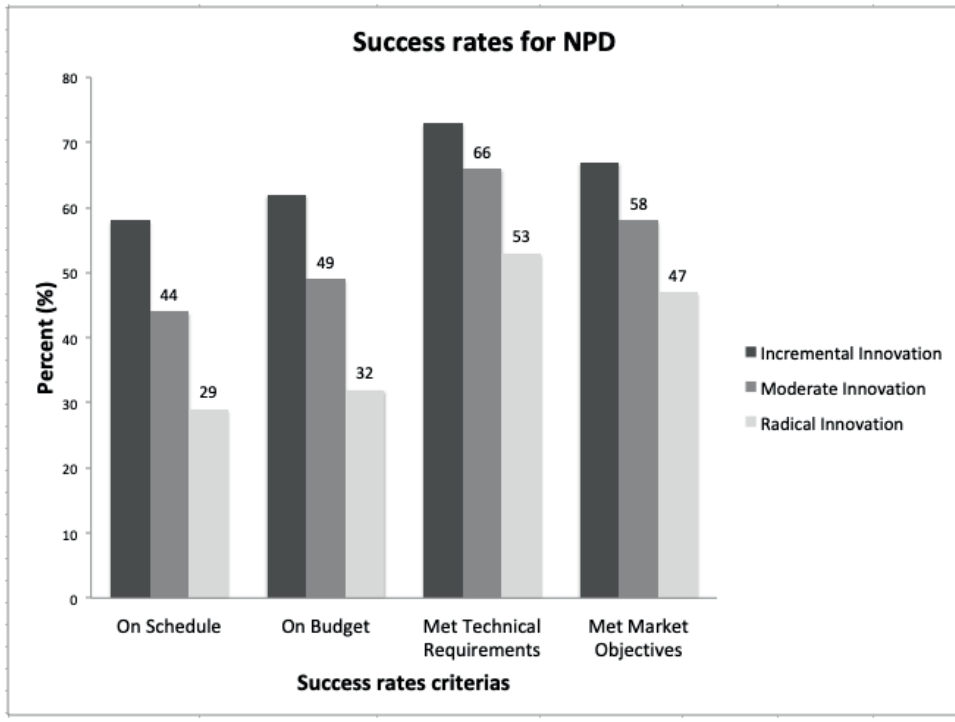


Figure 1.
Success rates for new product developments with different levels of innovation [Made by the author.]

U.S. Defense Performance Assessment for New Product Developments

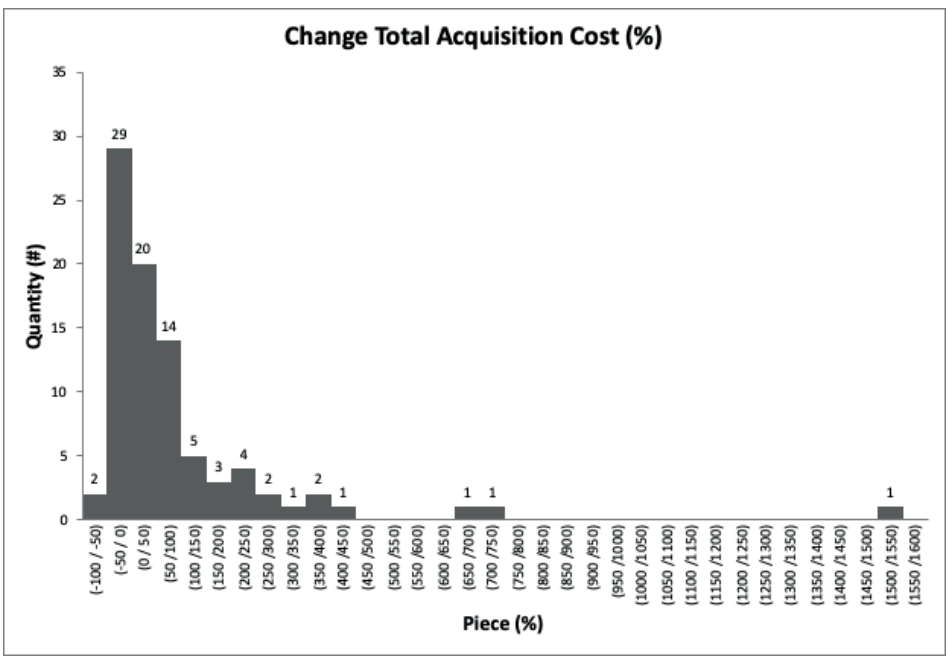
The performance of the defense acquisition has been widely discussed at many points in U.S. history. Recent years are no exception, as exemplified by the U.S. Government Accountability Office's Report (GAO[3]) and the U.S. DoD's[4] *Performance of the Defense Acquisition System Annual Report,* both listing the system for major weapon buying as "high risk" for nearly a quarter of a century. Some U.S. congressmen had pointed to the enormous total cost growth since the start of each program in the portfolio, which can mean going back to the 1990s. Under Secretary Kendall annual metrics were preferred, which show improvement in relation with previous periods.

[3] GAO – Independent, nonpartisan agency that works for Congress. GAO examines how taxpayer dollars are spent and provides Congress and federal agencies with objective, reliable information to help the government save money and work more efficiently.

[4] DoD – The Department of Defense (DoD, USDOD, or DOD) is an executive branch department of the federal government charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces.

Recent studies by other researchers, presented at CSIS[5] and the Naval Postgraduate School's Defense Acquisition Research forum [5], have particularly illuminated two metrics: cost and schedule growth.

For a performance metric of new product development within the U.S. DoD, the data contained in Table 13 of Appendix IV within the U.S. Government Accountability Office's Report to Congressional Committees (GAO-18-360SP) entitled *Weapon Systems Annual Assessment* [6] is considered. An analysis of these data reveals that of 86 programs in the portfolio of U.S. DoD's major weapon acquisition programs 2017, only about 37% of these are in a condition equal to or less than the first full estimate of total acquisition cost. This seems to be on par with the global performance records of new products that observe a medium to a high level of innovation, presented in Figure 1.



Count	Min	Max	Bin Width	# Bins	Mean	Median
86	–89	1.566	50	34	90.44	7.40

Figure 2.

Frequency histogram percent change in total acquisition costs from first full estimates
[Made by the author.]

[5] CSIS – U.S. Center for strategic and international studies. Established in Washington, D.C., CSIS is a bipartisan, nonprofit policy research organisation dedicated to providing strategic insights and policy solutions to help decision-makers chart a course toward a better world.

To get a complete state of the results obtained in the development of new products in relation to costs, data must be evaluated beyond a simple one measure of the pass–fail test. Figure 2 shows the cost distribution of 86 programs as a histogram with the associated descriptive statistics. It should be noted that although a large number of programs are effectively in or under the estimated budget line (65 programs were under 100% of the budget in relation with the first full estimate), the total cost growth for those programs that failed may be very large, with at least seven projects that failed their target costs, compared to which they amounted nearly 300% or even more. Additionally, Table 2 shows the 2017 portfolio aggregate changes in research and development (R&D), and total acquisition costs, as well as average delays in delivering operational capability since the programs' first full estimates.

Table 2.

2017 portfolio aggregate changes in R&D, total acquisition costs, as well as average delays in delivering operational capability, since the programs' first full estimates [Made by the author.]

Fiscal year 2018 - Dollars	
	Since first full estimate (baseline to December 2016)
Change in total research and development cost	$ 103.1 billion 48.9%
Change in total procurement cost	$ 430.8 billion 47.9%
Change in total other acquisition costs	$ 2.9 billion 26%
Change in total acquisition costs	$ 536.8 billion 47.9%
Average delay in delivering initial capabilities	$ 27.4 months 37.7%

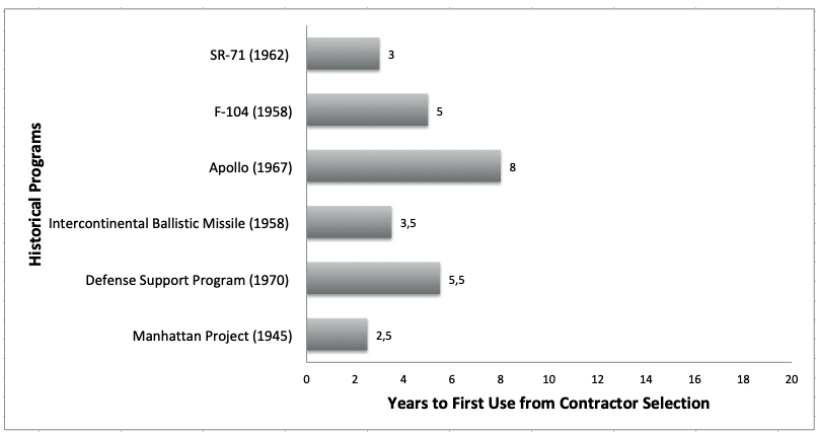
According to U.S. DoD's *Performance of the Defense Acquisition System 2016 Annual Report* [7], nearly 22 of the largest defense procurement programs have been cancelled between 1997 and 2015 before reaching the stage of production of significant quantities. Although it is not reasonable or expected that all research and development (R&D) projects reach the manufacturing stage, a defense procurement process with a high level of efficiency should be able to identify those projects destined to fail before using higher resources.

In order to have an insight into the impact on the costs of those cancelled programs, Table 3 provides the sunk costs of five cancelled development projects. This information was obtained from GAO-14-77 [8] and it can be seen that it is not uncommon for the U.S. MoD to spend several billions of dollars on development programs in pre-completion stages. The opportunity cost associated with sunk-cost products of possible cancellations is that these funds could be used elsewhere in the portfolio of development programs and thus increase the rate at which superior capacities are finally delivered to the armed forces and the end-user.

Table 3.

2017 portfolio aggregate changes in R&D, total acquisition costs, as well as average delays in delivering operational capability, since the programs' first full estimates [Made by the author.]

Program	Service	Centract Termination	Sunk Costs
Aerial Common Sensor	Army lead, Navy participation	2006	$186 million
Comanche Helicopter	Army	2004	$5.9 billion
Future Combat System	Army	First partial termination in 2009, final termination in 2011	Estimated $20 billion
Transformational Satellite Communications System	Air Force	2009	Estimated $2.9 billion
VH-71 Presidential Helicopter	Navy	2009	$3.3 billion



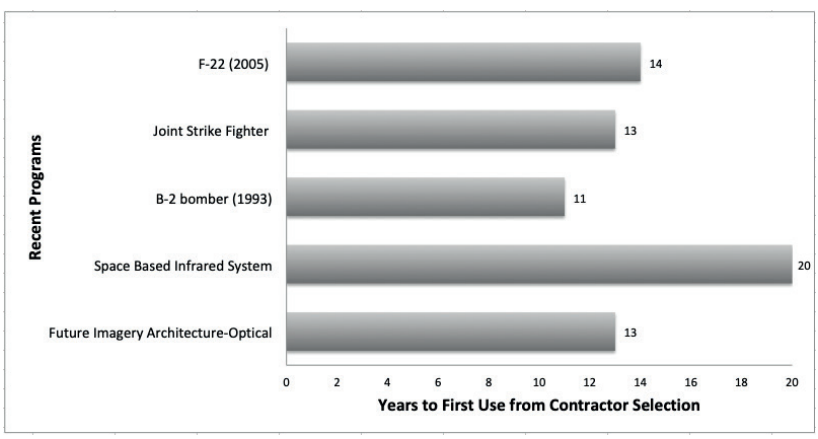


Figure 3.

Development duration of historical and recent programs [Made by the author.]

Unwanted trends in defense procurement are not only limited to the issue of costs. A recent report from the National Research Council (NRC[6]) called *Pre-Milestone A and Early-Phase Systems Engineering: A Retrospective Review and Benefits for Future Air Force Systems Acquisition* [9], highlights that in an era where product development of commercial technologies has been reduced considerably, the development time of much of the major weapons systems has increased dramatically. Figure 3 shows the duration time of historical and more recent development programs, whose data was obtained from the NRC report 2008, from which it can be concluded that the development times required for the most recent programs double or even triple the development times of historical programs.

U.S. MoD Defense Acquisition Process and Recent Reforms

The Defense Acquisition System has its foundation in the country's policy and public law. The development, acquisition, and operation of military systems are governed by a multitude of public laws, formal MoD directives, instructions and manuals, numerous Service and Component regulations, and many inter-service and international agreements. Managing the development and fielding of military systems requires three basic activities: technical management, business management, and contract management. In the U.S., systems engineering management is one of the main pillars and has to deal with the technical management component of MoD acquisition management of DAU[7] (2000) [10]. Systems Engineering Management bridges these processes and must resolve the dichotomy of event-driven needs, event-driven technology development, and the calendar-driven budget throughout its whole life cycle.

In the U.S., the Defense Acquisition System is regulated by DoD instruction (DoDI) 5000.02 *Operation of Defense Acquisition System* dated August 10, 2017. This regulation provides policies and principles that govern the defense procurement system and forms the basis for all U.S. DoD programs that include weapon systems, services and automated information systems (AIS), and also establishes a management framework for interpreting the user requirements and technological opportunities in stable, affordable and well-managed procurement programs. It also identifies the reports, regulations and other information requirements for each milestone and point of decision.

The U.S. DoD 5000 document series were revised in 2000 to make the process more flexible, enabling the delivery of advanced technology more rapidly and at reduced total ownership cost. The new process encourages multiple entry points, depending on the maturity of the fundamental technologies involved, and the use of evolutionary methods to define and develop systems. This encourages a tailored approach to acquisition and engineering management, but it does not alter the basic

[6] NRC – Organised by the U.S. National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government.

[7] DAU – Defense Acquisition University (DAU) is a corporate university of the United States Department of Defense offering "acquisition, technology, and logistics" (AT&L) training to military and federal civilian staff and federal contractors.

logic of the underlying systems engineering process. Later on, 2015 brought one of the major changes in the revised acquisition system with an increased emphasis on systems engineering trade-offs made between capability requirements and life-cycle costs early in the acquisition process in order to ensure that realistic program baselines are established in such a way that associated life-cycle costs of a contemplated system are affordable within future budgets.

The changes from the previous version of DoDI 5000.02 2013 to DoDI 5000.02 2015 [11], [12] are significant. DoDI 5000.02 2015 document sets "affordability" as one of the central themes and cites the early application of systems engineering assessments and trade-off analyses used together with a solid analysis of alternatives (AoA) as the model for reaching the desired outcomes. Concepts as "affordability", "systems engineering", "trade-off analyses" and "analysis of alternatives (AoA)" have been strongly incorporated since the revision of DoDI 5000.02 2015. In relation with "affordability", the revised defense acquisition system requires that meaningful trade-offs between capability requirements and lifecycle costs be explored early and often in order to ensure that realistic program baselines are established in such a way that associated lifecycle costs will likely fit within future budgets; the new instruction signals the increased emphasis on the AoA by dedicating an entire enclosure to the topic (Enclosure 9 DoDI 5000.02 January 2015). Finally, trade-off analysis being part of the system engineering analysis has been added to the systems engineering enclosure of DoDI 5000.02 January 2015. Table 4 shows the topics added to the Systems Engineering Enclosure of DoDI 5000.02 January 2015 considering trade-off analysis a part of the system engineering process.

Topic	DEC 2008 DoDI 5000.02	JAN 2015 DoDI 5000.02
Development Planning	Not available	Included
Systems Engineering Trade-off Analyses	Not available	Included
Technical Risk and Opportunity Management	Not available	Included
Technical Performance Measures and Metrics	Not available	Included
Modelling and Simulation	Not available	Included
Manufacturing and Producibility	Not available	Included
Software	Not available	Included
Reliability and Maintainability	Not available	Included
Program Protection	Not available	Included
Insensitive Munitions	Not available	Included
Program Support Assessments	Not available	Included

Table 4.

Topics added within the systems engineering enclosure of JAN 2015 DoDI 5000.02 [Made by the author.]

Conclusions

In this research, the defense industry dilemma was introduced concerning how to deliver new military equipment at a reasonable price, with appropriate quality, and

with a reasonable time frame under a constantly changing environment with high levels of uncertainty. New product development performance was evaluated with international studies not only for the global market but the military industry as well concluding that both shares similar performance under development with medium or high levels of innovation.

The U.S. official reports were analysed in order to visualise the performance of new weapons development programs inside U.S. DoD and how cost and time is still a big issue with the total cost of program portfolio growing by 48% in relation with the first full estimate baseline and with an average delay in delivering initial capabilities in nearly 38% of the programs. Additionally, in relation to the duration of historical and recent U.S. DoD programs, it could be concluded that recent programs in comparison with some historical programs have double or even triple development time.

Finally, we could appreciate the recent reforms made by the U.S. MoD in relation with U.S. DoD 5000 Instructions documents in order to improve the outcomes and performance of current programs, reinforcing and adding "affordability", "systems engineering", "trade-off analysis" and "analysis of alternatives (AOA)" activities and directives as a new enclosure, further strengthening its development process of new weapons systems in its main areas of technical management of development engineering, such as systems engineering, the use of analysis of alternatives (AoA) as a tool and trade-off analysis in earlier stages and in a greater number of milestones, as a way to strengthen the outputs of the new defense programs in relation to costs and time frames, given the changing prioratisation of operational requirements due to the fluctuating changes in the threat.

References

[1] W. D. Jones, *Arming the Eagle: A History of U.S. Weapons Acquisition since 1775.* Defense Systems Management College Press, 1999.

[2] J. M. García, "Planeamiento por capacidades," ***infodefensa.com,*** 2016. [Online]. Available: www.infodefensa.com/wp-content/uploads/EMD_planeamiento.pdf [Accessed Nov. 30, 2018].

[3] S. K. Markham and H. Lee, "Product Development and Management Association's 2012 Comparative Performance Assessment Study," *The Journal of Product Innovation Management,* vol. 30, no. 3, May, pp. 408–429, 2013. DOI: https://doi.org/10.1111/jpim.12025

[4] G. Castellion and S. K. Markham, "Perspective: New Product Failure Rates: Influence of *Argumentum ad populum* and Self-Interest," *The Journal of Product Innovation Management,* vol. 30, no. 5, Sept., pp. 976–979, 2013. DOI: https://doi.org/10.1111/j.1540-5885.2012.01009.x

[5] J. Ellman, S. Cohen, A. Hunter, K. Johnson, R. McCormick, and G. Sanders, "Defense Acquisition Trends, 2016," *Center for Strategic & International Studies, 2017.* [Online]. Available: https://books.google.hu/books?id=-Ex2DgAAQBAJ [Accessed Dec. 04, 2018].

[6] S. Oakley, *Weapon Systems Annual Assessment: Knowledge Gaps Pose Risks to Sustaining Recent Positive Trends.* United States Government Accountability Office, 2018.
[7] F. Kendall, *Performance of the Defense Acquisition System: 2016 Annual Report.* Washington, D.C.: Department of Defense, 2016.
[8] C. Chaplain, *Canceled DoD Programs: DoD Needs to Better Use Available Guidance and Manage Reusable Assets.* United States Government Accountability Office, 2014.
[9] National Research Council, *Pre-Milestone A and Early-Phase Systems Engineering: A Retrospective Review and Benefits for Future Air Force Acquisition.* Washington, D.C.: National Academies Press, 2008. DOI: https://doi.org/10.17226/12065
[10] Defense Acquisition University (DAU), *Systems Engineering Fundamentals.* Virginia: Fort Belvoir, Defense Acquisition University Press, 2001.
[11] U.S. Department of Defense, *Department of Defense Instruction 5000.02 (DoDI).* Washington, D.C., 2013.
[12] U.S. Department of Defense, *Department of Defense Instruction 5000.02 (DoDI).* Washington, D.C., 2015.

HADMÉRNÖK
VÉDELMI INFORMATIKA

15. évfolyam (2020) 1. szám 133–158.
DOI: 10.32567/hm.2020.1.10

István Balajti[1]

General Overview on the Radar Conference in Boston 2019

A bostoni 2019-es radarkonferencia általános áttekintése

Nowadays, 70–85% of the cost of modern warfare equipment is software-based solutions and services. These software modules define the quality and efficiency of the signal and data processing of the information of different sensors types. They are playing key roles in the artificial intelligence supported cognitive data processing and the effectiveness of the soldiers/decision-making commanders. The modernisation of the Hungarian Army, and the success of the Zrínyi 2026, basically depend on the understanding and professional service of the new technologies.

Keywords: radar, electronic attack/electronic protection, passive radar systems, bi- and multistatic radar systems, cognitive radar, Spectrum Sharing Technique, weather radar

Napjainkban a modern haditechnikai eszközök költségeinek 70–85%-át szoftver-alapú megoldások, szolgáltatások teszik ki. Ezek a szoftvermodulok határozzák meg a különböző típusú érzékelők jel-, és adatfeldolgozásának hatékonyságát és minőségét. Kulcsfontosságú a katonák-/döntést hozó parancsnokok feladata a mesterséges intelligencia által támogatott kognitív adatértékelés megvalósításában. A Magyar Honvédség modernizálása, a Zrínyi 2026 sikere, alapvetően az új technológiák megértésén és professzionális szintű kiszolgálásán múlik.

Kulcsszavak: rádiólokátor, aktív zavarás és zavarvédelem, passzívradar-rendszerek, bi- és multistatikus radarrendszerek, kognitív rádiólokátor, spektrumfelosztási technológiák, időjárásradar

[1] National University of Public Service, Faculty of Military Sciences and Officer Training, e-mail: balajti.istvan@uni–nke.hu, ORCID: https://orcid.org/0000-0003-3566-2904

Introduction

The USA hosted the International Radar Conference held in Boston at the end of April 2019. The invitation of the Conference pointed out the following fact: "A radar revolution is underway, made possible by the rapid evolution of digital electronics, and powered by new innovative architectures, advanced components, novel waveforms and sophisticated processing techniques" [1].

The author's findings in this article are subjective and focused on the main topics, which may interest the Hungarian and Eastern-European readers.

The focal points of the conference were:

- Radar system related education such as Radar Systems Prototyping and Radar Summer School – Built-A-Radar at MIT
- Spectrum Sharing Techniques between radars and communication systems
- Passive radar systems
- Bistatic and Multistatic radar
- Electronic Attack (ECM)/Electronic Protection (ECCM)
- Weather radar
- Machine Learning Technology and Cognitive Radar
- Emerging technologies

All information on the conference is available at the link: www.radarconf19.org/

Technical Matters of the Conference

Tutorials

The most powerful and compact part of the radar conferences are usually the Tutorial sections. This time, sixteen Tutorials were presented with titles that covered all relevant subjects, such as: Convex Optimization for Adaptive Radar; Over-the-Horizon Radar; Machine Learning Techniques for Radar ATR; Adaptive Arrays: Principles and Applications; Introduction to Synthetic Aperture Radar; Radar Systems Prototyping; Inverse Synthetic Aperture Radar Satellite Imaging; Radar Tracking State Estimation and Association; Phased Arrays for MIMO Radar; Passive Radar – From Target Detection to Imaging; Ultra-Wide Band Surveillance Radar; Bistatic and Multistatic Radar Imaging; Advanced Radar Processing Techniques; Communications and Radar Spectrum Sharing; Detection, Performance, and CFAR Techniques; Signal Processing for Passive Radar.

Two Tutorials were visited, which were the followings:

Radar Systems Prototyping and Radar System Related Education

Dr. Lorenzo Lo Monte – Chief Scientist at Telephonics: Radar Systems Prototyping [2]

It is essential for radar engineers and managers to be aware of the radar performance design/upgrade feasibility or applicability of the new concept to the already existing radar. This tutorial refreshed the critical points of radar developments and demonstrated how could a radar prototype in the lowest and fastest way be built. These types of topics are essential for students, researchers and new requirement characterisations, because even the "old fashioned" radar subsystem obsolescence engineering requires proper analyses and feasibility study preparation. The reviewed solutions are characterised by much of the engineering requirements with the cost reduction realisations.

The key messages of the presentation are as follows: The design based on the KISS principle states that most systems work best, if they are kept simple rather than made complicated. See Figure 1.

Figure 1.
The radar design required application of the KISS principle (The author's modification based on [2])

Then the presenter went through all the steps of rapid radar design issues starting with the RF connector selection, attenuators/amplifiers mixers, etc. The selection ended at the Close/In and Broadband Phase Noise characterisation. The main part of the tutorial focused on the "Back End Design" critical factors. It started with the observation that Modern Radars perform Digital Signal Processing (DSP) using I/Q Data. Note: These are outdated methods and nowadays we use Direct Digital Demodulation techniques, where the signal sample rate is about 2.5 times of the signal Bandwidth and the unwanted signal filtering is solved by polyphase filters.

The chain of the modern radar receiver is structured as shown in Figure 2.

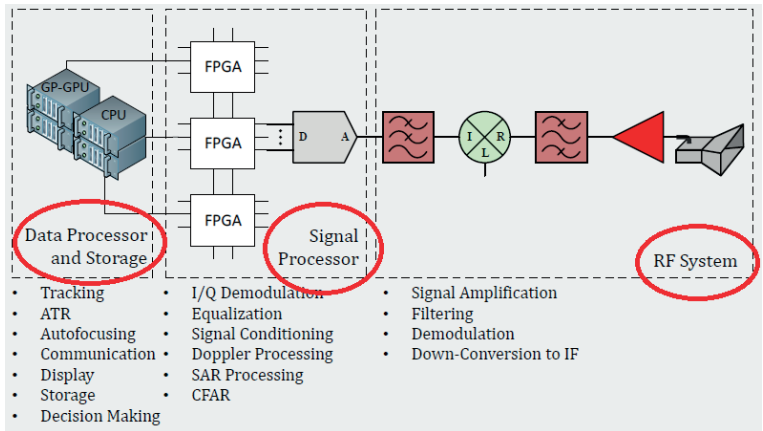


Figure 2.

Main tasks of the chain of the modern radar receiver (The author's modification based on [2])

The "RF system" is usually based on the "Superheterodyne Baseband Sampling" principle. The Signal Processor contains Analog Digital Converters (ADC), and Digital Analog Converters (DAC) for exciter, transmitter and for stable reference RF signals, Digital Signal Processors and FPGA, while for the Data Processor and Storage the most popular solutions are based on Graphical Modules and fast commercial workstations.

After the task clarification, the survey of available resources, devices, test equipment and know-how shall be accomplished. The radar equation is used for the determination of the subsystem design characteristics and performance specification of the radar subsystems. Figure 3 and 4 show the ADC selection of the "RF system".

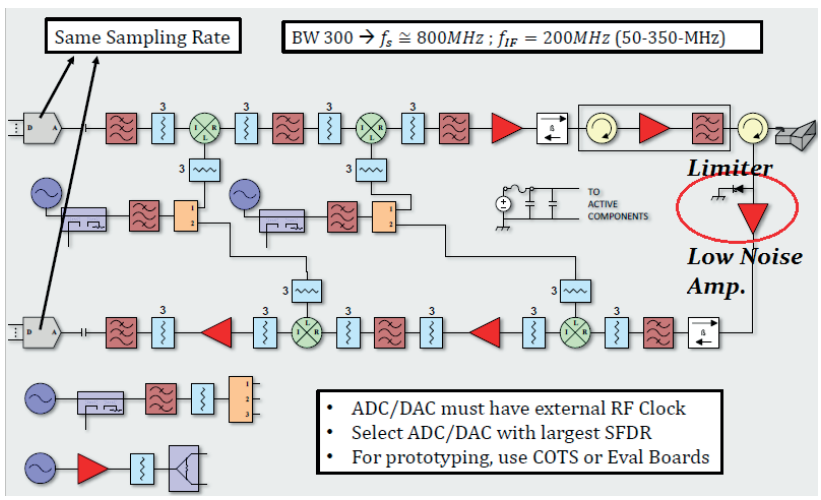


Figure 3.

The ADC selection requirements for the "RF subsystem" (The author's modification based on [2])

The weak signal must be amplified so that it can be measured well at the ADC
- Too little amplification will reduce SNR
- Too high amplification won't change SNR but will reduce dynamic range
- We need to find the right value

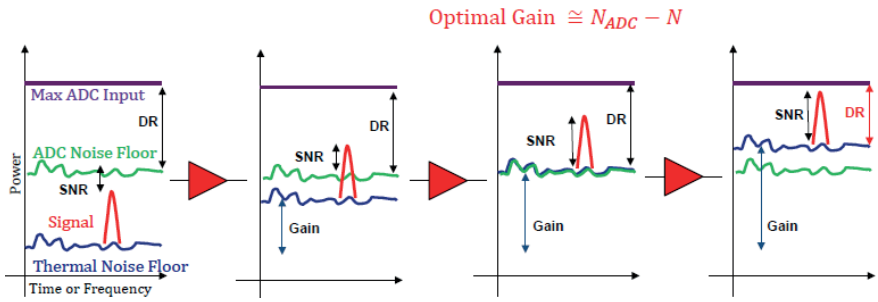


Figure 4.

The ADC dynamic range step up to the "RF subsystem" thermal noise [2]

Mitigation mismatching, unwanted spurious signal filtering and maximising linearity are the core requirements as the example in Figure 5 shows.

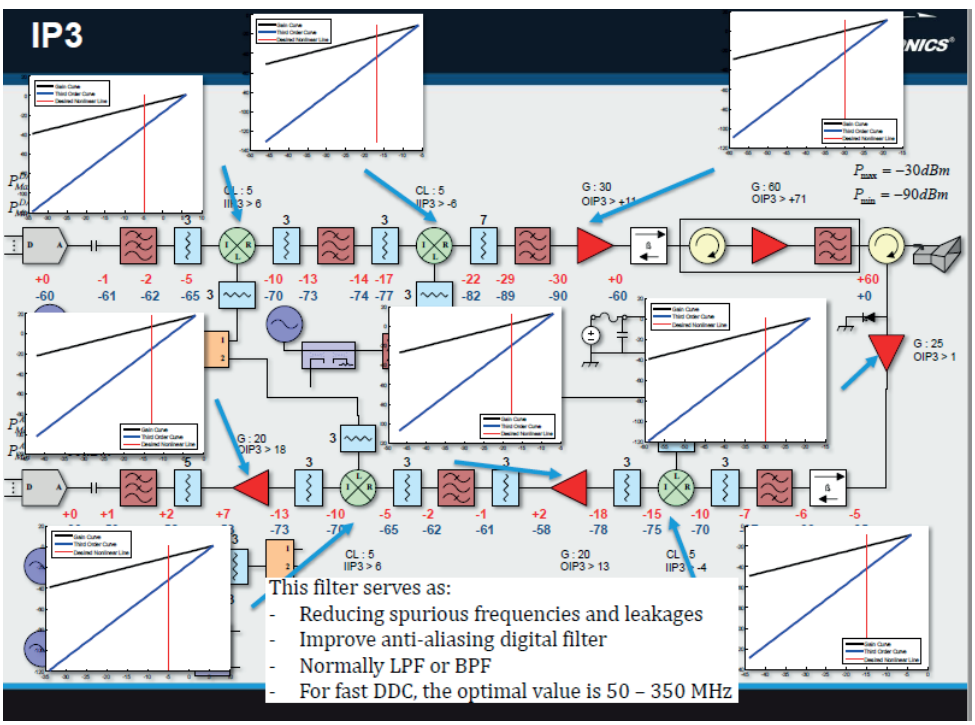


Figure 5.

Example for the linearity requirements of the RF components (The author's modification based on [2])

The presentation ended with emphasising the importance of further research as Figure 6 summarises.

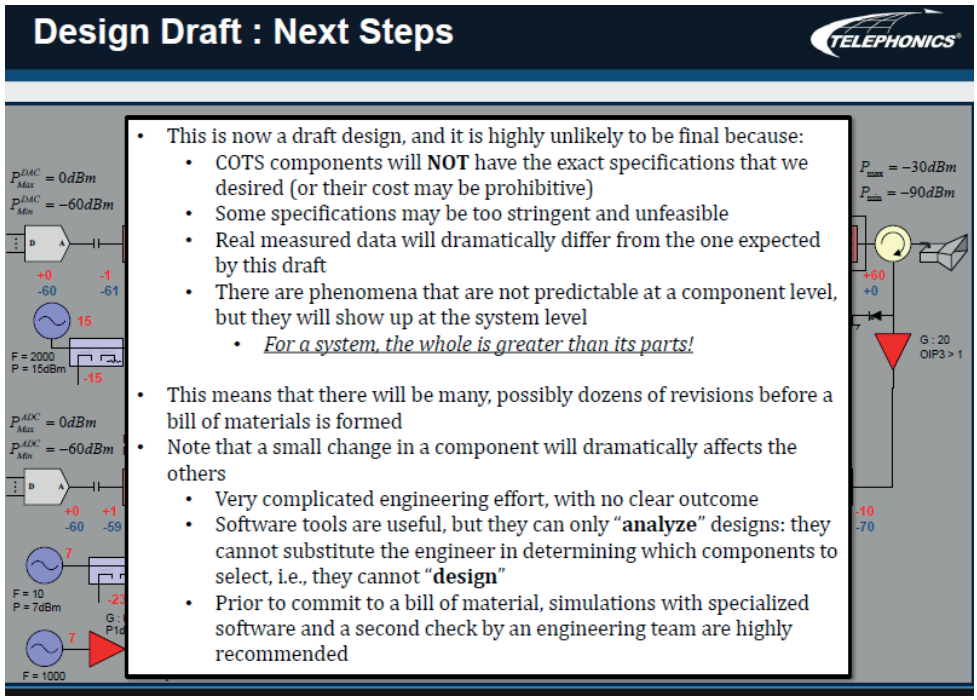


Figure 6.
The reasons why the prototype of the radar is not the final solution [2]

Radar Summer School – Built-A-Radar at MIT

The presentations and the two days of "Summer School – Built-A-Radar at MIT" are managed by Kenneth E. Kolodziej, Patrick J. Bell, Alan J. Fenn, Elizabeth Kowalski, John W. Meklenburg, William F. Moulder, Julia S. Mullen and Bradley T. Perry. The presentation of these authors entitled *Build-a-Radar Self-Paced Massive Open Online Course* (MOOC) gives a quick overview of the subject offered possibilities [3]. The success of the courses highlights that Electromagnetic Education can be greatly enhanced by providing students with a practical hands-on project that helps illustrate the different theoretical concepts covered.

Figure 7 shows the radar which could be built by enthusiastic students or teams demonstrating the beauty, possibilities and importance of the radar related topics.

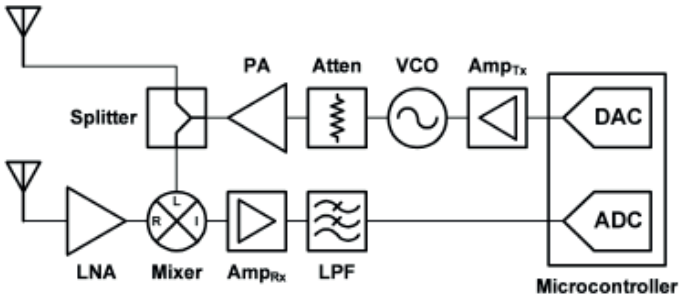


Figure 7.
Block diagram of the radar highlighting the connection of the microcontroller to the RF components and two antennas [3]

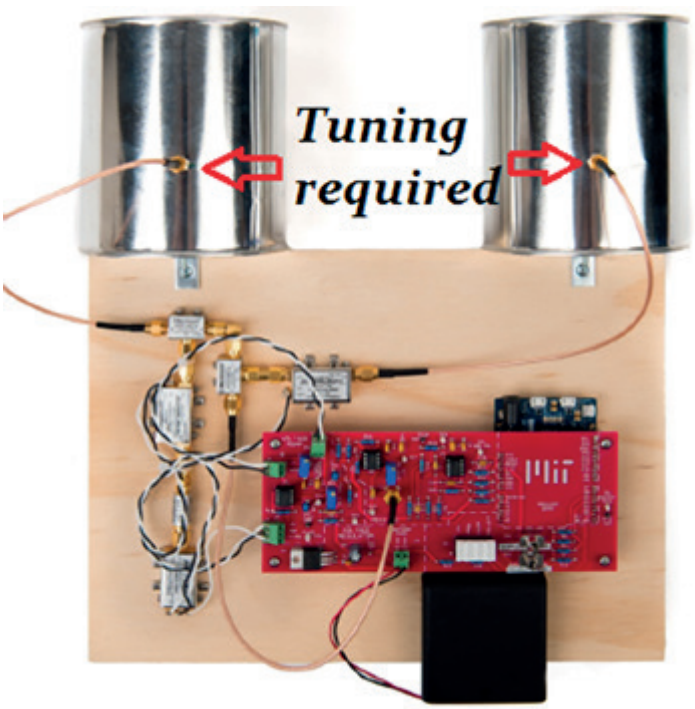


Figure 8.
Completely assembled build-a-radar system capable of Doppler, ranging and synthetic aperture imaging modes (The author's modification based on [3])

The course also contains a detailed set of instructions to guide students through the radar construction using a hardware kit that is also available online from 250 to 600 USD. Together, these combined offerings present a novel teaching tool for all students interested in radar and electromagnetics as a whole. The build-a-radar course site is free and open to everyone at https://llx.mit.edu after creating a simple

personal account that is used to track your progress. This online material addresses the second challenge mentioned, and offers video-recorded lectures, step-by-step built instructions and knowledge questions to serve as a tool for both students and other teachers. Further details are available at: www.radarconf19.org/index.php/radar-summer-school/.

Ultra-Wideband Surveillance Radar and Spectrum Sharing

Mark Davis: Ultra-Wideband Surveillance Radar [4]

The Ultra-Wideband (UWB) Surveillance Radar is an emerging technology for detecting and characterising targets and cultural features for military and geosciences applications.

This Tutorial is divided into five parts such as:

1. Early history of battlefield surveillance radar
2. UWB Phased Array Antenna: Electronically scanned antennas and Wideband Waveforms
3. UWB Synthetic Aperture Radar (SAR) image and fixed object detection capability
4. UWB Ground Moving Target Indication/Space Time Adaptive Processing (STAP) and UWB Radar Spectrum Compliance
5. New research in Multi-mode Ultra-Wideband Radar, with the design of both SAR and moving target indication (MTI) FOPEN systems

The summary of the first part indicates that:

- UWB Radar Systems have been in development for over 40 Years – Primarily for military applications
- Commercial and Personal Communications are Ubiquitous:
  - eCommerce is the major source of many Businesses
  - Digital Communications is important for Security
- The regulations and frequency allocation process has changed significantly in the past 15 years:
  - UWB Standards in IEEE and NTIA/CEPT
  - Compliance Standards are Conservative and Inflexible
- The International Radar Community needs to adapt and develop new technologies – Analogous to Cognitive Radio

Further key arguments for UWB radars applications are as follows:

- Modern radar systems demand more bandwidth
  - Enable improved resolution of targets
  - Provide better obstacle detection and tracking
- Impediment: international regulations on frequency allocation:
  - Creates a "barrier for entry" for many new radar applications
- Important reasons for uwb operation of radars for commercial and military system applications:

  - Humanitarian and natural disaster monitoring operations
  - Characterisation of biomass for global warming research
  - Foliage penetration for detecting objects under dense canopy
  - Discriminating obscured objects in close proximity
- Radar require long wavelength and modest power within VHF to L-band to "see" objects under foliage and terrain cover
  - Recent focus of Earth Resources Monitoring Community
- Resolutions less than 0.5 m are needed for object discrimination
  - This qualifies as Ultra-Wide Band (UWB) – 25 percent bandwidth
- UWB characterisation immediately causes more intense spectrum regulations, compliance and testing

Figure 9 depicts the differences between the photographic picture and radar images of the UWB. The UWB "VHF" ("m" wavelength) radar image has the highest target detection capabilities with relatively low resolution. The combination of different types, frequency bands, SAR images gives the required performances.

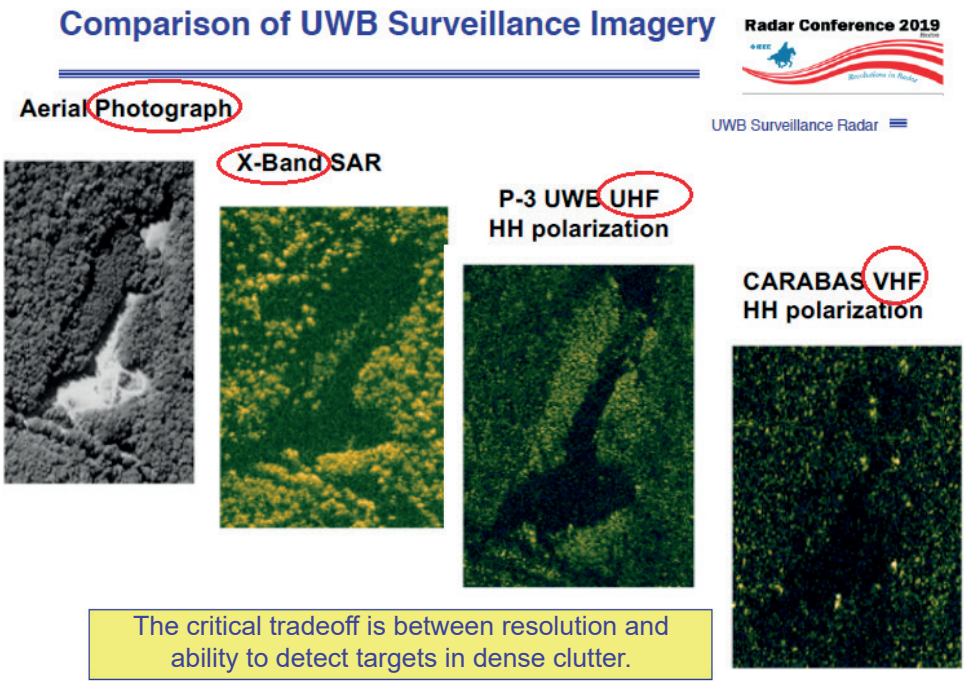


Figure 9.

UWB radar targets detection performances are increasing in radar of "dm", "m" wavelength
(The author's modification based on [4])

Figure 10 summarises the requirements of the UWB radar waveforms, which are radar with very short or very complex sub-pulse modulation.

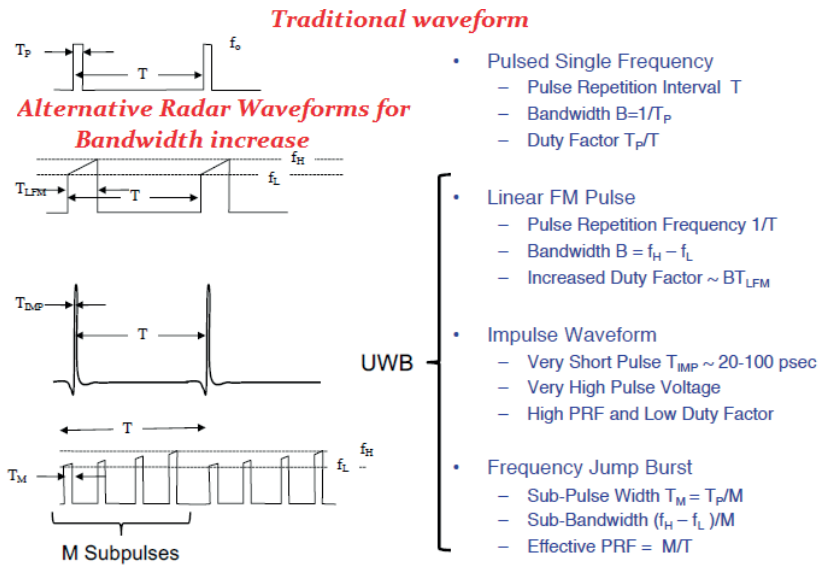
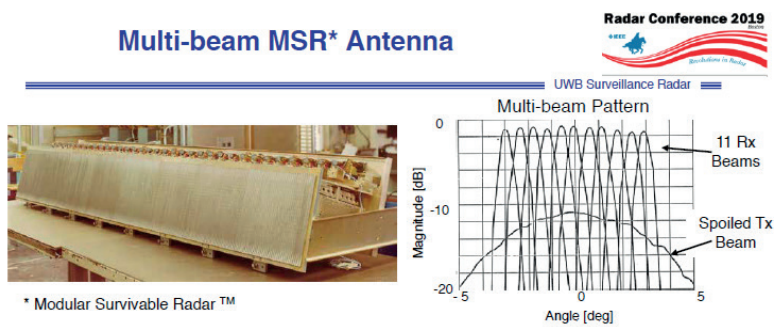


Figure 10.

Main parameters of the traditional and UWB radar waveforms [4]

Figure 11 shows one of the first UWB phased array antenna structure.



- Ku-band Multi-beam Antenna developed c.a. 1983 for AFWAL/DARPA to demonstrate potential for new Surveillance Radar Capabilities
- 256 Column Radiators with 32 Subarrays at RF, and Down Conversion to L-band for Analog Beam Forming
- Electronic Scan over +/- 60 degrees with 8-bit Ferrite Phase Shifters
- Transmit Beam spoiled with Quadratic Phase across Array
- 11 Separate Multiple Σ and Δ Beams Forrned with IF Beam Former
- Flight demonstration with GE Modular Survivable Radar

Figure 11.

UWB phased array with different type Receive and Transmit diagrams [4]

The UWB Radar Spectrum Compliance is the most challenging task to be solved and it is a good example for Spectrum Sharing requirement managements of other radar systems such as automobile radar and its communication systems.

Radio Frequency Interference has an impact on Radar Imaging as shown in Figure 12, where the received data streams are corrupted heavily.

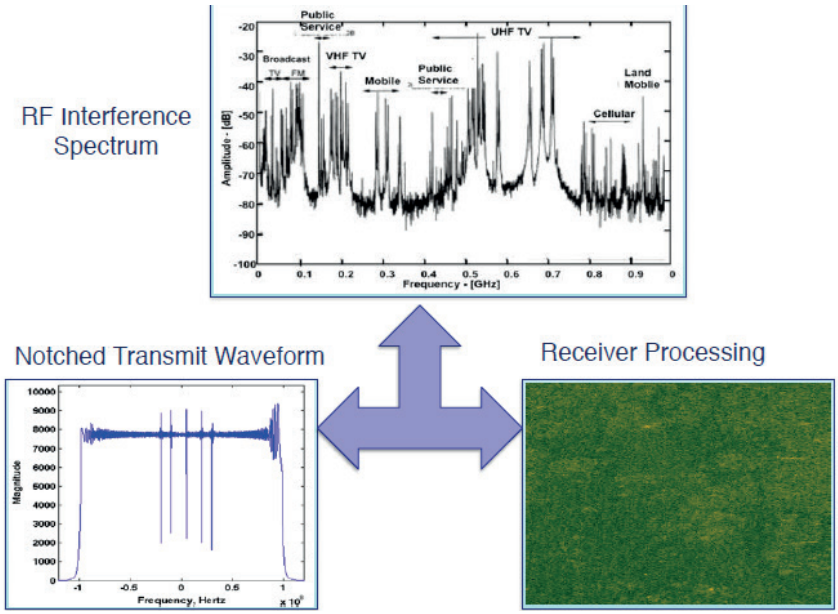


Figure 12.

Heavily corrupted SAR image due to local interference (The author's modification based on [4])

The tasks are connected to interference spectrum reduction or UWB Spectrum Sharing which are an emerging task for radar users that requires some preliminary studies. The National Telecommunications and Information Administration (NTIA) is an agency of the United States Department of Commerce and it is the governing body for any system that transmits. We have similar definitions and regulations in Europe. Restricted Bands are a Potential Interference to Sensitive Radio Communications such as Aircraft Radio Navigation, Radio Astronomy and Search and Rescue Operations. Figure 13 summarises the key requirements.

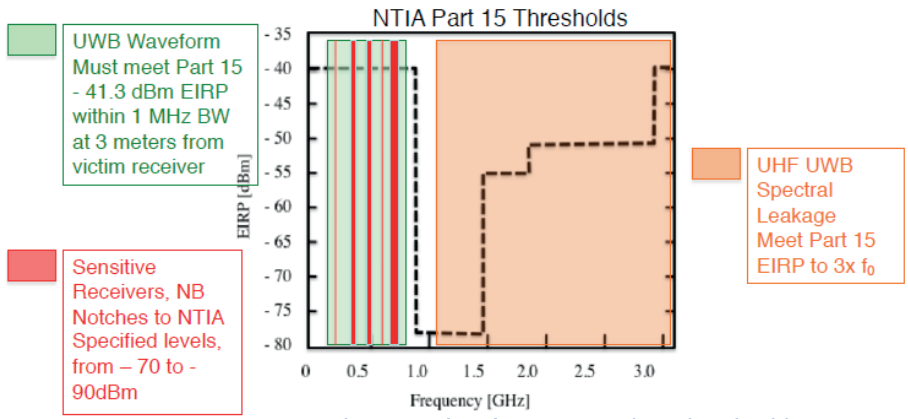


Figure 13.
The NTIA Requirements of the U.S. on UWB Waveforms (The author's modification based on [4])

Selling off of radar spectrum is a significant issue , which requires much more attention and inter-service coordination, than in the past, among radar service providers and governing bodies. The Radio Frequency Interference Removal could be solved or reduced significantly at the radar side by the Adaptive Transversal Filter and Adaptive LMS Processing.

Dr. Mark E. Davis's Tutorial ended with the following conclusion:

- Moving Target Indication (MTI) exploits Target DOPPLER to separate from:
  - Main beam clutter spread
  - Fast radar platform or low frequency complicates GMTI detection
- STAP technology demonstrated for moderate bandwidth GMTI:
  - Target motion through range and DOPPLER cells makes adaptive
  - Weights less effective
  - Wideband operation for high resolution moving target imaging
  - Requires multiple parallel STAP cancellation processes
- Along track interferometry enables detection and geolocation of:
  - Slow moving targets
  - ATI phase enables repositioning of moving targets in SAR image
  - Phase centre baseline creates DOPPLER ambiguities
- Continued research in simultaneous SAR and GMTI needed

Radar and Communication Systems Spectrum Sharing [5]

The importance of the subject is highlighted by the fact that one tutorial and four sections have been focused on it such as: Daniel W. Bliss, Arizona State University, had a Tutorial on: RF Convergence – Joint Communications and Radar Spectrum/

Communications and Radar Spectrum Sharing RF Convergence. Special Session on Dynamic Spectrum Interactions between Radar and Communication systems; Spectrum Sharing and Automotive and Commercial Radar.

Professor Bliss pointed out in his tutorial that there are potential performance advantages availed by joint operations such as both logistical benefits of RF system reuse, and some interesting system benefits by having access to more sophisticated RF topologies. It is likely to be a significant growth in commercial interest in these joint systems, because of the quickly falling costs of RF systems and a growing range of non-traditional applications. Figure 14 indicates the challenges of the Spectrum Sharing.

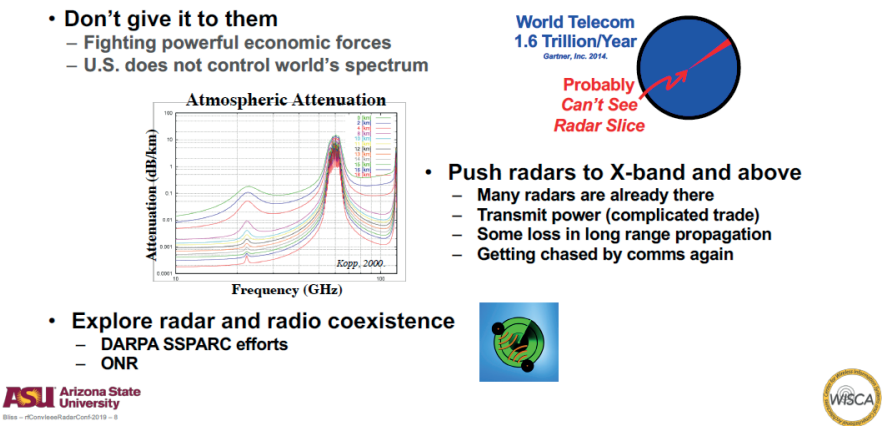


Figure 14.

Potential solutions from traditional radar perspective [5]

Figure 15 is an example for optimizing joint radar and communications operation.

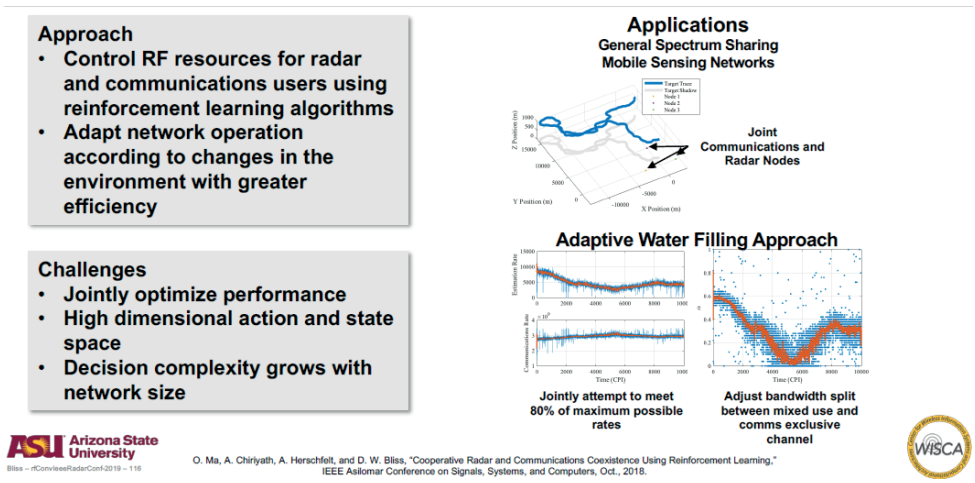


Figure 15.

Reinforcement learning of spectrum sharing [5]

The joint communications and radar systems may be the first examples of truly cognitive RF networks which have been illustrated in Figure 16 by Professor Bliss.

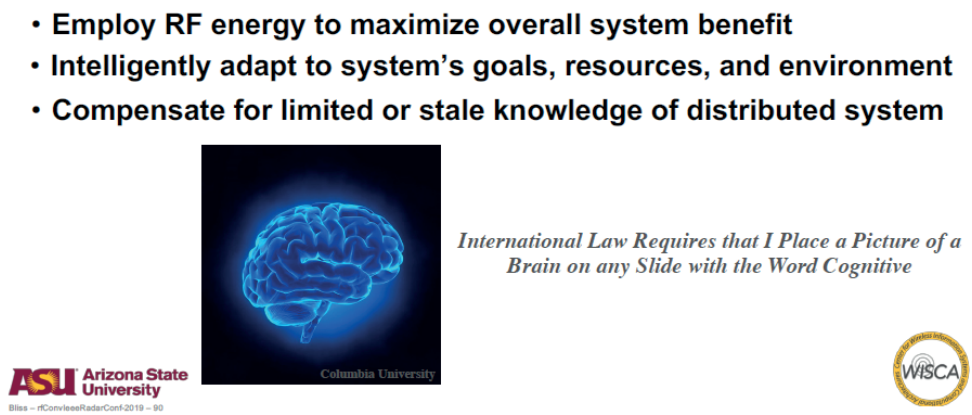


Figure 16.
The "Real" Cognitive RF System [5]

The paper of Mate Toth, Paul Meissner, Alexander Melzer and Klaus Witrisal entitled *Performance Comparison of Mutual Automotive Radar Interference Mitigation Algorithms* gives a comprehensive framework for the comparative analysis of automotive radar interference mitigation algorithms. A simulation methodology is developed with the general performance measures which are suitable for a statistical performance analysis. The paper concludes that "ramp filtering performs very well in terms of interference suppression, but strongly alters the RD map and the object peak value in the process, which is not the case for time domain methods" [6].

The article of Cenk Sahin, Patrick M. McCormick, Justin G. Metcalfy and Shannon D. Blunt entitled *Power-Efficient Multi-Beam Phase-Attached Radar/Communications* is important because it shows that the introduced combined approach is capable of transmitting independent data streams in multiple spatial directions (up to the number of antenna elements) simultaneously, including in the radar mainbeam, achieving a rate on the order of the time-bandwidth product times the PRF (Pulse Repetition Frequency) per stream [7].

PhD students from the University of Luxemburg, Sayed Hossein Dokhanchi, M. R. Bhavani Shankar, Kumar Vijay Mishra, Thomas Stiftery and Bjorn Ottersten got the student paper prize for Performance Analysis of mmWave Bi-static PMCW-based Automotive Joint Radar-Communications System. They propose a millimetre-wave joint radar-communications (JRC) system that employs a single waveform for its constituent bi-static automotive radar and vehicle-to-vehicle communications. The suggested radar and communications multiplexing strategies are to improve the parameter identifiability with limited set of measurements. The introduced super-resolution algorithm in conjunction with unique multiplexing methods offers a low-complexity receiver processing with enhanced performance that is imperative to any JRC system [8]. This paper proves also that the quality of the radar related

university studies could be increased with permanent effort and smart, enthusiastic students and professors.

Presentations which were in the scope of our interest at the conference

Three plenary speakers started the Technical Programs. The first speakers were Professor David McLaughlin, University of Massachusetts and Michael Dubois from Raytheon with their contribution entitled *Dense Networks of Short-Range Radars.* Their opinion that introduce the potential for using dense networks of small, low power, collaborative short range (tens of kilometres) X-band radars as a supplement – or perhaps as an alternative – to today's long-range radars has been studied over the past decade and has gained some support in the audience [9]. However, a few experts' opinion is that the combined passive radar networks with the combination of the automotive radar and communication potentials will be the future of dense radar systems solutions.

The second Plenary Speaker was Mark Markel from Waymo with his contribution entitled *Self-Driving Vehicles, and Radar Opportunities.* He emphasised the concept that the self-driving cars could be a potential solution to improve the quality and safety of our mobility. The concept offers an attractive option of other sensors in weather. The findings of the Google's Self Driving Car Project (now Waymo) were introduced [10].

The next Plenary Speaker was Dr. Jian Wang, his contribution entitled *Project Soli: Pico-Radar System for Ubiquitous Gesture Sensing* also dedicated to Google. The team developed the physical radar, including circuitry and antennas, to a single chip, while robustly tracking and recognising complex and fine gestures at close range with sub-millimetre accuracy. The SWaP-C of the chip is optimised to be readily adopted by most consumer electronics such as watch. Most of the audience accepted the speaker's opinion that: "The success of Project Soli will not only revolutionize the way we interact with electronic devices, but also create a brand-new market for radar technology and give it new life in consumer world – a new era for radar" [11].

Findings on Passive Radar systems

The most active nation in this topic was Poland. Professor Mateusz Malanowski, Piotr Samczyński and Professor Krzysztof S. Kulpa, Warsaw University of Technology, had a tutorial entitled *Passive Radar – From Detection to Imaging* [12] and several presentations. The main message of their presentation was that the universities and economy of Poland has reached that level in the field of Passive Radar technology when their experts are able to design, fabricate and implement multistatic passive radar for target detection and imaging with various possible illuminators of opportunity (e.g. FM radio, digital television, cellular telephony), and features of different signals from the point of view of radar detection. The most advanced radar network concept of Deployable Multiband Passive/Active Radar was presented, in which a combination of active and passive radars is used. Figure 17 shows one Passive Radar Unit of Poland under construction.

Figure 17.
Passive Radar Unit of Poland [12]

Martin Ummenhofer, Michael Kohler, Jochen Schell and Daniel O'Hagan: *Direction of Arrival Estimation Techniques for Passive Radar Based 3D Target Localization,* Fraunhoferstraße, Germany [13]. It presents a comparative analysis of direction of arrival (DOA) estimation techniques for the application in a linear antenna array of a Passive Bistatic Radar (PBR). The viability is demonstrated with experimental data obtained from a field trial with a PBR that exploits illuminations by the digital transmissions standard DVB-T2. This in conjunction with the system's DOA capability allows to accurately estimate 3D positions of air targets within the controlled traffic region.

The paper proves that the low TDOA estimations based on the illumination by network of transmitters in conjunction with the direction-finding capability of the linear array can be exploited for target localisation in 3D Cartesian coordinates. Further studies are required, because the low altitude of 3D measurement is problematic not only for long range 3D surveillance radars but for passive radar systems, too. The topic has got some attention to investigate further the beam position caused elevation angle measurement degradation.

Clément Berthillot, Agnès Santori, Olivier Rabaste, Dominique Poullin and Marc Lesturgie from France published the results on: *DVB-T Airborne passive radar: Clutter Analysis and Experimental Results* [14]. In this context, the difference between airborne and ground passive radar is reviewed by the authors. The first difference lies in the aeronautical channel, which requires the reference signal reconstruction from decoding the transmitted DVB-T signal. The receiver mobility emphasises the necessity of Doppler mask oversampling to mitigate rejection artefacts due to multipath Doppler

mismatch with the analysis grid. Figure 18 shows the RIVERA (aiRborne passIVE RAdar) passive radar on the BUSARD plane with the RIVERA receiver configuration.

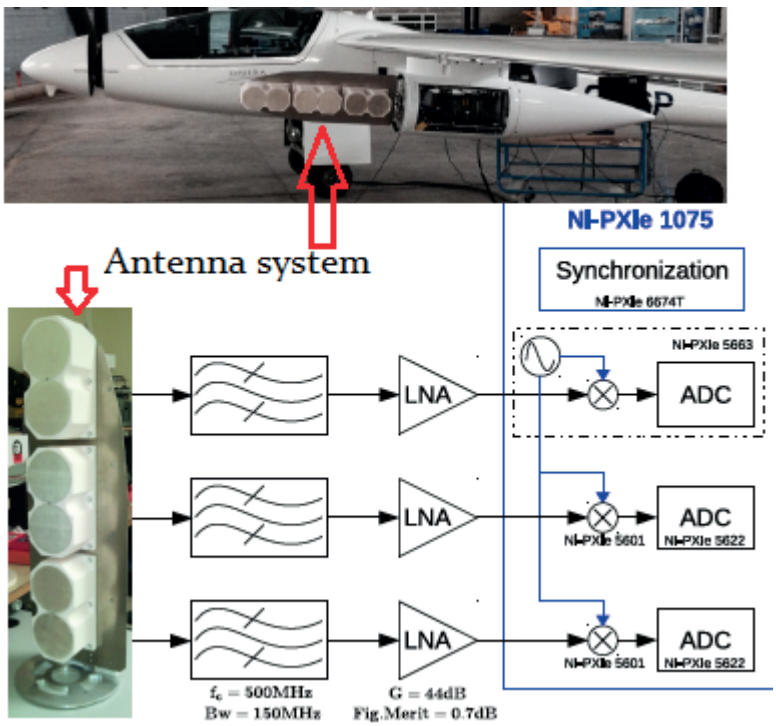


Figure 18.
RIVERA radar and its receiver configuration (The author's modification based on [14])

RIVERA radar has been developed and qualified, which gives a solid basis for meaningful experimental data collection, to understand the impact of the propagation channel on the reference signal and to strengthen the understanding of the clutter spread. The next challenging step to further enhance detection capacities of airborne passive radars is the mitigation of the significant clutter power which is largely spread in the Doppler dimension and along the range axis.

Brent H. Gessel and James R. Lievsay: *Three-Dimensional Emitter Selection Optimization,* Air Force Institute of Technology [15]. The paper introduces the primary concepts in passive radar and STAP that directly impact the performance of three-dimensional emitter selection optimisation for Passive GMTI. It is important, because ground moving target indication (GMTI) from an airborne platform and emitter selection requires more than just distance calculations to achieve optimal performance. The authors highlight the importance of bistatic angles, target and clutter characteristics, and emitter waveform properties as tuneable parameters that can change the course of emitter selection. The final result of the genetic algorithm tool is shown in Figure 19. The receiver's (red diamonds) position is optimised

against a target (first value next to the diamond) with the optimised tower to pair with (second number next to the diamond). The targets, yellow circles, are labelled 1–25. The transmitters, green stars, are randomly placed and labelled 1–7.

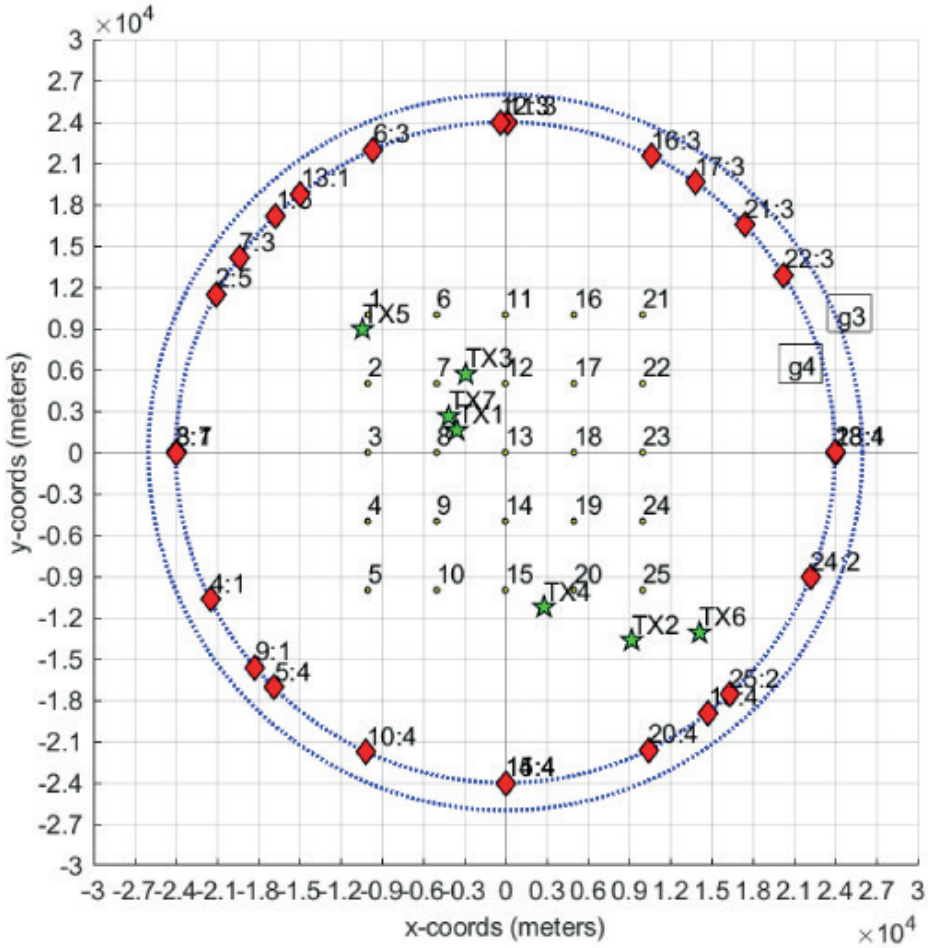


Figure 19.
The graphic displays the final result of the study [15]

Volker Winkler, Dietrich Fränken, Christian Erhart, Oliver Zeeb and Steffen Lutz: *Multistatic Multiband Passive Radar – Architecture and Sensor Cluster Results,* Hensoldt Sensors. The system architecture and relevant system components like the antenna, the receiver and the multi-hypothesis tracking system are introduced [21]. Figure 20 indicates the target tracking of a helicopter (marked blue) and some airliner targets (marked green) of opportunity. False targets due to the rotor blade echoes (red) are suppressed by an algorithm in the tracking system. A sensor cluster on various frequency bands offers a tremendous passive radar performance, which

will address new applications and fulfilment of customer demands for military surveillance, support of Ground Based Air Defence and civil ATC. The applied multi hypothesis tracking offers a tracking performance which is comparable to active radars, feasible of handling more than 100 targets in a single tracker. In multistatic cluster configurations, the system is feasible to handle up to 4 sensors in a cluster integrated in a multi hypothesis tracking system. In such a configuration, the coverage of large areas would be possible and the system will be able to support nationwide air surveillance programs like the U.S. Sensor program.

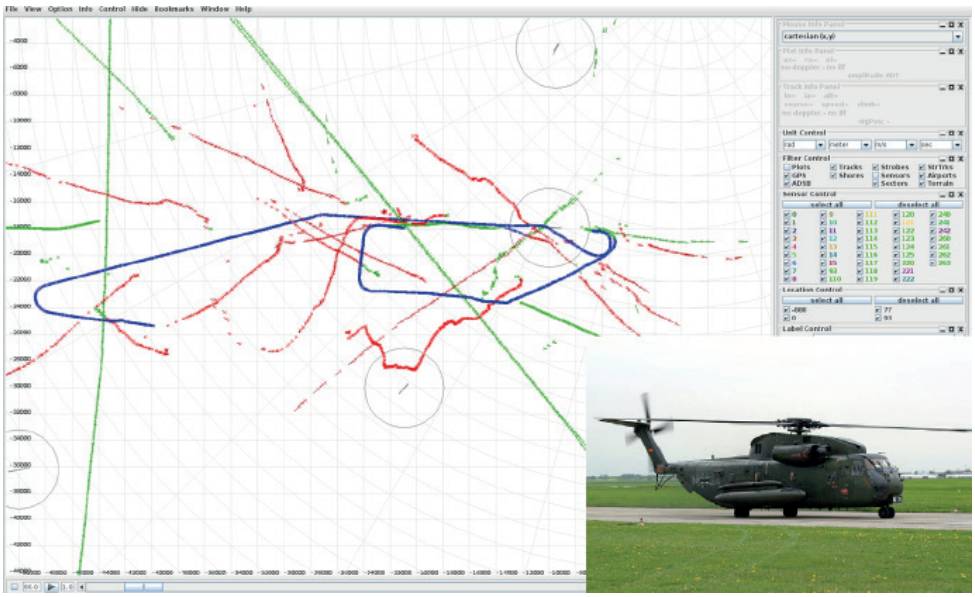


Figure 20.
Target tracking of a helicopter [21]

Findings on bistatic and multistatic radar

De-ping Xia, Liang Zhang, Tao Wu and Xiang-dong Meng: *A Mainlobe Interference Suppression Algorithm Based on Bistatic Airborne Radar Cooperation,* China. The approach based on a bistatic radar system and mainlobe interference is suppressed through the cooperation of the two radars. A functional block diagram of the cooperated bistatic radar system is shown in Figure 21 [16].

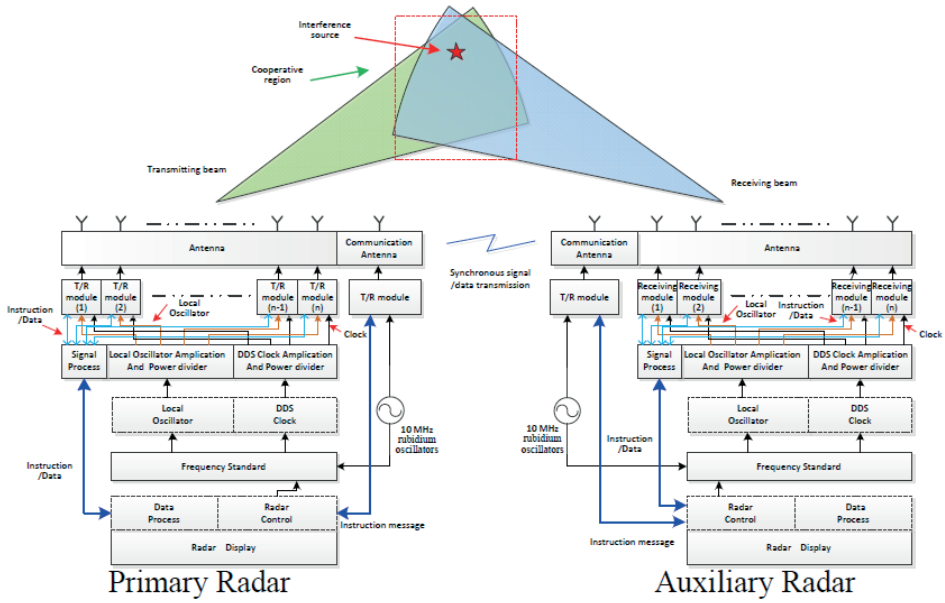


Figure 21.

Mainlobe interference suppression based on bistatic radar cooperation [16]

The radar at left acts as the primary radar, playing the role of transmitter and receiver, while the other acts as the auxiliary radar, acting as a receiver. A pair of 10 MHz rubidium clock oscillators provides stable phase and reference signals for the local oscillator and pulse timing signals within the major transmitter and the second receiver system, as shown. Synchronisation and data transmission of the two radars is realised through broadband communication links. The red pentagram indicates the region of interference. The system specifications for this radar are summarised in Table 1.

Table 1.

Bistatic airborne radar specification [16]

Characteristics	Primary Radar Specification	Auxiliary Radar Specification
Carrier frequency	1.25 GHz	1.25 GHz
Pulse Repetition Frequency	1,000–8,000 Hz	1,000–8,000 Hz
Pulse-width	12–100 μs	
Peak output power	1 kW	
Transmitter/Receiver number	48	48
Signal bandwidth	5 MHz	
Antenna Beamwidth Tx.	2.9 deg.	
IF bandwidth		130 MHz
IF sample frequency		100 MHz
Noise figure		3 dB

Characteristics	Primary Radar Specification	Auxiliary Radar Specification
Antenna Beamwidth Rx.		3.4 deg.
Polarisation	Horizontal	Horizontal

The simulation is based on MUSIC estimation algorithm. Numerical examples show that the mainlobe interference is effectively restrained, and clear improvements in the Signal Interference Noise Ratio (SINR) are demonstrated.

John Summerfield and Dayalan Kasilingam: *Narrowband Bistatic Synthetic Aperture Radar Ambiguity Function Analysis and Design using Angular Harmonics* [17]. In order to develop new BSAR applications, new tools are needed to describe imaging performance for any bistatic collection geometry. The point spread function (PSF) and the associated ambiguity function (AF) fully describe coherent imaging performance but they are nonlinear and spatially variant that makes them difficult to use as a design tool. To overcome this spatially variant limitation and nonlinearity, a convolutional back projection kernel (CBPK) technique is used. The CBPK was transformed into a Fourier series domain in order to decouple the waveform spectrum from the collection geometry such as the pseudo monostatic geometry. Figure 22 shows the Bistatic Range Signature correction principle. Further research is required in the field of multi-static simultaneous transmit and receive system for finalising the work.

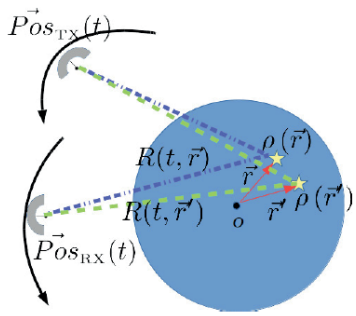


Fig. a. A graphical representation is shown of the bistatic range signature $R(t,\vec{r})$ defined as the instantaneous path length from the transmitters position $\vec{Pos}_{TX}(t)$ to position $\vec{r}$ to the receivers position $\vec{Pos}_{RX}(t)$.

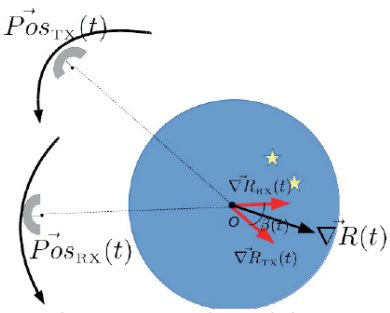


Fig. b. A graphical representation is shown of the bistatic range gradient $\nabla\vec{R}(t)$ defined as the vector sum of the transmitter line of sight vector $\nabla\vec{R}_{TX}(t)$ with the receiver line of sight vector $\nabla\vec{R}_{RX}(t)$. The length of the bistatic range gradient depends on the bistatic angle $\beta(t)$, the angle between the platform line of sight vectors $\nabla\vec{R}_{TX}(t)$ and $\nabla\vec{R}_{RX}(t)$.

Figure 22.
Bistatic Range Signature correction principle [17]

Findings on Electronic Attack (ECM)/Electronic Protection (ECCM)

Taniza Roy, Neha Agarwal, Lgm Prakasam: *Digital Implementation of Electronic Counter Counter Measure Features in Radar Transmitter,* India [18]. The digital implementation of Electronic Counter Counter Measure (ECCM) techniques are employed as part of radar transmitters. Digital implementation of realisation measures such as Pulse Repetition Frequency jitter, waveform coding, frequency diversity, least jammed frequency computation and different modes have been explained. Design methodology of each

module has been explained and hardware realisation presented. Figure 23 shows the timing diagram of the Directional Jamming Analysis module. The design has been used in ground-based radar systems and the performance in field has been found satisfactory as per radar requirement.

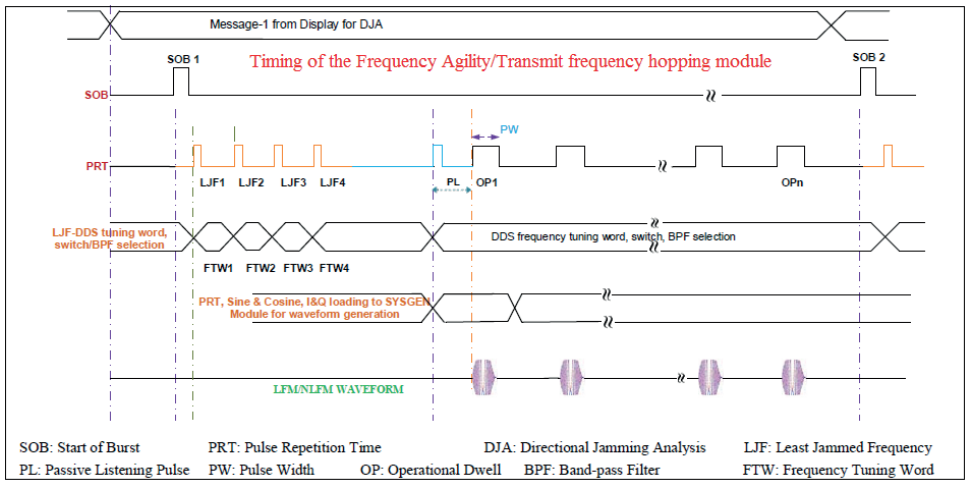


Figure 23.
Timing of the Directional Jamming Analysis/Frequency Agility module [18]

Robert Achatz: *Method for Evaluating Solid State Marine Radar Interference in Magnetron Marine Radars,* Institute for Telecommunication Sciences, National Telecommunications and Information Administration, USA [19]. The goal of the paper is to support the development of the interference protection criteria (IPC) and the corresponding minimum separation distance (MSD) for a specific frequency separation between radars which are operating in the same region with Solid State and Magnetron type transmitters. The simulation method was developed with in-situ field measurement data collection. Both results analyses were completed for combinations of short, medium, and long-range operation, filter settings, 55 and 135 MHz frequency separation between the Magnetron and Solid State type radars. Replicating the field test results was successful when the researchers set the Magnetron operating in short range or operating in medium-range with the short-range detection filter bandwidth. More comprehensive comparisons between method and field test results are needed to fully understand the method's predictive efficacy.

John Kota, Charles Topliff, Ravi Prasanth, Greg Ushomirsky and Stephen Kogon: *Radar Waveform Design Using Lagrangian Dynamics for Co-Channel Interference Mitigation,* Systems and Technology Research, Sensors and Signal Processing Group, USA [20]. A novel radar waveform phase function design is presented that constructs a radar waveform that spectrally manoeuvres around in-band co-channel interference (CCI) from active communications users that are co-channel with the radar system. The suggested design approach treats the CCI problem as the physical interpretable problem of optical refraction where the Time–Frequency (TF) signature of the radar

waveform is made to be analogous to a light ray propagating from a start time and position (frequency) to an end time and position (frequency). The radar waveform design will generally result in a nonlinear-frequency modulated (NLFM) waveform that provides improved SINR. Figure 24 plots plot of interference Power Spectral Density PSD (blue) for two interference sources, radar Instantaneous Bandwidth (IBW) (dotted yellow), and GMM refraction model (green). The interference consists of two OFDM model users occupying approximately 8.37% of the radar IBW and a single narrowband tone.

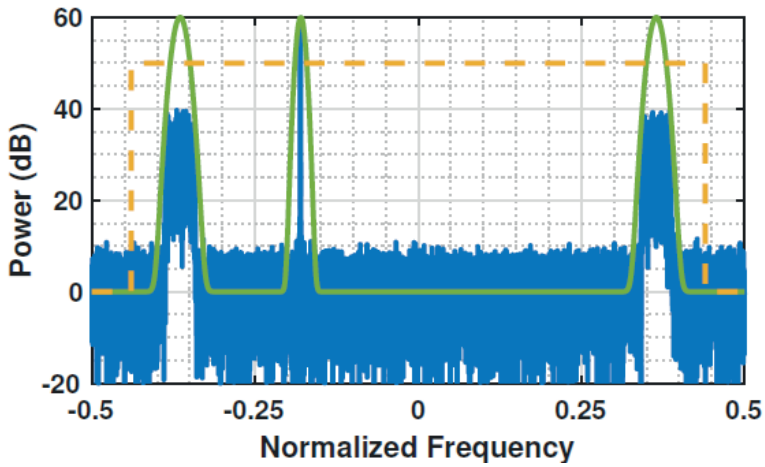


Figure 24.
Power Spectral Density of the interference [20]

Figure 25 compares the radar waveforms: (left) ideal TF signature for LFM and designed NLFM waveforms, (right) radar waveform power spectral density.

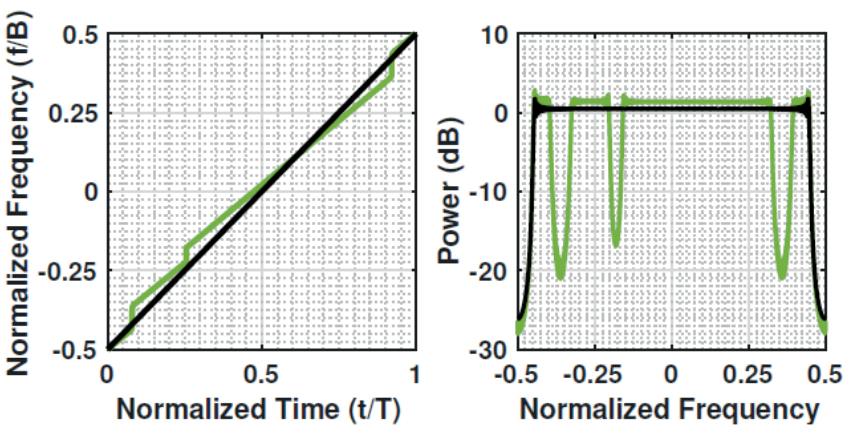


Figure 25.
Comparison of the radar waveforms [20]

A future work is planned for designing a cooperative CCI reduced communications spectral location. For achieving this, a joint radar and communications design that enables simultaneous sharing the RF spectrum will be presented.

Conclusion

The paper presents a selective review of the most remarkable radar topics, papers of the conference, all which captured the attention of this paper's author. He would like to kindly draw the reader's attention to the fact that radar technology is growing fast from the monostatic radar solutions to the radio signal fuzzed network centric solutions. This happens, because the radar measurement's degree of freedom has to be extended in space, frequency and polarisation, due to new customer needs such as automobile radar, civilian air traffic control, the growth of safety requirement and advanced military requirements.

The fast-growing computer and IT technology, the Spectrum Sharing Techniques between radars and communication systems, are essential parts of the modern Bistatic and Multistatic radar, Passive radar systems, Weather radar with Emerging Quantum and photonics-based radar solutions. The radar system-related Electronic Warfare techniques and tactics are advancing from the achievements of the current, above-mentioned state of the art technologies, while the radar performance measures could be supported and maintained for life-time cycle of the sensors, and they shall be part of the modern radar networks.

References

[1] 2019 IEEE Radar Conference Program, Boston, 22–26 April 2019, Proceedings of Revolution in Radar and Tutorial Material. [Online]. Available: www.radarconf19.org [Accessed Aug. 21, 2019].

[2] L. Lo Monte, "Radar Systems Prototyping," Tutorial, Telephonics Co. USA, Proceedings of Revolution in Radar and Tutorial Material.

[3] K. E. Kolodziej, P. J. Bell, A. J. Fenn, E. Kowalski, J. W. Meklenburg, W. F. Moulder, J. S. Mullen and B. T. Perry, "Radar Summer School: Built-A-Radar at MIT," USA, Proceedings of Revolution in Radar and Tutorial Material.

[4] M. Davis, "Ultra-Wideband Surveillance Radar," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835510

[5] D. W. Bliss, "Communications and Radar Spectrum Sharing RF Convergence," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835827

[6] M. Tóth, P. Meissner, A. Melzer and K. Witrisal, "Performance Comparison of Mutual Automotive Radar Interference Mitigation Algorithms," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835681

[7] C. Sahin, P. M. McCormick, J. G. Metcalfy and S. D. Blunt, "Power-Efficient Multi-Beam Phase-Attached Radar/Communications," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835583
[8] S. H. Dokhanchi, M. R. B. Shankar, K. V. Mishra, T. Stiftery and B. Ottersten, "Performance Analysis of mmWave Bi-static PMCW-based Automotive Joint Radar-Communications System," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835577
[9] D. McLaughlin and M. Dubois, "Dense Networks of Short-Range Radars," Plenary Speaker, University of Massachusetts, Raytheon Co., USA, Proceedings of Revolution in Radar and Tutorial Material.
[10] M. Markel, "Self-Driving Vehicles, and Radar Opportunities," Waymo Co., USA, Proceedings of Revolution in Radar and Tutorial Material.
[11] J. Wang, "Project Soli: Pico-Radar System for Ubiquitous Gesture Sensing," USA, Proceedings of Revolution in Radar and Tutorial Material.
[12] M. Malanowski, P. Samczyński and K. S. Kulpa, "Passive Radar – From Detection to Imaging," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835658
[13] M. Ummenhofer, M. Kohler, J. Schell and D. O'Hagan, "Direction of Arrival Estimation Techniques for Passive Radar Based 3D Target Localization," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835841
[14] C. Berthillot, A. Santori, O. Rabaste, D. Poullin and M. Lesturgie, "DVB-T Airborne passive radar, Clutter Analysis and Experimental Results," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835763
[15] B. H. Gessel and J. R. Lievsay, "Three-Dimensional Emitter Selection Optimization," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835715
[16] D. Xia, L. Zhang, T. Wu and Xiang-dong Meng, "A Mainlobe Interference Suppression Algorithm Based on Bistatic Airborne Radar Cooperation," China, Proceedings of Revolution in Radar and Tutorial Material. DOI: https://doi.org/10.1109/RADAR.2019.8835562
[17] J. Summerfield and D. Kasilingam, "Narrowband Bistatic Synthetic Aperture Radar Ambiguity Function Analysis and Design using Angular Harmonics," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835524
[18] T. Roy, N. Agarwal and L. Prakasam, "Digital Implementation of Electronic Counter Counter Measure Features in Radar Transmitter," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835698
[19] R. Achatz, "Method for Evaluating Solid State Marine Radar Interference in Magnetron Marine Radars," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835684

[20] J. Kota, C. Topliff, R. Prasanth, G. Ushomirsky and S. Kogon, "Radar Waveform Design Using Lagrangian Dynamics for Co-Channel Interference Mitigation," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835710

[21] V. Winkler, D. Fränken, C. Erhart, O. Zeeb and Steffen Lutz, "Multistatic Multiband Passive Radar – Architecture and Sensor Cluster Results," In Proc. of 2019 IEEE Radar Conference (RadarConf), Boston, USA, 2019. DOI: https://doi.org/10.1109/RADAR.2019.8835688

HADMÉRNÖK
VÉDELMI INFORMATIKA

15. évfolyam (2020) 1. szám 159–182.
DOI: 10.32567/hm.2020.1.11

Paráda István,[1] Farkas Tibor[2]

Felderítés és analízis a penetrációs tesztben – 1. Információgyűjtési technikák

Reconnaissance and Analysis in the Penetration Test 1 Information Gathering Techniques

Jelen cikksorozat a penetrációs tesztek szakaszán belül a felderítés és analízis szintjeinek bemutatásával foglalkozik. Az egyik alapvető szemlélet szerint a kiberműveletekben és informatikában vett penetrációs tesztek felderítési és analízisszintjén lévő információgyűjtési tevékenységek azonosítják (kockázati szinten) a szervezetekhez kapcsolódó, nyilvánosság számára hozzáférhető információkat. Az információgyűjtés a penetrációsteszt-végrehajtás lépésének első szakasza, amely a célhálózatról és célkörnyezetről való információk begyűjtését takarja. Az információgyűjtési technikákat használva számos lehetőség nyílik a célszervezet hálózatának illetéktelen hozzáférésére. Ennek segítségével létrehozható egy biztonsági profil a célszervezet hálózatáról, rendszeréről és részben magáról a szervezetről is. Nincs egységes módszer az információgyűjtésre, hiszen azok számos módon beszerezhetők. Viszont a lehető legtöbb információt be kell gyűjteni, így érdemes ezt a fázist szervezett módon végrehajtani [1].

Kulcsszavak: **információgyűjtés, keresőmotorok, DNS, WhoIs**

This series of articles deals with the detection and analysis levels within the penetration tests section. One basic approach is that information gathering activities at the detection and analysis level of penetration tests in cybersecurity and information technology (at risk level) identify publicly available information related to organisations. Gathering information is the first step in the penetration test implementation process, which involves gathering information about the

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: paradaistvan@gmail.com, ORCID: https://orcid.org/0000-0002-3083-6015

[2] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, egyetemi docens, e-mail: farkas.tibor@uni-nke.hu, ORCID: https://orcid.org/0000-0002-8868-9628

target network and target environment. Using information gathering techniques, there are many opportunities for unauthorised access to the target organisation's network. This allows you to create a security profile of the target organisation's network system, and partly the organisation itself. There is no standard way to collect information, as there are many ways to obtain it. However, as much information as possible must be collected, therefore, it is worthwhile to carry out this phase in an organised manner.

Keywords: **information gathering, search engines, DNS, Whois**

Bevezetés

Az információgyűjtés a penetrációsteszt-végrehajtás lépésének első szakasza, amely a célhálózatról és célkörnyezetről való nyilvános információk begyűjtését takarja, informatikai és informatikához kapcsolódó technikákon, módszereken keresztül. Az információgyűjtés e cikkben taglalt része magában foglalja a kibertéri műveletek közül az elektronikai felderítés OSINT[3]-fajtáját, amely a széles körben hozzáférhető, nyílt adatforrások felhasználásával gyűjt adatokat, illetve a számítógéphálózati műveletek felderítés fajtáját. „A számítógép-hálózati felderítés a hálózatok struktúrájának feltérképezését, az adatbázisokhoz való illetéktelen hozzáférést és a támadható pontok meghatározását jelenti. Megvalósulhat a szemben álló fél számítógépes rendszereibe való szoftveres vagy hardveres úton való behatolással. Célja az adatbázisokban tárolt adatokhoz, információkhoz való hozzáférés és azok felderítési céllal való hasznosítása, illetve a későbbi károkozással járó támadás kivitelezéséhez a hálózat támadható pontjainak és a támadás leghatékonyabb formáinak meghatározása. A felderítés az elszenvedő hálózat részéről általában nem észlelhető formában valósul meg, így a hálózat üzemeltetője és felhasználója számára a felderítés ténye többnyire nem ismert" [2].

A cikk egy lehetséges penetrációsteszt-módszertan felderítés és analízis első szintjének bemutatásával foglalkozik, ahol még nem feltétlenül a technikai megvalósításokon van a hangsúly, sokkal inkább a kibertér hatásáról a társadalomra, cégekre, nemzetekre. Ezeknek a hatásoknak és magának az információs társadalomnak a következményeként írhatunk olyan technikákat, olyan eljárásokat, amelyek magukban foglalják a penetrációs teszt módszertanának információgyűjtési egységét.

[3] Az OSINT (Open Source Intelligence) a nyílt forrású hírszerzés nemzetközileg is elfogadott angol nyelvű rövidítése. Az OSINT fő forrásait a NATO OSINT kézikönyve a következők szerint határozza meg:
nyomtatott és elektronikus média;
internet, beleértve a láthatatlan web információit;
kereskedelmi (fizetős) online szolgáltatók tanulmányai, adattárai;
„szürke irodalom", azaz nem publikált, de nem is minősített, szűk körben hozzáférhető, nyomtatott és digitális dokumentumok, tanulmányok;
személyes tapasztalatok;
kereskedelmi műholdak felvételei. Ezek pontossága a 21. században gyakran megközelíti a katonai műholdak teljesítményét;
tudományos kutatószervezetek, egyetemek.

Felderítés- és analízisszintek:

- Információgyűjtés;
  - A közzétett adatok elemzése;
    - információgyűjtés keresőmotorok segítségével,
    - információgyűjtés webszolgáltatásokon keresztül,
    - weboldal-információgyűjtés,
    - e-mail-információgyűjtés.
  - Alapvető hálózati információk lekérdezése;
    - WhoIs,
    - DNS-információk kibontása.
- Hálózat-feltérképezés;
  - célpontfelfedés,
  - Port Scan,
  - OS-ujjlenyomat,
  - hálózatiforgalom-elkapás, lehallgatás.
- Sérülékenység elemzése és értékelése.

Ahhoz, hogy a cikkben kontextusba tudjuk helyezni a bemutatni kívánt információgyűjtési metódusokat, gyakorlatokat és felkínált végrehajtási lehetőségeket, definiálni kell magát a tevékenység hatókörét, ami nem más, mint a kibertér. „Kibertér: felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva” [3]. Ebből kiderül, hogy mivel sokféle elemet érintő, dinamikusan változó tartományról beszélünk, a benne végrehajtható információgyűjtés is több síkon értelmezhető. Például nyilvános adatok összegyűjtésének emberközpontú, emberi kapcsolati nézőpontjából vizsgálva vagy szervezeti, illetve intézményi szempontok alapján, valamint ezek technikai oldalú megközelítésén keresztül.

A közzétett adatok elemzése

A kiberműveletek képességein belül a számítógép-hálózatokba való bejutást, azok felderítését, az adatbázisokhoz való hozzáférést, azok módosítását, tönkretételét, a távközlési hálózatok lehallgatását a közzétett adatok elemzésével érdemes kezdeni.

Az információgyűjtés-módszertan egy eljárás a célszervezettel kapcsolatos információk gyűjtésére az összes kibertérben rendelkezésre álló forrásból. A közétett adatok elemzése megmutatja a célszervezettel kapcsolatos információkat, mint például az URL[4] helyét, a telephely adatait, az alkalmazottak számát, a domainnevek konkrét tartományát, elérhetőségi adatait és egyéb kapcsolódó információkat. Itt nem feltétlenül technikai információk begyűjtése a cél, inkább a keresési mechanizmus legjobb hatásfokkal való alkalmazása [4].

[4] Az URL (*Uniform Resource Locator* [egységes erőforráshely] rövidítése), az interneten megtalálható bizonyos erőforrások szabványosított címe.

Információgyűjtés keresőmotorok segítségével

Az internetes keresőmotorok a fő források a célszervezettel kapcsolatos kulcsinformációk megkereséséhez. A keresőmotorok kinyerhetik a célokról szóló információkat, beleértve például technológiai platformokat, alkalmazottak adatait, bejelentkezési oldalakat, intranetportálokat, elérhetőségeket és így tovább. Ezért fontos szerepet töltenek be a kritikus részletek felderítése terén, hiszen ezek a viszonylag egyszerűen kinyert információk képezhetik az alapját vagy előkészületét egy támadás indításának, egyfajta információs adatbázist képezhetnek, amelyből szükség esetén már összegyűjtve és nagyobb támadáshoz rendszerezve, előkészítve lehet meríteni a támadások támogatásához. Ez az információ segíti a támadót a social engineering[5] és más típusú támadások végrehajtásában. A keresési eredmények böngészései gyakran értékes információkat nyújtanak például a fizikai helyről, elérhetőségekről, a szolgáltatásokról, az alkalmazottak számáról és így tovább.

A támadók az ezekkel a keresőmotorokkal elérhető speciális keresési operátorokat használhatják, és létrehozhatnak kötelező lekérdezéseket a célhoz kapcsolódó információk keresésére, szűrésére és rendezésére. A keresőmotorokat más, a nyilvánosság számára hozzáférhető információforrások forrásainak keresésére is használják. Például beírható a „Legjobb munkaportálok" elem, olyan főbb munkaportálok kereséséhez, amelyek kritikus információkat nyújtanak a célszervezetről. A Google[6] hackelés mint kifejezés, a fejlett Google keresési operátorok használatára utal, hogy összetett keresési lekérdezéseket hozzon létre az érzékeny vagy rejtett információk kinyerésére. Ezután a támadók a hozzáférhető információkat a sebezhető célok felkutatására használják. Az információgyűjtés fejlett Google-hackelési[7] [9] technikákkal történő összegyűjtésével a Google a keresési eredmények speciális szövegrészeit egy speciális operátor és a Google keresőmotorja segítségével hajtja végre. Google-operátorok segítenek megtalálni a szükséges szöveget és elkerülni az irreleváns adatokat, azaz segítenek a keresési lekérdezés szűkítése és a legrelevánsabb és pontosabb output elérésében.

[5] A social engineering amikor egy jogosultsággal rendelkező felhasználó jogosulatlan személy számára bizalmas adatokat ad át, vagy lehetőséget biztosít a rendszerbe történő belépésre a másik személy megtévesztő viselkedése miatt.

[6] A Google LLC egy részvénytársaság, aminek a nevéhez fűződik a Google keresőmotor kifejlesztése és üzemeltetése.

[7] A Google Dorking egy nagyon egyszerű módszer annak ellenőrzésére, hogy vannak-e biztonsági rések az adott hálózaton vagy számítógépen. A meghatározás szerint a Google dork lekérdezés egy olyan string típusú keresés, amely fejlett keresési operátorokat használ olyan információk megkeresésére, amelyek nem érhetők el könnyedén a weboldalon. Ebbe a körbe olyan információk tartoznak, amelyeket nem a nyilvánosság számára szántak, de nincsenek megfelelően levédve. Passzív támadási módszer esetén a Google dorking segítségével a következő adatokat lehet megszerezni: felhasználónevek és jelszavak, e-mail-listák, érzékeny dokumentumok, gazdasági információk (PIFI) és az adott weboldal sebezhetőségei. Az egész legális.

1. táblázat

Főbb operátorok [5]

Egyszerű operátorok	Haladó operátorok
Filetype: • Csak a megadott kiterjesztésű (például PPT, pdf) fájlokat adja vissza a Google.	Allintext/intext: • Az allintext kifejezést a keresés elején kell használni. Csak olyan oldalakat fog visszaadni a Google, ahol a szövegben minden szó szerepel, ami az allintext után van írva.
Site: • Csak a megadott domainen belül fog keresni és találatokat adni. A „site" operátort ki lehet egészíteni kifejezésekkel is, és akkor csak az adott oldalon belül fog keresni a megadott kifejezésekre.	Intitle /allintitle: • Működése teljesen hasonló az intext/allintext pároshoz, annyi a különbség, hogy itt a keresés a címben történik.
Related: • Ennek az operátornak a segítségével meg lehet találni egy adott oldalhoz hasonló oldalakat. Fontos megjegyezni, hogy csak domainekkel és URL-ekkel működik, keresőszavakkal nem. Illetve, ha a kettőspont után szóköz kerül, akkor csak egy sima keresés lesz. Ez főleg angol nyelvű oldalak esetében működik jól.	Inurl/allinurl: • Az előző kettőhöz hasonlít ezeknek az operátoroknak is a működése, viszont itt a keresés az URL-ben történik.
Cache: • Ennek az operátornak a segítségével meg lehet nézni egy adott oldalnak a Google által utoljára eltárolt (cache-elt) változatát. Hasznos lehet olyan oldalak esetében, amelyeket már esetleg valamilyen okból töröltek.	Inanchor/allinanchor • Ennek a párosnak az esetében pedig a keresés a horgonyszövegekben történik.
Define: • A keresett kifejezésnek a definícióját dobja ki a Google. Csak angol kifejezések esetében működik.	
Location: • Akkor érdemes ezt az operátort használni, hogyha egy adott földrajzi helyre szűkítve történik a keresés.	

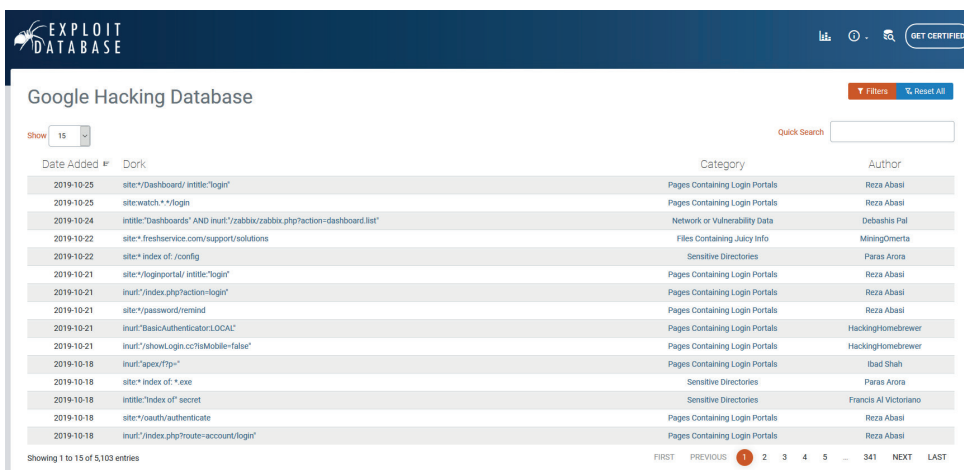
A támadó egyszerűen nem tud specifikus, részletes, mélyreható esetleg műszaki információt gyűjteni az információs oldalról, csak egy normál keresőmező segítségével, hiszen az rengeteg irreleváns információt is tartalmazna, amely nem teszi lehetővé a további hatékony feladatvégrehajtást. A bonyolult keresés számos egymással összefüggő feltételt érint. A Google speciális keresési funkciója segít a támadónak összetett internetes keresést végrehajtani. A Google Advanced Search és az AdvancedImage Search segítségével az interneten sokkal pontosabban lehet keresni. Ezeket a keresési funkciókat ugyanazon pontosság eléréséhez használhatja, ha fejlettebb operátorokat használ, de gépelés vagy emlékezet nélkül (1. táblázat).

A Google Hack-módszerek segítségével, egy esetleges támadó [3: 169–187.] összetett keresőmotor-lekérdezéseket hozhat létre a keresési eredmények nagy

mennyiségének szűrése érdekében. A támadók a Google-operátorokat használják, amelyek segítenek megtalálni az ilyen konkrét szövegsorokat a keresési eredmények között. Tehát egy támadó felfedezheti a kizsákmányolásra felhasználható webhelyeket és webes felhasználókat, valamint hozzárendeli őket a személyes, érzékeny információikhoz, például hitelkártyaszámok, szociális biztonsági számok, jelszavak és így tovább. Ha a kiszolgáltatott célt azonosítják, a támadók különféle lehetséges támadásokat próbálnak indítani, mint például puffer-túlcsordulások[8] és többek között SQL Injection.[9]

Ahogy az 1. ábra is mutatja, számos példa létezik a nyilvános kiszolgálókra hagyott érzékeny információkra, amelyeket a támadó a Google Hacking Database (GHOB) lekérdezéseivel kivonhat:

- érzékeny információkat tartalmazó hibaüzenetek;
- jelszavakat tartalmazó fájlok;
- érzékeny könyvtárak;
- a bejelentkezési portálokat tartalmazó oldalak;
- hálózati vagy sebezhetőségi adatokat tartalmazó oldalak;
- szerversérülékenységek;
- a szoftver verziószáma;
- webes alkalmazás forráskód.



1. ábra

Google hacking database [6], [10]

A keresőmotoros információgyűjtés napjaink egyik legalapvetőbb információbeszerzési módszere. Az internet széles körű elterjedése és globális tulajdonsága miatt

[8] A puffertúlcsordulás (buffer overflow) olyan szoftverhiba, sokszor biztonsági rés, amelynél egy processz a fix hosszúságú tömbbe (puffer) történő íráskor nem ellenőrzi annak határait, így azt túlírva a szomszédos memóriaterületet írja felül.

[9] Az SQL-injection egy olyan támadás, amivel sérülékeny SQL-szerverekből lehet kibányászni hasznos információkat, például felhasználóneveket, jelszavakat, jelszó-hasheket.

a legkönnyebben és legegyszerűbben használható információforrás. A rajta lévő keresőmotoroknak információszerzésre való kifinomult, részletes és tudatos használata a penetrációs teszt feladatvégrehajtásában jelentős könnyítéseket, előkészületi fázisokat, annak a már-már készségszinten való használatát teszi lehetővé. A keresőmotorok megfelelő hatásfokkal való használata keresési időt, erőforrást takaríthat meg, valamint leszűrheti a lényegtelen, nem releváns információkat. Ezek a felesleges többletinformációk hátráltatást jelentenek egy munkafolyamat során. Egy kiberműveleti penetrációs teszt munkafolyamatának szemszögéből az effektív munkavégzést segíti.

Információgyűjtés webszolgáltatásokon keresztül

Az olyan webszolgáltatások, mint például a személyes keresési szolgáltatások érzékeny információkat szolgáltathatnak a célról. Az internetes archívumok bizalmas információkat is tartalmazhatnak, amelyeket eltávolítottak az internetről. Közösségi hálózati oldalak, a riasztások, pénzügyi szolgáltatások és munkahelyek biztosítanak információt egy célról, például az infrastruktúráról, fizikai helyről és az alkalmazottak adatairól. Sőt, a csoportok, fórumok és szervezetek segítenek a támadóknak érzékeny információk gyűjtésében, olyan célokról, mint például a nyilvános hálózati információk, rendszerinformációk és személyes adatok. Ezen információk felhasználásával a támadó penetrációs stratégiát készíthet, hogy betörjön a célszervezet hálózatába, és egyéb típusú fejlett rendszeri támadásokat hajtson végre.

A célpont legfelső szintű domainjei és aldomainjei

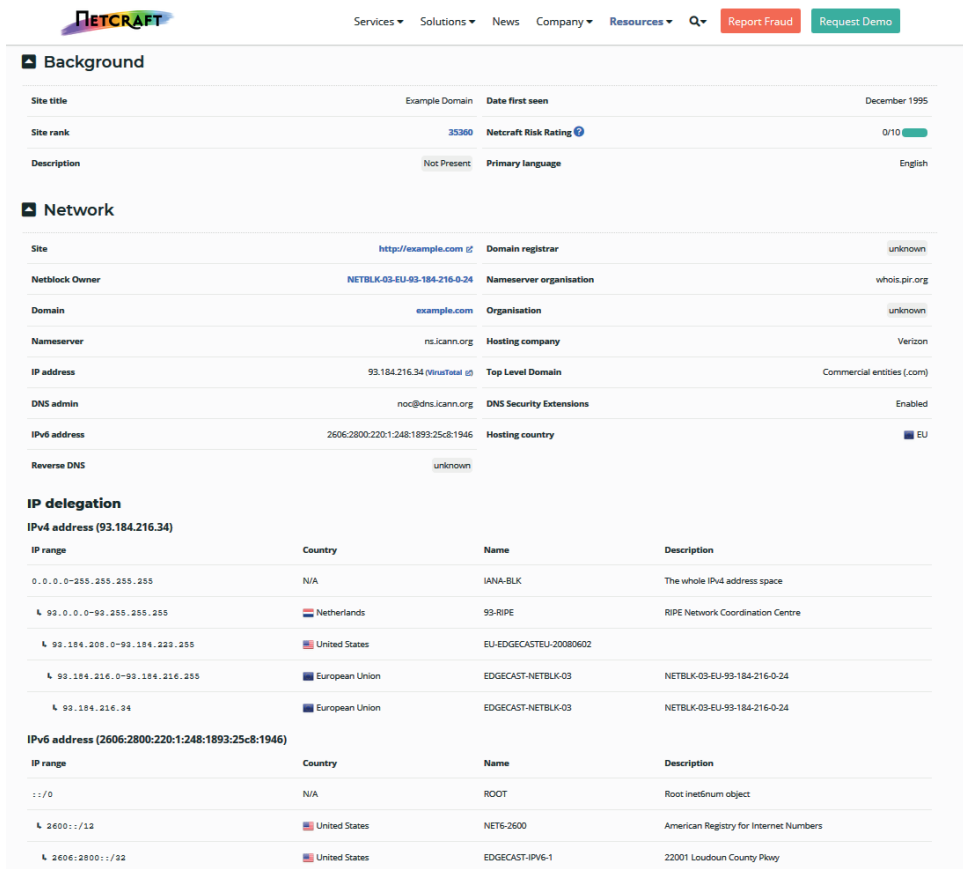
A vállalati felső domain és aldomainek sok hasznos információt nyújthatnak a támadó számára. A nyilvános webhelyeket arra tervezték, hogy megmutassák egy szervezet jelenlétét az interneten. Ingyenesen elérhetők és bárki el is érheti azokat, az ügyfelek és partnerek vonzására szolgálnak. Tartalmazhatnak olyan információkat, mint például a szervezeti előzmények, szolgáltatások és termékek, valamint elérhetőségi adatok. A cél külső URL-je megtalálható a keresőmotorok, például a Google vagy a Bing segítségével.

Az aldomainek csak néhány ember számára elérhetők. Ezek a személyek lehetnek foglalkoztatottak vagy egy osztály tagjai valamely szervezetnél. Az altartományok betekintést nyújtanak a célvállalat különböző szervezeti és üzleti egységeibe. A hozzáférési korlátozások a következők alapján alkalmazhatók: az IP-cím, domainalhálózat, felhasználónév és jelszó. A legtöbb szervezet általános formátumokat használ az altartományokhoz.

- Netcraft.com
  A Netcraft internetes biztonsági szolgáltatásokat nyújt, ideértve a csalás és az adathalászok, az alkalmazások tesztelését és a PCI-scanning[10] szolgál-

[10] A PCI-vizsgálat általában a negyedéves külső sebezhetőségi vizsgálatokra vonatkozik, amelyeket a PCI-jóváhagyott gyártónak kell elvégeznie. A PCI (Payment Card Industry) adatbiztonsági szabványa a Visa és a MasterCard közötti együttműködés eredményeként jött létre, hogy közös ipari biztonsági követelményeket hozzon létre.

tatásait is (2. ábra). Elemzi továbbá a webszerverek, az operációs rendszerek, a host-szolgáltatók és az SSL-tanúsító[11] hatóságok piaci részesedését és az internet egyéb paramétereit.

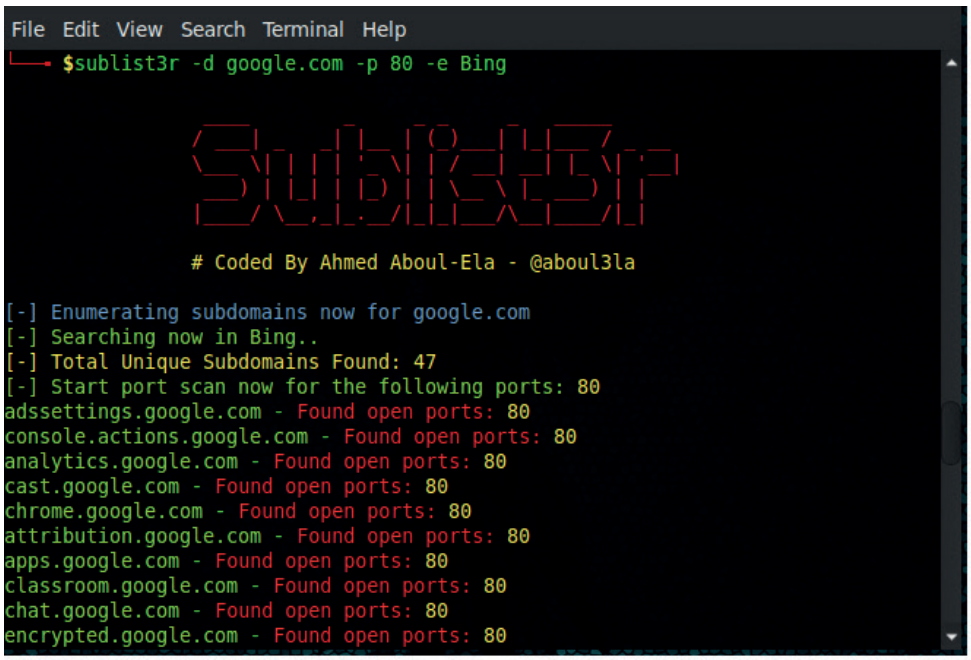


2. ábra
Netcraft az Example.com példán keresztül [7], [11]

- Sublist3er
  A Sublist3r egy python szkript, amely az OSINT használatával a webhelyek aldomaineinek felsorolására szolgál (3. ábra). Ez lehetővé teszi az aldomainek

[11] Az SSL tanúsítványok arra szolgálnak, hogy létrejöhessen egy biztonságos, titkosított csatorna a kliens és a szerver között. Bizonyos információknak, mint a hitelkártyaadatok, fiókbelépéshez szükséges adatok és egyéb kényes információk átvitelének titkosítás alatt kell történnie, hogy kizárjuk az adatok kiszivárgását.
SSL tanúsítvánnyal adataink titkosításon esnek át, mielőtt azok interneten keresztül átvitelre kerülnének. A titkosított adatot csak a célszerver képes lefordítani. Ez biztosítja, hogy a weboldalon megadott adatainkat nem tulajdoníthatják el.

felsorolását több forrásból egyszerre. Segít a penetrációs tesztelőknek és a hibakeresőknek a megcélzott domain domainjeinek összegyűjtésében.



3. ábra
Sublist3r google.com példán keresztül [8]

A cél földrajzi helyzetének megkeresése

Az olyan információk, mint például a szervezet fizikai elhelyezkedése alapvető szerepet játszanak az információgyűjtés folyamatában. A fizikai elhelyezés mellett a támadók olyan információkat is gyűjthetnek, mint például a közeli nyilvános WiFi, amely valószínűleg egy módja annak, hogy elérjék a célszervezet hálózatát. A támadók, akik tudják a célszerv helyét, megkísérlik a szemétbúvárkodást, megfigyelést, social engineering-et, és egyéb nem technikai támadásokat további információk gyűjtése érdekében. Amint a támadók ismerik a cél elhelyezését, részletes műholdas képeket kaphatnak a helyről, az interneten elérhető különböző források, például a Google Maps[12] felhasználásával. A támadók ezt az információt felhasználhatják jogosulatlan hozzáféréshez az épületekhez, vezetékes és vezeték nélküli hálózatokhoz, rendszerekhez.

A Google Earth eszköz lehetővé teszi, hogy megtalálja a cél pontos lokációját, még hozzáférést is biztosít 30 képhez, amely a lakott Föld felületének nagy részét nagy felbontással és részletességgel ábrázolja. A részlet lehetővé teszi az utcakép,

[12] A Google által fejlesztett ingyenes internetes térképszolgáltatás.

a magasság és a koordináták megtekintését. Az olyan eszközök, mint a Google Maps, még az épület bejáratait, a biztonsági kamerákat és a kapukat is megtalálják. Ezek az eszközök interaktív térképeket, vázlatos térképeket, műholdas képeket és információkat nyújtanak a saját térképekkel való interakcióról és azok létrehozásáról. Példák webszolgáltatásra, amely alkalmas a cél földrajzi helyzetének megkeresésére

- https://earth.google.com;
- Wikimapia.org;
- www.bing.com/maps.

Információgyűjtés közösségi oldalakon keresztül

Egy adott személyre való keresés a közösségi oldalakon könnyebb, mint ahogy a legtöbb ember gondolná. Közösségi hálózati hálózatok: olyan online szolgáltatások, platformok vagy webhelyek, amelyek a társadalmi hálózatok kiépítésére vagy az emberek közötti társadalmi kapcsolatok elősegítésére koncentrálnak. Ezek a webhelyek olyan információkat tartalmaznak, amelyeket a felhasználók profiljukban nyújtanak. Segítik az emberek közvetlen vagy közvetett kapcsolatát egymással, olyan különböző területeken keresztül, mint a közös érdekek, a munkahely és az oktatási közösségek. A közösségi oldalak olyan online szolgáltatások, platformok vagy egyéb webhelyek, amelyek lehetővé teszik az emberek számára, hogy kapcsolatba lépjenek egymással és személyes kapcsolatokat építsenek ki. Az ilyen webhelyek például a LinkedIn, a Facebook, a Twitter, a Google, az Instagram stb. A közösségi oldalak lehetővé teszik az emberek számára az információk gyors megosztását, mivel valós időben frissíthetik személyes adataikat. Minden közösségi hálózati webhelynek megvan a maga célja és funkciója. Az egyik oldal kapcsolatba hozhatja a barátokat, ismerősöket, míg a másik segít a felhasználóknak megosztani a munkahelyi profilokat. A közösségi oldalak mindenki számára nyitva állnak. A támadók kihasználhatják ezt a lehetőséget, hogy érzékeny információkat gyűjtsenek a felhasználóktól, akár a felhasználók böngészésével, akár hamis profil készítésével.

Egyes webhelyek lehetővé teszik a felhasználók számára, hogy ellenőrizzék, aktív-e egy fiók, amely ezután információt nyújt a keresett személy állapotáról. A közösségi oldalak lehetővé teszik a támadónak, hogy név, kulcsszó alapján keressen embereket, társaságokat, iskolákat, a célpont barátait, kollégáit és a körülöttük élő embereket. Ezeken a webhelyeken keresve személyes információk érhetők el, például névről, beosztásról, szervezet nevéről, jelenlegi helyéről és oktatási képesítésekről. Ezenkívül olyan professzionális információkat is találhat, mint például a vállalat vagy az üzleti vállalkozás, a telefonszám, e-mail, fényképek, videók és így tovább. Szociális hálózati webhelyek, például a Twitter, tanácsok, hírek, aggodalmak, vélemények, pletykák, és tények gyűjtőhelye. A közösségi hálózati szolgáltatásokon keresztüli keresés révén a támadó kritikákat gyűjthet össze, olyan információkat, amelyek hasznosak a social engineering vagy más típusú támadások végrehajtásában.

A cél figyelése riasztással

A riasztások olyan tartalomfigyelő szolgáltatások, amelyek automatikusan frissítik a felhasználó preferenciáit, általában e-mailben vagy SMS-ben. A riasztások fogadásához a felhasználónak regisztrálnia kell a webhelyen, és e-mail-címet vagy telefonszámot kell megadnia. Online riasztási szolgáltatások automatikusan értesítik a felhasználókat, ha a hír, a biográfia és a beszélgetéscsoportok új tartalma megfelel a felhasználás által kiválasztott keresett kifejezések készletének. Ezek a szolgáltatások a legfrissebb információkat jelenítik meg a versenytársakról és az iparról. Ezen toolok némelyike segít a szervezet nevét, tagjainak nevét, weboldalát, illetve a fontos embereket vagy projekteket is kideríteni. A támadók rendszeresen összegyűjthetik a figyelmeztető szolgálatok által frissített információkat a célról, és felhasználhatják azokat további támadásokra. A Google Alerts[13] automatikusan értesíti a felhasználókat, ha új tartalom kerül fel a hírekből, az internetről, a blogokról, ha a videó- és/vagy beszélgetőcsoportok megegyeznek a felhasználó által kiválasztott és a Google Alerts szolgáltatás által tárolt keresési kifejezések halmazával.

Információgyűjtés fórumok, blogok segítségével

Sok internet-felhasználó veszi igénybe a csoportos blogokat és fórumokat tudásmegosztási célokra. Ezen okból kifolyólag a munkatársak gyakran csoportokra, fórumokra és blogokra összpontosítanak, hogy információkat találjanak a célszervezetről és annak embereiről. A szervezetek általában nem figyelik ezeket, amely esetben az alkalmazottak más felhasználók számára adnak ismereteket – fórumok, blogok és csoportos beszélgetések során. A támadók előnyt kovácsolva ebből, érzékeny információkat gyűjtenek a célokról, publikus hálózati információkat, rendszerinformációkat és személyes adatokat. A támadók hamis profilokkal regisztrálhatnak csoportokba és próbálhatnak csatlakozni a célszervezet munkavállalói csoportjaihoz, ahol megoszthatják a személyes és vállalati információkat. A támadók információs csoportokat, fórumokat és blogokat keresnek a hibás domainnevek, IP-címek alapján is. A munkavállalói információk, amelyeket a támadó csoportokból, fórumokból és blogokból gyűjthet:

- az alkalmazott teljes neve;
- a munka- és lakóhely;
- otthoni telefonszám, mobiltelefonszám vagy irodai szám;
- személyes és szervezeti e-mail-cím;
- képek a munkavállalói lakóhelyről vagy munkahelyről, amely azonosítható információkat tartalmaz;
- képek a munkavállalói díjakról és jutalmakról vagy a közelgő célokról.

A mai információs társadalom kibertérben történő jelentléte egyik részét képezi a webszolgáltatásokon való megjelenés. Az internet világot összekapcsoló hálózatos jellege miatt rengeteg olyan weben található szolgáltatás létezik, amely elősegíti az információ

[13] A Google Alerts egy tartalomváltozásészlelési és -értesítési szolgáltatás, amelyet a Google keresőmotorja kínál.

begyűjtését. Még mindig nem feltétlenül technikai információ begyűjtése a cél, sokkal inkább a környezet, a kapcsolatok, alapvető adatok, nevek, érdeklődési körök, webes megjelenés, fizikai elhelyezkedés. Ezek a közétett adatokkal összefésülve puzzle- vagy építőkocka-szerűen egészítik ki egymást, így az esetleges hiányokat információs átfedésekkel egy komplexebb információt kaphatunk a célról és a célhoz kapcsolódó pontokról. Egyfajta profilozást lehet szintről szintre végrehajtani a weben található szolgáltatások, a keresőmotorok helyes kihasználásával.

Weboldal-információgyűjtés

A webhelyről való információgyűjtés a célszervezet weboldalának figyelemmel kísérése és elemzése. Itt már technikai információk kinyerése is a célok között szerepel. A támadó elkészítheti a weboldal szerkezetének és architektúrájának részletes térképét anélkül, hogy a rendszergazda gyanúját felkeltené.

A támadók alapvető toolokat is használnak, amelyek az operációs rendszerek beépített egyszerű programjai is lehetnek, mint például Telnet[14] vagy böngésző. Ezenfelül szofisztikált segédprogramokat is, mint a Netcraft,[15] ami összegyűjti a weboldal adatait, például az IP-címet, a domaintulajdonos regisztrált nevét és címét, a domainnevet, a webhely hosztját és az operációs rendszer részleteit. Habár nem biztos, hogy megadja ezeket az adatokat minden webhelyre vonatkozóan.

A céloldal böngészése jellemzően a következő információkat nyújtja:

- használt szoftver és verziója: A támadó könnyedén megtalálja a használt szoftververziót;
- használt operációs rendszer: Általában a használt operációs rendszer is meghatározható;
- alkönyvtárak és paraméterek: A keresések feltárják az alkönyvtárakat és a paramétereket azáltal, hogy feljegyezik az URL-eket, miközben a célwebhelyet böngészik;
- fájlnév, elérési út, adatbázis-mezőnév vagy lekérdezés: A támadó gyakran alaposan vizsgál minden olyan lekérdezést, amely fájlnév, elérési út, adatbázis-mezőnév vagy lekérdezésnek tűnik, annak ellenőrzése érdekében, hogy az lehetőséget kínál-e az SQL-injection támadásra;
- szkripting platform: A szkriptfájlnév-kiterjesztések segítségével, például.php,. asp vagy.jsp, könnyen meghatározható a szkript[16] platform, amelyet a célwebhely használ;
- kapcsolatfelvételi részletek és CMS[17]-adatok: A kapcsolattartó oldalak szokásos részleteket tartalmaznak, például neveket, telefonszámokat, e-mail-címeket

[14] A Telnet lényege, hogy a saját számítógépéről be tud jelentkezni egy másik (mindegy, hogy a világ melyik részén lévő) számítógépre.

[15] A Netcraft egy internetes szolgáltató cég, amely számos iparágban nyújt kiberbűnözés-megszakító szolgáltatásokat.

[16] Az informatikában a szkript névvel rövid programokat illetnek, amelyek gyakran egy-egy részfeladat automatizálására szolgálnak.

[17] A CMS magyarul tartalomkezelő rendszer, az elnevezésből pedig következik, hogy segítségével a tartalmaidat tudod létrehozni vagy változtatni. A CMS tulajdonképpen egy webes szoftvercsomag a weboldalad kezeléséhez.

és az adminisztrátorok vagy támogató személyek adatait. A támadó ezeket az adatokat felhasználhatja socialengineering-támadások végrehajtására.

A HTML[18]-forráskód vizsgálata

A támadók érzékeny információkat gyűjthetnek a HTML forráskódjának megvizsgálásával, valamint a manuálisan beillesztett vagy a CMS-rendszer által létrehozott megjegyzések követésével. A megjegyzések utalást adhatnak a háttérben futó eseményekre. Ez akár a webes fejlesztő vagy az adminisztrátor részletes adatait is tartalmazhatja. A fájlrendszer struktúrájának feltérképezése érdekében az összes hivatkozást és képcímkét meg kell őrizni. Néha lehetséges a forráskód szerkesztése.

Sütik[19] vizsgálata

A futó szoftver és annak viselkedése meghatározásához meg lehet vizsgálni a szerver által beállított sütiket. Azonosítani lehet a szkriptplatformokat munkamenetek és más támogató sütik megfigyelésével. A sütik nevére, értékére, domainméretére vonatkozó információk szintén kibonthatók.

Web spider programok használata

A web spider (más néven webbejáró vagy webrobot) egy olyan program vagy automata szkript, amely módszeresen böngészi a webhelyeket, hogy összegyűjtse a meghatározott információkat, például a munkavállalók nevét, e-mail-címét és így tovább. A támadók ezután felhasználják az összegyűjtött információkat különböző támadások végrehajtására. A webes spider elbukik, ha a célwebhelyen a robots.txt fájl található a gyökérkönyvtárban, a könyvtárak felsorolásával a bejárások megakadályozása érdekében.

Példák a webspider-programokra:

- Webextractor (www.webextractor.com);
- Spiderfoot (www.spiderfoot.net);
- Scrapy (https://scrapy.org);
- Screaming Frog (www.screamingfrog.co.uk);
- Beam Us Up SEAo SpiderSEO (http://beamusup.com).

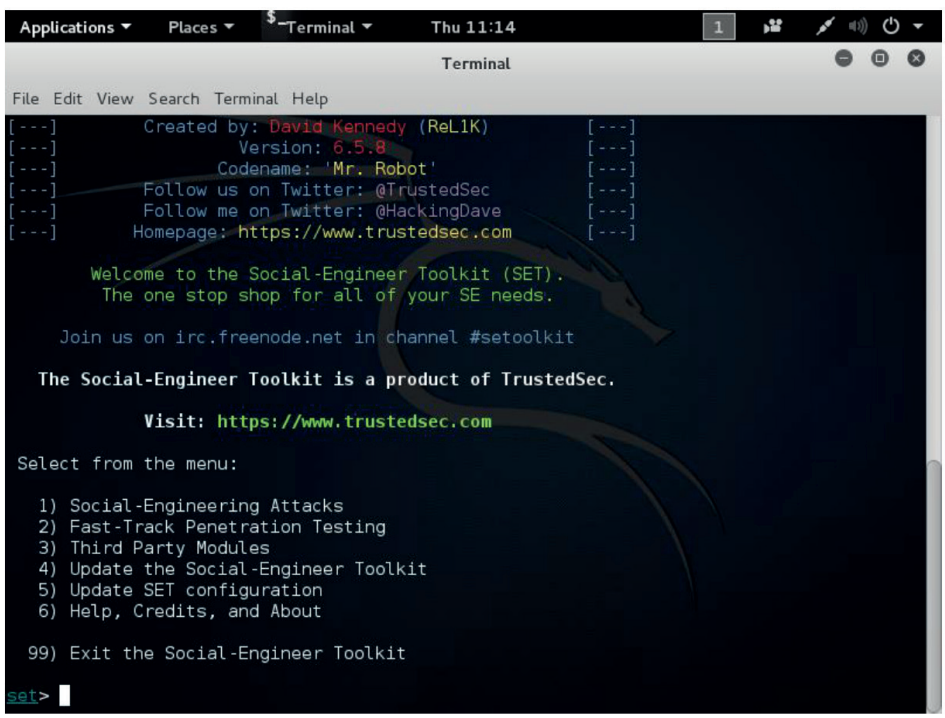
[18] A HTML (angolul: HyperText Markup Language) egy leíró nyelv, amelyet weboldalak készítéséhez fejlesztettek ki.

[19] A HTTP-süti (általában egyszerűen süti, illetve angolul cookie) egy információcsomag, amelyet a szerver küld a webböngészőnek, majd a böngésző visszaküld a szervernek minden, a szerver felé irányított kérés alkalmával.

Teljes webhely tükrözése

A webhelytükrözésnél az eredeti webhely pontos mását vagy klónját hozzák létre, ahogy az a 4. ábrán is látható, ahol saját teszt során végeztem el ezt a műveletet. A felhasználók a weboldalak másolatát a HTTrack Web Site Copier és az NCollector Studio tükrözőtolljaival is elvégezhetik. Ezek az toolok letöltik a weboldalt egy helyi könyvtárba, rekurzív módon felépítve az összes mappát (HTML, képek, flash, videók és egyéb fájlok) a webszerverről egy másik számítógépre. A webhely tükrözésének a következő előnyei vannak:

- hasznos az offline böngészéshez;
- támogatja a támadót abban, hogy több időt töltsön el a weboldal megtekintésében és elemzésében a sebezhetőség szempontjából;
- elősegíti a címtárszerkezet és más értékes információk megtalálását a tükrözött másolatból, anélkül, hogy több kérést kellene adnia a webszervernek.



4. ábra

SET-toolkit website klónozás egyik lehetséges példája [6]

Példák tükröző toolokra:

- Pavuk (http://pavuk.sourceforge.net);
- BackStreet Browser (www.spadixbd.com);
- SurfOffline (www.surfoffline.com);

- BlackWidow (www.softbytelabs.com);
- NCollector Studio (www.calluna-software.com);
- Teleport Pro (www.tenmax.com);
- Portable Offline Browser (www.metaproducts.com);
- Offline Explorer Enterprise (www.metaproducts.com);
- Website Ripper Copier (www.tensons.com).

Metaadatok kibontása nyilvános dokumentumokból

Hasznos információk találhatók a célszervezet weboldalán pdf[20]-dokumentumok, Microsoft Word[21]-fájlok és egyéb formátumok formájában. Képesnek kell lennie a támadónak az értékes adatok kinyerésére, ideértve a metaadatokat és az ilyen dokumentumokba rejtett információkat is. Elsősorban rejtett információkat tartalmaznak az elemzés céljából elemezhető nyilvános dokumentumokról, például az oldal címét, leírását, kulcsszavakat, a létrehozási/módosítási adatokat és a tartalom idejét, felhasználási címeket és a célszervezet alkalmazottainak e-mail-címeit.

A metaadat-kibontó segédprogramok automatikusan kinyerik a kritikus információkat, amelyek magukban foglalják az ügyfelek felhasználónevét, az operációs rendszereket (a kihasználások operációs rendszerekre vonatkoznak), az e-mail címeket, a használt szoftverek listáját (verzió és típus), a szerverek és a dokumentumok létrehozásának/módosításának dátumát, a weboldal szerzőinek listáját és így tovább.

- ExtractMetadata (www.txtroctmetadata.com);
- FOCA (www.tkvenpoths.com);
- Meta Tag Analyzer (www.seocentro.com);
- BuzzStream (http://tools.bullstream.com);
- Analyse Metadata (www.exodium.com);
- Web Data Extractor (www.webextractor.com).

A weboldal-információgyűjtés technikailag kifejezetten http adatkapcsolati kérésekben működő weboldalszoftverek és programnyelvek, beállítások által kinyert információkat takarnak, amely paraméterekkel már könnyebb behatárolni a kihasználható sérülékenységeket, vagy legalábbis realizálni a nem frissített, elavult megoldásokat használó célpontokat. Ezenfelül a könyvtárstruktúrából következtetéseket lehet levonni, például hogy az elérni kívánt különböző prioritású adatok hol találhatók.

E-mail-információgyűjtés

Az e-mail-kommunikáció követése, az Emailtracking[22] egy adott felhasználó e-mailjeit figyeli. Ez a fajta nyomon követés a digitális időbélyegzés révén lehetséges, amikor

[20] A Portable Document Format (PDF) az Adobe Systems által kifejlesztett, dokumentumok tárolására alkalmas fájlformátum.
[21] A Microsoft Word a Microsoft által készített dokumentumszerkesztő program.
[22] E-mail-követés.

a célpont megkap és megnyit egy adott e-mailt. Az e-mail-nyomkövető toolok lehetővé teszik a támadó számára az információk gyűjtését, például IP-címeket, e-mail-kiszolgálókat és az e-mail küldésében részt vevő szolgáltatót.

Az e-mailek nyomon követésének tooljai közé tartozik az eMailTrackerPro, a Yesware, a Contact Monkey stb. Információk az áldozatokról az emailtrack-toolok segítségével:

- címzettrendszer IP-címe: lehetővé teszi a címzett IP-címének nyomon követését;
- helyzet: megbecsüli és megjeleníti a címzett helyét a térképen, és kiszámíthatja a távolságot a támadó helyétől;
- érkezett és olvasott e-mail: értesíti, hogy mikor fogadja és olvassa el az e-mailt a címzett;
- olvasás időtartama: az az időtartam, amelyet a címzett a küldött levél olvasására fordít;
- proxy[23] észlelése: információt szolgáltat a címzett által használt kiszolgáló típusáról;
- linkek: ellenőrzi, hogy ellenőrizték-e a címzettnek e-mailben elküldött linkeket;
- operációs rendszer és a böngésző adatai: információkat jelenít meg a fogadó által használt operációs rendszerről és böngészőről. A támadó ennek az információnak a felhasználásával meg tudja találni az operációs rendszer és a böngésző verzióját, hogy további támadásokat indítson;
- e-mail-továbbítás: meghatározza, hogy a felhasználónak küldött e-maileket továbbítják-e egy másik személynek;
- eszköz típusa: információt nyújt az e-mail megnyitásához és olvasásához használt eszköz típusáról, például asztali számítógép, mobileszköz vagy laptop.

Információ gyűjtése az e-mail-fejlécből

Az e-mail-fejléc tartalmazza a feladó adatait, a routing-információkat,[24] a dátumot, a tárgyat és a címzettet. Mindegyik kiváló információforrás a támadó számára a cél elleni támadások indításához. Az e-mail-fejléc megtekintésének folyamata a különböző e-mail-programoktól függ. Az e-mail fejléce a következő információkat tartalmazza:

- a feladó e-mail-szerver;
- a feladó e-mail-szerverei által kapott adatok és idő;
- a feladó e-mail-szervere által használt hitelesítési rendszer;
- az adatok és az üzenet elküldésének ideje;
- az mr.google.com által kiosztott egyedi szám, amely azonosítja az üzenetet;
- a feladó teljes neve;
- a feladó IP-címe és a cím, ahonnan az üzenet el lett küldve.

[23] Számítógép-hálózatokban proxynak, helyesebben proxyszervernek nevezzük az olyan szervert (számítógép vagy szerveralkalmazás), amely a kliensek kéréseit köztes elemként más szerverekhez továbbítja. A kliens csatlakozik a proxyhoz, majd valamilyen szolgáltatást (fájlt, csatlakozást, weboldalt vagy más erőforrást) igényel, ami egy másik szerveren található.

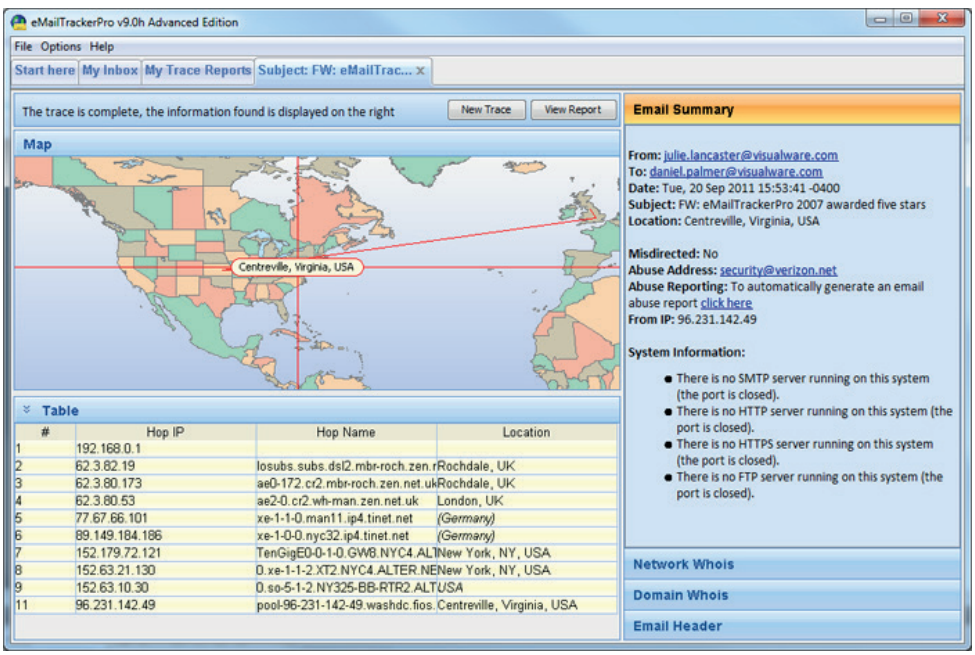
[24] Az útválasztás, hálózati forgalomirányítás vagy routing az informatikában annak kiválasztását jelenti, hogy a hálózatban milyen útvonalon haladjon a hálózati forgalom.

A támadó a teljes e-mail fejlécének részletes elemzésével nyomon tudja követni és összegyűjti ezeket az információkat.

E-mail-követő toolok

Az e-mail-követő toolok lehetővé teszik a támadónak egy e-mail nyomon követését és olyan információk kinyerését, mint például a feladó azonosítója, a levelezőszerver, a feladó IP-címe és így tovább. Ezek az eszközök nem automatikusan küldik el a fájlokat, ha a címzettek megnyitják a levelet és adnak állapotinformációt arról, hogy az e-mail sikeresen kézbesítve lesz-e vagy sem. A támadók a kibontott információt használják, hogy megcélozzák a szervezetet és annak rendszereit kártékony e-mailek küldésével.

- eMailTrackerPro (www.emailtrackerpro.com)
  Az eMailTrackerPro elemzi az e-mailek fejléceit, és olyan információkat tár fel, mint például a feladó földrajzi elhelyezkedése, IP-címe és így tovább (5. ábra). Ez lehetővé teszi a támadó számára, hogy később megtekintse a nyomokat a korábbi nyomok mentésével.



5. ábra
eMailTrackerPro [12]

További széles körben elterjedt toolok:

- PoliteMail(www.politemail.com);
- Yesware (www.yesware.com);

- ContactMonkey (https://contactmonkey.com);
- Zendio (www.zendio.com);
- ReadNotify (www.readnotify.com);
- DidTheyReadIt (www.didtheyreadit.com).

Az e-mail-információgyűjtés a technikai és nem technikai adatok gyűjtésébe is beletartozik, hiszen a technikai oldalról közelítve a dolgot ezen információk felhasználásával jelentős támadásokat lehet előkészíteni. Mint például e-mail-fejléccsere, ezáltal másnak kiadni magunkat, levelezőszerver IP-címe DoS[25]-támadásokra, linkek beágyazva rosszindulatú kódokkal, malware-ekkel. Ezenfelül, szintén átfedve az előző kettő kategóriát, személynevek, cégnevek, a levél tartalmából kapcsolatok, kontextusok nyerhetők ki. Folyamatos e-mailnyomonkövető-eszközökkel a kiberműveleti penetrációs munkafolyamatok az információktól függően frissíthetők, változtathatók a támadási irányvonalak. Ezzel a négy közétett adat elemzésével egy összeségében olyan információhalmaz állítható össze, amely egy általános képet ad a célpontról, és ennek birtokában haladhatunk az összetettebb, komplexebb és technikai információk begyűjtéséhez.

Alapvető DNS-információk lekérdezése és vizsgálata

Ebben a fejezetben látható, hogy számos tool használható, amelyek hasonló eredményeket generálnak, ennek oka az, hogy ellenőriznünk kell az összegyűjtött információkat. Ha azok egynél több tool segítségével is kinyerhetők, akkor megbízhatóbbak. A felsorolt lehetőségek főként nyílt forráskódú szoftvereken, toolokon keresztül alapvető technikai információk begyűjtésére szolgálnak, amelyek így a közétett adatokkal összhangban egy optimális, várhatóan elegendő információhalmazt hoznak létre. Ezután a kiberműveleti penetrációs teszt munkafolyamatában tovább lehet haladni a még részletesebb hálózat-feltérképezésre, illetve sérülékenységelemzésre [7], [8].

WhoIs

A tervezésnél fontos összegyűjteni a hálózattal kapcsolatos információkat, például a „WhoIs"-információkat a célszervezetről. A WhoIs egy lekérdezési és válaszprotokoll, olyan adatbázisok lekérdezésére, amelyek tárolják a regisztrált felhasználókat vagy internetes erőforrások jogosultjait, például egy domainnevet, egy IP-cím-blokkot vagy egy autonóm rendszert. Ez a protokoll a 43-as porton (TCP[26]) lévő kérésekre vonatkozik. A regionális internetes nyilvántartások (RIR[27]) fenntartják a WhoIs-adatbázisokat, amelyek a domaintulajdonosok személyes adatait tartalmazzák. Minden

[25] A szolgáltatásmegtagadással járó támadás (Denial of Service vagy DoS), más néven túlterheléses támadás, illetve az elosztott szolgáltatásmegtagadással járó támadás (Distributed Denial of Service, DDoS) informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése.

[26] A Transmission Control Protocol (TCP) az internet gerincét alkotó TCP/IP-protokollcsalád egyik fő protokollja.

[27] A regionális internetes regiszter (RIR) olyan szervezet, amely az IP-címek blokkjait földrajzi hatáskörébe helyezi.

egyes erőforrás esetében a WhoIs-adatbázis szöveges nyilvántartásokat tartalmaz magáról az erőforrásról, valamint a meghatalmazottakról, regisztrálókról és az adminisztrátori információkról (létrehozás és lejárati dátum).

Parancsa:
#whois example.com

A WhoIs-lekérdezés a következő információkat adja vissza:

- domainnév részletei;
- domaintulajdonos kapcsolattartási adatai;
- domainnévszerverek;
- lejárati rekordok;
- utoljára frissített rekordok;
- domain létrehozásának dátuma.

A támadó lekérdezi a WhoIs adatbázis-kiszolgálót, hogy információkat szerezzen a céltartomány nevéről, a tulajdonos elérhetőségeiről, a lejárat dátumáról, a létrehozás dátumáról és így tovább. A WhoIs pedig a kérelemre válaszol a kért információkkal. Ezen információk felhasználásával a támadó elkészítheti a szervezet hálózatának térképét, és megtéveszthet a domaintulajdonosokat social engineeringgel.

WhoIs keresési eredmény analízise

A WhoIs például a http://whois.domaintools.com vagy a www.tamos.com segítségével segíthet a WhoIs-lookups-lekérdezésekben. A domaintools.com szolgáltatás a WhoIs számára olyan információkat nyújt, mint például a regisztráló információ, az e-mail, az adminisztrátori kapcsolatinformáció, a létrehozott és az érvényességi idő, valamint a domainszerverek listája. A SmartWhois elérhető a www.tamos.com webhelyen. Megadja az információt az IP-címről, hosztnévről vagy domainről, ideértve az országot, az államot vagy a megyét, a várost, a telefonszámot, a faxszámot, a hálózati szolgáltató nevét, az adminisztrátort és a műszaki támogatás elérhetőségét. Ezenkívül segít megtalálni a domain tulajdonosát, a tulajdonos elérhetőségét az IP-cím-blokk tulajdonosát, a domain regisztrált dátumát és így tovább.

Domain Name: EXAMPLE.COM
Registry Domain ID: 2336799_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.iana.org
Registrar URL: http://res-dom.iana.org
Updated Date: 2019-08-14T07:04:41Z
Creation Date: 1995-08-14T04:00:00Z
Registry Expiry Date: 2020-08-13T04:00:00Z
Registrar: RESERVED-Internet Assigned Numbers Authority
Registrar IANA ID: 376
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:

Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: A.IANA-SERVERS.NET
Name Server: B.IANA-SERVERS.NET
DNSSEC: signedDelegation

DNS-információk kibontása

Domain Name System információk kibontása információt szolgáltat a DNS-zóna-adatokról. A DNSzone-adatok tartalmazzák az DNS-domainneveket, a számítógépneveket, az IP-címeket és sok más részletet a hálózatról.

Az DNS-információk kibontása segít a cél DNS-re vonatkozó következő rekordok meghatározásában (2. táblázat):

2. táblázat
DNS-rekordok [4]

A	Rámutat a hoszt IP címére
MX	Rámutat a domain levelező szerverére
NS	Rámutat a hoszt név szerverére
CNAME	Kanonikus elnevezés lehetővé teszi az alias nevek használatát a hoszt
SOA	Irányadó információk a DNS-zónáról; az elsődleges névkiszolgáló, a tartomány rendszengazdájának e-mail-címe, a tartomány sorozatszáma, a zóna frissitési időközei.
SRV	Általános szolgáltatás-helymeghatározó rekord, újabb protokollok számára, elkerülendő a protokoll-specifikus rekordokat, mint az MX.
PTR	Kanonikus névre mutat. A CNAME-től eltérően nem történik további DNS-beli feldolgozás, maga a név a visszatérési érték. Leggyakrabban reverse DNS-lekérdezéseknel használják, de pl. az Apple DNS-SD-jében is használják.
RP	A tartományhoz rendelt felelős személy. Általában egy e-mail-cím, amiben a @ karaktert helyettesíti.
TXT	Text rekord (szöveges rekord)

A DNS-lekérdező toolok (például a www.dnsstuff.com) és a DNS-rekordok (http://network-tools.com) lehetővé teszik a felhasználó számára a DNS-adatok információgyűjtésének végrehajtását. A DNSstuff információkat gyűjt az IP-címekről, e-mail kiszolgáló-kiterjesztésekről, DNSlookupokról, WhoIs-keresésekről és így tovább. Ha a célhálózat lehetővé teszi az ismeretlen, jogosulatlan felhasználók számára a DNS-zónaadatok továbbítását, akkor a támadónak könnyű megismerkednie a DNS-ről szóló információkkal, a segédprogramok segítségével.

host

Miután megkaptuk a DNS-kiszolgáló adatait, a következő lépés egy host IP-címének megismerése:

#host www.example.com

A parancs eredménye a következő:

A www. example.com *címe 192.0.43.10*
A www.example.com *IPv6 címe 2001:500:88.200:10*

Az eredményt tekintve ismerjük az IPv4 és IPv6 címeit a www.example.com nevű hosztnak.

Alapértelmezés szerint a host parancs megkeresi a tartomány A-, AAAA- és MX-rekordjait. Bármely rekord lekérdezéséhez csak meg kell adni az -a opciót a parancshoz.

 # host -a example.com
Trying „example.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25153
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2
;; QUESTION SECTION:
;example.com. *IN ANY*
;; ANSWER SECTION:
example.com. *3201 IN SOA* dns1.icann.org.
hostmaster.icann.org. *2012080782 7200 3600 1209600 3600*
example.com. *46840 IN NS* a.iana-servers.net.
example.com. *46840 IN NS* b.iana-servers.net.
;; ADDITIONAL SECTION:
b.iana-servers.net. *1401 IN A 199.43.133.53*
a.iana-servers.net. *1401 IN A 199.43.132.53*

dig

A host parancson kívül a dig parancsot is használhatja a DNS-lekérdezéshez. A dig előnyei a hoszthoz viszonyítva a rugalmasság és a tiszta kimenet. A dig segítségével megkérhető a rendszer, hogy dolgozza fel a keresési kérelmek listáját fájlból.

Anélkül, hogy a domainnév mellett bármilyen lehetőséget megadna, a dig parancs csak a domain A-rekordját adja vissza. Bármely más DNS-rekordtípus szükséges, megadható a típus opció a parancssorban.

 # dig example.com
;<<>> DiG 9.8.4-rpz2+rl005.l2-Pl <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY,status: NOERROR, id:3786
;; flags: qr rd ra;,QUERY: I,ANSWER: I,AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:

;example.com. *IN A*
;; ANSWER SECTION:
example.com. *41023 IN A 192.0.43.10*
,, Query time: 14 msec
,, SERVER:10.17.3.245#53(10.17.3.245)
,, WHEN:Mon;May 13 18:33:09 2019
,, MSG SIZE rcvd:45

dnsenum

Információkat gyűjthetünk egy DNS-kiszolgálótól a dnsenum segítségével. Az összegyűjthető DNS-információk a következők:

- a host IP-címek;
- a domain DNS-szervere;
- a domain MX-rekordja.

A DNS-információk beszerzésén túl a dnsenum a következő tulajdonságokkal is rendelkezik:

- további nevek és aldomainek szerezhetők be a Google keresőmotorjával;
- az aldomainek nevét megtudhatja úgy, hogy brute forcing kikényszeríti a neveket a szöveges fájlokból;
- elvégzi a WhoIs-lekérdezéseket a C-osztályú tartományi hálózati tartományokban és kiszámítja azok hálózati tartományait;
- fordított keresést végez a hálózati tartományokban;
- szálakat használ a különböző lekérdezések feldolgozásához.

A dnsenum alapértelmezett beállításaival információkat szerezhetünk a hoszt címéről, a névszerver és a levelezőszerver IP-címéről. dnsenum.pl example.com

#dnsenum example.com
dnsenum.pl *VERSION:1.2.2*
—- example.com —-
Host's addresses:

_____
Name Servers:

_____
ns1.isp.com *10771 IN A 172.168.1.2*
ns0.isp.com *7141 IN A 172.168.1.1*
Mail (MX) Servers:

_____
hermes1.example.com *86400 IN A 192.168.10.3*
hermes.example.com *3600 IN A 192.168.10.2*
Trying Zone Transfers and getting Bind Versions:

_____
Trying Zone Transfer for example.com *on* ns0.isp.com …

AXFR record query failed: NOERROR
ns0.isp.com *Bind Version:*
DNS server

Az előzőkben alkalmazott parancsok a technikai DNS-információk lekérdezésére alkalmasak. Ezáltal olyan információkhoz segít hozzáférni, amelyek akár kulcsfontosságúak is lehetnek egy teszt vagy támadás felépítése, de legalábbis előkészítése során. Kinyerjük, hogy melyik szervezetnél regisztrált domain-nevet, mi a szerver IP-címe, mi a levelezőszervere, mi a névszervere, mikor regisztrált, mikor jár le a regisztráció, ki a kontakt és még pár nagyon hasznos információ, amelyeket a közzétett adatok elemzésével együtt használva egy erős információs adatbázist képezhet a munkafolyamat első lépcsőjében.

Következtetések

A kiberműveletekben és informatikában az információgyűjtési tevékenységek azonosítják a szervezetekhez kapcsolódó, nyilvánosság számára hozzáférhető információkat. Az információgyűjtési technikákat használva számos lehetőség nyílik a célszervezet hálózatának illetéktelen hozzáférésére. Nincs egységes módszer az információgyűjtésre, hiszen azok számos módon beszerezhetők. Viszont a lehető legtöbb információt be kell gyűjteni, így érdemes ezt a fázist szervezett módon végrehajtani. Jelen cikk összefoglalja ennek lehetőségeit, az alkalmazott technika alapján kategorizálja azokat, és konkrét megvalósítási példákat is felsorakoztat a megértés érdekében. A közzétett adatok elemzése, illetve az alapvető DNS-információk lekérdezése, valamint vizsgálata olyan fontos elemek, amelyeknek részletes tanulmányozásával penetrációs tesztünk kezdő fázisa elindítható, és jelentős eredmények érhetők el egy ilyen teszt módszertanának végrehajtásánál.

Következtetésként az információgyűjtési technikák bár sokrétűek és sokfélék, az egyszerűbb információgyűjtéstől haladva a nehezebb, már toolokat alkalmazó gyűjtés felé, minél több forrásból nyerjük ki az információkat, annál nagyobb hatásfokkal indítható el maga a penetrációs teszt módszertanának folyamata. Ezeket a megfelelő struktúrába rendezve és gyűjtve egy munkafolyamat első lépését lehet megtenni, amely hozzájárul az eredményes és effektív feladatvégrehajtáshoz. Levonható következtetésként, hogy a kibertérben zajló és teszthez kapcsolódó műveletek sokrétegűek, és nemcsak technikai információgyűjtést foglalnak magukban, hanem az emberi, szervezeti információk halmazára is irányulnak. Ötvözve és összefésülve a közzétett adatok elemzésekor, illetve az alapvető DNS-információk lekérdezésekor kapott információkat, egy biztos alapot kapunk az általunk végrehajtani kívánt teszthez, támadáshoz.

Hivatkozások

[1] I. Paráda, „Basic of Cybersecurity Penetration Test," *Hadmérnök,* 13. évf. 3. sz., pp. 435–442., 2018.

[2] Zs. Haig, *Információs műveletek a kibertérben.* Budapest: Dialóg Campus kiadó, 2018.

[3] L. Kovács, *A kibertér védelme.* Budapest: Dialóg Campus Kiadó, 2018.

[4] S.-P. Oriyano, *CEH™v9.* [Certified Ethical Hacker] 2016. DOI: https://doi.org/10.1002/9781119419303

[5] „Google Search: a keresési operátorok teljes listája," *thepitch.hu,* [Online]. Elérhető: https://thepitch.hu/google-keresesi-operatorok-listaja/ (Letöltve: 2019. 08. 16.)

[6] I. P. István Bodnár, „Jelszó ellopás social engineering, e-mail spoofing és fake url segítségével," *Hírvillám,* 7. évf. 1. sz., pp. 139–147., 2016. [Online]. Elérhető: http://comconf.hu/kiadvany/hirvillam_7evfolyam_1szam.pdf (Letöltve: 2019. 08. 16.)

[7] T. Heriyanto, L. Allen and S. Ali, *Kali Linux – Assuring Security by Penetration Testing.* Birmingham: Packt Publishing, 2014.

[8] R. W. Beggs, *Mastering Kali Linux for Advanced Penetration Testing.* Birmingham: Packt Publishing, 2014, pp. 47–52.

[9] „A Google dorking hackelési technika veszélyei és megelőzésének lehetőségei," *szoftver.hu,* 2016. [Online]. Elérhető: https://szoftver.hu/hirmorzsak/a-google-dorking-hackelesi-technika-veszelyei-es-megelozesenek-lehetosegei (Letöltve: 2020. 01. 07.)

[10] "Google hacking database," *exploit-db.com,* [Online]. Elérhető: www.exploit-db.com/google-hacking-database (Letöltve: 2020. 01. 07.)

[11] "Site report for http://example.com," *sitereport.netcraft.com,* [Online]. Elérhető: https://sitereport.netcraft.com/?url=http%3A%2F%2Fexample.com (Letöltve: 2020. 03. 03.)

[12] "Tracing an email header," *emailtrackerpro.com,* [Online]. Elérhető: www.emailtrackerpro.com/support/v9/tutorials/traceheader.html (Letöltve: 2020. 03. 03.)

HADMÉRNÖK
VÉDELMI INFORMATIKA

15. évfolyam (2020) 1. szám 183–194.
DOI: 10.32567/hm.2020.1.12

Szabolcs Prisznyák[1]

The Instruction of Information Technology in the Education of Non-Commissioned Officers in Hungarian Law Enforcement

Az informatika oktatása a magyarországi rendvédelmitiszthelyettes-képzésben

The author of the article presents the current situation of the instruction of information technology in the education of non-commissioned officers (NCOs) in the Hungarian law enforcement organisation. A survey was conducted through a questionnaire to assess experiences, consequences and to make suggestions for further improvement.

Keywords: **law enforcement, education, IT instruction, police, disaster management, prison service**

A cikkben a szerző bemutatja a magyarországi rendészeti tiszthelyettesképzésben az IT-oktatás jelenlegi helyzetét. Egy kérdőíves kutatással felméri az oktatásban részt vevők ismereteit, véleményét. A cikk végén a kutatás és a kérdőíves felmérés alapján összegzi a tapasztalatokat, következtetéseket von le, továbbá oktatásfejlesztési javaslatokat tesz.

Kulcsszavak: **rendvédelem, oktatás, informatikaoktatás, rendőrség, katasztrófavédelem, büntetés-végrehajtás**

Introduction

From a historical perspective, we can certainly claim that no matter which domain of life is affected, success can mostly be traced back to the improvement and more

[1] National Tax and Customs Administration of Hungary, Leader of the IT Department, e-mail: prisznyak.szabolcs@outlook.com, ORCID: https://orcid.org/0000-0002-3234-7485

effective organisation of trainings and instruction. In his writing dating back to the 5th century, *Epitome rei militaris* [Concerning Military Matters], the Roman Vegetius emphasised the importance of training with the following words: "He who wants victory, let him train soldiers diligently" [24: 797]. This fundamental principle also characterised the military history of the Middle Ages, as armies consisting of regular, well-trained units proved to be simply more successful [1].

As time passed, training became increasingly important since specialised skills were necessary in basically every domain. This phenomenon is rooted partly in the complexity of the world and the way it works, partly in the necessity of the practical application of the novel technical-technological advances. However, the structure of instruction and of an up-to-date curriculum can hardly keep pace with the rapid technological development. This statement especially applies to the field of information technology. Compared to other professions, it becomes quite obvious that technological novelties used to serve humanity for a generation, but in the area of information technology, development can be measured in cycles of only 3 to 6 years. As a consequence, skills acquired 5–10 years ago are already outdated, while in other professions competences can be made use of much longer. This applies to specialists as well as to users. Information technology is part of our everyday life, in fact, increasingly so. Thus is it absolutely essential that law enforcement studies should also entail a training in it.

Governments, ministries, the relevant bodies of the European Union have also taken measures regarding the field of IT studies. The recommendation of the European Parliament and Council issued on 18 December 2006 stresses the importance of key competences necessary for life-long learning [2: 4]. Consequently, the National Curriculum of Hungary also defines the key competences, including digital skills [3: 10–11]. In 2015, the Hungarian Government launched a package with the title *Digital Welfare Programme,* which formulated the need of a Digital Education Strategy and its presentation to the government [4: 3]. In 2016, the Government adopted the Digital Education Strategy [5: 1], which defines its focus as follows:

"By now the use of digital technologies has become an integral part of our everyday lives and most work processes, therefore, it is an essential economic and social requirement that the school should prepare students for the use of digital technologies and devices at the level of competence. In spite of this trend, however, in Hungary more than one third of the population aged 15 or older are digitally illiterate and most of them are threatened by the digital divide. The employability of workers who cannot use digital devices and applications is declining from day to day, and so is the competitiveness of companies refusing to join the digital world" [6: 28].

An important work focusing on the training of NCOs is István Bökönyi's dissertation [7]. This work written in 1987 describes the training history of law enforcement NCOs and outlines future improvement options. Bökönyi emphasised the importance of an independent training institution for NCOs and stressed the significance of the instruction of computer skills and foreign languages. The outlined paths of development – considering the date of release – proved rather forward-looking, and now we know that the author accurately recognised the real demands of the future.

In this paper, I will present the NCO training in three Hungarian law enforcement areas: the police, disaster recovery and prison service. Besides, I will also explore the current situation of the instruction of information technology, demonstrating how information technological solution plays a growing role in the various activities of law enforcement. Based on the above mentioned facts, a preparative training for the application of IT devices and systems can fundamentally influence the professional effectiveness of law enforcement organisations.

Modular Training

Until quite recently, the three bodies in focus conducted their internal training according to their own unique systems. It was mainly due to the fact that each one of them was under the control of different authorities, operated in differing structures and had a different legal status. The police operated – as its largest organisation – as part of the Ministry of the Interior. On 29 June 2006, the Ministry of the Interior ceased to exist, and its responsibilities were partly taken over by the Ministry of Local Government and partly by the Ministry of Justice and Law Enforcement until the Ministry of the Interior was re-established in 2010. In the period between 2006 and 2010, the police were controlled by the Ministry of Justice and Law Enforcement.

Prison service was governed by the Ministry of Justice from the 1970s onwards, but from 2006, it was also moved under the control of the Ministry of Justice and Law Enforcement. In 2010, the newly established Ministry of the Interior got in charge of the prison service, as well [8: 37 § d].

The Fire Service, then Department of Disaster Recovery used to belong partly to the Ministry of the Interior, partly to local councils. Its structure was neither consistent nor operated in a strictly hierarchical way. Not only its structure but also its responsibilities got fundamentally changed by the act on disaster recovery which entered into effect in 2012 [9: 22–24 §].

Since 2010, all three organisations have been under the umbrella of the Ministry of the Interior, and thanks to this, legal acts and provisions governing their activities – more specifically their training duties – are also partly identical.

One of the main goals set by the newly established Ministry of the Interior was the transformation of the training system, which would – among other things – allow transition from one profession to another within law enforcement. In December 2010, a government decision was issued on the new modular training system of the law enforcement organisations [10]. In practice, it translates into a training system consisting of general and specific professional modules. According to this new concept, each law enforcement organisation provides a foundation for the competences of their personnel with the same general module. Having completed that, they can move on to more specific modules connected to the basic responsibilities of their individual organisation. Today, the training system of all three organisations is modular, and all applicants must have passed their secondary school final exams.

Training System in the Police Forces

In Hungary, four educational institutions are in charge of the training of NCOs in the police forces. I will present the curriculum – with specific focus on the instruction of information technology – of secondary schools for aspiring police officers by analysing the curriculum of the Vocational School of Law Enforcement in Körmend. These schools provide qualification for aspiring police NCOs after their secondary school final exams; their operation is regulated by the Act on National Public Education [11].

The school in Körmend has 22 general and 8 specialised classrooms. Out of the 8 specialised classrooms, 4 are computer labs [12: 17]. The qualification period lasts for two years and fits into the public education system. The two years contain five modules in total:

- Core Duties in Law Enforcement
- Duties of Assistant Patrolling Officers
- Team service
- Patrolling Duties
- Maintenance of Public Order, Border Control, Traffic Management or Crime Prevention and Investigation (according to the specialisation of the students' choice)

The enumeration clearly shows that out of the five modules only the fifth differs, the remaining four are the same for all law enforcement students. During the 4-term training, the total number of classes is 2,506 [12: 83], the course being equally split between 50% theory and 50% practice. In the module Core Duties in Law Enforcement, there are ten school subjects in 370 lessons in total [12: 175–176]. Information Technology I comprises 20 lessons divided into 6 lessons of Basic IT in Law Enforcement and 14 lessons of Basic Telecommunication. The rough outline of the curriculum of the above subjects is the following:

Basic IT in Law Enforcement:

- The significance of information technology in the various fields of law enforcement, interrelatedness of information technology and crime.
- Basic terminology in information technology, the definitions of information and data.
- Computer systems, hardware and software.
- Use of the school computer network and of the distance learning system.

Basic Telecommunication:

- General telecommunication skills, the construction, use and application rules of the TETRA network EDR (Unified Digital Radio Communications System) [12: 181].

In the module Duties of Assistant Patrolling Officers, we find 13 subjects in 524 lessons: Information Technology II in 48 lessons [12: 184–185]. Its rough curriculum outline is the following:

- Basic word processing skills, typing, formatting (20 lessons).

- Registration and management programmes in law enforcement (Robotzsaru Neo, HERR, HERMON and SIS – 8 lessons).
- Use of the documentation management and the case handling programme of the police force "Robotzsaru Neo" (20 lessons) [12: 184].

The Team Service module comprises 12 subjects in 344 lessons: Information Technology III takes up 12 lessons [12: 196–197]. The material focuses on the practice of "Robotzsaru Neo" and its better and deeper understanding [12: 200].

The module Patrolling Duties contains 552 lessons in total split into 16 subjects: Information Technology IV takes up 8 lessons [12: 205–206] and concentrates on the generation of documentation management in the maintenance of law and order in "Robotzsaru Neo" [12: 215].

The specialised fifth module comprises 556 lessons in all four fields [12: 217–218, 227–228, 239–240, 251–252], and information technology is instructed in 12 lessons with specialised material content [12: 225, 236–237, 248, 260].

In total, information technology is taught in 100 lessons, which are distributed to five modules. Information technological systems and infrastructure are targeted only in the first two modules: in Information Technology I and II IT skills gradually become inherent parts of other subjects, in particular of subjects relevant to border control (e.g. NEKOR, FADO, iFADO, PRADO, SIS, VIS). In police schools, all subjects connected to information technology – besides Information Technology I and II – are taught by IT specialists. As some of the material may have been acquired during the students' early studies in public education, I personally believe that the curriculum of the information technology courses could already be based on previously acquired knowledge and skills. I also endorse the instruction of IT skills in the fields of IT security and corporate IT systems.

Training System in the Prison Service

Virtually, throughout its entire history, the organisation of prison service operated its own internal training system. Today courses are held at the Further Training and Conference Centre of the Prison Service.

In 2010, upon the initiative of the Ministry of Interior, the Government set the new goal of a uniform training system for all law enforcement organisations [13]. Following the development and adoption of the new qualification system, the newly established penitentiary professions showed up in the National Qualification Registry.

While making the training more up-to-date, the training system of the prison service remained outside the education system due to professional considerations. The duration and the structure of the training in prison service are established in a way that the subsequent modules in a logical order already form a part of the qualification.

In this still functioning modular system, the first module of Core Duties in Law Enforcement is directly followed by specialised modules, such as Prison Guard Service, Assistant Prison NCO, then Prison NCO. If these are completed successfully, students must pass a complex professional test which will eventually provide them with their

full qualification. The instruction period of the four modules is 27-week long and covers 870 lessons in total: out of these 522 focuses on theory, while 348 are practical classes. Students take part in 690 lessons at school and in 180 practical lessons in prisons [14: 7]. Information technology is instructed in 16 lessons only in the first module within the framework of Basic Telecommunication [14: 10]. The institution has a computer lab necessary for the instruction [14: 20], which is based on the notes prepared by the instructor [15]. The notes are well-structured, the material is informative and corresponds to the number of classes. The contents are the following:

- Regulations of IT Security
- Basic IT skills (computer skills, internet use, word processing, creating tables and presentations, etc.)
- IT Security (basics, viruses, the IT systems in prison service)
- IT systems in prison service (software, hardware, network infrastructure)
- The radio communications system "EDR"

Work-related computer training is also conducted in later modules. Students learn about the structure and operation of the security system within the framework of the subject Security and also during practical classes in prisons.

Again, having seen the contents of the school material, we see that – similarly to the IT training of the police forces – the material covers skills that students must or may have acquired previously in public education.

Training System in Disaster Management

The main responsibilities of disaster recovery consist of an ever-increasing number of part activities. Today's organisation of disaster management is based on the organisation of the fire service, thus its training is also based on that of professional fire fighters, which dates back in Hungary to 150 years [16: 8–9]. Their training institution has been called the Disaster Management Training Centre (KOK) since 2000. Since 2008, the training has had a modular structure, which brought rather large-scale changes to the training structure, to the teaching and learning process as well as to the examination procedure. The general transformation of law enforcement training in 2010 also affected the training system of the KOK.

The training consists of three modules: the first – as in the other two law enforcement organisations – is Core Duties in Law Enforcement. A part of the instruction of this module is not carried out in the KOK but in law enforcement vocational schools. Out of the three months, the students of disaster recovery attend their classes (in total 250 lessons) for two months alongside policing students in law enforcement schools. In the third month, however, in 130 lessons, they receive specialised instruction. The second and third modules last for two months each. The entire training duration is 7 months. Consequently, the contents of the school material resemble that of the students of prison service. Information technology is taught within the framework of the uniform Core Duties in Law Enforcement with the 20 lessons in Information Technology I. Further IT training is also part of the module Fire Service II. The subject

Communication of Information comprises 12 lessons out of the module of 276 lessons in total. As far as its material is concerned, it concentrates on wired and wireless communication, with special focus on the structure, operation and practical use of the radio network system EDR. In the module Fire Service I (283 lessons), students do not receive further instruction in information technology. All in all, students trained in fire service receive IT instruction in only 32 lessons.

Information Technology in Public Education

Today, information technology skills can primarily be acquired in elementary and high schools, I have therefore investigated its current application, curriculum and situation in public education. Before 1990, the instruction of information technology was divided into several parts, and the term "information technology" was not used at all. The instruction of wired and wireless communication, however, has a past of several decades and an important present in technical secondary and higher education as well as higher-level military training.

From the 1960s, computer skills were mainly taught in higher education specialised in technology or economy. Secondary-level computer instruction was carried out in special IT-specialised vocational schools. In the second half of the 1980s and in the early 1990s, more and more elementary and high schools launched extra-curricular IT-related courses, which enriched the education range of information technology. At the time, programming represented the backbone of IT-instruction, especially the programming language Basic [17: 34–41].

In 1995, the National Curriculum of Hungary was adopted, which – as a novelty – contained digital literacy. According to the curriculum, the instruction of information technology had to be introduced in junior high schools. The material stressed the importance of user-oriented programmes, such as the word processor, creation and management of charts and tables [18: 47]. However, the introduction of IT-studies was not entirely successful, as there was neither a sufficient number of computers nor enough specialised teachers.

The infrastructural foundation of the instruction of information technology was supplied by the SuliNet programme announced in 1996 and launched in the school year of 1997/1998. Within its framework, internet access was provided first to high then to elementary schools, and in total, 11 thousand new computers got installed in schools [19: 29].

In addition to the provision of the assets, it was also an important step that the framework curriculum was passed as a law, which ensured new perspectives from the school year of 2001/2002 onwards. In summary, we can establish that the compulsory instruction of information technology began between 1998 and 2001 in elementary and high schools. Thus, children born in 1984 had the opportunity to study IT if they wanted to, while those born after 1988 had to study IT in public education.

Presently, the mandatory number of classes is governed by the Act issued by the Ministry of Human Resources in 2012 on the rules of issuing and approval of framework curricula [20]. The framework curriculum for the years 5 to 8 of elementary

schools defines "digital competences" among the key competences and competence development aims, as follows: "Students become increasingly motivated to use ICT-devices. They are capable of using basic computer applications (word processor, data handling) during their curricular and extra-curricular activities as well as in their everyday life. With increasing confidence, they are able to make use of the information provided by computers and the internet, even in collection tasks according to given criteria" [21: 6]. In accordance with the framework curriculum, information technology is a compulsory school subject in the 6th, the 7th and the 8th grades of elementary school in 1 lesson/week, which comes to 36 lessons per school year [21: 8–10]. The school material focuses on the importance of problem solving and regards the proficient use of user programmes as essential [21: 654–660].

In grammar schools, information technology is taught in 1 lesson/week in the years 9 and 10 (which makes 36 lessons a year) [22: 9–11]. The curriculum concentrates on the use of applications, internet literacy and its efficient use, but the emphasis is again on problem solving with the use of IT in the most various domains [22: 578–600]. In vocational schools, the framework curriculum regards digital competences as a key competence, similarly to the framework curriculum of grammar schools [23: 5]. The number of IT lessons in vocational schools can differ, however, from that of grammar schools, depending on its specialisation, but it can be established that in the majority of vocational schools, information technology is a compulsory subject in at least 2 lessons/week in the years 9 and 10, which adds up to 72 lessons a school year [23: 8–18]. The description of the material is roughly identical with that in the grammar school curriculum [23: 694–711].

Questionnaire Survey

In order to be able to assess the information technology training of NCOs in law enforcement, in 2018 I conducted a questionnaire survey with the participation of 122 policing students, 98 prison service students and 98 disaster management students. The questionnaire listed 16 questions, which focussed on previous training in IT, previously acquired IT-skills and on the IT-infrastructure of law enforcement organisations in addition to statistics-related questions.

Nearly three-quarters of the participants were male in the police forces, in the prison service the ratio of men and women was 57%–43%, while in disaster recovery, all participants (100%) were male. There are serious differences in age between the three organisations, see below:

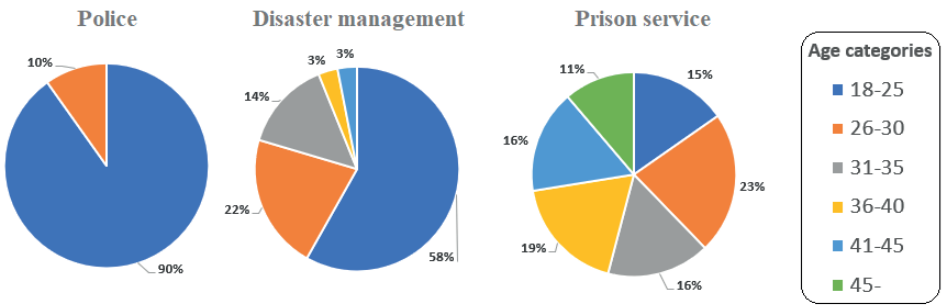


Figure 1.
Distribution of students by age [Compiled by the author.]

In the police forces, it is quite typical that students move on to the policing vocational schools right after their secondary final examination. Among disaster management students, age distribution is more varied, but there are only a few students over 35 years of age due to the demanding physical requirements. In prison service, all age groups are present in significant numbers.

Based on the answers to my questions, I could establish that the great majority of the participants have the necessary devices to access digital services (PC, laptop, smart phone, tablet) supplied with a wired and/or mobile broadband internet connection. 92% of the informants had studied information technology at school (100% of policing students, 98% of the disaster recovery students and 78% of prison service students). The differences result from the varying age distribution. About 16% of the informants had passed a secondary final exam in information technology, and most of the participants had felt satisfied with the available computing devices, the informativeness of the teachers and the quality of the material.

It is due to the age difference that 95% of the prison service students had had a job before, and 80% of them would have used computers. Having explored the students' user habits, we can see that most of them use the internet to reach social media sites, manage their email correspondence or read the news and access other information. Most of the participants have already done shopping online. Finance- and public services-related issues are mostly managed online by those who run their own household.

The majority of the informants of the survey regard their word processing, table and presentation creating skills at least average or, more often, good. On the other hand, regarding corporate network systems and security, they deem their skills poor, as also reflected by the questions focusing on IT systems and products. All participants agreed that information technology was crucial for their jobs, and IT-related training was completely essential.

In public education, the instruction of information technology has been obligatory since 2001, but most of the elementary and high schools had started giving IT courses before that. Students take three years of information technology in elementary and

two years in high school, but most schools exploit their possibilities and extend their IT-instruction.

As a result, most students who study to be NCOs in law enforcement have taken IT lessons in public education. Those applicants who wish to work in law enforcement, have begun their relevant training and are older than 35, have almost invariably held a job before, where most of them would have used IT devices and systems, thus they also do have basic computer skills. My questionnaire survey conducted in the training of NCOs also supports my statements.

Based on the above claims, I conclude that the instruction of basic competences in information technology (word processing, creating tables and presentations, use of operation systems, internet literacy and online search, etc.) is not at all necessary unless for helping candidates with poorer skills (established through a placement test) to catch up. However, with the quick-paced technological development and extended use of technology, the instruction of corporate IT-systems and IT-security would be essentially important, including the management of unusual events (reporting, error detection and localisation or reduction of damage).

Conclusion

In this paper I demonstrated that information technology is completely indispensable in all domains of life. Consequently, fewer and fewer jobs can be performed without computer skills. Law enforcement is no exception. I therefore decided to carry out an analysis of the training of NCOs, more specifically, their training in information technology.

The law enforcement training has been made uniform and modular by the Ministry of Interior, yet the training of policing students still greatly differs from that of students of prison service and disaster recovery. Having studied the school subjects, I established that information technology is taught in several of them. The activities, administration performed by IT devices or systems in a specific area should be instructed within or connected to the subject relevant to the given area by a specialist. The reason for this is that professional and specific areas do not change but, because of the technological development, the platforms of the collection, processing, forwarding and servicing of data and information do (see digital technology instead of an analogue one, IT devices or systems instead of paper).

I conducted a questionnaire survey among law enforcement students with the main conclusions that most students enter the training with IT-skills previously acquired in public education. They, however, do not have sufficient knowledge of IT-security and corporate IT-systems. Comparing this with the IT-instruction in elementary and high schools, I concluded that a part of the IT-training could be omitted and more advanced IT-related topics should be taught instead. The changes that I suggest in this paper serve a better quality IT-training provided to the students of vocational schools of law enforcement.

References

[1] B. Kákóczki, "Az „Epitoma" hatása a középkori (had)tudományos irodalomra," PhD dissertation, University of Debrecen, Doctoral School of History and Ethnography, Debrecen, 2012.
[2] Recommendation 2006/962/EC of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning (16 December 2006).
[3] A. Abonyi-Tóth and M. Turcsányi-Szabó, *A digitális írástudás fejlesztésének lehetőségei.* Budapest: Educatio Kft., 2015.
[4] Digital Welfare Programme of the Hungarian Government, based on Government Resolution 2012/2015 (XII. 29.) and the results of the national consultation on the internet and digital development projects (InternetKon).
[5] Government Resolution 1536/2016 (X. 13.) on the digital reform of public education, vocational education, HE and adult training system and on the Hungarian Digital Education Strategy
[6] The Digital Education Strategy of Hungary, Supplement of the Government proposal, Budapest, 2016.
[7] I. Bökönyi, "A rendőr tiszthelyettes- és zászlósképzés felszabadulás utáni története, helyzete, fejlesztésének lehetőségei," dissertation, Miklós Zrínyi Military Academy, Budapest, 1987.
[8] Government Decree 212/2010 (VII. 1.) on the scope of activities and competence of the individual ministers and the State Secretary heading the Prime Minister's Office.
[9] Act CXXVIII of 2011 on the amendment of the Act on Disaster Management and of other Acts in relation.
[10] Government Resolution 1282/2010 (XII. 15.) on the measures necessary for the uniform modular training system of law enforcement organisations.
[11] Act CXC of 2011 on National Public Education.
[12] Curriculum of the Vocational School of Law Enforcement in Körmend (Körmend, 2017).
[13] Government Resolution 1282/2010 (XII. 15.) on the measures necessary for the uniform modular training system of law enforcement organisations.
[14] "Iskolarendszeren kívüli büntetés-végrehajtási felügyelő szakképesítés képzési programja," [Qualification training programme of prison officers outside the education system], identification number OKJ 52 861 02, BVOTRK, 2016.
[15] B. Tuba Kovács, "Büntetés-végrehajtási informatikai ismeretek," notes, 2017.
[16] I. Berki and Á. Berkiné Ványi, Eds., *A Katasztrófavédelmi Oktatási Központ és jogelőd szervezeteinek hét évtizedes története.* Budapest: Disaster Management Training Centre, 2018.
[17] Á. Nagy, "Információs írástudás és informatikai intelligencia. Az informatika oktatás paradigmaváltásai Magyarországon," *Új Pedagógiai Szemle,* vol. 50, no. 4, 2000.

[18] B. Czékmán and P. Fehér, "A számítógéppel támogatott tanítás és tanulás története a közoktatásban Magyarországon (1983–2016)," *Képzés és Gyakorlat,* vol. 15, no. 1–2, 2017.
[19] I. Kónya, "Az informatika fejlődése a magyar közoktatásban," M. A. thesis, University of Debrecen, Faculty of Information Technology, Debrecen, 2007.
[20] Ministerial Decree 51/2012 (XII. 21.) of the Ministry of Human Resources on the rules of issuing and approval of framework curricula.
[21] Framework curriculum for grades 5–8 of elementary schools, Appendix 2 of Ministerial Decree 51/2012 (XII. 21.) of the Ministry of Human Resources.
[22] Framework curriculum for grades 9–12 of high schools, Appendix 3 of Ministerial Decree 51/2012 (XII. 21.) of the Ministry of Human Resources.
[23] Framework curriculum for grades 9–12 of vocational schools, Appendix 14 of Ministerial Decree 51/2012 (XII. 21.) of the Ministry of Human Resources.
[24] I. Hahn, ed., *A hadművészet ókori klasszikusai.* Budapest: Zrínyi Katonai Kiadó, 1963.

HADMÉRNÖK
FÓRUM
15. évfolyam (2020) 1. szám 195–206.
DOI: 10.32567/hm.2020.1.13

Haláchy Enikő,[1] Radnóty Gábor[2]

A magyar egészségügyi tartalékolás intézményrendszerének történelmi áttekintése 1. rész

The Historical Review of the Hungarian Healthcare Supply Part 1

A háború az egész történelem folyamán az egészségügy fejlődésének egyik legintenzívebb mozgatórugója volt. A fegyverek és hadigépezetek fejlődése magával vonta a harctéri sérültellátás egyre komolyabb kihívásait, mennyiségi és minőségi szempontból egyaránt. Ehhez fejlődnie kellett a sebesültellátók képességeinek és az egészségügyi anyagok tartalékolásának, diszlokációjának, logisztikájának és hatékony felhasználásának is. A szerzők a fejlődés folyamatát mutatják be az első részben a 17. századtól az 1848–49-es szabadságharc bukásáig, illetve a második részben az első világháborút megelőző évtizedektől napjainkig.

Kulcsszavak: **egészségügyi tartalék, kórház, gyógyszer**

In the course of history, war was the most intensive inducement of the evolution of healthcare. The evolution of guns and war machines involves more and more serious challenges in the care of battle injuries both in quantitative and qualitative ways. Therefore, the capabilities of battlefield medics logistics and efficient use of healthcare materials had to improve. In the first part of the article, the authors show this process beginning with the 17th century until the breakdown of the 1848–1849 independence war, and in the second part, from the decades prior to the First World War until nowadays.

Keywords: **healthcare supply, hospital, medicine**

[1] Állami Egészségügyi Ellátó Központ, egészségügyi készletgazdálkodási főosztályvezető, e-mail: halachy.eniko@gmail.com, ORCID: https://orcid.org/0000-0001-7528-4990
[2] Nyugdíjas orvos, volt EMMI védelmi referens, e-mail: garadn@freemail.hu, ORCID: https://orcid.org/0000-0003-0874-9713

Bevezetés

Az egészségügyi tartalékolás intézményrendszerének áttekintése előtt alapvető fontosságú a tartalékolás – ezen belül az egészségügyikészlet-tartalékolás – fogalmának tisztázása. Ez azért is indokolt, mivel időről időre felmerülő elképzelés, hogy a tartalékkészletek ne csak tárolva legyenek egy esetlegesen bekövetkező – a működő egészségügyi intézmények ellátókapacitást meghaladó – beteg vagy sérült tömeg ellátásához, hanem a készletek vagy azok egyes elemei – gazdaságossági szemléletből kiindulva – minél nagyobb mértékben kerüljenek napi használatba is.

A magyar nyelv értelmező szótára a tartalékot általánosan a következőképpen határozza meg: A tartalék: „Későbbi felhasználás végett megtakarított, félretett v. felhalmozott pénz v. más anyagi eszköz" [1].

A tartalék tehát egyértelműen egy meghatározott célra tárolt, elraktározott és állagmegóvott készlet, amelyet olyan esemény bekövetkezésekor vesznek használatba, illetve használnak fel, amelyhez nélkülözhetetlen az igénybevétele a meghatározott cél eléréséhez.

Az egészségügyi tartalékot az Állami Egészségügyi Tartalékkal való gazdálkodás szabályairól szóló 1/2016. (I. 13.) EMMI rendelet 3. § (1) bekezdése az alábbiak szerint definiálja: „A tartalék a Kormány által meghatározott rendeltetésű és mértékű, az egészségügyi ellátórendszer kapacitásának bővítéséhez, valamint az egészségügyi feladatok ellátásához szükséges tartalékelemeket tartalmazza" [2].

Az egészségügyi tartalékolás jogi alapját az egészségügyről szóló 1997. évi CLIV. törvény képezi, amelynek a 230. § (1) bekezdése úgy rendelkezik, hogy „az egészségügyi válsághelyzeti ellátás biztosítása és finanszírozása állami feladat", a (2) bekezdés pedig kimondja, hogy „az egészségügyi válsághelyzeti ellátás biztosításának állami kötelezettsége magába foglalja az erre történő felkészülési tevékenység, valamint a tényleges működés megszervezését és lebonyolítását". Továbbá a (3) bekezdésében kimondja, hogy az egészségügyi válsághelyzeti ellátásra való felkészülési tevékenység kiterjed az egészségügyi készletek tartalékolására is [3].

Az egészségügyi válsághelyzeti ellátásról szóló 521/2013. (XII. 30.) Korm. rendelet 10. §-a alapján „az állam egészségügyi válsághelyzet esetére a tömeges ellátás feltételeinek biztosítása, a szükséggyógyintézetek működéséhez, továbbá az egészségügyi válsághelyzeti ellátáshoz szükséges gyógyszerek, egészségügyi anyagok és eszközök azonnali rendelkezésre állása céljából" Állami Egészségügyi Tartalékot tart fenn, és ezt az egészségügyért felelős miniszter felügyeli [4].

Az egészségügyi tartalékolás megjelenése néhány jelentősebb történelmi korszakban

Az orvostörténeti szakirodalomban számos publikáció foglalkozik egy-egy adott korszak katona-egészségügyével, részletezve annak szervezeti felépítését, működését, személyi állományának tevékenységét, finanszírozását stb. A publikációk rálátást biztosítanak az adott kor orvosi eljárásaival, a sérültek ellátásával, gyógyításával, elhelyezésével kapcsolatos tudnivalókra is. Sajnálatos módon azonban alig találhatók adatok arról, hogy

milyen úton-módon történt az egészségügyi szervezetek anyagbiztosítása, illetve annak során képeztek-e tartalékkészleteket.

Az időben visszatekintve a korábbi évszázadokban már akadtak példák rövid időn belül felhasznált kisebb tartalékok képzésére, de természetesen a mai értelemben vett egészségügyi tartalékolás még nem létezett. Az egyes hadvezérek részéről – a korabeli feljegyzések szerint már voltak törekvések, hogy egy-egy konkrét katonai művelet – csata, várvédelem stb. – esetén a sereg a sérültek ellátásához rendelkezzen szükséges eszközökkel, a kötözésekhez tépésekkel.

A 17–18. században sem a békeidejű, sem hadműveletek előtti tartalékképzés nem létezett, és az egészségügy akkori fejlettségi szintjén több okból nem is létezhetett.

A mai értelemben vett gyógyszerek még nem léteztek, a füves gyógymód volt az uralkodó, a sokféle levélből, gyökérből, sóból előállított készítmények használata volt a jellemző, amelyeket gyakorlatilag a füves asszonyok, szerzetesek, illetve a kis számban működő borbélyok, patikáriusok vagy orvosdoktorok állítottak elő.

Kötszerekként tépéseket, gyolcsokat használtak, ezeket is jellemzően a harci sérülteket ellátó helyeken, az aktuális szükségletek kielégítése céljából, a mindenkori lehetőségek függvényében állították elő.

Az orvostechnikai eszközök tartalékolása szintén nem jöhetett szóba, mivel a hadakat kísérő korabeli borbélyok, felcserek, orvosok a saját eszközeiket használták, így azokból külön készleteket nem alkottak. A sebek varrására selymet, lenfonalat és bélhúrt használtak.

1. ábra
Savoyai Jenő herceg császári altábornagy[3] [5]

Fektetőanyagokra – ágyakra, takarókra – sem volt igény, mert a könnyebb, rövid időn belül újra harcképes sérültek a csapataiknál maradtak, a járni, lovagolni nem képes

[3] CC-BY-SA-3.0 licenc szerinti felhasználás.

súlyosabb sérülteket pedig a seregek vonulási útvonalain lévő falvakban, városokban ad hoc helyezték el – az akkori igen szűkös borbély-, felcser- és orvosellátottság miatt – többnyire a helyi lakosság gondoskodására bízva.

Az 1600-as évek végén a Savoyai Jenő herceg, császári altábornagy által vezetett osztrák hadseregnek az észak-olaszországi hadműveletekben már volt egy mozgó tábori kórháza (Fliegendes Spital), amely csak egyszer települt.

A hadseregtörzsnél működő orvosok, sebészek, patikusok az egyetlen mozgó egészségügyi anyagraktár (Bewegliche halbe Apotheke) készleteivel elsősorban a sebesültjeiket ellátó polgári kórházak felszereltségét erősítették. Feltehetően ez nem egy békeidejű tartalék háborús felhasználása volt, hanem csak az adott hadművelet – mai terminológia szerint – egészségügyi biztosítására hozták létre.

A Rákóczi-szabadságharc idején

A Rákóczi-szabadságharc alatt a gyógyszerkészítés az orvosi tényked̈és részét is képezte, de gyógyszerészektől (patikáriusoktól) és szerzetesrendektől is szereztek be gyógyszereket, amelyeket sokféle gyógynövény leveleiből, virágaiból, gyökereiből főzetekként készítettek, külső vagy belső használat céljára [6].

A szabadságharc első éveiben az elfogyott gyógyszerek utánpótlását alapvető módon a seregek mozgási útvonalának környékén, helyben szerezték be.

A betegellátás legsúlyosabb kérdése a gyógyszer- és kötszerellátás volt, mert egyrészt az országban csak egy-két tucatnyi patika működött, ezek azonban nem voltak képesek nagyobb mennyiségek előállítására, másrészt a háborús gazdasági helyzetben nem voltak elégséges pénzügyi források a gyógyszeralapanyagok megvásárlására.

A központi gyógyszerellátást Láng Jakab Ambrus, a hadsereg tábori főorvosa (protomedicus) szervezte meg, aki a sereg egészségügyi ellátásának irányításán túl, 1706 őszén a selmecbányai patikára alapozva szervezte meg a kuruc sereg gyógyszerellátását, és ettől kezdve a selmeci patika központi ellátószervként működött.

Láng Jakab ezer rajnai aranyat kapott a kincstártól, hogy Lengyelországból vásároljon gyógyszer (alapanyag) utánpótlást. Az első nagyobb beérkező szállítmányt Selmecbányára irányította, itt alakították ki 1708-ban az ország központi patikáját (Apotheca Regni principalis), ahonnan az ott elkészített gyógyszereket a csapatokhoz, illetve a várakba juttatták el. Mivel Láng doktor a selmeci patikát egészségügyi anyagi bázisnak nevezi (Fundus noster), ez tekinthető a központi egészségügyi anyagraktárnak. A továbbiakban is ide irányították a szállítmányokat, amelyek elsősorban Lengyelországból érkeztek.

Ismerve a szabadságharc hadműveleteinek kiterjedését, felmerülhet a kérdés, miért az ország egy viszonylag távoli, felvidéki patikája kapta ezt a feladatot. Ennek az a magyarázata, hogy 1700 elején még csak néhány év telt el a 150 éves török megszállás, illetve az attól felszabadító, súlyos pusztításokkal járó háború befejezése óta, és ebben az időben csak néhány északi bányavárosban voltak működő patikák.

Ez a selmeci központi raktár még nem készlettartalékoló, hanem elosztóbázisként működött, és kuruc hadviselésjellegénél fogva nem is egyedül biztosította a gyógyszerek utánpótlását.

Erre a kuruc csapatok jellegzetes portyázó hadviselési módja, illetve a gyors csapatmozgásokat követni nem képes logisztika okán nem is lett volna lehetőség.

A gyorsan mozgó kuruc csapatoknál a sebesültek csak rövid ideig maradhattak az egységeknél, mert igyekeztek őket a legelső faluban vagy városban elhelyezni.

A hátországban működő „tábori kórházak" sem katonai intézmények voltak, hanem a legtöbb esetben a hadsereg a már korábban is működő városi ispotályokat vette igénybe, amelyek polgári sebészét a katonák ellátásáért külön megfizették, valamint a lehetőségekhez képest a szükséges gyógyszerekkel, pontosabban az elkészítésükhöz való alapanyagokkal is ellátták.

Működtetésükről a helyi elöljáróság intézkedett, kiadásaikat a hadbiztosság fizette ki. A gyógyszereket leginkább a helyi patikában vásárolták meg, illetve a protomedicus a selmeci központi gyógyszerraktárból hozatta meg [7].

A gyógyszerekhez szükséges anyagok szállítása és így az ellátás is 1709-ig folyamatos volt, azt követően azonban a kincstár forrásai kimerültek, továbbá a császári csapatok térnyerésükkel nemcsak elzárták a lengyelországi beszerzési útvonalakat, hanem még a selmeci raktárt is elfoglalták és a készleteket elkobozták. Ekkor még sikerült Károlyi Sándor közreműködésével egy nagyobb mennyiségű alapanyagot beszerezni német, illetve orosz területről [8], [9].

Az 1848–49-es forradalom és szabadságharc idején

A Jelasics bán császári-királyi táborszernagy által vezetett támadás idején, 1848. szeptember 20-án Sauer Ignácot nevezték ki a nemzetőrség igazgató főorvosává, aki ebben a minőségében intézkedéseket tett a honvédsereg egészségügyének megszervezésére.

2. ábra
Stáhly Ignác[4] [10]

[4] Klauzál Gábor Társaság honlapja.

Kossuth javaslatára, 1848. október 13-án a Honvédelmi Minisztérium a szervezés alatt álló honvédorvosi kar élére tábori főorvosnak Stáhly Ignácot nevezte ki, és megbízta a minisztérium egészségügyi osztályának megszervezésével.

Kossuth 1848. december 12-én utasította Stáhlyt, hogy intézkedjen a pesti Károly kaszárnya gyógyszertárnak központi katonai gyógyszertárrá történő alakításáról, továbbá egy vegyészi laboratóriummal való kiegészítéséről, hogy onnan tudják biztosítani a tábori gyógyintézetek gyógyszerellátását.

A kialakítandó Pesti Középponti Gyógyszertár, és a vegyészeti gyár, valamint a raktár igazgatójává Leifer János gyógyszerész századost nevezte ki [11].

3. ábra

Pest, az egykori Gránátos utcai Károly laktanya, az első gyógyszergyár és raktár[5] [12]

A Tiszához történt 1849. januári visszavonulás után a csapatok egészségügyi ellátása kritikus helyzetbe került. A Tiszántúlon minden jelentékenyebb településen tábori kórház működött, és a haderő létszámának növekedésével, valamint a tiszai központi hadsereg összevonásával egyre több kórházra volt szükség.

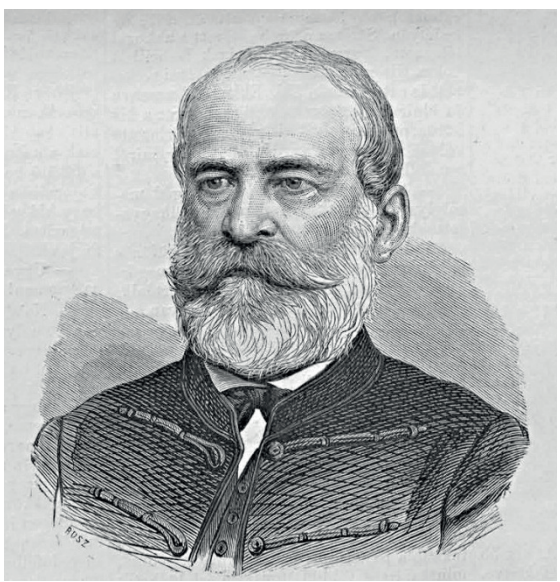
Ezek néhány nap alatt kialakított rögtönzött intézetek voltak, és rendszerint a helyi községi vagy városi elöljáróságnak kellett fektetőanyagokkal (ágyakkal, lepedőkkel, takarókkal, párnákkal, szalmazsákkal, szalmával) és tűzifával ellátnia, amelyeket – mivel ebben az időszakban más beszerzési forrás nem állt rendelkezésre – az elöljáróságok a lakosságtól gyűjtöttek be.

[5] Ma városházaként üzemel.

A tábori kórházakat orvosi eszközökkel, különösen a műtétekhez szükségesekkel, valamint sebkötöző anyaggal és gyógyszerekkel csak szűkösen tudták ellátni, mert a Tiszántúlon már komoly nehézséget jelentett az utánpótlások beszerzése. Magyarországon egyébként sem létezett önálló orvosi műszergyártás, az orvosi felszereléseket elsősorban bécsi és német műszergyártóktól lehetett csak beszerezni.

A kötözőszerek megszerzése valamivel könnyebb volt, mert többnyire elegendő mennyiségben rendelkezésre állt az ehhez szükséges vászonanyag, és a harcok kezdete óta tömegesen érkeztek a városi nőegyletek, iskolák, kaszinók, olvasóegyletek, egyházak által előállított különböző sebkötő pólyák és kötszerek [13].

Mivel Stáhly – egészségi állapota miatt – nem követhette a császári csapatok elől Budáról Debrecenbe költöző kormányt, az egészségügyi ellátás irányítása átmenetileg Töltényi János titoknokra hárult, majd Szemere Bertalan hadügyminiszter Stáhly utódjaként Flór Ferenc főorvost, Pest tisztiorvosát, a Rókus Kórház igazgatóját nevezte ki a Hadügyminisztérium Egészségügyi Osztálya élére [14].



4. ábra
Flór Ferenc[6] [15]

Flór elsősorban a betegellátás gyakorlati megszervezését és biztosítását tekintette elsődleges feladatának, de emellett folytatta a katonaorvosi kar megszervezését is.

1949 elején néhány nap alatt felmérte a hadsereg egészségügyi szolgálatának helyzetét, a honvédorvosi és ápolói személyzet létszámát, a tábori kórházak helyzetét, ellátókapacitását, gyógyszer- és kötszerigényét. „A gyakorlati ellátás területén szigorú követelményeket állítottak fel, pontosan meghatározták a kórházak szükséges felszerelését (ágy, párna, takaró stb.), szabványosították a kórházak műszerezettségét" [11].

[6] Rusz Károly metszete. CC-BY-SA-3.0 licenc szerinti felhasználás.

A tábori és a hátországi honvédkórházak műszerellátásának biztosítása érdekében a Hadügyminisztérium Egészségi Osztálya egyrészt 1849. január 18-án felszólította a törvényhatóságokat, hogy a birtokukban lévő műtőszereket, ideiglenes használatra engedjék át a sérült honvédek ellátására, másrészt intézkedett a gyártás beindításáról is.

1849 februárjában Nagyváradon – a rögtönzött kardgyár egy szobájában – megkezdték a sebészi eszközök gyártását, és április első felében már kikerültek az első példányok.

5. ábra
Nagyváradi vár[7] [16]

Az Egészségügyi Osztály Debrecenben is létesített orvosi műszerkészítő műhelyt, és mindkettő Grósz Albert törzsorvos, a váradi katonai kórházak főorvosának felügyelete alatt működött.

Flór a tábori kórházak és a hadsereg rendszeres gyógyszerellátása céljából, a kényszerűségből Pesten hagyott központi katonai gyógyszertár pótlására Debrecenben központi gyógyszerkészítő laboratóriumot és gyógyszerraktárat állított fel. Ez irányította a mozgó tábori patikákat, és ide gyűjtötték össze a tiszántúli gyógyszertárakban előállított készítményeket.

Az ország ellen hozott gazdasági embargó, amely nemcsak a fegyverbehozatalra, hanem minden egyébre kiterjedt egyre jobban éreztette hatását.

[7] A kardgyár egyik helyiségében folyt a sebészeti eszközök gyártása.

A Honvédelmi Minisztérium 1849. január 18-án felhívást intézett a Tisza-vidék és különösen Debrecen város hölgyeihez, sebkötöző tépésanyagok készítését kérve. Ennek eredményeképpen a város hölgyeinek példájára Debrecen tíz leányiskolájának növendékei is tépéseket készítettek tanóráik után.

Meszlényiné Kossuth Zsuzsanna 1849 januárjától az egyik főszervezője volt az Országos Nőegylet gyűjtési munkáinak. A súlyos kötszer, tépés és egyéb kórházi ápolási felszerelések hiányának enyhítése érdekében, 1849 februárjában az országosan alakuló önkéntes nőegyletekhez fordultak segítségért.

Jelentős változást hozott a kötszerellátásban és a kórházi ápolási anyagok tekintetében Kossuth Zsuzsanna 1849. áprilisi országos főápolónővé való kinevezése.

Az ő hatáskörébe került az akkor létrehozott Országos Kórodai Főápolónői Intézet, amelynek többek között feladata lett a kórházi ápoláshoz szükséges felszerelések begyűjtése, tárolása és szétosztása.

Az intézet Debrecenben a Kereskedelmi Minisztérium épületében, a Czeglédi úton kapott elhelyezést.[8] Itt állították fel a központi kórházi anyagraktárt is, amely felett a szintén az országos főápolónő rendelkezett.

Az Országos Nőegylet szintén rendelkezett saját készletekkel, amelyeket rendszeresen a főápolónő rendelkezésére bocsátottak, vagy az általa kijelölt helyre szállíttatták. Mindkét anyagraktárban kizárólag csak az ápoláshoz szükséges felszereléseket (ágyakat, párnákat, takarókat, fehérneműket, kötszereket stb.) tárolták [17].

A leiratokból úgy tűnik, hogy az Országos Kórodai Főápolónői Intézet megalakulását követően a kötszerellátás két úton jutott el a csapatokhoz és a tábori kórházakba. A különböző városi nőegyletek, iskolák, kaszinók, olvasóegyletek, egyházak által készített vagy gyűjtött kötszereket részben – a megyei hatóságok, lelkészek, kormánybiztosok, rendőri hivatalok, katonai parancsnokságok közvetítésével vagy közvetlenül – a környéken állomásozó csapatok és kórházak főorvosai kapták, részben

[8] Ettől eltér Tóth Béla Magyar Országos Levéltár főigazgató-helyettese által a *Honismeret* 1999. évi 1. számában közreadott, *A szabadságharc kormányának debreceni szálláshelyei* című levelezés. Ebben Karl Geringer, a szabadságharc bukása után teljhatalmat kapott politikai biztos Uray Bálinttól, a Debreceni Kerületi Főispántól kért tájékoztatást, hogy 1849 januárjától júniusáig Debrecenben tartózkodó kormány hol, melyik középületben vagy kinek a házában telepedett le. Uray a Debreceni Tanácshoz fordult, kérve az adatok közlését.
A Tóth Bálint által teljes terjedelmében eredeti helyesírásával közölt válaszlevél a következő:
„Méltóságodnak folyó Junius hónapi 13-ról 4855-k szám alatt – a vót Magyar Ministérium hiányzó actainak keresése tárgyában – kelt rendeletére – hivatali tisztelettel válaszoljuk:
A vólt Magyar Ministerium Debreczeni szállásolása ideje alatt
Az elnöki hivatal működött folytonosan a Város házánál, honnan 1849-ki Junius elején Pestre elköltözvén, minden irományait össze packolva magával vitte.
A Pénzügyi Minisztérium hivatal szobái voltak a Péterfia utczán az Oláh Miklós ur házában, ezen iigyérség is részint Junius elején, részint Junius végén (a múlt évben) innen eltávozván, maga minden iratait magával vitte.
A Hadügyi Minisztérium szállásolt a Beck féle házban, honnan mindgyárt az Ország-gyűlés itteni bevégzésekor eltávozván hasonlóúl minden iratait magával elszállította.
A Bel-ügy Ministerium szállásolt részint a Komáromi féle városi háznál, részint az Orbán János -részint a Zsebők féle házaknál, de ez is minden iratait 1849-ki Junius elején innen eltakarította;
A Kereskedés és Közlekedés ügyszintén a Vallás, és Közoktatási Ministeriumoknak rendezett irodájok ott Debreczenben nem volt.
Melly fentebb megnevezett helyeken a volt magyar Ministeriumnak semmi iratai sem találtattak.
Kik egyébiránt mély tisztelettel vagyunk.
Debreczenben 1850 Junius 26-án.
Méltóságos Udvari Tanácsos és Debreczen Kerületi Cs. K. főispán Urnák alázatás szolgái
Debreczen Sz. K. Város Tanács" [18].

az Országos Honvédelmi Bizottmányhoz, a Hadügyminisztériumhoz, az országos főápolónőhöz, illetve a nagyváradi központi ruhabizottmányhoz kerültek, és onnan lettek kiosztva a csapatokhoz, valamint a tábori kórházakba.

Az Országos Kórodai Főápolónői Intézet által felügyelt központi kórházi anyagraktár, valamint az Országos Nőegylet általi készletezés már a mai értelemben vett egészségügyi tartalékolás előfutárának tekinthető, még ha a készletek felhalmozása és tárolása nem békeidőben kezdődött, és viszonylag rövid időtartamú volt is.

A Hadügyminisztérium a kötszerek utánpótlását az adományokon kívül kisebb kötszer-előállítóktól történő vásárlásokkal, illetve állami gyártással is igyekezett biztosítani.

A kötszerellátás mindezeknek a szervezési intézkedéseknek ellenére is folyamatos nehézséget jelentett, ezért 1849. májusában a Belügyminisztérium felszólította Szabolcs és Szatmár megyéket, hogy a háborútól kevésbé szenvedett helységekben gyűjtsenek be sebkötözésre alkalmas vászonneműt [13].

Összefoglalás

Az orvostörténeti szakirodalom bőségesen feldolgozta a különböző korok ellátórendszereinek szervezetét, működését, intézményi felépítését, műszerezettségét, az orvosi beavatkozások szakmai tartalmát és a használatos egészségügyi anyagokat, de csak elvétve találhatók adatok, információk arra vonatkozóan, hogy mikor, milyen formában jelent meg és fejlődött az egészségügyi készletezés, tartalékolás.

Az egészségügyi tartalékképzés sohasem szerepelt a figyelem vagy a közérdeklődés reflektorfényében, és az orvostörténeti szakirodalom sem dolgozta fel ezt a témakört. Ennek több oka is lehet. A távolabbi múltban az adott korra jellemző egészségügyi anyagok és eszközök összetétele okán nem merült fel különösebb igény a mai értelemben vett tartalékolásra, mivel iparilag előállított gyógyszerek egyszerűen nem léteztek, a sebészi eszközök az orvosok, borbélyok és a patkolókovácsok saját műszerei voltak, hadi sérültek elhelyezésének módozatai a fektetőanyagok készletezését sem tették szükségessé. Másrészt a honvédegészségügyi ellátás anyagi-technikai biztosítása jellemzően „periodikum": békeidőben nem- vagy alig használt képesség, ami háborús vagy haváriahelyzetben sorsdöntő fontosságú tényezővé emelkedik.

A szerzők néhány kiválasztott történelmi periódus hadi eseményeinek egészségügyi biztosítása kapcsán vizsgálják, hogy azok egészségügyi anyagbiztosításában és logisztikájában mikor és milyen formában jelenik meg a tartalékok képzése. Míg kezdetben csak egyes hadvezérek egy-egy konkrét hadművelet előkészítése vagy végrehajtása során esetlegesen hozott döntéseinek köszönhető egészségügyianyagbiztosítás, addig az 1848–49-es szabadságharc időszakára már körvonalazódni látszik egyfajta központi, állami szinten elrendelt tartalékolási tevékenység is, igaz, ez még nem a békeidőszakban létrehozott tartalékolás volt.

Mindenképpen említésre méltó, hogy 1849 elején Flór Ferenc a kórházi ellátás területén szigorú követelményeket állított fel, amelyek alapján meghatározták a kórházak kötelező felszereltségét (ágy, párna, takaró), a műszerek szabványosítását. Az intézkedésekkel olyan eszköz- és anyagnormákat alakítottak ki, amelyek – ha a hadi

események alakulása lehetővé tette volna – meghatározhatták volna a készletek pótlására történő beszerzések összetételét is, és ez már hasonlóságot mutat az Állami Egészségügy Tartalék összetételét meghatározó normákkal.

Hivatkozások

[1] A magyar nyelv értelmező szótára, „tartalék," *arcanum.hu,* [Online]. Elérhető: www.arcanum.hu/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/t-4D5B8/tartalek-4E212/ (Letöltve: 2018. 12. 12.)

[2] 1/2016. (I. 13.) EMMI rendelet az Állami Egészségügyi Tartalékkal való gazdálkodás szabályairól

[3] 1997. évi CLIV. törvény az egészségügyről

[4] 521/2013. (XII. 30.) Korm. rendelet az egészségügyi válsághelyzeti ellátásról

[5] Wikipédia a Szabad Enciklopédia, „Savoyai Jenő," *Wikipédia a Szabad Enciklopédia,* [Online]. Elérhető: https://hu.wikipedia.org/wiki/Savoyai_Jenő (Letöltve: 2018. 12. 18.)

[6] L. Takáts, „A Rákóczi-szabadságharc egészségügye," *mek.oszk.hu,* [Online]. Elérhető: http://mek.oszk.hu/05400/05419/05419.pdf (Letöltve: 2018. 12. 12.)

[7] K. Kapronczay, „Egészségi és katona-egészségügyi állapotok a Rákóczi-szabadságharc idején," *orvostortenelem.hu,* [Online]. Elérhető: www.orvostortenelem.hu/tankonyvek/tk-05/pdf/3.8.1/kapronczay_egeszsegi_allapotok.pdf (Letöltve: 2018. 11. 28.)

[8] L. Takáts és E. Takáts, „Lang Jakab Ambrus, a hadsereg tábori főorvosa," *orvostortenelem.hu,* [Online]. Elérhető: www.orvostortenelem.hu/tankonyvek/tk-05/pdf/3.8.1/takats_lang_jakab_ambrus.pdf (Letöltve: 2018. 11. 28.)

[9] K. Kapronczay szerk., „Háború és orvoslás," Magyar Orvostörténelmi Társaság, *real.mtak.hu,* 2015, [Online]. Elérhető: http://real.mtak.hu/52116/1/haboru_es_orvoslas.pdf (Letöltve: 2018. 11. 28.)

[10] „Dr. Stáhly Ignác," *klauzal.hu,* [Online]. Elérhető: www.klauzal.hu/image/zimage1264069650s.jpg.html?PHPSESSID=4e8c851468a28389ef8a9050cb6d0154 (Letöltve: 2018. 12. 12.)

[11] K. Kapronczay és E. Szemkeő, „A betegápolás szervezése a szabadságharc idején," *orvostortenelem.hu,* [Online]. Elérhető: www.orvostortenelem.hu/tankonyvek/tk-05/pdf/3.8.2/1981_093_096_kapronczay_szemkeo_betegapolas_szervezese.pdf (Letöltve: 2018. 11. 28.)

[12] „Laktanya," *fortepan.hu,* [Online]. Elérhető: www.fortepan.hu/?view=all&lang=-hu&tags[]=laktanya (Letöltve: 2018. 12. 25.)

[13] E. Varga, „Kötszerek a szabadságharcban," *orvostortenelem.hu,* [Online]. Elérhető: www.orvostortenelem.hu/tankonyvek/tk-05/pdf/3.8.2/Szh_Varga_kotszerek.pdf (Letöltve: 2018. 11. 28.)

[14] Á. Szállási, „A Kossuth-kormány egészségügye Debrecenben," *orvostortenelem.hu,* [Online]. Elérhető: www.orvostortenelem.hu/tankonyvek/tk-05/pdf/3.8.2/Szh_Szallasi_Kossutheu_Debrecen.pdf (Letöltve: 2018. 11. 28.)

[15] Wikipédia a Szabad Enciklopédia, „Flór Ferenc," *Wikipédia a Szabad Enciklopédia,* [Online]. Elérhető: https://hu.wikipedia.org/wiki/Fl%C3%B3r_Ferenc (Letöltve: 2018. 12. 28)
[16] Hungaricana képcsarnok, „Nagyváradi vár," *Hungaricana képcsarnok,* [Online]. Elérhető: https://gallery.hungaricana.hu/hu/OSZKKepeslap/24963/?img=0 (Letöltve: 2019. 02. 02.)
[17] K. Kapronczay és E. Szemkeő, „Kossuth Zsuzsanna országos főápolónő működése az 1848–1849. évi szabadságharcban," *orvostortenelem.hu,* [Online]. Elérhető: www.orvostortenelem.hu/tankonyvek/tk-05/pdf/3.8.2/Szh_Kapronczay_Szemkeo_KossuthZs.pdf (Letöltve: 2018. 12. 12.)
[18] B. Tóth, „A szabadságharc kormányának debreceni szálláshelyei," *Honismeret,* 27. évf. 1. sz., pp. 39–40., 1999. [Online]. Elérhető: https://epa.oszk.hu/03000/03018/00146/pdf/EPA03018_honismeret_1999_01_039-040.pdf (Letöltve: 2019. 01. 27.)

HADMÉRNÖK
FÓRUM
15. évfolyam (2020) 1. szám 207–220.
DOI: 10.32567/hm.2020.1.14

Zoltán Őze[1]

Special Features of the Russian–Ukrainian Armed Conflict

Az orosz–ukrán háború érdekességei

Russia's position in the ex-soviet region as a country with natural geopolitical interest toward neutrality and/or alliance with neighbouring states is in direct confrontation with Western European and U.S. ambitions in that region. Ukraine always represented a red line for Russia, who decided to act to preserve its regional interests. Russia intervened in a very uncommon way, utilising the new generation warfare. The article analyses the special features of the Russo–Ukrainian war in Eastern Ukraine.

Keywords: **Ukraine, hybrid warfare, Russian intervention**

Oroszország hatalmi érdekei a volt szovjet érdekszférában teljesen ellentétesek Nyugat-Európa és az USA érdekeivel. Ukrajna mindig is egy határvonalat képviselt Oroszország számára, ezért amikor úgy tűnt elveszítheti befolyását a régióban, úgy döntött beavatkozik, hogy megőrizze hatalmi fölényét a térségben. Oroszország egy nagyon sajátos, és tegyük hozzá rendkívül sikeres módszert választott a beavatkozásra, egy újfajta hibrid háború formájában. A cikk ezen beavatkozás sajátosságait elemzi.

Kulcsszavak: **Ukrajna, hibrid hadviselés, orosz beavatkozás**

[1] National University of Public Service Hadtudományi és Honvédtisztképző Kar, Katonai Tanfolyamszervező Intézet, kiemelt főtiszt, e-mail: ozezoltan@gmail.com, ORCID: https://orcid.org/0000-0003-4959-0294

"I would like to remind you Alexander III,
our emperor, who once said that Russia has just
two allies, the armed forces and the navy."
Vladimir Putin

Introduction

Since spring 2014, there has been an armed conflict between Ukraine and the Russian Federation. What started as a relatively bloodless intervention in the Crimea has grown into an unfinished, serious armed conflict in Eastern Ukraine.

This war has many surprises. First of all, even the best security experts in 2013 did not think that a war on land would soon take place in Europe and the East–West opposition would intensify again, evoking the Cold War atmosphere. Second, very few people in the West have been paying attention to Russian "new generation" or "hybrid" warfare, and even the NATO was unexpectedly affected by its Ukrainian manifestation. The third surprise is how little effort has been made by both the European Union and the U.S. to support Ukraine from a military point of view, even though the fighting has been expanding in scope and intensity for years [1].

Strategic Aspects of the Conflict

Ukrainian strategy

After the creation of the independent Ukrainian state, the history of Ukraine is divided into several periods. One of these significant periods was the ambition to join the EU and NATO. These foreign policy goals were supported by the international engagement of the Ukrainian Armed Forces and all political and military efforts to obtain Western guarantees to preserve its independence.

Like many other countries in Eastern Europe, Ukraine did not have a serious military strategy after declaring its independence from the Soviet Union. There was no foreseeable security threat or financial resources to modernise the army, so why waste time on the strategy? The Ukrainian army, which was once one of the largest ex-Warsaw Treaty armed forces, was steadily decreasing, and the luxury of modernisation was rendered impossible by the existing military budget [1].

After the collapse of the Yanukovych regime, when the Russians unexpectedly invaded the Crimea, deployed troops on the Russian–Ukrainian border and actively supported the East-Ukrainian conflict, the Ukrainians had to make up for the lost 20 years in two months [1].

At the time of the annexation of Crimea, Ukraine had no effective strategy, only an outdated army.

Russian strategy

In 1999, a former KGB agent, Vladimir Vladimirovich Putin came to power in Russia, and in 2005, a famous statement, according to which "the collapse of the Soviet Union was the biggest geopolitical catastrophe of the 20th century", predicted changes in European security policy [10].

Historically, Russia's most important defence strategy is to keep a potential opponent away from Russian borders, dating back to the time of Tsar Peter the Great. According to the ruler of the turn of the 17th and 18th centuries, Russia is only safe if it conquers the surrounding countries, thus preventing any direct attack on Moscow. (Both Napoleon and Hitler experienced the effectiveness of the principle.) In fact, today NATO is about 160 kilometres away from St. Petersburg, while that distance was 1,600 kilometres at the time of the Soviet Union [7].

Based on this, it is understandable that a Western-friendly Ukraine is an unacceptable option for the interests of Russia.

Behind the intervention in Ukraine was a Russian army, modernised in the light of the experience of the wars against Chechnya and Georgia [5], applying the principles of the "Gerasimov doctrine". This title is based on an article published in March 2013 by the Russian Chief of Staff, considered by many to be a revolutionary milestone in the hybrid war [17]. In fact, the concept of Russian next-generation warfare is the result of a long, organic development process in which Gerasimov's writing is only one link (and not the last one!), despite its unusually high international attention due to the Ukrainian war. Interestingly, the article's narrative is defensive all the time, meaning that the general does not write about how Russia should wage war, but how the West wages war on Russia [4], [9].

The most important feature of the Russian hybrid warfare is the more coordinated use of military and non-military assets. Non-military assets include diplomatic and economic pressure, the use of secret service activities and special operations, cyberattacks, the use of criminal groups and psychological and information operations that require the use of traditional and electronic media [9], [20], [21].

However, hybrid warfare is not some kind of ultimate secret weapon: it does not replace military power; it is just a new way of applying it, combined with the effective exploitation of the non-military weaknesses of the targeted state and society. If the threat of a military attack can be eliminated, the range of tools available to the hybrid attacker will be significantly reduced immediately. In Ukraine, however, all conditions were met to exploit the potential of the hybrid warfare [9].

The implementation of the new Russian strategy was so ingenious that by the time the Ukrainians realised who are the "little green human beings", they had practically lost the entire Crimea.

Special Features of the Operations

Mobilisation and deployment

While the annexation of the Crimea succeeded in a few weeks without a single gunshot in the spring of 2014, the unrest in Eastern Ukraine has turned into a protracted armed conflict. On April 15, in spite of the fact that Russian military exercises were constantly taking place along the border and there was always the danger of a Russian attack, the government in Kiev decided to use regular armed forces against the separatists, and initiated the so-called "Counter-terrorism operations" [9].

Despite the obvious difficulties – outdated organisational structure, lack of modernisation, lack of rapid reaction force – the Ukrainian army made the largest mobilisation in Europe since World War II, and has moved 15 brigades to the area in order to stabilise the region [1], [2].

The Russian deterrent force near the border was over 40,000 [18]. The deterrence was all the more credible because the war in Georgia in 2008 has shown that Russia is ready and capable of launching a conventional war against its weaker neighbour by invoking the protection of its own citizens [9].

Unlike in the Crimea, Moscow never officially acknowledged that it had anything to do with the separatist movement in Eastern Ukraine, although Russian support was clear from the beginning.

The most effective forces in the Donetsk and Luhansk Separatists were armed with Russian weapons; they used Russian equipment and military vehicles. They were often without identifiers, but wearing Russian type uniforms and even the Russian officials referred to them as members of the local resistance. The truth is that most of them were highly skilled Russians.[2]

In August of 2014, when the Ukrainian army was winning, Russian regular forces showed up in the area, also without any identifier [9].

Initial Ukrainian successes

After the transitional peace talks failed, a comprehensive Ukrainian operation was launched in the summer of 2014 against the rebels. The operation had three main objectives: first, to reduce the territorial base of the separatists, especially in areas where they received less support; second, to close the Russian–Ukrainian border, thereby cutting the supply lines of the rebels, and finally, to block the rebellious Luhansk and Donetsk provinces.

A great example of the successful use of Special Forces in operations is the battle of Sloviansk.

In early July 2014, the Ukrainian Special Forces and the 95th Airborne Brigade re-occupied Donetsk's third most important city in a quick, decisive battle. A special unit of 60 people infiltrated the city centre. When the rebels noticed that the enemy

[2] By mid-August 2014, only a few hundred special operations troops and up to 10,000,000 volunteers, mercenaries, and a few dozen half-regular units could participate in the battles [10].

were getting behind their posts, they immediately fought the invaders. Meanwhile, the forces of the 95th Brigade began to encircle the city. This initiated panic among the separatists, fearing that they would be cut off from their supply lines. Afraid of being trapped, they retreated 50 kilometres from the city, leaving their posts behind. Even the Ukrainian forces were surprised by the huge success [1].

After that in early August 2014, the 95th Airborne Assault Brigade executed a raid on enemy lines [1]. The 95th was the most skilled unit in Ukraine, which was even reinforced with two battalions of armoured infantry, a tank battalion and a self-propelled artillery battalion by mid-summer. The brigade crushed the positions of the separatists all the way to the Russian border, splitting the two "People's Republics" [1].

During the operation, in order to avoid civilian casualties, artillery and armoured forces were deployed to a minimal magnitude; this has led to protracted fighting in villages and cities, mainly involving the infantry [1].

Because of the successful Ukrainian operation, the Russians began to weaken Ukrainian forces in mid-July with artillery strikes across the border. In six weeks, 53 artillery shots were fired at 40 different targets. The most devastating of these was the decimation of two Ukrainian mechanised battalions near Zelenopillya [1]. As a consequence, the Ukrainians had withdrawn and surrendered large sections of the border to the Russian-backed forces, effectively giving the Russian military complete control of over 100 kilometres of Ukraine's south-eastern border. The Ukrainian Air Force played a crucial role in the initial success. The light-armed, undisciplined separatists were essentially unprotected from Ukrainian combat aircrafts and helicopters. In particular, the Sukhoi Su-25 crash planes and Mi-24 helicopters caused heavy losses to the rebels. The psychological impact of the air strikes was also significant and severely weakened the morale of the separatist teams, which were mainly local and Russian volunteers at the time.

Russian counter offensive

Because of the Ukrainian offensive, the separatists were forced to defend and retreat everywhere, and in the summer of 2014, this desperate defence suddenly turned into an offensive. Throughout July and August 2014, large infusions of new weapons and soldiers crossed the border to join the separatist fight against the Ukrainian Government. One such weapon transported across the border was the T-72 main battle tank. Not only had the Ukrainian military never used this tank in the conflict, but several variants of the tank spotted in Eastern Ukraine were never possessed by the Ukrainian military because they were updated versions of a tank that Russia never exported. The first recorded T-72 on Ukraine's battlefields appeared in the hands of the infamous Vostok Battalion mentioned earlier, and the tanks were later spotted at key battles across Eastern Ukraine, including Ilovaisk, which were major turning points in the war.

In the last week of August 2014, when the Ukrainian victory seemed almost certain, 6 Russian battalion tactical groups crossed the border to attack Ukrainian forces by surprise from the rear. The intervention force swept through the surprised Ukrainian light and mechanised battalions, weakened by artillery strikes in previous weeks [23].

The Russians were able to join the separatists in Donetsk in less than a week, and in addition, surrounded the regular and voluntary Ukrainian combat forces stationed near Ilovaisk. When the Ukrainians dispatched more troops to attempt to break the siege, they quickly found themselves outgunned. During this battle, Chechen fighters, equipped with BTR-82A armoured personnel carriers that were only put into service in the Russian military in 2013, played a key role in closing the trap on the Ukrainian troops. Although Putin promised a free retreat for the trapped soldiers, he did not keep his promise. The retreating Ukrainian forces received a massive artillery fire that forced them to flee on foot, leaving their equipment and the wounded behind. The separatists shot some of the wounded, others imprisoned them and the less fortunate were tortured [1].

As the Ukrainian military rapidly lost territory over the next week and with Russian troops poised to launch an assault on Mariupol, Poroshenko negotiated a ceasefire with Putin at a meeting in Minsk, Belarus. The ceasefire only partially froze the conflict.

Following the successful summer offensive, the Russians embarked on a powerful winter campaign on January 17, 2015, disregarding the Minsk Ceasefire Convention.

Figure 1.
The main terminal of the Donetsk International Airport is hit by shelling [26]

Russian-backed forces worked to consolidate their victories by proceeding to shell various Ukrainian military positions every day. The particular interest to the Russian-backed separatists was Donetsk Airport, a strategically important position at the northwest corner of their capital city, and the site of perhaps their most humiliating defeat. In Donetsk, the defenders were able to create a supply line, although not very stable, and artillery support was available. Despite this favourable operational situation, the Ukrainian forces, who became known as "Cyborgs" for their stalwart defence of the position, came under increasingly heavy artillery, rocket, sniper, small arms and tank attack [25]. After 240 days of successful defence, the shelled terminal collapsed along with the Ukrainian defenders, and buried the Ukrainian hopes. After losing the airport, the defenders dug into their prepared defence positions along the line of villages west of Donetsk, which they had been able to hold.

The fighting in Donetsk only set off another wave of fighting in the area around the city, particularly near Debaltsevo, on the road between Donetsk and Lugansk.

Anti-Kiev militants, led by elite soldiers using Russian tanks and weaponry, such as T-72 models only used by the Russian military, led the assault on Debaltsevo, surrounding a large number of Ukrainian soldiers and inflicting heavy casualties on them. In the third week of the winter campaign, the forces stationed there have been slammed by the separatists on three sides because of the nonstop attacks. Putin also used this advantageous position to negotiate a full-fledged Minsk II ceasefire. Just a week after the conclusion of the negotiations, the Russian war machine was in action again. The fire of a long-range Russian MLRS and the debilitating seizures of more modern Russian tanks forced the Ukrainian forces to flee. The Ukrainian 128th Mechanised Rifle Brigade equipment was completely lost, the soldiers escaped on foot to a nearby forest. With a huge effort, a stable defensive line was built 30 km away, which stopped the Russian advance [1], [24].The success of the Russian offensive was due to the non-precision artillery strikes guided by unmanned aerial vehicles and the superiority of the Russian armed forces in the massive area combined with unmanned aerial vehicles. From June 2014, to neutralise the Ukrainian Air Force, Moscow began supplying separatists with light air defence weapons, primarily shoulder-fired anti-air missiles. The rebels were able to shoot at least seven Ukrainian aircraft between June and July, including an Iljusin Il76 heavy transport aircraft with forty paratroopers on board and three Sukhoi Su-25 ground attack aircraft. Due to severe losses, the Ukrainian Air Force ceased operations over Eastern Ukraine by the end of summer 2014[3] [1], [25].

Figure 2.
Operational situation after the Russian intervention [3]

[3] A terrible memento of the separatists' air defence capability was the Malay BOENIG-777 passenger aircraft, which was allegedly shot down on July 17, 2014, causing the death of 300 innocent civilians.

Following the Minsk II Ceasefire Agreement signed on 12 February 2015, the intensity of the fighting decreased significantly, but the ceasefire was not achieved under this Convention either.

Tactical and Technological Innovations

The most important tactical and technological innovations of the conflict are as follows [1]:

- Ubiquitous presence of unmanned aerial vehicles
- Increased lethality of indirect fires
- Antitank guide missiles and the armed counterrevolution
- Declining survivability of light infantry vehicles

Bulk deployment of drones

Unmanned aerial vehicles, also known as drones, have been part of modern warfare for some time. The Russo–Ukrainian War was also able to show new ways of applying them. Although both sides used the drones, by mid-July 2014 the Russians almost flooded the air with them. At least 14 different types were observed during the summer offensive, which can be divided into 5 main categories [1]:

- Very long-range strategic surveillance high-altitude UAV
- Long range higher-altitude fixed wing drone flying over Ukrainian positions beyond Brigade rear area
- Medium-range fixed wing drone used in target acquisition and real-time engagement with less than 15-minute response time, associated with Uragan and Smersh Multiple Launch Rocket Systems
- Short-range fixed wing drone particularly associated working with BM-21 MLRS targeting
- Very short-range tactical quad-copter used for scouting defence positions and post-strike Battle Damage Assessment (BDA)

The astonishing thing about the Russian use of drones is not the combination of vehicles themselves or their unique features, but rather their capability to combine multiple sensing platforms into a real-time targeting system for massed, not precision, fire strikes. This is a different approach from Western warfare, because NATO looks at drones as a long-range detector, apart from the few and very expensive combat types like the Predator. The Russian method is based on three fundamental pillars: the sensor platforms, which are often used at multiple altitudes over the same target with complimentary imaging; a command and control system, which webs their input and provides a strike order; and an on-call ground-based delivery system which can produce strikes within short order [1].

Increased lethality of artillery fires

According to unofficial statistics, artillery fires on both sides caused approximately 85% of the losses. It happened because of the heavy use of new-generation sub-munitions, top-attack and thermobaric ammunition types, mainly used by the Russians. In addition, the Russians have substantially increased their ratio of rocket launchers to artillery so that, in the Donbas, it is now nearly 40%, so they almost doubled the amount.

Table 1.
Main types of MLRS used in the conflict [1]

Type	Calibre	Range	Type of Ammunition
BM-21 GRAD (Hail)	40 round 122 mm rocket	20 km	traditional
BM-21 1 GRAD (Hail)	40 round 122 mm rocket	30 km	traditional, dual-purpose improved conventional munition
TOS-1	12 round 220 mm rocket	6 km	thermobaric
BM-27 URAGAN (Hurricane)	16 round 220 mm rocket	35 km	traditional, dual-purpose improved conventional munition, thermobaric
BM-30 SMERCH (Whirlwind)	12 round 300 mm rocket	90 km	traditional, dual-purpose improved conventional munition, thermobaric

The Russian emphasis on the massive use of area fire is in stark contrast to the Western concern over the last decade with precision strike. While individual artillery strikes in NATO member states usually appear at brigade level, in Eastern Ukraine Russian battalions already had this capability [1].

Russian artillery devices outnumbered Ukrainians in number and range. A good example for the dramatic effect of the combination of new types of ammunition and MLRS is the destruction of two Ukrainian mechanised battalions in the summer of 2014 near Zelenopillya.

The increasing role of main battle tanks

The Yom Kippur War of 1973 showed how effectively anti-tank infantry can fight against tanks. In Eastern Ukraine, due to the lack of modern anti-tank devices ("tandem" warheads, and "top-attack" munitions), this trend was reversed and older Ukrainian tanks were unable to compete with modern Russian tanks.

At the outset of the conflict, separatists had the same types of tanks as Ukrainian regular forces (T-64, early T-72, T-80, both sides equipped with explosive reactive armour).[4] However, with the Russian offensive in the late summer of 2014, more advanced tank types, like the T-72B3 and T-90, appeared [22]. The technical superiority of the T-72B3 and T-90 is well illustrated by the loss ratios. Against tanks of equal generation and capability, the Ukrainian gunners had generally been able to achieve a favourable loss exchange ratio. However, when the modern T-72Ms were introduced,

[4] ERA = Explosive Reactive Armour.

Ukrainians lost three tanks to every one killed. In five company-size engagements documented where T-90s participated, the Ukrainians took double their normal losses and there is no evidence they were able to kill a single T-90 [1], [26].

The appearance of the T-90s was also a decisive moment in the battles of Luhansk (September 2014), Donetsk (January 2015) and Debalceve (February 2015). The anti-tank missiles of the Ukrainians were ineffective against the active defence system of the T-90s (Arena system). Only the artillery could keep the modernised Russian army away.

Declining efficiency of Light Infantry Vehicles

Since the end of the Cold War, armoured vehicles have become increasingly prominent in the world's armies. However, the experience of the Russo–Ukrainian war strongly questions the survival of these types of combat vehicles in modern wars. Light infantry vehicles are particularly decimated by sub-munitions and thermobaric type artillery ammunitions. The effects of this were also obvious on the battlefield: troop losses were so high that soldiers on both sides prefer riding on top of the vehicle. Assaults tend to be conducted with dismounted rather than mounted infantry; and the vehicles mounting the automatic cannon tend to be used for providing cover-fire from a distance rather than advance with the infantry [1].

Figure 3.
Ukrainian servicemen patrol in Donetsk in 2014 [26]

Conclusions

A few years ago, NATO seemed to be losing its significance. European members of the Alliance spent less and less on armaments, while U.S. foreign policy turned more and more toward the Middle East and then Asia.

The organisation was originally set up in 1949 precisely to prevent Soviet military expansion. As the first Secretary General of NATO, Hasings Ismay said: "The purpose of the NATO alliance is to keep the Russians out, the Americans in, and the Germans down." [19]

NATO has developed a fundamentally cooperative policy with Russia after the collapse of the Soviet Union, but the revived Russian superpower policy has created a new situation.

The war under the new Russian doctrine poses a serious challenge, because its essence is that the aggression is implied, and does not cross the threshold over which NATO should introduce Article 5. Still, there is no war because the Russian TV talks about nonsense things.

The conflict with Russia should not be extensive, meanwhile deterring the Russian military force remains the key purpose, especially where Russia has been posing physically the most significant threat: the Baltic States, Poland and Romania [8].

In 2014, NATO Allies in Wales agreed to implement the Readiness Action Plan. The size of the NATO Response Force has tripled to 40,000, with a Spearhead Force at its core able to move within days. Eight small headquarters have been established in Bulgaria, Estonia, Hungary, Latvia, Lithuania, Poland, Romania and Slovakia to facilitate training and reinforcements, if needed. NATO began to adapt its defensive posture in response to major changes in the security environment – changes that have rendered that environment more complex and demanding.

In the face of these changes, the Allies agreed at the NATO Summit in Warsaw in July 2016 to further strengthen the Alliance's deterrence and defence posture in order to better protect their citizens and to enhance NATO's efforts to project stability in its neighbourhood. One of the most important decisions of the NATO summit was the approval by the military alliance of a rotating battalion of about 4,000 people in Poland and the three Baltic States in response to the threat posed by Russia. NATO soldiers are stationing under four different headquarters in four countries: American in Poland, Canadian in Latvia, British in Estonia and German in Lithuania. The latter is perhaps the most important development of the current summit: the deployment of the German army within Europe, and right on the fringes of Russia, clearly indicates that one of the three doctrines that was agreed upon when NATO was founded, i.e. to hold the Germans down, is not valid anymore [13], [15], [14], [16].

NATO must also step in to stop Russian disinformation propaganda. In recent years, internet portals of unidentified origin, thousands of trolls spreading Russian propaganda about the refugee crisis or about the United States have proliferated across Europe. Brexit has only worsened the problem set; indeed, political uncertainty in Europe poses a security risk in itself. This uncertainty is precisely what Russia wants [6], [12], [14], [27].

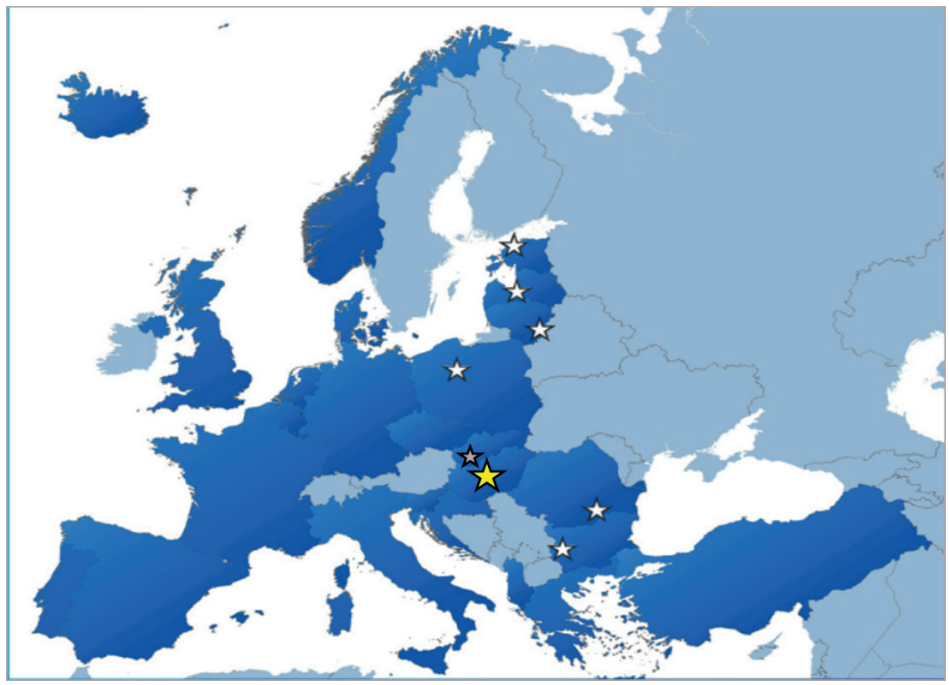


Figure 4.
NFIUs established in Europe (Compiled by the author from [28])

One thing is for sure: Russia took a step ahead of NATO and showed the world that if anyone violates Russian interests in the world, they have to face grave consequences.

References

[1] Ph. A. Kaber, *Lessons Learned from the Russo–Ukrainian War, Draft.* Johns Hopkins Applied Physics Laboratory & U.S. Army Capabilities Center (ARCIC), 8 July 2015. [Online]. Available: https://prodev2go.files.wordpress.com/2015/10/rus-ukr-lessons-draft.pdf [Accessed Sept. 27, 2019].

[2] "Comparison of the military strength of Russia and Ukraine," [Online]. Available: www.globalfirepower.com/countries-comparison-detail.asp?form=form&-country1=ukraine&country2=russia&Submit=COMPARE [Accessed Sept. 26, 2019].

[3] "JFO: MAP – 07.09.2019," [Online]. Available: http://mediarnbo.org/2019/09/07/jfo-map-07-09-2019/?lang=en [Accessed Sept. 26, 2019].

[4] J. Deák, "Oroszország új (pontosított) katonai doktrínájának megjelenése az orosz katonai gondolkodás változásainak tükrében," *Felderítő Szemle,* vol. 14, no. 1, March, pp. 37–47, 2015.

[5] R. Thornton, "Military Modernization and the Russian Ground Forces," [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a545442.pdf [Accessed Sept. 26, 2019].
[6] "Defence Committee third report. Towards the next Defence and Security Review: Part Two-NATO," [Online]. Available: www.publications.parliament.uk/pa/cm201415/cmselect/cmdfence/358/35802.htm [Accessed Aug. 15, 2019].
[7] N. Iancu, A. Fortuna, C. Barna, and M. Teodor, Eds., *Countering Hybrid Threats: Lessons Learned from Ukraine.* Amsterdam: IOS Press BV, 2016.
[8] I. Riba, "A nagy bukás is benne van Putyin többfrontos hazárdjátékában," *hvg.hu.* [Online]. Available: http://hvg.hu/gazdasag/201549_putyin_tobbfrontos_hazardjateka_voros_terer [Accessed Aug. 11, 2019].
[9] A. Rácz, "Oroszország hibrid háborúja Ukrajnában," *KKI tanulmányok,* 2014 [Russia's Hybrid War in Ukraine], [Online document]. Available: www.academia.edu/8833545/Oroszorsz%C3%A1g_hibrid_h%C3%A1bor%C3%BAja_Ukrajn%C3%A1ban_Russias_Hybrid_War_in_Ukraine_ [Accessed Sept. 04, 2019].
[10] A. Standish, "Az orosz titkosszolgálatok újjászületése," [Online]. Available: http://prominoritate.hu/wp-content/uploads/2019/05/ProMino06-2-02-Alex.pdf [Accessed Sept. 10, 2019].
[11] P. Fehér G., "Az orosz birodalom visszavág?" *Válasz.hu,* 2014. 11. 15. [Online]. Available: http://valasz.hu/vilag/az-orosz-birodalom-visszavag-106191 [Accessed Aug. 09, 2019].
[12] "Orosz hekkerek törhették fel a Clinton Alapítvány rendszerét," *24.hu,* 2016. 07. 31. [Online]. Available: http://24.hu/kulfold/2016/07/31/clinton-az-orosz-titkosszolgalat-inditott-tamadast/ [Accessed Sept. 09, 2019].
[13] "Több mint elégedettek Varsóban a NATO-csúcs után," [Online]. Available: www.hirado.hu/2016/07/11/tobb-mint-elegedettek-varsoban-a-nato-csucs-utan/ [Accessed Aug. 15, 2019].
[14] Zs. Szelényi, "Miért fontos nekünk a varsói NATO-csúcs?" *hvg.hu,* 2016. 07. 08. [Online]. Available: http://hvg.hu/itthon/20160708_Varso_NATO_csucs_oroszok_menekultugy [Accessed Aug. 10, 2019].
[15] "Varsói NATO-csúcs: erősítik a keleti szárnyat," *Krónika Online,* 2016. 07. 10. [Online]. Available: www.kronika.ro/kulfold/varsoi-nato-csucs-erositik-a-keleti-szarnyat [Accessed Aug. 22, 2019].
[16] P. Magyari, "A német hadsereg a NATO-csúcs igazi nyertese," *444.hu,* 2016. 07. 11. [Online]. Available: http://444.hu/2016/07/11/a-nemet-hadsereg-a-nato-csucs-igazi-gyoztese [Accessed Aug. 22, 2019].
[17] V. Geraszimov, "Cennoszty nauki v predvigyenyii," *Vojenno-promislennij kurjer,* 2013/8. [Online]. Available: www.vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf [Accessed Sept. 04, 2019].
[18] "Satellite images reveal Russian military buildup on Ukraine's border," *The Guardian,* Apr. 10, 2014. [Online]. Available: www.theguardian.com/world/2014/apr/10/satellite-images-russian-military-ukraine-border [Accessed Sept. 04, 2019].
[19] M. Dérer, "A NATO születése," *rubicon.hu.* [Online]. Available: www.rubicon.hu/magyar/nyomtathato_verzio/a_nato_szuletese/ [Accessed Aug. 22, 2019].

[20] "Hybrid war Hybrid response?" [Online]. Available: www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-crisis-war/EN/index.htm [Accessed Sept. 04, 2019].
[21] F. Kajári, "Hibrid háború Ukrajnában?" *Honvédségi Szemle,* vol. 143, no. 5, pp. 36–43, 2015.
[22] J. Dempsey, "Russia deploys latest tank variant to Ukraine border," [Online]. Available: www.iiss.org/en/militarybalanceblog/blogsections/2014-3bea/april-7347/russia-deploys-latest-tank-fa72 [Accessed Sept. 04, 2019].
[23] Askai707, "Russia's 200th Motorized Infantry Brigade in the Donbass: The Hero of Russia," [Online]. Available: www.bellingcat.com/news/uk-and-europe/2016/06/21/russias-200th-motorized-infantry-brigade-in-the-donbass-part-2/ [Accessed Sept. 04, 2019].
[24] "Battle of Debaltseve: A Turning Point in the Russian War in Ukraine," *potomacfoundation.com,* [Online]. Available: http://potomacfoundation.com/2016/03/battle-of-debaltseve-a-turning-point-in-the-russian-war-in-ukraine/ [Accessed Aug. 04, 2019].
[25] J. Miller, P. Vaux, C. A. Fitzpatrick, and M. Weiss, „An Invasion by Any Other Name: The Kremlin's Dirty War in Ukraine," *The Institute of Modern Russia,* 2015. [Online]. Available: www.interpretermag.com/wp-content/uploads/2015/09/IMR_Invasion_By_Any_Other_Name.pdf [Accessed Sept. 10, 2019].
[26] G. Botelho, "Ukraine accuses Russia of sending dozens of tanks into its territory," *CNN,* Nov. 7, 2014. [Online]. Available: https://edition.cnn.com/2014/11/07/world/europe/ukraine-unrest/index.html?hpt=hp_t1 [Accessed Sept. 04, 2019].
[27] S. Tatham, "The Solution to Russian Propaganda is not EU or NATO Propaganda but Advanced Social Science to Understand and Mitigate its Effect in Targeted Populations," [Online]. Available: www.naa.mil.lv/sites/naa/files/document/4_PP%2004-2015.pdf [Accessed Sept. 04, 2019].
[28] "NFIUs established in Europe," [Online]. Available: https://pbs.twimg.com/media/CaOMrXmXEAAwU0d.jpg [Accessed Sept. 04, 2019]

HADMÉRNÖK
FÓRUM

15. évfolyam (2020) 1. szám 221–231.
DOI: 10.32567/hm.2020.1.15

Krisztina Takács[1]

Analysis of Microbiological Methods Applicable to Water Testing in Our Country

Hazánkban vízvizsgálat céljára alkalmazható mikrobiológiai módszerek elemzése

It is essential for our daily life to produce drinking water of the right quality and quantity. Water supply also includes the regular testing of drinking water to deliver impeccable water quality to consumers. 201/2001 (X. 25.) Government Decree on Quality Requirements for Drinking Water and Procedures for Monitoring contains the frequency of sampling and the designation of microorganisms to be detected in each test and the different standards on the basis of which the tests should be carried out. However, these methods are often time-consuming, it takes several days for the samples to produce results. However, there is a newer and more modern method to shorten the time.
This is particularly important in case of unexpected disasters, water pollution when it is extremely important to react quickly.
The aim of this article is to introduce (overview) the microbiological methods used for water testing in Hungary, describing the advantages and disadvantages of their application based on the author's own laboratory experience.

Keywords: water testing, microbiological test methods, water quality, test algorithm

A mindennapi élethez elengedhetetlen a megfelelő minőségű és mennyiségű ivóvíz előállítása. A vízellátás biztosításához hozzátartozik az ivóvíz rendszeres vizsgálata is, amelynek célja, hogy kifogástalan minőségű víz jusson el a fogyasztókhoz. Az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről szóló 201/2001. (X. 25.) Korm. rendelet tartalmazza a mintavételek gyakoriságát, illetve az egyes vizsgálatok során a vízből kimutatandó mikroorganizmusok megnevezését és a különböző szabványokat, amelyek alapján a vizsgálatokat el kell végezni. Ezek a módszerek

[1] National University of Public Service, PhD student, e-mail: takacs.krisztina@uni-nke.hu, ORCID: https://orcid.org/0000-0002-9481-814X

azonban többnyire időigényesek, több nap, míg eredményhez vezetnek. Létezik azonban újabb, korszerűbb eljárás is, amellyel e vizsgálati idő lerövidíthető. Ez kiemelten fontos a váratlanul bekövetkező katasztrófahelyzetekben, vízszennyezések esetén, mikor rendkívül fontos a gyors reagálás.
A cikk elkészítésével célom volt, hogy bemutassam a hazánkban vízvizsgálat céljára alkalmazott mikrobiológiai módszereket, ismertetve alkalmazásuk előnyeit és hátrányait saját laboratóriumi vizsgálatok tapasztalataira támaszkodva.

Kulcsszavak: **vízvizsgálat, mikrobiológiai vizsgálati módszerek, vízminőség, vizsgálati algoritmus**

Introduction

Potable water is an essential element of life and daily activities. In Hungary, the quality requirements for potable water are strictly regulated by Hungarian and European legislation. It is a strategic public health task, under the control of the competent authorities, to provide drinking water of sufficient quality. In Hungary, the classification of potable water is dealt with in 201/2001 (X.25.) Government Decree (hereinafter: Government Decree) on drinking water quality requirements and inspection procedures.

The determination of water quality consists of professional sampling and physical, chemical, bacterial and biological tests on site and in laboratories.

Annex 1 to the Government Decree contains the microbiological and chemical test parameters for water and the associated limit values. On this basis, water meets the legal requirements if it does not contain a microorganism, parasite, chemical or physical substance that may endanger human health. In addition, there are so-called indicative water quality indicators, which have a primary control role. In such cases, exceeding the limit value does not pose an immediate public health hazard [1].

In the following, from the parameters of water quality, I will deal only with microbiological tests and methods, given the scope of the article. One of my goals is to introduce the microbiological methods used in Hungary to determine the microorganisms present in water. I consider it important to compare these methods and to present their advantages and disadvantages, because the method used in a given situation can play an important role. For example, in case of an unexpected event that may occur, it is essential to obtain results as soon as possible, while other factors, such as the need for equipment and cost effectiveness, play a role in the regular sampling of water from the water networks. Taking into account all these parameters I examined the applied methods.

Generally speaking, in Hungary, in accordance with the Government Decree, microbial cultivation methods are used for water quality purposes. However, there are also methods that reduce the incubation time so that results can be achieved faster. In the following, I introduce these methods in detail, and highlight the weaknesses and strengths of the methods using SWOT analysis.

Frequency of Water Tests and Parameters to Be Tested

The frequency of sampling for water tests is determined by the Government Decree. The number of samples to be tested depends on the amount of drinking water supplied each day. The given waterworks takes an average of 4 samples per year in its area of operation, that is, in certain parts of the settlements at which a control test is performed. The purpose of this is to provide regular information on the organoleptic and microbiological quality of drinking water for human consumption, certain chemical water quality characteristics, changes in water quality and the efficiency of water treatment. The following parameters are checked during the test: colour, odour, taste, turbidity, pH, conductivity, Escherichia coli, Coliform bacteria, colony count at 22°C and 37°C, respectively. Methods for microbiological testing are contained in the Government Decree. In addition to the inspection, a detailed inspection is carried out once a year to determine whether the drinking water meets all the requirements of the Government Decree [1].

The parameters to be tested are listed in Table 1 and the standard by which the various tests are performed in an accredited water testing laboratory is also listed, i. e. the testing standards required by the regulations and the microbiological characteristics required therein. The Government Decree states that Escherichia coli, Enterococcus bacteria, Pseudomonas aeruginosa should not be present in the water. The Legionella limit is set out in EMMI Decree 49/2015 (XI. 6.) on Public Health Requirements for Media and Facilities Posing a Legionella Infection Risk (hereinafter: EMMI Decree) [2].

Table 1.

Microbiological water quality characteristics and standards
(Compilation of the author based on [1] [2])

T est specific	Standard	Regulation
Escherichia coli	MSZ EN ISO 9308-l	20112001.(X.25.) Govermment Decree
Enterococci	MSZ EN ISO 7899-2	
Pseudomonas aeruginosa	MSZ EN ISO 16266	
Colony number at 22°C	MSZ EN ISO 6222	
Colony number at 37°C	MSZ EN ISO 6222	
Legionella	MSZ EN ISO 11731:20 17	49/2015.(XI.6.) EMMI Decree

Microbiological Water Test Methods Used in Hungary

Regular water quality tests are performed according to the parameters prescribed by the MSZ standards specified in the regulations. These standards describe in detail the assay procedure, the medium required for the detection of each microorganism, the amount of water needed for the sample and the incubation time after the result.

In addition to the method in the Government Decree, there is another method for detecting microorganisms in water. These methods are described below.

Breeding procedures

In Hungary, the water testing laboratories apply microbiological methods for cultivation in accordance with the Government and EMMI regulations. As shown in Table 1, besides the microorganisms to be detected, there is a standard upon which the assays should be performed.

The plate count method is used to determine the colony count. The number of microorganisms is determined at two different temperatures, one at 22°C and the other at 37°C. Plates are incubated for 72 hours at 22°C and 24 hours at 37°C. The result is then reported using the battery count method.

For the detection of E. coli, Pseudomonas aeruginosa and Enterococci, the water sample is filtered through a standard pore size membrane filter, then the membrane filter is placed on the surface of a selective medium and incubated as prescribed. In all three cases, after 24–48 hours, colony counts are obtained.

For Legionella, it is most necessary to wait for results, as incubation of this microorganism takes up to 10 days.

Generally speaking, these methods include a relatively longer time, from 24 to 72 hours, but up to 10 days before incubating colonies.

Other novel procedures

In addition to the culture methods, there are other methods by which microorganisms in the water can be identified. In the following, I briefly describe how the detection of each microbe occurs.

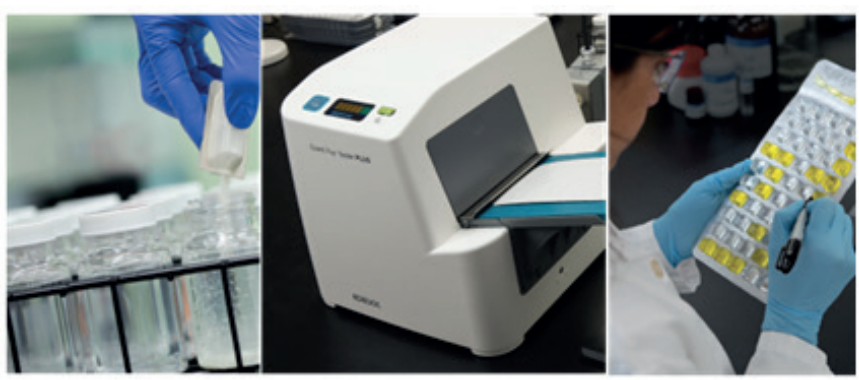


Figure 1.
Test method images [3]

The principle of the methods is similar, the reagent is filled into the water sample and, after reconstitution, the Quanti-Tray is filled. The sample tray is then sealed and incubated at the appropriate temperature and time and the result is evaluated according to the method.

Detection of Coliform and E. coli is performed using Colilert 18 methods by pipetting a defined amount of the water sample into a bottle and then adding sterile water or Colilert reagent containing various salts, vitamins and sugars. All of this should be placed in a sachet, which is incubated at 36°C for 20 hours. Coliform positivity, as shown in Figure 1, is indicated by yellow cells.

For the detection of Coliform, the Colilert 18 method is based on the enzymatic degradation of ortho-Nitrophenyl-β-D-galactopyranoside (ONPG) by β-galactosidase. As a result of the enzyme activity, the sample changes from colourless to yellow. The procedure does not require UV light [4], [5], [6], [7].

However, for E. coli, it is based on the enzymatic degradation of 4-methylumbelliferyl-β-D-glucuronide (MUG) by β-glucuronidase. As a result of the enzyme activity of the coliform positive yellow bubbles in the sample, the E. coli positive fluoresces blue under UV light [4]. Based on the number of coloured cells, the result can be read from a statistical table using the MPN method. Depending on the volume of the water sample, the results are given at 1, 10, 50 or 100 ml.

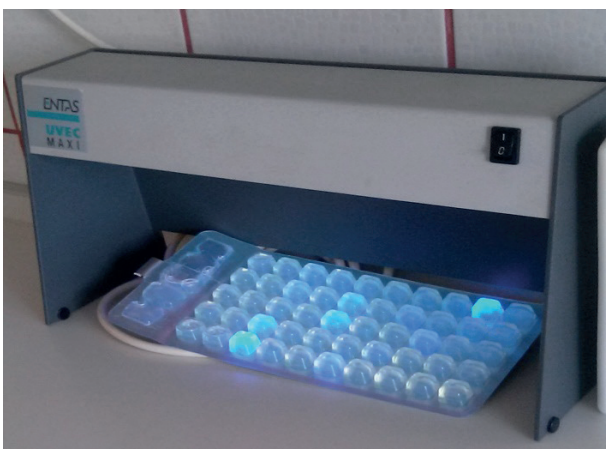


Figure 2.
Detection of E. coli by the Colilert method [Made by the author.]

Detection of Pseudomonas aeruginosa was performed by the Pseudalert method, which operates on a similar principle to the Colilert mentioned above. Incubate the pouches at 38°C for 24 hours and then count the number of positive bubbles fluorescing blue under UV light. The result is also given by the MPN method [4].

The Enterolert-DW method is suitable for the determination of Enterococci. This is also based on the enzymatic degradation of ortho-Nitrophenyl-β-D-glucoside (ONPG) to glucoside. During incubation at 41°C for 24 hours, the colour of the positive

sample changes from blue to green as a result of enzyme activity. The procedure does not require UV light.

For the detection of Legionella, a mixture of mineral salts and vitamins has also been developed and added to the water sample to give results within 7 days [8].

These methods are not yet widespread in Hungary, as they are quite expensive, but they have the great advantage over conventional breeding methods that they can produce results in a much shorter time. These procedures allow the results to be evaluated within 1 day, thereby gaining significant time compared to the culture methods.

A further advantage of the practical application of the new methods is that the treatment of microbiological contaminants and the disinfection of affected areas can be started sooner, thus reducing the further spread of infections [9], [10].

Own Examinations

In order to illustrate the microbiological methods used, I carried out laboratory tests aimed at examining the results obtained with each method. To do this, I took 5 samples from different locations, public wells and taps. From each sample I show the 5 parameters (colony number at 22°C, colony number at 37°C, E. coli, Enterococcus, Pseudomonas aeruginosa) contained in the Government Decree by the conventional breeding method as well as by the Colilert method. For each sample, I worked with 3 replicates, using the average of these results. The microorganisms to be detected were compared by sample, their results and their uncertainty are shown in Figures 3, 4 and 5. E. coli and Enterococcus were not detectable in either sample.

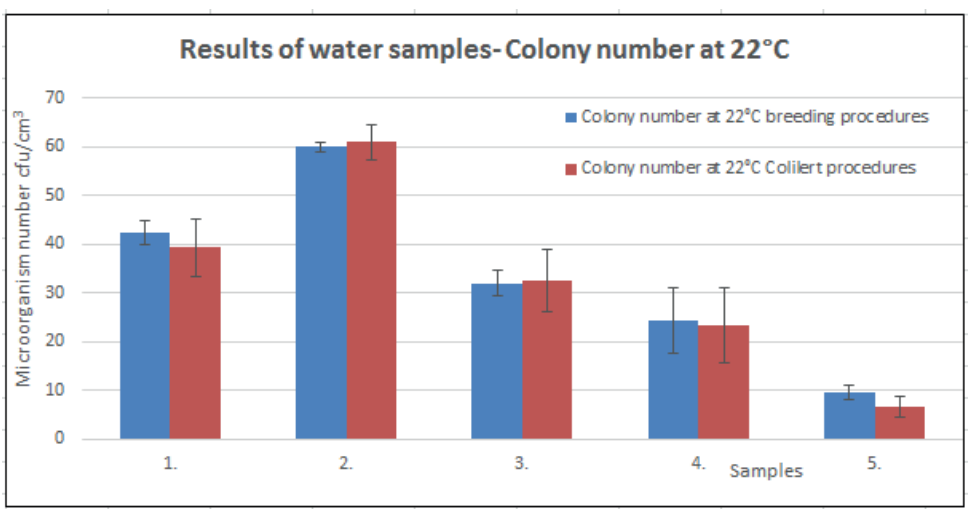


Figure 3.
Determination of colony number at 22°C [Compiled by the author.]

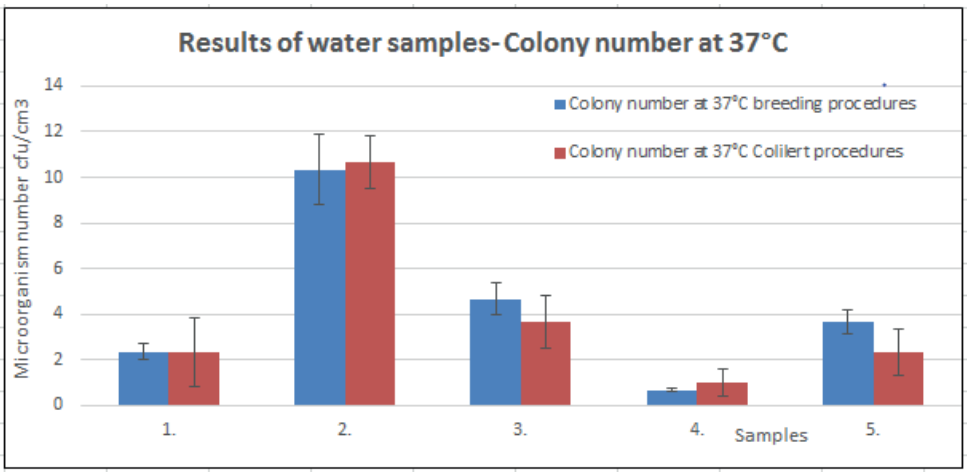


Figure 4.
Determination of colony number at 37°C [Compiled by the author.]

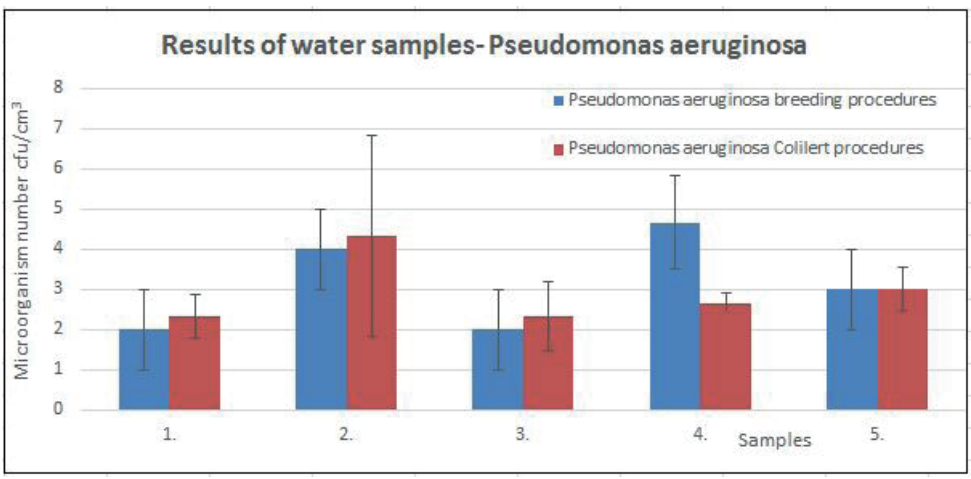


Figure 5.
Definition of Pseudomonas aeruginosa [Compiled by the author.]

The results of the measurements show that the data of the 2 methods correlate well, and similar results were obtained for each sample.

Therefore, no decision can be made about the method to be chosen for the water test on this basis, so after further research, my goal was to show the advantages and disadvantages of the methods. Based on my own experience, I conducted a SWOT analysis to demonstrate the viability of a product through the following features:

- strengths
- weaknesses
- opportunities
- threats – dangers

Figure 6 shows the analysis of the culture method according to 4 parameters.

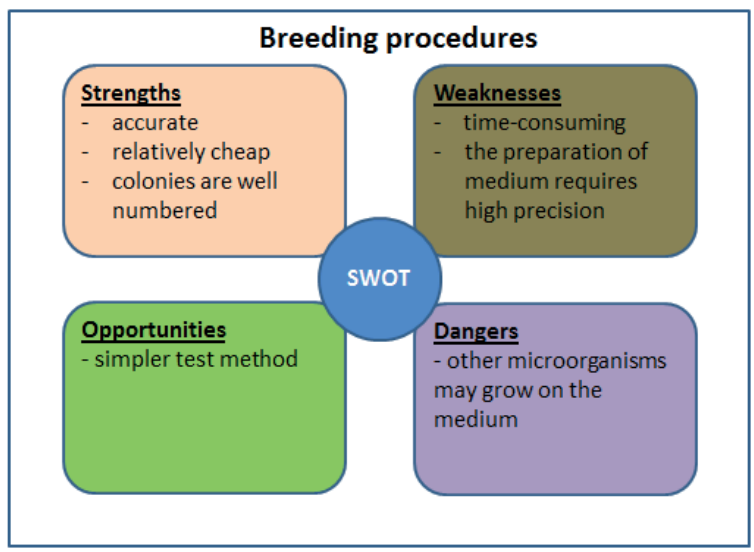


Figure 6.
Breeding procedures – SWOT analysis [Compiled by the author.]

As can be seen in Figure 6, one of the advantages of the culture methods is that they are relatively inexpensive thanks to the colony count method. However, it should also be noted that colonies grown on culture media may not originate from a microorganism and may be included in the results due to negligence in the calculation of colonies. As an option, the test method may be shortened. The medium also has to be weighed and made up of different ingredients, salts and minerals. In many cases, pre-weighed media, which only needs to be diluted with water, has been developed, but it is time-consuming to prepare as it can only be used for testing in petri dishes and incubated at a suitable temperature.

Figure 7 shows the parameters of the other novel procedure.

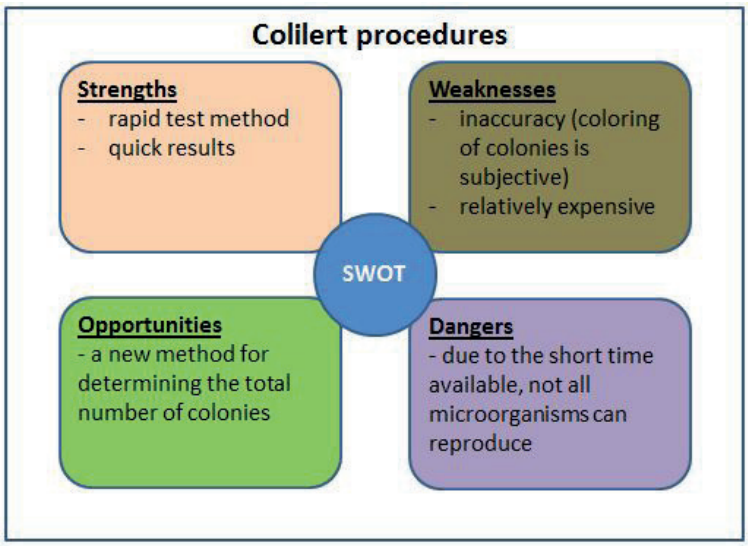


Figure 7.
Other procedures – SWOT analysis [Compiled by the author.]

The biggest advantage of other bagged methods is that the whole test method is quick, only adding a mixture of pre-purchased minerals and salts to the water sample, then pouring the mixture into the bags, sealing them and incubating at a suitable temperature. This gives results in a short time. After incubation, the results are based on the coloration of the pockets of the sachets, which in many cases is subjective, for example what is still yellow and what is not. The disadvantage is that this procedure and the equipment needed for it are relatively expensive. As a new option, another method could be developed that is capable of detecting all colony numbers, as this parameter is included in the Government Decree.

Conclusions

In my research, I have come to the conclusion that there are several factors to consider when choosing the right water test method. If an official water quality test is carried out in an accredited laboratory, then the regulations in force in Hungary must be followed, so the breeding procedures must be applied. In this case, after a relatively lengthy and tool-intensive sample preparation, the inoculation itself comes in, followed by an evaluation of the colonies after an incubation period of 1–2 days. If, on the other hand, a disaster or any unexpected incident occurs where drinking water is contaminated, then Colilert, Pseudalert, etc. should be used to achieve results in less time. All of this can increase the effectiveness of the damage elimination process and the faster disposal of the pollutant. The great advantage of these methods over

the breeding methods is that they are obtained in a relatively short time and that the whole assay method is quick and simple.

Regular testing of potable water, including microbiological parameters, is essential to guarantee adequate drinking water supply for consumers. In this article, I have presented the features of other novel microbiological methods that are included in the legislation in force in Hungary and that are not yet in the current legislation. Laboratory test results show that there is no significant difference between the results of the two methods.

Therefore, when comparing the methods, I also applied SWOT analysis, which can be used to determine the advantages and disadvantages of each method based on the 4 parameters. I have described the factors that can act as obstacles in some cases. The knowledge of these is essential in order to apply the best method in the given situation.

With the results of my research I wanted to help the work of the experts dealing with the testing of potable water.

References

[1] 201/2001. (X.25.) Kormányrendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről [Government Decree on Quality Requirements for Drinking Water and Procedures for Monitoring].

[2] 49/2015. (XI. 6.) EMMI rendelet a Legionella által okozott fertőzési kockázatot jelentő közegekre, illetve létesítményekre vonatkozó közegészségügyi előírásokról [EMMI Decree on Public Health Requirements for Media and Facilities Posing a Legionella Infection Risk].

[3] "Colilert." [Online]. Available: www.arachem.com.my/index.php?cat=1173 [Accessed March 02, 2019].

[4] M. Reskóné Dr. Nagy, Sz. Dömötör, *Gyors vizsgálati módszerek a víz mikrobiológiai ellenőrzésében.* Budapest: Hungalimentaria, 2015. [Online document]. Available: https://docplayer.hu/282216-Gyors-vizsgalati-modszerek-a-viz-mikrobiologiai-ellenorzeseben.html [Accessed March 02, 2019].

[5] K. Takács, "Marcal folyó mikrobiális állapotának vizsgálata a vörösiszap katasztrófa tükrében," *Hadmérnök,* vol. 13, no. 3, Sept., pp. 290–305, 2018 [Online serial].

[6] D. Kapetanović, I. Vardić Smrzlić, D. Valić, and E. Teskeredžić, "Occurrence, characterization and antimicrobial susceptibility of *Vibrio alginolyticus* in the Eastern Adriatic Sea," *Marine Pollution Bulletin,* vol. 75, no. 1–2, Oct., pp. 46–52, 2013. DOI: https://doi.org/10.1016/j.marpolbul.2013.08.008

[7] J. M. Pisciotta, D. F. Rath, P. A. Stanek, D. M. Flanery, and V. J. Harwood, "Marine Bacteria Cause False-Positive Results in the Colilert-18 Rapid Identification Test for *Escherichia coli* in Florida waters," *Applied and Environmental Microbiology,* vol. 68, no. 2, Feb., pp. 539–544, 2002. DOI: https://doi.org/10.1128/AEM.68.2.539-544.2002

[8] "Water." [Online]. Available: www.idexx.com/en/water/products/?cy=y_category_252&ts=all [Accessed Feb. 04, 2019].

[9] R. Kuti, "Intézkedési program belvízvédekezési munkálatokhoz," *Védelem, Tűz- és Katasztrófavédelmi Szakkönyvtár,* essay 67, pp. 1–12, 2007. [Online serial]. Available: www.vedelem.hu/letoltes/anyagok/67-intezkedesi-program-belviz-vedekezeshez.pdf [Accessed Apr. 12, 2019].
[10] R. Kuti, "Mentesítési feladatok új dimenziói," *Bolyai Szemle,* vol. 16, no. 1, pp. 62–67, 2007.

Tartalom