# HADMÉRNÖK

A ZMNE Bolyai János Katonai Mûszaki Kar
és a Katonai Mûszaki Doktori Iskola
on-line tudományos kiadványa

**III. Évfolyam 2. szám 2008. június**

**ZMNE**
**BUDAPEST**

*A szerkesztőség elérhetősége:*
Zrínyi Miklós Nemzetvédelmi Egyetem, 1101. Budapest, Hungária krt. 9-11. A. épület 8. emelet
*Postacím:* 1581. Budapest Pf.:15.
*Telefon:* +36-1-432-9048
*Fax:* +36-1-432-9208
*HM:* 29-734
*e-mail:* hadmernok@zmne.hu

**Kiadó:** Zrínyi Miklós Nemzetvédelmi Egyetem (ZMNE)
**Kiadásért felelős:** Prof. Dr. Szabó János, a ZMNE rektora
**ISSN 1788-1919**

**Jelen számban megjelent írások szerzői:**

**Bucsky György** – Veszprémi Egyetem, Szerves Vegyipari Kutatóintézet
**Dr. Földi László** mk. őrnagy – ZMNE BJKMK, egyetemi docens
**Fürjes János mk. őrnagy** – MK. Katonai Felderítő Hivatal, ZMNE doktorandusz
**Gábri Máté** – ZMNE KLHTK, egyetemi hallgató
**Dr. Gyarmati József** mk. őrnagy – ZMNE BJKMK, egyetemi docens
**Gyányi Sándor** – Budapesti Műszaki Főiskola, ZMNE doktorandusz
**Prof. Dr. Halász László** – ZMNE BJKMK, egyetemi tanár
**Hanák Tibor** – LSI Informatikai Oktatóközpont Alapítvány
**Horváth Zita** – ZMNE BJKMK, egyetemi hallgató
**Dr. Huszár András** o. ezredes – PTE ÁOK Igazságügyi Orvostani Intézete
**Illési Zsolt** – Proteus Consulting Kft., ZMNE doktorandusz
**Juhász Zsolt** – Magyar Honvédség, Honvéd Egészségügyi Központ, ZMNE doktorandusz
**Kerti András** mk. őrnagy – ZMNE BJKMK, egyetemi adjunktus
**Koronváry Péter** – ZMNE BJKMK, egyetemi adjunktus
**Kovács Judit** – Budapesti Műszaki Főiskola
**Dr. Kovács László** mk. őrnagy – ZMNE BJKMK, egyetemi docens
**Körmendi Krisztina** – PROTAN Zrt.
**Kucsera Péter** – Budapesti Műszaki Főiskola, ZMNE doktorandusz
**Kuti Rajmund tű. őrnagy** – ZMNE doktorandusz
**Majer Milán** r. fhdgy – ZMNE BJKMK, egyetemi hallgató
**Nagy Rudolf mk. pv. alezredes** – OKF főosztályvezető-helyettes, ZMNE doktorandusz
**Pántya Péter** – ZMNE BJKMK, egyetemi hallgató
**Prof. Dr. Solymosi József** – ZMNE BJKMK, egyetemi tanár
**Tolvaj Balázs** – ZMNE doktorandusz
**Ujhidy Aurél** – Veszprémi Egyetem, Szerves Vegyipari Kutatóintézet
**Varga Péter János** – Budapesti Műszaki Főiskola, ZMNE doktorandusz
**Vass András** – Veszprémi Egyetem, Szerves Vegyipari Kutatóintézet
**Dr. habil Vincze Árpád** – ZMNE BJKMK, egyetemi docens

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Juhász Zsolt**
Magyar Honvédség, Honvéd Egészségügyi Központ
juhaszzsolt@citromail.hu

# FIZIKAI ALKALMASSÁG-VIZSGÁLAT AZ ÚJJÁSZERVEZETT, ÖNKÉNTES HADERŐ LOGISZTIKAI RENDSZERÉBEN

***Absztrakt***

*A fizikai alkalmasság-vizsgálat minden hadsereg humán erőforrás-gazdálkodása szempontjából egy nagyon fontos kritérium. A szerző áttekinti az eredményeket, a vizsgálati és kutató módszerek helyét, szerepét problematikáját az ujjászervezett önkéntes haderő logisztikai rendszerében.*

*Checking of the physical suitability considered as one of the very important factors in point of view of HR (Human Recourse) in any Army. Subject of this article is about the physical suitability of the voluntary members of the reorganized Hungarian Defense Forces. The author gives global overview about the results, methods of checking up, the lows, the system of research works and problems in points of view of logistic system of HDF.*

***Kulcsszavak:*** *Fizikai alkalmasság-vizsgálat, vizsgálati módszerek, önkéntes ~ checking of the physical suitability, methods of checking up, voluntary*

## BEVEZETÉS

Az Észak Atlanti Szervezethez és az Európai Unióhoz történő csatlakozást követően hazánk nemzetközi megítélése jelentősen megváltozott. Új, más jellegű személyi feltételek teremtődtek, a nemzetközi szerepvállalásunk töretlen maradt, sőt bővült, elismertségünk növekedett. A feladatok, melyeknek egy része külföldön – műveleti vagy hadműveleti területen –, más része pedig itthon történik, új kihívások elé állítják katonáinkat. Logisztikai rendszerünk a szövetség és az unió elvárásainak megfelelően megváltozott, EU és NATO konformmá vált.

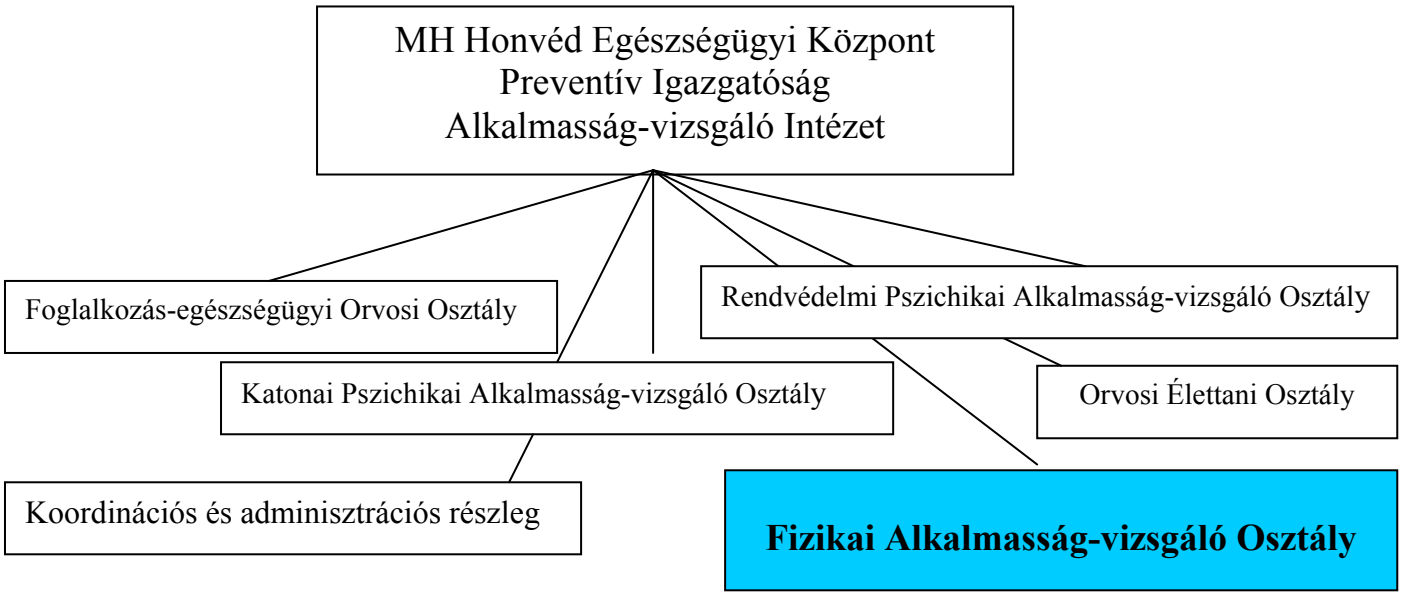
A haderőreform 1997-es éve meghatározó időszaka volt a Magyar Honvédség fizikai alkalmasság-vizsgálatát tekintve. A NATO és Európai Uniós követelményeknek megfelelően az említett tárgyévben létrejött egy olyan intézet – a Magyar Honvédség Egészségvédelmi intézete –, mely az elvárásokhoz mérten központilag, egy helyen, egyszerű, de ugyanakkor az adott kor körülményei között korszerű módszerekkel volt képes háromirányú (egészségügyi,

pszichikai és fizikai) vizsgálatok végrehajtására. Azóta eltelt több mint 10 év. A NATO-hoz való csatlakozás (1999) és az önkéntes haderőre történő átállás (2004) okán úgy szervezeti, mint minőségi átalakítások történtek. Számos szervezet, így az alkalmasság-vizsgáló rendszerek is a feladatokhoz mérten megváltoztak.

## A KATONAI FIZIKAI ALKALMASSÁG-VIZSGÁLAT KAPCSOLÓDÁSI PONTJAI, AZ ÖNKÉNTES HADERŐ LOGISZTIKAI RENDSZERÉBEN

A NATO által meghatározott fő logisztikai funkciók alapján, az alkalmasság-vizsgálat háromirányú rendszere - és így természetesen a fizikai alkalmasság-vizsgálat is - az úgynevezett orvosi és egészségügyi szolgáltatások támogatásához köthető. A NATO logisztikai kézikönyv 1. fejezetének definíciókkal foglalkozó része, tartalmaz egy 103/e pontot, mely az Orvosi és egészségügyi támogatásról szól, melynek a hazai katona-egészségügy vonatkozásában fontos része a fizikai alkalmasság-vizsgálat. Hazánkban a kapcsolódási pont a 20/2002. (IV.10.) HM rendelet, mely részleteiben konkretizálja és meghatározza a különböző logisztikai beosztásokhoz tartozó alkalmassági követelményeket, így többek között a fizikai alkalmasság-vizsgálati teljesítmény szinteket is.

## A MAGYAR HONVÉDSÉG HONVÉD EGÉSZSÉGÜGYI KÖZPONT, PREVENTÍV IGAZGATÓSÁG, ALKALMASSÁG-VIZSGÁLÓ INTÉZETE (MH HEK PI AVI)




**1. sz. ábra:**
Az MH HEK PI Alkalmasság-vizsgáló Intézetének szervezeti felépítéséről[2]

Az MH Egészségvédelmi Intézet (az MH EVI), mint olyan megszűnt (2007 tavaszán) és megalakult a Magyar Honvédség Honvéd Egészségügyi Központja (MH HEK). Az Alkalmasság-vizsgáló Intézet, az MH HEK Preventív Igazgatóságán belül tovább működik és Lényegében ugyan azt a funkciót látja el mint azelőtt, de mégis egy kicsit másként. Megváltozott a létszáma, a szervezeti felépítése, de a 10 éve megkezdett nemzetközileg is elismert munkája töretlen maradt.

A négy szakterület - mely az alkalmasság-vizsgálatokért felelős - nevezetesen: a **Foglalkozás-egészségügyi Orvosi**, a **Katonai Pszichikai Alkalmasság-vizsgáló**, a **Rendvédelmi Pszichikai Alkalmasság-vizsgáló,** a **Fizikai Alkalmasság-vizsgáló,** az **Orvosi Élettani Osztályok** és az **Adminisztrációs Részleg** szorosan együttműködve, kölcsönösen egymást kiegészítve folytatja tovább az eddigi tevékenységét. Az egyik a másik nélkül nem tud létezni, nem tud működni.

A fent említett öt osztályról és egy részlegről elmondható, hogy teljes mértékben korszerű NATO és EU szintű vizsgálati rendszerekkel, műszerparkkal és szakember állománnyal dolgozik. Összességében több mint 100.000 egyén hatósági alkalmassági vizsgálatát végezte el, munkáját itthon és külföldön egyaránt elismerik, színvonalát a különböző nemzetközi fórumok NATO és Euro-standardnak tekintik, 2005-ben pedig ISO-9001 minősítést kapott. Az intézet infrastruktúrája viszonylag új, személyzete gyakorlott, jól szervezett és hatékony.

## A KÜLFÖLDI KATONAI SZOLGÁLATRA TÖRTÉNŐ FIZIKAI ALKALMASSÁG-VIZSGÁLAT TARTALMA ÉS ALAPJA JELENLEG


**1. sz. kép:**
Az MH HEK PI Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály, Terhelés-élettani laboratórium spiroergometriás terheléses vizsgálatáról[3]

A **Fizikai Alkalmasság-vizsgáló Osztály** és az **Orvosi Élettani Osztály** terhelés-élettani alapokon (orvosi tevékenység), a magyarországi populáció antropometriai adottságait messzemenően figyelembe véve dolgozta ki a teljesítmény-élettani alapszinteket.

A Magyar Honvédség fizikai alkalmasság-vizsgálatának alapja - amire az egész korszerű vizsgálati rendszer épül - a magyarországi populáció antropometriai adottságainak és a különböző mozgásformák, az adott speciális feladatokra (munkakörökre) jellemző sajátos tevékenységek energetikai hátterének vizsgálata.

Nevezetesen az, hogy az anaerob (anaerob alaktacid és anaerob laktacid), valamint az aerob vizsgálatok alapján a felmért személy milyen teljesítménymutatókkal rendelkezik. Gyakorlatilag, amit konkrétan vizsgálunk az a testsúlykilogrammra felvett oxigén mennyisége, pulzusfrekvenciára deriváltan, melyek mellé empírikusan pontszámokat rendeltünk.

Az alapszinteket úgy határoztuk meg, hogy azokat egy egészséges, átlagos testfelépítésű, közepes edzettséggel bíró jelölt is képes legyen teljesíteni. A felmérések végrehatása során a szakszerűség mellett az egyszerűségre törekedtünk, valamint arra, hogy a gyakorlatok (figyelembe véve a felkészültség minőségi mutatóit is) ne csupán laboratóriumi körülmények között, hanem praktikusan bárhol, (pl. sík terepen) és nagy tömegben is végrehajthatóak legyenek. Külön figyelmet fordítottunk arra, hogy a vizsgálandó jelöltek a felkészülésük során önmagukat is képesek legyenek ellenőrizni és értékelni. Meggyőződésünk, hogy csak az egészséges, a pszichikailag megfelelő állapotban lévő és a jó fizikai képességekkel (koordinációs és kondícionális) bíró katonák képesek az elvárt szinten végrehajtani a különböző meghatározott feladatokat és elérni a számukra kitűzött célokat.

Nem szorul különösebb magyarázatra, hogy amíg az egészségi állapot adott, a pszichés teljesítőkészség és az ahhoz szorosan kapcsolódó pszichés teljesítő képesség többé-kevésbé állandó, addig a fizikai teljesítőképesség csak a rendszeres testedzéssel tartható, fejleszthető, alakítható. Ez gyakorlatilag életmódbeli szemléletváltást, rendszeres és következetes testedzést, az úgynevezett motoros fizikai képességfejlesztést kíván. A magyarországi populáció közismerten túlsúlyos, javarészt rendszertelenül és korszerűtlenül étkezik, keveset mozog, és még kevesebbet, - azt is rendszertelenül - sportol. Bármennyire is közhely a közmondás, miszerint „Ép testben ép lélek” a populáció körében felvilágosító előadások és bemutatók sorával törekednünk kell arra, hogy a rendszeres testedzéseket szokássá tegyük, beépítsük a mindennapi életvitelükbe. Elismert tény, hogy a jó állóképesség és erőálló-képesség jó pszichés állóképességet feltételez, másrészt perspektivikusan csökkenti számos megbetegedés megjelenését is.

A jó fizikai és pszichés állóképesség, valamint a jó megjelenés joggal várható el minden NATO és természetesen, így minden magyar katonától is. A három alapfeltétel megléte és azok rendszeres vizsgálata - a szoros ok-okozati összefüggések tudatában - elengedhetetlen feladat és alapkövetelmény.

## A KÜLFÖLDI KATONAI SZOLGÁLATRA TÖRTÉNŐ FIZIKAI ALKALMASSÁG-VIZSGÁLAT KUTATÁSÁNAK CÉLJAI

A külföldi katonai szolgálatra történő fizikai alkalmasság-vizsgálat kutatásának céljai az alábbiak:

- A külföldi katonai szolgálatra történő fizikai alkalmasság-vizsgálati rendszer vizsgálata és továbbfejlesztése.
- Az alkalmas jelöltek arányának növelése.
- A hatékonyság érdekében előre jelezhetővé tenni, hogy milyen élettani adottságokkal bíró jelöltek jöjjenek vizsgálatra (meghatározott testmagasság, testsúly, testzsír százalék, BMI értékek stb.).
- Terhelés-élettani alapokra építve új vizsgálati eljárások bevezetése (futószalag, sífutógép, stb.) és azok alkalmazása.

## A KÜLFÖLDI KATONAI SZOLGÁLATRA TÖRTÉNŐ FIZIKAI ALKALMASSÁG-VIZSGÁLAT KUTATÁSÁNAK JELENLEGI MÓDSZEREI

A külföldi katonai szolgálatra történő fizikai alkalmasság-vizsgálat kutatásának jelenlegi módszerei:

- Egyszerű antropometria vizsgálatok (testsúly, testmagasság, testzsír százalék, BMI mérés stb.).
- Egyszerű és összetett teljesítmény-élettani vizsgálatok laboratóriumi és pályakörülmények között (kerékpár ergometria, futás, gyorsított menet, karhajlítás-nyújtás mellső fekvőtámaszban, karhajlítás-nyújtás függésben, felülés stb.).
- A vizsgálati eredmények dokumentálása és elemzése.
- A témával kapcsolatos nemzetközi és hazai szakirodalom tanulmányozása.

## A MOZGÁSFORMÁK

**2. sz. kép:**
Az MH HEK PI Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály, szabadtéri pályakörülmények között végrehajtott terheléses vizsgálatáról (3200 m síkfutás, 6000 m gyorsított menet)[4]

**3. sz. kép pár:**
Az MH HEK PI Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály, Teljesítmény-élettani laboratórium kerékpárergometriás terheléses vizsgálatáról ($VO_2$max típusú kerékpár ergométeres terheléses vizsgálatok)[5]

**4. sz. kép pár:**
az MH HEK PI Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály, Teljesítmény-élettani laboratórium, vállöv izom erő-állóképesség vizsgálatáról (karhajlítás-nyújtás mellső fekvőtámaszban 2 perc alatt)[6]

**5. sz. kép pár:**
Az MH HEK PI Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály, Teljesítmény-élettani laboratórium, vállöv izom erő-állóképesség vizsgálatáról (karhajlítás-nyújtás függésben 2 perc alatt)[7]

**6. sz. kép:**
Az MH HEK PI Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály, Teljesítmény-élettani laboratórium, hasizom erő-állóképesség vizsgálatáról (módosított felülés 2 perc alatt)[8]

**7. sz. kép pár:**
Az MH HEK PI Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály, Teljesítmény-élettani laboratórium, hasizom erő-állóképesség vizsgálatáról (hasprés vagy lapockaemelés 2 perc alatt)[9]

**8. sz. kép pár:**
Az MH HEK PI Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály, Teljesítmény-élettani laboratórium, vállöv izom erő-állóképesség vizsgálatáról (karhajlítás-nyújtás függésben társ segítségével 2 perc alatt)[10]

Az előírt mozgásformák közül egy keringésrendszeri állóképességet (2-3. sz. képek) és két helyi izom erő-állóképességet (4, 5, 8. sz. kép párok, 6. sz. kép) felmérő mozgásforma végrehajtását írtja elő a hatályos 7/2006. (III.21.) HM rendelet. A T1 és T2 könnyű fizikai munkát jelző munkakörökben a keringésrendszeri állóképességet vizsgáló 6 km gyorsított menet és a 3200 méter síkfutás (2. sz. kép) választható. A T3 és T4 közepes és nehéz fizikai munkavégzést jelölő munkakörökben a 3200 méter síkfutás kötelező mozgásforma (2. sz. kép). Szakmailag indokolt esetekben a felmérő bizottság dönthet úgy, hogy ergométeres vizsgálatot (3. sz. kép pár) alkalmaz (pl.: magas vérnyomás, balesetveszélyes pályakörülmények stb.). Az ergométereken végzett terhelések teljes kimerülésig tartó úgynevezett vitamax jellegű vizsgálatok (3. sz. kép pár). Ezek során a fokozatosan emelkedő intenzitás 1 perces terhelési lépcsőben testtömeg kilogramm/0,25 wattot jelent. Az erő-állóképességet felmérő mozgásformák közé tartoznak a karhajlítás-nyújtás mellső fekvőtámaszban (4. sz. kép pár, a továbbiakban: fekvőtámasz), a karhajlítás-nyújtás függésben (5. sz. kép pár, a továbbiakban: húzódzkodás) és a felülés gyakorlatcsoport

(6. sz. kép: módosított felülés, 7. sz. kép pár: hasprés) gyakorlatai. A férfiaknál (T1-T4 kategóriákban) és a közepes, nehéz fizikai munkát végző nőknél (azaz a T3-T4 kategóriákban) a fekvőtámasz mellett a húzódzkodás (6. sz. kép pár) is választható. Az ülő és a könnyű fizikai munkát végző nőknél (T1-T2 kategóriákban) alkalmazásra kerülhet a mellső térdelőtámaszban történő karhajlítás-nyújtás mozgásforma is (7. sz. kép pár). A húzódzkodás nőknél társ segítségével is végrehajtható (8. sz. kép pár).
A T1 és T2 ülő és könnyű fizikai munkavégzést jelölő munkaköri kategóriákban, a térdben hajlított emelt lábhelyzetben hanyattfekvésből végrehajtott törzsemelés/lapockaemelés (hasprés) választható (7. sz. kép pár). A T3-T4 nehéz fizikai munkát jelentő munkaköri kategóriákban a törzs izomzatának részleges tesztelésére hivatott módosított felülés során a láb talajhoz történő rögzítése nem megengedett.

## A KÜLFÖLDI KATONAI SZOLGÁLATHOZ SZÜKSÉGES FIZIKAI ALKALMASSÁG ELBÍRÁLÁSA, MINŐSÍTÉSE (7/2006. (III. 21.) HM rendelet)

**(a) T4 követelményszint (260 pontos teljesítmény):**

„Fegyveres béketeremtő, illetve békefenntartó, vagy különleges megterhelést jelentő katonai szakfeladat végrehajtása, annak időtartamától függetlenül.”[11]

**(b) T3 követelményszint (240 pontos teljesítmény):**

„Béketeremtő, illetve békefenntartói szolgálat törzsbeosztásban, vagy nem fegyveres szolgálat saját szakmájában, illetve NATO beosztás ellátása, annak időtartamától függetlenül.”[12]

**(c) T2 követelményszint (220 pontos teljesítmény):**

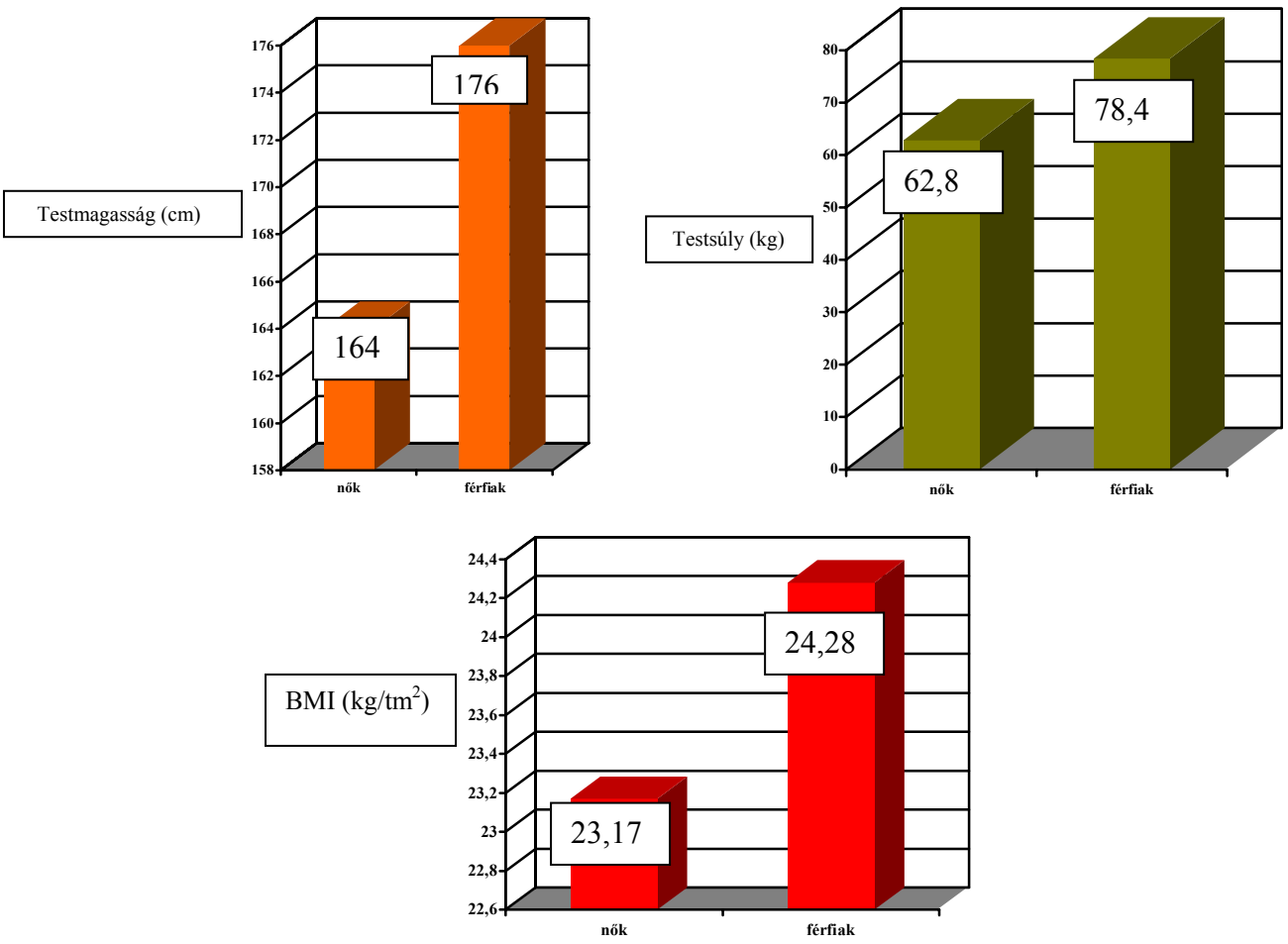
„Egy évet meghaladó tanulmány (pl. katonai oktatási intézményben) vagy kutató munka végzése estében, de nem lehet alacsonyabb a beosztásának megfelelő besorolási szintnél.”[13]

**(d) T1 követelményszint (200 pontos teljesítmény):**

„Egy évnél rövidebb ideig tartó tanulmányi vagy kutatói tevékenység végzése esetében a fizikai követelmény, de nem lehet alacsonyabb a beosztásának megfelelő besorolási szintnél.”[14]

A katonai feladatok végrehajtása fokozott fizikai és pszichikai igénybevétellel jár. Függetlenül a különböző beosztásokra jellemző terhelési sajátosságoktól, a katonáknak, - a katonai „mesterség” jellegéből adódóan - rendelkeznie kell egy bizonyos szintű fizikai erőnléti állapottal. Ezért a vizsgálati módszereink több irányúak és összetettek. Elsősorban az állóképesség és az erő-állóképesség, mint két meghatározó fizikai motoros kondícionális képesség mérésére hivatottak.

A háromirányú (egészségi, pszichikai, fizikai), komplex pályaalkalmassági vizsgálat részeként a katonai fizikai alkalmasság-vizsgálat egy rendkívül összetett tevékenység. Olyan teljesítmény-élettani vizsgáló eljárások összessége, amelyek egy adott munkakör betöltéséhez, illetve adott munkafeladatok elvégzéséhez szükséges fizikai adottságok, és képességek meglétét vizsgálja. A terhelés- és teljesítmény-élettani laboratóriumi, valamint pálya vizsgálatokat minden esetben egy speciális célorientált szakorvosi, életmódprofil és testösszetétel vizsgálat előzi meg, mely alapjául szolgál a későbbi terhelési protokollok meghatározásakor.

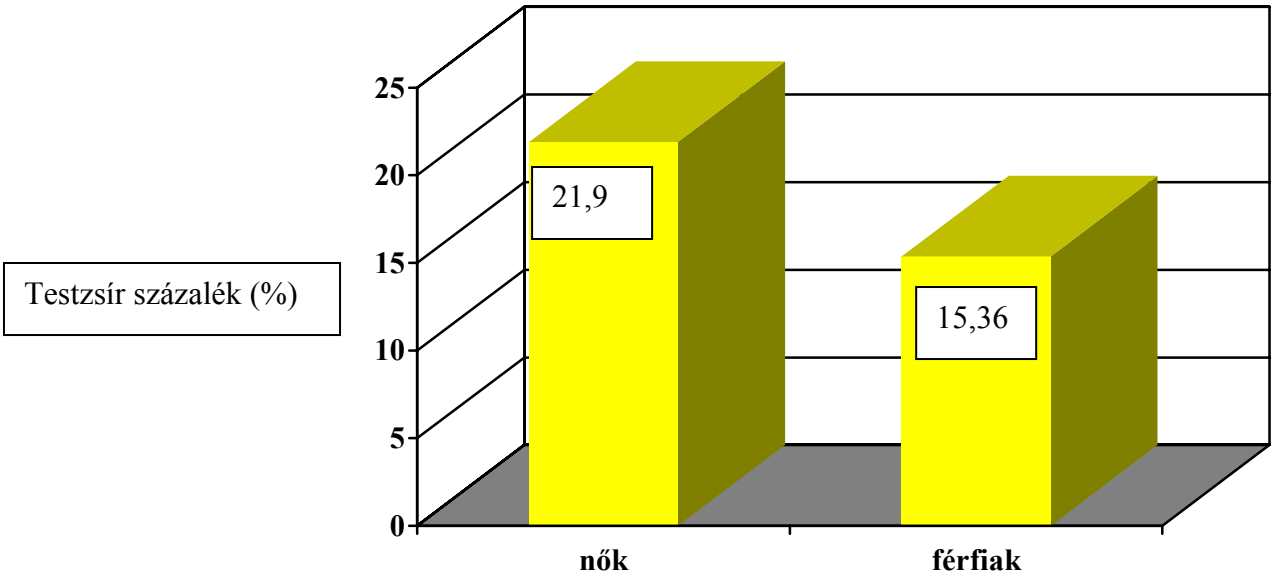



**2. sz. ábracsoport:**
A külföldi katonai szolgálatra jelentkező hivatásos és szerződéses állomány testmagasság, testsúly és BMI átlagértékeinek nemenkénti megoszlásáról
(2007. január 01 - december 31. között)[15]

A fenti ábracsoporton keresztül látható, hogy a tárgy időszakban megvizsgált külszolgálatra jelentkező állomány antropometriai mutatói nemenkénti bontásban miként oszlanak meg. A vizsgált populáció 25 és 55 év közötti katonák értékeit tartalmazza. A BMI (Body Mass Index, számolása: testsúly kilogramm/testmagasság$^2$), mely az elhízás mértékének pontosabb mennyiségi meghatározására hivatott. A fent olvasható átlag testsúly és testmagasság értékek alapján a nőknél: 23,17 a férfiaknál pedig: 24,28, mely „a normális BMI: 18,5-24,9 kg/m$^2$" [16] értékeket figyelembe véve elfogadható, azaz normális.

„A túlsúly és az elhízás mértéke:

| BMI | WHO |
|---|---|
| <18,5 | Sovány |
| 18,5-24,9 | Normális |
| 25,0-29,9 | Túlsúly |
| 30,0-34,9 | Elhízás I |
| 35,0-39,9 | Elhízás II |
| 40,0 fölött | Elhízás III”[17] |




**3. sz. ábra:**
A külföldi katonai szolgálatra jelentkező hivatásos és szerződéses állomány testzsír százalék átlagértékeinek nemenkénti megoszlásáról
(2007. január 01 - december 31. között)[18]

A testzsír százalékméréseket a Bioelektromos Impedancia Analízis módszerrel végeztük, mellyel a zsír testsúlyhoz viszonyított abszolút mennyiségi értékét tudtuk meghatározni. Egy speciális műszer segítségével minimális elektromos áramot vezettünk át a testen és megmértük a testszövetek ellenállását. Mivel a testzsírszövet elektromos vezetőképessége rosszabb, mint más szöveté (pl. izom-, csontszövet stb.) lehetővé válik az elektromos vezetőképességek egymáshoz történő viszonyítása. Méréseink alapján az átlag testzsír százalékértékek a nőknél: 21,9 %, míg a férfiaknál 15,36 % -ot mutattak, mely arra utalt, hogy az általunk vizsgált célcsoport megfelelő átlagértékekkel bír, de ez természetesen nem jelenti azt, hogy nem vizsgáltunk kórosan elhízott vagy sovány katonákat. A férfiaknál a 10-19%, a nőknél 20-29% megfelelő mennyiségnek, viszont a férfiaknál a 25% és a nőknél a 30% feletti értékek aggodalomra adnak okot, mert veszélyt jelent elsősorban a szív-keringési szervrendszerre és természetesen összességében - az élettani folyamtok összefüggéseinek tudatában - az egész emberi szervezetre, annak zavartalan működésére.

## VÁLTOZÁSOK, EREDMÉNYEK

| 2001-2006 között alkalmazott mozgásformák | 2006-tól alkalmazott új mozgásformák |
|---|---|
| ▪3200 m futás | ▪3200 m futás |
| ▪4 km gyaloglás (már nincs) | ▪6 km gyorsított menet (új) |
| ▪10 km kerékpár-ergometria (már nincs) | ▪VO2max típusú kerékpár-ergometria (új) |
| ▪Mellső fekvőtámaszban karhajlítás-nyújtás (T1-T4 kategóriákban) | ▪Mellső térdelőtámaszban karhajlítás-nyújtás (új) (T1-T2 kategóriákban, csak nőknél) |
| ▪Függésben karhajlítás-nyújtás, húzódzkodás (T1-T4 kategóriákban) | ▪Húzódzkodás társ segítségével (új) (T1-T2 kategóriákban, csak nőknél) |
| ▪Hanyattfekvésből felülés társ segítségével (már nincs) (T1-T4 kategóriákban) | ▪Hanyattfekvésből lapockaemelés (új) (T1-T2 kategóriákban) |
| | ▪Hanyattfekvésből felülés társ segítsége nélkül (új) |

## ÖSSZEHASONLÍTÓ VIZSGÁLATI STATISZTIKAI ADATOK

A haderő átalakulásának, illetve az új típusú feladatok következményeként a vizsgálatok túlnyomó többsége **a külföldi katonai szolgálatra jelentkezők (47,4%)**, a hivatásos és szerződéses állományba (39,2%) jelentkezők körében történt. A fennmaradó 13,4% a következő képpen oszlik meg: katonai oktatásra jelentkezők (9,1%), fizikai állapotfelmérések (1,8%), külföldi katonai oktatásra jelentkezők (1,1%), fizikai felülvizsgálatok (0,7%), előmenetel előtti vizsgálatok (0,7%).

1998-tól az önkéntes haderőre történő áttérésig (2004) a vizsgálati létszám folyamatosan növekedett. 2004 óta a haderő átalakításával párhuzamosan csökkenő tendenciát mutatott a végrehajtott vizsgálatok száma. Azonban az előző (2006) év adataival összehasonlítva: a vizsgálatra berendeltek létszáma 1483 fővel nőtt (22,4%). A megjelenési arány 2006. és 2007. évben a következő képpen alakult, 92%-ról 89,6%-ra csökkent, így a megjelenési mutató 2,4%-ot romlott. Az alkalmassági mutató 16,86%-kal visszaesett. Az alkalmatlansági mutató 16,1%-kal nőtt, míg a nem terhelhetők száma 0,24%-kal csökkent. A változó statisztikai adatok hátterében valószínűleg a hivatásos és szerződéses katonai szolgálatra, valamint a katonai oktatási intézményi tanulmányokra való egészségi, pszichikai, fizikai alkalmasság elbírálásáról szóló 7/2006 (III.21.) HM rendelet szigorúbb alkalmasság-vizsgálati követelményrendszere és a már említett állandó problémaként említhető nem megfelelő mozgásszegény életmód áll.

| | Év | Berendelt | Megjelent | Alkalmas | Alkalmatlan | Nem terhelhető |
|---|---|---|---|---|---|---|
| 1. | 1998 | 1930 | 1087 | 279 | 672 | 136 |
| | | 100% | 55% | 25% | 62% | 13% |
| 2. | 1999 | 7480 | 3566 | 1637 | 1657 | 272 |
| | | 100% | 47% | 46% | 46% | 8% |
| 3. | 2000 | 6250 | 4363 | 2210 | 1823 | 330 |
| | | 100% | 69% | 51% | 42% | 7% |
| 4. | 2001 | 8267 | 6380 | 4168 | 2146 | 65 |
| | | 100% | 77% | 65,50% | 33,60% | 0,90% |
| 5. | 2002 | 7673 | 6983 | 6755 | 45 | 183 |
| | | 100% | 91% | 97% | 0,50% | 2,50% |
| 6. | 2003 | 9705 | 9149 | 8668 | 198 | 283 |
| | | 100% | 94% | 95% | 2% | 3% |
| 7. | 2004 | 7296 | 6558 | 6084 | 388 | 76 |
| | | 100% | 90% | 93% | 6% | 1% |
| 8. | 2005 | 6749 | 6398 | 6028 | 204 | 166 |
| | | 100% | 95% | 94% | 3% | 3% |
| 9. | 2006 | 6599 | 6095 | 5136 | 696 | 263 |
| | | 100% | 92% | 84% | 12% | 4% |
| 10. | 2007 | 8082 | 7242 | 4934 | 2035 | 273 |
| | | 100% | 89,6% | 68,14% | 28,1% | 3,76% |

**1. sz. táblázat:**

Az 1998. 03. 01-től 2007. 12. 31-ig terjedő időszak összehasonlító vizsgálati statisztikai adatairól[19]

## JÖVŐBENI TERVEIM ÉS A VÁRHATÓ TUDOMÁNYOS EREDMÉNYEK

A jövőbeni terveim között szerepel:

- A pálya és laboratóriumi vizsgálatok további elemzése, továbbfejlesztése.
- Futószalag ergometriás vizsgálatok kísérleti szinten történő megkezdése és összehangolása a már rendszerben lévő kerékpár ergometriás vizsgálatokkal.
- A vizsgálati eredmények elemzése, feldolgozása, értékelése külszolgálat előtt és után.
- A fegyveres testületek egységes fizikai alkalmasság-vizsgálati rendszerének kidolgozása

A munka várható új tudományos eredményei a következők lehetnek:

- Az általam kidolgozott és bizonyított új módszertan alapján kerülnek jövőben a jelöltek vizsgálatra.
- Az alkalmasok aránya növekszik – gazdaságosság.

- Költséghatékonyabb vizsgálati rendszer alakul ki, mely egyben új vizsgálati eljárás is lesz.
- A magyar haderő alkalmazásának hatékonysága növekszik.
- A magyar fegyveres testületek fizikai alkalmasság-vizsgálati rendszere egységessé válik.

## ÖSSZEGZÉS

A fizikai alkalmasság-vizsgálati rendszer több mint tíz éves fejlődési folyamata hazánk honvédségének életében meghatározó jelenség volt. Mindig a kor elvárásainak megfelelően változott és változik a mai napig is. Haderőnk ma már korszerű, NATO és EU kompatibilis, melyhez elengedhetetlen a leendő katonák fizikai erőnléti állapotának előzetes vizsgálata és a már rendszerben lévők külföldi missziós elvárásokhoz szükséges egyéni fizikai teljesítményének növelése. A XXI. század modern, korszerű hadseregeinek katonái egészségileg, mentálisan és fizikálisan mindig készen kell, hogy álljanak a különböző kihívások, feladatok eredményes végrehajtására. Ma Magyarországon az alkalmasság-vizsgálati rendszer részeként a Fizikai Alkalmasság-vizsgáló Osztály az, „aki" a szakmai hátteret biztosítja és megtesz mindent azért, hogy csak a lehető legjobb fizikai erőnléti állapotban lévő személyekből válhasson katona, és csak azok szolgálhassanak külföldön, akik arra fizikálisan is a legalkalmasabbak. A tudományos kutatói tevékenységemmel arra törekszem, hogy a rendszer fejlődése töretlen maradhasson és ez által haderőnk működése gazdaságosabbá és sikeresebbé váljon.

### Irodalmi hivatkozások

1 Juhász Zsolt osztályvezető, doktorandusz, Magyar Honvédség, Honvéd Egészségügyi Központ, Preventív Igazgatóság, Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály

2, 18 Magyar Honvédség, Honvéd Egészségügyi Központ, Preventív Igazgatóság, Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály ábrái

3-10 Magyar Honvédség, Honvéd Egészségügyi Központ, Preventív Igazgatóság, Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály képanyaga

11 Magyar Közlöny, 31. szám, I kötet, 7/2006. (III. 21.) HM r., VII. fejezet, 22. § (1) a), 2469. o.

12 Magyar Közlöny, 31. szám, I kötet, 7/2006. (III. 21.) HM r., VII. fejezet, 22. § (1) b), 2469. o.

13 Magyar Közlöny, 31. szám, I kötet, 7/2006. (III. 21.) HM r., VII. fejezet, 22. § (1) c), 2469. o.

14 Magyar Közlöny, 31. szám, I kötet, 7/2006. (III. 21.) HM r., VII. fejezet, 22. § (1) d), 2469. o.

15 Magyar Honvédség, Honvéd Egészségügyi Központ, Preventív Igazgatóság, Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály ábrái

16-17 Magyar Közlöny, 31. szám, I kötet, 7/2006. (III. 21.) HM r., 1. melléklet, 2490 o., b)

19 Magyar Honvédség, Honvéd Egészségügyi Központ, Preventív Igazgatóság, Alkalmasság-vizsgáló Intézet, Fizikai Alkalmasság-vizsgáló Osztály adatbázisa

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Halász László**
Zrínyi Miklós Nemzetvédelmi Egyetem, egyetemi tanár
halasz.laszlo@zmne.hu

**Vincze Árpád**
Zrínyi Miklós Nemzetvédelmi Egyetem, egyetemi docens
vincze.arpad@zmne.hu

**Solymosi József**
Zrínyi Miklós Nemzetvédelmi Egyetem, egyetemi tanár
solymosi.jozsef@zmne.hu

**Vass András**
Veszprémi Egyetem, Szerves Vegyipari Kutatóintézet

**Bucsky György**
Veszprémi Egyetem, Szerves Vegyipari Kutatóintézet

**Ujhidy Aurél**
Veszprémi Egyetem, Szerves Vegyipari Kutatóintézet

# ÚJ ELJÁRÁS KATONAI IMPREGNÁLT SZENEK ELŐÁLLÍTÁSÁRA

***Absztrakt***

*A különböző ipari és katonai szűrőkben impregnált aktív szenet használnak a levegőben gáz és gőzállapotú káros anyagok kiszűrésére. A jelenleg alkalmazott impregnálási technológia során a környezetre káros, toxikus anyagokat is felhasználnak, a hagyományos impregnálási eljárásnak nagy az energiaigénye és gyakran a szén morfológiai tulajdonságai is kedvezőtlenül változnak az eljárás alatt. Egy új mikrohullámmal kombinált impregnálási eljárás és hőkezelési technológia került kifejlesztésre. Az új technológia hatékonyságát a katonai gázálarcokban alkalmazott NBC impregnált aktívszén előállítása bizonyította.*

*Impregnated activated carbon is used in different industrial and military air filters to remove dangerous vapours and gases from the air. The impregnation technologies generally are using some toxic material and the energy consumption is significant and sometimes changes the microstructure of activated carbon. A new impregnation method combined with the use of microwave and microwave*

*drying and heating treatment processes have been developed. The effectiveness of the new technology was proven preparing a good quality NBC impregnated activated carbon.*
***Kulcsszavak**: aktvíszén, impregnálás ~ activated carbon, impregnate*

## Bevezetés

A gázálarc szűrőbetétekben, nagyméretű levegőszűrő berendezésekben, a levegőben lévő gáz és gőzállapotú káros anyagok kiszűrésére aktívszenet illetve megfelelően impregnált aktívszenet használnak. Az impregnálás feladata, hogy a fizikai megkötés mellett kémiai reakciókkal elősegítse a káros anyagok ártalmatlanítását. Az impregnált szenek klasszikus előállítási módszereiben, az impregnáló berendezésben az aktív szenet az impregnáló oldattal adott érintkezési ideig keverik normál vagy csökkentett nyomáson. Az impregnálást követően szárítják termikus hőkezeléssel. A szárítást követően az impregnálószer összetételétől függő hőkezelési folyamat következik, amely az aktív szén felületén lévő impregnátum átalakítását segíti elő. Egy új eljárás került kialakításra mikrohullámú terek alkalmazásával.

## Új gyártási módszerek kidolgozása

Az impregnálási eljárások célja az adszorbensek tulajdonságainak módosítása. A módosítások hatása lehet:

- *Az aktívszén tulajdonságainak optimálása.* Az aktívszén egyes szerves és szervetlen vegyületeket katalitikusan oxidál. Ezt a tulajdonságot javítani lehet például KJ-os impregnálással.
- *Szinergelizmus az impregnáló anyag és az aktívszén között.* Normál hőmérsékleten a kén a higanyt kéndiszulfid formában köti meg. Ha a kenet aktivszénre viszik fel, a szulfidképződés alacsonyabb hőmérsékleten is végbemegy.
- *Az impregnálószer kémiai reakcióban vesz részt, amikor az aktívszén, mint pórusos hordozó játszik szerepet.* A foszforsavval impregnált aktívszén, például jól használható ammónia elnyeletésére. Az impregnálási folyamatokat feloszthatjuk:
    - egyszeres impregnálási,
      kétszeres impregnálási,
    - többszörös impregnálási folyamatokra. (Az utóbbi eljárások elsősorban a katonai aktívszenek előállításakor használatosak.)

Az impregnálás általában három lépésből áll:

1. Itatás - az aktívszén kezelése az oldott impregnálószerrel
2. Szárítás - az oldószer eltávolítása tömegállandóságig történő szárítással.
3. Utó(hő)kezelés - az impregnátum átalakítása hőkezeléssel.

### Az aktívszenek *intenzív* kezelése az oldott impregnáló szer(ek)kel

***1. Itatás***

Célkitűzés: a feladatorientáltan kiválasztott (eredet, kémiai összetétel, szemcseméret, felületi és pórus tulajdonságok, stb.) aktívszénnel, az ugyancsak célorientáltan meghatározott minőségű, oldott komponensek megfelelő mennyiségű és struktúrájú megkötése.

Ez a folyamat valójában egy *kontakt adszorpció,* a folyadékban oldott anyagok adszorpciója. Ilyen feladatra, a diffúziós vegyipari műveletek előírásai szerint, leggyakrabban szakaszos,

vagy félfolyamatos működésű, álló(rögzített)ágyas és/vagy fluidizált ágyas adszorbereket használnak. A műveletben, az egyensúly elérésével szemben, ellenállások jelentkeznek:

1. Az egyes adszorbens részecskéket körülvevő folyadékban az oldott anyag átvitelével szemben keletkező lamináris folyadékfilm ellenállás, ami jelentősen csökkenthető intenzív keveréssel létrehozott turbulens áramlással.

2. Diffúziós ellenállás a szilárd adszorbens pórusaiban levő folyadékban, amely akkor lép fel, amikor az oldott anyag a részecske külső felületéről a pórusok belső felülete felé diffundál, ahol végül adszorbeálódik. (A pórusokban levő folyadékot nem befolyásolja a részecskét körülvevő folyadék turbulenciája, nem áramlik, ezért benne az oldott anyag átvitele *molekuláris diffúzió* útján megy végbe. A diffúzió útja viszonylag hosszú és tekervényes, sebessége „szerkezet" érzékeny, függ az adszorbens megkötési tulajdonságaitól, a kialakuló kapilláris nyomásoktól, az oldott anyag molekuláris tulajdonságaitól, annak koncentrációjától, az oldat sűrűségétől, viszkozitásától, felületi feszültségétől stb.)

3. Az ellenállás magával az adszorpcióval szemben, ami akkor lép fel, ha az adszorbeálandó molekuláknak a felület őket megkötő pontjára történő érkezése és az adszorpció megtörténése között véges idő telik el, például amiatt, mert az oldott anyag molekuláinak e felülethez viszonyítva megfelelő irányba kell beállniuk.

Adott rendszer és adszorbens esetén sem a 2. sem a 3. típusú ellenállást nincs módunkban befolyásolni.
Az oldott komponenseket tartalmazó impregnáló folyadékkal történő aktívszén kezelés a perkolálás speciális esete. Ennek alapján, a feladatra célszerűen egy félfolyamatos működésű, álló és/vagy fluidizált ágyas aktívszenes adszorbert célszerű használni, ahol az impregnáló oldat adott ideig tartó és adott térfogatáramú recirkulációs áramoltatásával lehet biztosítani a szemcsés halmaz optimálisan szükséges turbulens kevertségét. (Az álló és/vagy fluidizált ágyas áramlási állapotok közötti választást vagy kombinált alkalmazást, kísérleti vizsgálatokkal kell megalapozni, figyelemmel a szén-szemcsék nem kívánt porlódására is.)

A kialakított impregnálási eljárás alapvető újdonsága az, hogy az oldott anyag adszorpciója során az *adszorbens szemcsék lokális hőmérsékletét ciklikusan változtatva* - adott frekvenciájú és teljesítményű *mikrohullámú erőtér időközönkénti alkalmazásával* - magasabb értéken tartjuk, mint a recirkuláltatott és állandó értékre hűtötten használt impregnálószer tartalmú folyadékét. A lokálisan létrehozott mikrohullámú felmelegítésre, az adszorbensnek az oldott anyagtól és oldószertől eltérő dielektromos tulajdonsága ad lehetőséget. Ezzel elérhető, hogy a diffúziós sebesség szerkezet-érzékeny ellenállása csökkenthető legyen a lokális hőmérséklet növelésével vélelmezhetően és különösen még a kapilláris belsejében is. Az oldatnak, a recirkuláció során történő állandó visszahűtése azért szükséges, hogy a szemcse felületéről a hűtés minél gyorsabban éreztesse hatását a szemcse belsejére, biztosítva ezzel, hogy a lehetőleg minél rövidebb ideig tartó, rövid ciklusú mikrohullámú fűtést lokálisan gyors lehűlés kövesse. A rövid ciklusidejű és váltakozó hőközlés és hőelvonás, a pórusokon belüli ellenállást nemcsak a molekuláris diffúzió sebességének növelésével csökkenti, hanem *a kapilláris nyomás ingadoztatásán* keresztül is kedvező hatást gyakorol az impregnálószer „itatásának" intenzitására.

A ciklikusan alkalmazott mikrohullámú energiaközléssel kombinált, recirkulációs, hűtött folyadékárammal működtetett álló és/vagy fluidizált ágyas áztató adszorber alkalmazása a következő előnyökkel jár.

- gyorsabb anyag átalakítás, rövidebb műveleti idő
- intenzív, aprítódás mentes áramlási viszonyok,
- váltakozó, szelektív és lokális melegítés és hűtés, az anyagi minőség függvényében,
- jól ellenőrizhető folyamatirányítás, gyors és hatékony beavatkozás,
- tiszta, hulladékmentes energiaforrás,
- környezetbarát, anyagtakarékos, hulladékszegény technológiai megoldás.

**Egy nagylaboratóriumi méretű, ~ 5 kg/h aktívszén kapacitásra vonatkozó gyártástechnológia kidolgozása**

*A kísérleti berendezés* (1. ábra) félfolyamatos, álló és/vagy fluidizált ágyas, recirkulációs folyadékárammal működő, cserélhető rétegtartó-betétes adszorber. A berendezés további részei a cirkulációs szivattyú és a nyomóköri hűtő, amivel az állandó koncentrációjú recirkulációs folyadékáram folyamatosan és hőfokszabályzottan hűthető. Az adszorbens mikrohullámú besugárzására alkalmazott energia nagysága és hullámhossza - előzetes kísérleti vizsgálatokkal megalapozottan - állandó, csak az energiaközlés ciklusideje változó. A cirkulációs kör része még az aktívszén-réteg esetleges kopását eltávolító szűrő is. A berendezés megfelelő műszerezéssel ellátott.

1. ábra: Félüzemi mikrohullámú impregnáló berendezés

## Impregnált aktív szenek mikrohullámú szárítása és utó(hő)kezelése

### *2. Szárítás*

Az impregnálás itatási lépése után, az impregnáló oldatból kiszűrt (pl. lecsurgatott vagy centrifugázott) aktív szenet szárítási eljárásnak kell alávetni. Ennek során el kell távolítani a felületen fizikailag megtapadt, továbbá az aktív szén pórusaiban kemoszorpcióval megkötött vizet.

A szárítási folyamat különféle eljárásokkal és berendezésekkel történhet, így mikrohullámú kezeléssel is.

Az impregnált aktív szén mikrohullámú szárítása - és hőkezelése is - különleges feladatot jelent. A mikrohullámú térben a felvett és a minta által hővé alakult energiát az elektromos térerő és frekvencia mellett - a minta dielektromos állandója határozza meg. Az impregnált aktív szén egy igen összetett anyagi rendszer, mivel adott származású és aktiválású szénből, az impregnálás során felvitt fémsók keverékéből, esetleg szerves vegyületekből és vízből áll. A szárítás során a víz eltávozásával megváltozik az anyagi minőség, részben a víz mennyiségének csökkenése, részben a korábban oldott sók felületen történő beszáradása miatt. Ennek következtében a minta dielektromos állandója, a felvett és hővé alakult energia, valamint a mintában kialakuló hőmérséklet is megváltozik. Bonyolítja a helyzetet, hogy a minta dielektromos állandója még a hőmérséklet függvényében is nő, vagy csökken.

A mikrohullámú szárítás során a gyors hőmérséklet emelkedés miatt a minta környezetében a relatív páratartalom gyorsan megnő, a szárítás hatásossága miatt ezt inert gázárammal folyamatosan el kell távolítani, másként a szárítási idő nem fog jelentősen csökkeni, így a mikrohullámú szárítási művelet végül is kombinált szárításnak is tekinthető.

### *3. Hőkezelés*

A hőkezelés az impregnált aktív szénre felvitt nehézfémsók hő hatására történő kémiai átalakítása, olyan vegyületekké, amelyek elősegítik, vagy végrehajtják a veszélyes anyagok ártalmatlanítását.

Ez a folyamat is elvégezhető termikusan hőközléssel, egy megfelelően megválasztott berendezésben, de mikrohullámú energiaközléssel is.

A szárítás során a már felsorolt tényezőkhöz egy további, lényeges elem kapcsolódik, nevezetesen az, hogy a hőkezelés során kémiai változás is bekövetkezik. Ez a változás a szárítás során felsoroltakhoz képes sokkal jelentősebb, mivel a minta dielektromos állandójában a legnagyobb változást okozza. A kémiai átalakulás az esetek többségében az $AgNO_3$, és a $Cu(NO_3)_2$ átalakulása $Ag_2O$ és CuO anyagokká. Az átalakulás ionos anyagokból nemionos anyagokat eredményez, ami a dielektromos állandó lényeges változását eredményezi. Az átalakulás időreakció, ennek során a dielektromos állandó is időben változik, ezzel időben változik a hővé alakult energia és a kialakuló hőmérséklet is. A mikrohullámú energia közlés során elvileg nem várható semmi olyan atermikus hatás, amely megváltoztatná a kémiai átalakulás termékeit. A mikrohullámú energiaközlés sajátságosságából eredően a termikus átalakításhoz képest várhatóan sokkal gyorsabb lesz az átalakulás, azaz csökken a reakcióidő, az átalakulás a minta teljes tömegében egyszerre játszódik le. Megtörténhet, hogy a minta dielektromos állandójának változása - akár a minőség változás, akár pozitív hőmérsékletfüggés miatt - drasztikusan megnövekszik, aminek következménye a hirtelen hőmérséklet megfutás (run away) lehet.

A mikrohullámú energia alkalmazása az impregnált aktív szenek előállításánál akkor igazán előnyös, ha szárítás után hőkezelés is szükséges, mert ebben az esetben a két folyamat összevonható és egy berendezésben elvégezhető. A mikrohullámú energiaközlés a következő előnyökkel jár.

- gyorsabb anyag átalakítás, rövidebb műveleti idő,

- teljes tömegű melegítés, nincs falhatás,
- szelektív melegítés az anyag minőség függvényében,
- a jól ellenőrizhető folyamatirányítás gyors és hatékony beavatkozás,
- kisebb készülék, folyamatos üzemvitel,
- energia megtakarítás,
- tiszta, hulladékmentes energiaforrás,
- környezetbarát, hulladékszegény technológiai megoldás.

A 2. ábra mutatja a mikrohullámú szárító és hőkezelő berendezést

2 ábra: Mikrohullámú szárító és hőkezelő berendezés

## Az új technológia alkalmazása katonai impregnált aktívszén előállítására

A katonai gázálarcokban, mobil és stabil légszűrőkben mérgező harcanyagok elnyelésére alkalmas impregnált aktív szeneket használnak. Ezek a szenek ezüst-, réz-, cinksókkal itatott szenek.

### A kísérletekben használt aktívszén jellemzői, az itató oldatok összetétele

Az alapszén megkövetelt jellemzői :

| | |
|---|---|
| BET-felület (min.): | 1200 $m^2/g$ |
| Pórustérfogat (min) | 0,9 $cm^3/g$ |

| | |
|---|---|
| Szilárdság (min.) | 0,99 % |
| Szemcseméret: | <1,5 mm 5%<br>1,5…2,5 mm 80%,<br>>2,5 mm 15% |
| Nedvességtartalom: (max) | 2% |
| Gyulladási hőmérséklet (min) | 330 $^0$C |
| Hamutartalom (max) | 4% |

A kísérletekben használt szén a Silcarbon 08.

Az impregnáló fürdő összetétele és elkészítése

59,5 m/m % ioncserélt, aktív szénen klorid-ion mentesített vízhez hozzáadtunk
5,1 m/m% szilárd $(NH_4)_2CO_3$ –ot, majd ennek feloldódása után
7,7 m/m% 25%-os tömény (0,91 g/ml sűrűségű) $NH_4OH$ oldatot, majd ebben
2,1 m/m% szilárd $ZnCO_3$ –ot oldottunk fel. Ezt követően hozzáadtunk további
19,3 m/m% 25%-os tömény (0,91 g/ml sűrűségű) $NH_4OH$ oldatot, majd ebben
6,1 m/m% szilárd $2CuCO_3.Cu(OH)_2$ – ot oldottunk fel. Végül a legkevesebb,
0,2 m/m% szilárd $AgNO_3$ beoldása következett, egy célszerű méretű zárt edényben, a vonatkozó munka- és egészségvédelmi előírások szigorú betartása mellett.

A kapott, impregnált aktív szén jellemzői:

| | |
|---|---|
| BET felület | 1000 $m^2/g$ |
| Rézoxid tartalom: | 6,5%, |
| Ezüstoxid tartalom | 0,1% |
| Cinkoxid tartalom | 1,8% |

## Impregnálási és hőkezelési kísérletek

Az impregnálási és hőkezelési kísérleteket a félüzemi impregnáló és a kísérleti hőkezelő mikrohullámú berendezésekkel végeztük. A munka során a kitűzött cél a kereskedelemben kapható legjobb minőségű katonai impregnált aktívszénnel (például a Pleisch NBC-T-vel) azonos tulajdonságú szén előállítása, amelyik nem tartalmaz krómot. Az impregnálás során a következő feladatokat kellett megoldani:

1. Az impregnálási folyamat ismétlési számának meghatározása,
2. Az alkalmazandó impregnáló oldat összetételének optimálása
3. A szárítási paraméterek meghatározása (időtartam, hőmérséklet).

Az elkészült minták alap minősítése a felvitt fém mennyiség, továbbá a BET-felület és a HCN elnyelő-képesség meghatározásával történt. Amelyik minta megközelítette a követelményekben megszabott értékeket, arra a mintára nézve optimáltuk a hőkezelési technológiát és a kapott anyagot további elnyelőképesség vizsgálatoknak vetettük alá.

## A felvitt fém mennyiségének meghatározása

A felvitt fém mennyiségét két módszerrel határoztuk meg, az egyikben 1:1 hígítású salétromsavval leoldást végeztek, a második módszerben mikrohullámú roncsolóban elroncsolták a szénvázat, és a maradékból határozták meg a fém mennyiséget.

Néhány vizsgálati eredményt tartalmaz a következő táblázat:

1. táblázat: Aktívszén minták fémtartalom vizsgálata

| Kód | | 06-228/10 | 06-228/11 | 06-228/12 | 06-228/13 |
|---|---|---|---|---|---|
| Minta jele | | 2006.06.13. 1 | 2006.06.13. 3 | 2006.06.13. 377/119-T | 2006.06.13. 377/119-IV |
| A minta előkészítés kezdete: | | 2006.06.14. | | | |
| A vizsgálat befejezésének ideje: | | 2006.06.19. | | | |
| Ag | mg/kg | 171 | 128 | 131 | 128 |
| Cu | mg/kg | 38800 | 35100 | 42400 | 43000 |
| Zn | mg/kg | 10200 | 8240 | 11000 | 9450 |

A roncsolásos vizsgálat megbízható eredményeket szolgáltatott réz és cink esetében, a kimutatott ezüst mennyiségét kissé kevésnek találtuk az oldatba bevitt ezüst mennyiségéhez képest. A probléma megvizsgálására egyrészt megvizsgáltattuk a K5M impregnált szén fémtartalmát, másrészt elemeztettük az impregnáló oldatokat. A K5M esetében az elemzés megbízhatónak bizonyult. Az oldatok elemzésének eredményei azt mutatták, hogy a módszer megbízható.

## A HCN elnyelő-képesség vizsgálata

A vizsgáló berendezés a 3.sz. ábrán bemutatott séma alapján működik.

**Nedvesítés:**
A vizsgáló oszlopba bemért ismert tömegű mintán 75-80% relatív páratartalmú levegőt áramoltatunk addig, míg az oszlopról lejövő levegő páratartalma el nem éri a 70%-t. A légforgalom 1,5 liter/perc.

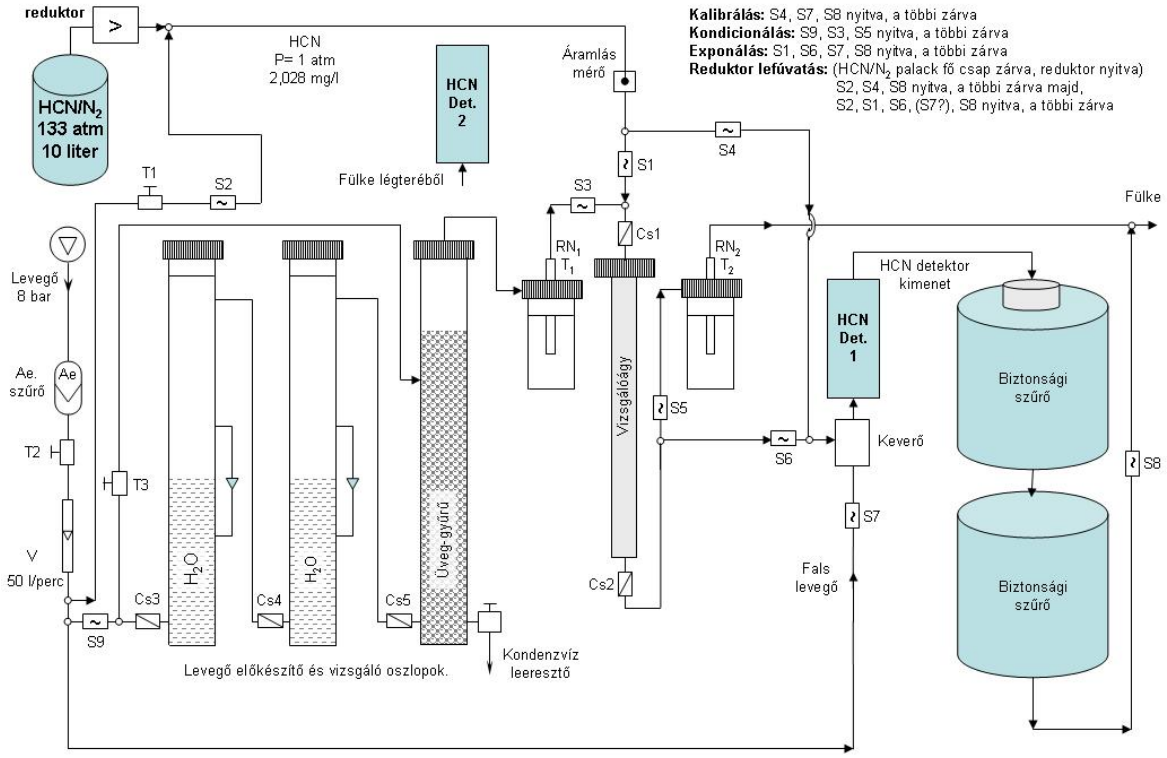
**Exponálás:**
Az előnedvesített mintán ciánsavat tartalmazó nitrogén gázt áramoltatunk át és mérjük az oszlop kimenetén a ciánsav koncentrációt.
A palack hitelesített HCN koncentrációja:
2,028 mg/m$^3$ ±5% , 1013 mbar, 273,15 K = 1887 ppm
Bemeneti koncentráció:
A környezeti hőmérséklet és nyomás függvénye, 32$^o$C-on, 1013 mbar:
1,689 mg/m$^3$ ±5% ~ 1689 ppm
Bemeneti áramlási sebesség: ~ 1,5 lpm

Az áttörési szakaszra az un. Wheeler – Jonas egyenletet illesztettük:

$$t_b = \frac{M \cdot W_e}{Q \cdot C_{BE}} - \frac{\rho_b \cdot W_e}{k_v \cdot C_{BE}} \ln\left(\frac{C_{BE} - C_{KI}}{C_{KI}}\right)$$

Ahol:
- $t_b$ : a $C_{KI}$ koncentrációhoz tartozó áttörési idő (min)
- M: a minta tömege (g)
- Q áramlási sebesség (cm$^3$/min)

- $C_{BE}$: bemeneti koncentráció (g/cm$^3$)
- $C_{KI}$: bemeneti koncentráció (g/cm$^3$)
- $\rho_b$: szénágy sűrűsége (0,46 g/cm$^3$)
- $k_v$ : adszorpciós sebességi együttható (min$^{-1}$)
- $W_e$: egyensúlyi adszorpciós kapacitás (g/$g_{szén}$)




3. ábra: A ciánsav penetrációt vizsgáló berendezés

A technológia és a receptúra optimálását követően előállított impregnált aktív szén jellemzőit mutatja a 2. sz. táblázat.

2. táblázat: Az optimált összetételű Sovecarbon NBC és a Pleisch NBC-T K1 jellemzői.

| | Pleisch NBC-T K1 | Sovecarbon NBC |
|---|---|---|
| • Szemcseeloszlás: | | |
| 0,5 – 1,0 mm | 4% | 5% |
| 1,0 – 1,5 mm | 81% | 82% |
| 1,5 – 2,0 mm | 9% | 7% |
| 2,0 – 2,5 mm | 3% | 6% |
| • rézoxid tartalom | 6,50% | 5,7% |
| • cinkoxid tartalom | 1,80% | 1,7% |
| • ezüstoxid tartalom | 0,06 | 0,04% |
| • Benzol elnyelő-képesség | 0,081 g/g | 0,128 g/g |
| • Széntetraklorid elnyelő-képesség | 0,053 g/g | 0,178 g/g |
| • Cián-hidrogén elnyelő-képesség | 0,028 g/g | 0,27 g/g |

A táblázat adatai azt mutatják, hogy az új mikrohullámú eljárással előállított Sovecarbon minőségi mutatói hasonlóak a Pleisch-NBC szénéhez.

## Felhasznált irodalom

[1] Bucsky Gy. Halász L, Solymosi J. Ujhidy A., Vass A., Vincze Á:
Eljárás és berendezés adszorbensek mikrohullámmal kombinált nedves impregnálására.
P0401518 sz. Szabadalmi bejelentés, 2004.

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Hanák Tibor**
**LSI Informatikai Oktatóközpont Alapítvány**
hanak@lsi.hu

# KATASZTRÓFAJELENTÉSI RENDSZEREK

***Absztrakt***

*A szerző cikkében bemutatja a különböző kommunikációs lehetőségeket a katasztrófák kezelése során. Első lépésként a tájékoztatási, illetve a válságmegoldással megbízottak kommunikációját tárgyalja, majd a különböző katasztrófák felosztására tér át. Ezután a védelmi igazgatás rendszerét elemzi. Az áttekintések után, a korábban használt kommunikációs rendszereket mutatja be röviden Az analóg technika után, a jelenleg használt digitális rádiórendszert a TETRA -t ismerteti részletesen. Végül a központhálózat, és a jelenleg kiépített rendszer rövid bemutatásával és értékelésével, illetve a teljes földi kommunikációs infrastruktúra összeomlása esetén alkalmazható megoldással foglalkozik.*

*This article introduces the possibility of communication in case of disaster.*
*Firs of all, the author introduces the communication of the information and the crisis management, than he shows different disaster partition analyzing the defensive administration. The paper shortly introduces some previous communication system from the analog technology to the up to date TETRA digital radio system. At the end of the paper the author focused on central grid and presently used system or rather the crash of the whole territorial communication infrastructure in case adaptable result.*

***Kulcsszavak:*** *tájékoztatási kommunikáció, krízisterv, készenléti kommunikációs rendszerek, EDR rendszer ~ disclosure communication, crisis plan, emergency communication systems, Hungarian TETRA system*

## A tájékoztatási kommunikáció

A katasztrófa, illetve a krízis kommunikáció meghatározó szerepű a válságidőszak kezelésében. A kis területű, illetve kiterjedtebb események következtében előforduló válságmegoldásban a lakosság, és a közelben tartózkodók tájékoztatása, és a válságkezelők megfelelő kommunikációja meghatározó jelentőségű.

Mindenképpen el kell választani a katasztrófa helyzetekben, a tájékoztatás és a katasztrófa felszámolásával megbízottak kommunikációját.

A tájékoztatás, a hatékony kommunikáció, az előzetes felkészülésen alapszik, tehát előzetes tervet kell rá készíteni, meg kell határozni ki, milyen területen, milyen mélységben nyilatkozhat, illetve mit nem szabad elmondania, a felesleges pánikkeltés elkerülése érdekében. Marlin Fitzwater, a Fehér Ház egykori sajtó titkára szerint: "A jó kríziskommunikáció egy eleve jól működő rendszeren alapszik. Ha krízis van, csak gördülékenyebbé és jobbá kell tenni. A krízis közben nem lehet egy új rendszert megformálni."

A krízistervet két fázisban kell létrehozni:

- Első fázis: Előtervezés. Ismerni kell a szervezetet veszélyeztethető tényezőket, a rizikókat.
- Második fázis: A krízis felbecsülése és enyhítése. Ehhez létre kell hozni a krízist lemenedzselő csoportot.
  - első szerep: a kárbecslők, nekik tisztán kell látniuk, hogy melyik krízisnek milyen hatásfoka lenne a szervezetre nézve
  - második szerep: a szervezetet vezetők egy csoportjának az a fő feladata, hogy tudomásul vegyék a kárbecslők visszajelzéseit, és meghozzák a fontos döntéseket
  - harmadik szerep: a belső, illetve a külső kommunikációt lebonyolító személyek [1]

A krízistervből is látszik, hogy a kommunikáció tervezése meghatározó jelentőségű. A hatékony és helyesen menedzselt kommunikáció azt sugallja, hogy a megbízott szervezet kézben tartja a helyzetet, megnyugtatóan képes azt megoldani. Ez mindenkinek az érdeke.

## A válságmegoldással megbízottak kommunikációja

A kommunikáció egyik legfontosabb területe a katasztrófahelyzetek megelőzésével, felszámolásával megbízottak kommunikációja. Ez a tevékenység napjainkban mobil egységek közötti kommunikációt jelent, természetesen nem kizárólag, de meghatározó mértékben.

A mobil kommunikációs eszközök használata hazánkban teljesen megszokott, a mindennapi életünk részévé vált. Az általános felhasználásuk, magán, üzleti, szolgálati célból mindenki számára elérhető, biztosított, nagyban megkönnyíti tevékenységét. Ezen gondolatok alapján könnyen belátható, hogy a mobil kommunikáció megléte és biztonságos, folyamatos működtetése alapkövetelmény mindennapi életünkben.

Magánfelhasználás esetén, a mobilszolgáltatás kimaradása egyéni problémákat okoz, például, családi, üzleti kommunikációs kieséseket. Ezek a problémák ugyan az egyén, vagy kisebb csoport számára nagy jelentősséggel bírhatnak, de komoly katasztrófákhoz, akár életveszélyes helyzetekhez általában nem vezetnek. Ezzel szemben, ha a készenléti szervek kommunikációjában történik kimaradás, vagy hosszabb leállás, beláthatatlan események sorozatához is vezethet. Példaképp említhetünk egy vasúti balesetet, ahol a mentéssel, a kárelhárítással, irányítással megbízott egységek nem tudnak egymással kommunikálni.

Mint lehetséges katasztrófahelyzetbeli kommunikációs megoldás, felmerül a polgári mobiltelefon hálózat használata is, ami egy megoldásnak megfelelő, és ha nem túlterhelt a hálózat, működőképes is. Viszont előfordulhatnak ennek kapcsán nagyon fontos problémák is, például ha a hálózat túlzsúfolt nem jön létre kapcsolás, egy helyi átjátszó torony valamilyen technikai okból történő meghibásodása az adás megszűnéséhez vezethet. A mobiltelefon hálózat kormányutasításra kikapcsolható, ha nemzetbiztonság érdeke úgy kívánja. Ezekben a helyzetekben a kommunikáció nem csak az egyéni felhasználóknak szünetel, hanem a készenléti szerveknek is.

A vezetési és irányítási funkciók megvalósíthatósága, illetve az információk megfelelő helyen és időben történő felhasználása a területi tevékenységek végrehajtása közben, döntően befolyásolhatja az eredményességet. Egy esetleges katasztrófánál, balesetnél, nagyobb tűzesetnél vagy árvíz idején emberek tömegének élete múlhat azon, hogy a készenléti szervek közötti kommunikáció mennyire hatékony.

A folyamatos fejlesztés alapvető követelmény, mivel a kihívások változása, a kockázati tényezők bonyolultsága megköveteli ezt, az állampolgárok azonos szintű védelmének biztosítása érdekében. Ugyanakkor figyelembe kell azt is venni, hogy katasztrófák nem állnak meg a határoknál, ezért jelentős mértékben felértékelődött a nemzetközi tapasztalatcsere és a segítségnyújtási tevékenység az országokkal, a régiókkal és a nemzetközi szervezetekkel történő együttműködésen belül. Az elmúlt évtized talán legfontosabb változása ez utóbbi megállapítás, amely az országunkon belüli felelősségeink mellett nemzetközi elkötelezettséget jelent az együttműködésre és a segítségnyújtásra, ugyanakkor a kölcsönösség alapján számíthatunk is erre.[2]

## A katasztrófák

A természeti és a civilizációs katasztrófák jellemzője, hogy nagy embertömegeket és nagy területeket érinthetnek.

Katasztrófahelyzet több módon alakulhat ki:

- természeti események következtében,
- termeléssel, üzemeltetéssel összefüggésben,
- szabotázs, vagy háborús cselekmény hatására.

A katasztrófák közös jellemzőjeként elmondható, hogy kárterületek keletkeznek, amelyek gyakran összefüggenek egymással. A katasztrófák lokalizálása, következményeinek felszámolása csak korszerű műszaki és egyéb technikával felszerelt, jól szervezett és kiképzett, mozgékony, különböző szakmai felkészültségű erők azonnali és szükség esetén, tömeges bevetésével lehetséges. Kiemelt szerepe van az összehangolt, hozzáértő és gyors irányító tevékenységnek.

## A védelmi igazgatás rendszere

A védelem kialakításának, és szervezésének feladatát a közigazgatási rendszer fogja át országos szinten.

A közigazgatás szervezetrendszere az ország fegyveres és nem fegyveres védelmét biztosító honvédelmi rendszer elemeként meghatározó szerepet tölt be. Az államvezetés e területe az ország védelemmel kapcsolatos rendkívüli időszakokban centrális irányítású, hierarchikus felépítésű rendszerben működik és az ország védelemmel kapcsolatos irányító, végrehajtó feladatait a védelmi felkészítés időszakában kialakított és begyakorolt eljárásmódok alkalmazásával, a jogszabályokban és az állami irányítás egyéb jogi eszközeiben felhatalmazott rendkívüli jogalkalmazási tevékenységével biztosítja.[3]

A védelmi igazgatás szervezete átfogja az állam normál (béke) időszakát veszélyeztető valamennyi helyzetet. A veszélyhelyzeteket megelőzi a felkészülés időszaka, míg a veszély kezelése a hatáskörrel rendelkező szervek azonnali, hatékony és szervezett beavatkozását igényli.

A védelmi igazgatás szervezetrendszerébe az általános hatáskörű, valamint a szakigazgatási feladatokat ellátó állami szervek tartoznak. Általános hatáskörű szervek csoportjába tartoznak a védelmi igazgatás központi (az Országgyűlés, a Honvédelmi Tanács, a Köztársasági Elnök, a Kormány, a minisztériumok és országos hatáskörű szervek), területi (megyei, fővárosi védelmi bizottságok, helyi védelmi bizottságok) valamint települési (polgármester, jegyző)

szervei. Alapvető feladatuk, hogy centrális irányítási rendszerben biztosítsák a fegyveres erők, rendvédelmi szervek és a védelemben részt vevő állami és nem állami szervek, továbbá az önkormányzati szervek és a lakosság felkészítését, mozgósítását a védelmi feladatok érdekében. A védelmi igazgatás szakigazgatás szervei közé tartoznak az ország védelem sajátos feladatait ellátó katonai igazgatás szervei, valamint a polgári lakosság oltalmazását és az anyagi javak védelmét, mentését végző polgári védelmi szervek. A védelmi igazgatás általános, illetve szakigazgatási szervein túl bevonásra kerülnek a rendvédelmi és polgári szervek is.
A bekövetkező katasztrófák, bármelyike esetén szükség van egy megfelelő kommunikációs rendszerre, amely képes a katasztrófa védelemmel, elhárítással megbízott szervezetek közötti adatátvitel lebonyolítására.

## A kommunikációs lehetőségek

A korábban használt rádiórendszerekről néhány jellemző, a teljesség igénye nélkül, figyelembe véve, hogy ezek lecserélése 2007. februárjában megtörtént a később ismertetendő TETRA[1] - EDR[2] rendszerre:

- A rendőrségi rádiórendszer
  A rendőrség alapvetően a felhasználás módját tekintve osztotta fel rendszereit, úgymint: ügyeleti és mozgószolgálati, szimplex, valamint egyéb rendszerek.
  Alapvetően a rádiórendszerek nyíltak, így az MRKB I. és MRKB II. kivételével beszédfedő vagy titkosító eszköz nincs alkalmazásban, ami azt jelenti, hogy a kereskedelmi forgalomba kapható URH rádiókészülékekkel ezen adások foghatók, illetve véletlenül vagy szándékosan lehallgathatók.
- Tűzoltósági rádiórendszer:
  A megyei ügyeletek az önkormányzati tűzoltó parancsnokságokkal csak a 150 MHz sávban képzett szimplex csatornán keresztül álltak összeköttetésben, valamint ebben a tartományban forgalmaztak a vonuló egységek is. A TOP megyénként egy-egy üzemi szimplex csatorna mellé 2 db csatornát tartalékolt a rendelkezésére álló 12 db frekvenciából.
- A határőrizeti rádiórendszer
  A határőrségnél alkalmazott rádiókommunikáció alapvetően az országhatár mentén telepített 76 db bázisállomásra épült. Műszaki megoldását tekintve a rendőrségi ügyeleti és mozgószolgálati rádiórendszertől csak annyiban tér el, hogy alkalmazása során 2 db rádiócsatorna felhasználásra van lehetőség. Egy bázisállomás általában két határőrizeti kirendeltség működési körzetét sugározta be oly módon, hogy azon keresztül a köz- és zártcélú (vezetékes) távközlő hálózatok is elérhetők szükség esetén.
- A mentőszolgálat rádiórendszere
  A mentés irányításban, a fővárosban és a megyei mentőszervezeteknél félduplex rendszer üzemelt. A Budapesten elkülönített csatornákon folyt az úgynevezett szállítási feladatok és a sürgősségi feladatok irányítása. A megyeszékhelyeken általában egy csatornán folyt mindkét feladattal kapcsolatos forgalmazás. Az ottani, aránylag kevés esetek számából adódóan torlódást ez nem okozott. A félduplex üzemnek köszönhetően minden olyan állomás, ami az átjátszó besugárzási területén belül van, hallja a közleményeket. Ennek akkor van nagy jelentősége, ha az adott

[1] TETRA (TErrestrial Trunked RAdió – földfelszíni trönkölt rádió) a digitális, földi mobil rádiótávközlés új generációjának egyezményes szabványa.
[2] EDR (egységes digitális rádió-távközlő rendszer) A TETRA rendszer magyar elnevezése

területen tömeges baleset történik, a mentőegységek rögtön a mentéssel kapcsolatos forgalmazásba be tudnak kapcsolódni.[4]

- Az Országos Katasztrófavédelmi Főigazgatóság rádiórendszere

  A katasztrófák elleni védekezés központi irányítását az Országos Katasztrófavédelmi Főigazgatóság látja el. Az ő bázisukon található a Veszélyhelyzet Kezelési Központ, az ügyeleti rendszer, és ennek infrastruktúrája. Hierarchikus felépítésük piramis jellegű, átszervezhető, módosítható. Az alsó szintű struktúra, a városi átjátszók, és központok, 300 MHz-es sávban üzemeltek, 4 telefonbekötési ponttal. Az átjátszókat egy BGY 9000-es vezérlő vezérli. A rendszer áramkimaradás ellen is védett, képes a társszervekkel együttműködni, de önmagában is használható. A következő szint a megyei rádiós hírrendszer, amely egy BGY 9500-as digitális automatikára épül, amely képes független rádióhálók összekapcsolására, és trönkölésre is. Ezekbe a központokba már 10 rádiócsatorna, és 5 telefonvonal köthető be. A beszélgetések egyes adatait naplózza, és 40 napig megőrzi. A rendszer csúcsán az országos központ áll, Budapesten, egy számítógépes központból és 300 MHz –en bekötött országos átjátszókból áll.[5]

  A katasztrófavédelem, hat híradó rendszerrel rendelkezik, ezek:

  1. Egységes Digitális Rádiórendszer
  2. Dunai Információs Segélyhívó Rendszer
  3. Tiszai Információs Segélyhívó Rendszer
  4. Balatoni és Velencei-tavi Viharjelző rendszer
  5. Lakossági riasztó és tájékoztató rendszerek
  6. Monitoring és Lakossági Riasztó Rendszer

  Az OKF rendszeri kapcsolhatók az Egységes Kormányzati Gerinchálózatra, ezen keresztül lehetőség van gyors és biztonságos kapcsolattartásra. A Katasztrófavédelmi Országos Információs Rendszer lehetővé teszi a főigazgatóság és a területi szervek munkaállomásainak kapcsolatát, az adatbázisok elérését. A Központi Ügyeleti Információs Rendszer lehetőséget teremt az elektronikus kapcsolattartásra, adatszolgáltatásra, és a beavatkozások esetén a pontos tevékenységek összehangolására.[6]

  A katasztrófavédelem egyik lényeges eleme a pontos helymeghatározás. Jelenleg ma Magyarországon ez idáig nem megoldott a katasztrófavédelem témakörében, ezen belül is a veszélyes anyagokat előállító, raktározó veszélyes üzemekre vonatkoztatottan egy az egész országra kiterjedő olyan térinformációs rendszer működtetése, mely nemcsak egyszerű térképalapú, helyhez kötött, adatok leíró jellegű tulajdonságadatait jeleníti meg egy adatbázisból a kisméretarányú térképeken, hanem széleskörű elemzéseket lehetővé tesz az egyes üzemek nagyméretarányú céltérképeinek szintjén.[7] A Katasztrófavédelem rövid távú céljai között szerepel, ennek megoldása, központi adattár feltöltése, térképfrissítések, és szakemberek képzése.

  Az Országos Katasztrófavédelmi Főigazgatóság azzal hogy egyes esetekben, a katasztrófák kezelése során önkéntes, és létesítményi tűzoltóságok, valamint a speciális feladatokat ellátó civil mentőszervezetek munkáját is igénybe veszi egyedi helyzetbe került a TETRA rendszer alkalmazásával. Ennek oka, hogy a digitális rendszer beüzemelése után az analóg frekvenciák visszavonásra kerülnek. Ezáltal az említett szervezetekkel megszűnik a korábbi rádiós kapcsolat. Tehát biztosítani kell, az EDR nem EDR felhasználók közötti összeköttetést.[8]

Az ismertetett analóg rendszereket Magyarországon felváltotta a TETRA rendszer, amely digitális, és titkosított, de elsősorban általánosan használható minden készenléti szerven belül, illetve szervezetek között, valamint kapcsolódik az egyéb kommunikációs hálózatokhoz is.

## A digitális[3] rádiórendszer

Az 1990-es évek korlátozott jellegű hazai fejlesztési munkálatait befolyásolta, hogy a nyugat európai országokban üzemeltett rádiórendszerekben, már a nyolcvanas évek végén jelentkezett a forgalmi zsúfoltság, illetve a frekvenciakijelölés problémája. A probléma megoldása érdekében kiadásra került műszaki ajánlások értelmében a hatékonyság növelését a digitális, trönkölt rendszerek keretén belül célszerű megoldani, így az évtized közepén megkezdődött az időosztásos többszörös hozzáférés technológián alapuló TETRA szabványok kidolgozása.
A készenléti szervek rendszer elvárásai

- Technikai elvárások:
  közvetlen üzemmód: lehetővé teszi az állomások számára, hogy szimplex üzemmódban, minden infrastruktúra nélkül kommunikáljanak.
  relézett üzemmód: ebben az esetben az állomások egyetlen hordozható csatornaismétlőn keresztül kommunikálnak.
  azonos idejű kisugárzás (simulcast): igen jó megoldást kínál a spektrumhatékonyság szempontjából egyes vidéki körzetekben ahol a felhasználó sűrűség nagyon csekély és a nyitott csatornák gyakran több adáshelyet szolgálnak ki.
- Üzemeltetési elvárások:
  A készenléti szolgálatok esetében az üzemi rendelkezésre állásnak kiemelkedően magas szintűnek kell lennie, mivel a hálózatokat a nap 24 órájában, az év 365 napján megszakítás nélkül üzemeltetik.
- Biztonsági követelmények:
  A rendszerek biztonsági követelményei rendkívül széleskörűek, melyek kiterjednek a jogosultság megállapítás, rendelkezésre állás, biztonságot érvényesítő funkciók, adatkezelés területeire. A biztonsággal kapcsolatos területek többsége a védelem fokozása érdekében nem írható le nyilvános szabványban, ugyanakkor a rögzítésnél a közcélú hálózatok jellemzőit is igénylik. Ilyen terület például a titkosítás, mely többek között a határőrség és rendőrség esetében végponttól-végpontig kell, hogy megvalósuljon, szemben a hagyományos, polgári felhasználás elvárásaival.
- Összefoglalva:
  Az elvárásokat és követelményeket összegezve az újonnan létesítendő kommunikációs hálózatoknak az alábbi fő tulajdonságokkal kell rendelkezniük:
    1. jó rádióellátottság
    2. adattovábbítási lehetőség
    3. könnyen ki- és átalakítható csoportkonfiguráció
    4. a rádiócsatornákhoz történő gyors hozzáférés
    5. közvetlen üzemmódú működés
    6. az infrastruktúra gyors telepíthetősége és felszerelhetősége
    7. biztonságos üzemeltetés.

[3] A "digitális" szót leggyakrabban a számítástechnika és az elektronika területén használják, különösen azokon a területeken, ahol a való világ információit konvertálják át bináris számokká. Ilyenek például a digitális hang(zás) és a digitális fényképezés. A digitális adat-átvivő jelek az elektronikus, vagy optikai impulzus két lehetséges értéke közül az egyiket vehetik fel. A logikai 1 (van impulzus) vagy 0 (nincs impulzus) értékeket.

Az előzőekben meghatározott feladatra a TETRA rendszert választották ki Magyarországon, hasonlóan több más európai államhoz. A megnevezése nálunk EDR, Egységes Digitális Rádió lett.
A TETRA rendszerek alapvető jellemzője, hogy egy közös távközlési infrastruktúrát több felhasználói szervezet használ. Mind a polgári, mind a készenléti rendszerek esetében fontos az, hogy ezek a szervezetek kommunikációjukat egymás zavarása nélkül, sőt, egymástól biztonságosan elkülönítve tudják lebonyolítani. Ezt az elkülönítést teszik lehetővé a virtuális magánhálózatok (Virtual Private Network, VPN).

- A virtuális magánhálózat
  Egy adott virtuális magánhálózat felhasználói úgy érzékelik, hogy a teljes hálózati infrastruktúra az ő rendelkezésükre áll.
  A TETRA rendszerben a VPN-ek rendkívül rugalmasan, akár a tényleges felhasználó szervezetek struktúrájának leképezésével is létrehozhatók. Bármely VPN rendelkezhet saját adminisztrátorral, előfizetői számtartománnyal, IP cím tartománnyal, vezetékes alközponti kapcsolattal, stb., de több VPN akár közösen is adminisztrálható. Az egyes szervezetekhez tartozó rádió felhasználók alapesetben saját virtuális magánhálózatukon belül forgalmaznak, de természetesen jogosultság adható nekik más VPN-ek, illetve nyilvános vagy alközponti telefonhálózatokkal történő kommunikációra is.
- A beszédkommunikáció
  A beszédkommunikáció TETRA rendszerek egyik fő szolgáltatása. A hívásban résztvevők számától függően beszélhetünk csoport- (pont-többpont), vagy egyéni (pont-pont) hívásokról.
  A TETRA rendszer fontos tulajdonsága a rendkívül gyors (300 ms-nál is rövidebb idejű) hívásfelépítés, amely valamennyi hálózaton belüli hívás esetében igaz. A gyakorlatban a felhasználók ezt a kapcsolat azonnali létrejötteként érzékelik, ami csoporthívások esetében természetes követelmény, egyéni hívások esetében viszont számottevő előny a hagyományos hálózatokban megszokott kapcsolási időkhöz képest, különösen készenléti, közbiztonsági alkalmazások esetében.
- A csoporthívások
  Azok a szervezetek, amelyeknek tagjai munkájukat egy diszpécser irányítása alapján végzik, a kommunikációjukat döntően csoporthívások segítségével bonyolítják le. A csoporthívást a csoport bármely tagja kezdeményezheti, de egyszerre csak egy tag beszélhet, amit a csoport valamennyi tagja vesz.
- Beszédváltó
  A beszédcsoportokat az adott szervezethez (azaz virtuális magánhálózathoz) tartozó rádió felhasználók operatív felügyeletét ellátó adminisztrátor vagy diszpécser állítja össze. Egy felhasználó tagja lehet több csoportnak is. Azt a beszédcsoportot, amelyben éppen forgalmazni kíván, a rádiókészülékén választja ki.
- A diszpécser lehetőségei a beszédkommunikáció mellett
  A diszpécser a beszédcsoport tagjaként nemcsak a beszédkommunikációban vehet részt. Számítógépes diszpécser munkaállomáson folyamatosan figyelemmel követheti az általa felügyelt csoport tagjainak helyzetét, azt, hogy éppen egyéni hívást bonyolítanak le, vagy egy másik csoport forgalmában vesznek részt, de akár üzeneteket küldhet nekik és fogadhat tőlük. A megfelelő jogosultságokkal rendelkező diszpécser kezelheti a felügyelt beszédcsoportokhoz, illetve rádió felhasználókhoz tartozó paramétereket, azaz pl. a csoporthoz tagokat adhat, vagy onnan törölhet, állíthatja az egyedi felhasználók jogosultságait, stb.
- A beszédcsoportok összevonása

Alapesetben a kommunikáció a beszédcsoportokon belül zajlik, de előfordulhatnak olyan esetek is (pl. egy súlyos közúti vagy ipari baleset), amikor több, akár más-más felhasználói szervezethez (azaz VPN-hez; pl. rendőr, mentő, tűzoltó) tartozó csoportnak kell egymással kommunikálnia. Ilyen helyzetben a megfelelő jogosultságokkal rendelkező diszpécser a különböző csoportokhoz tartozó felhasználókat a dinamikus csoport hozzárendelés szolgáltatás segítségével, egy közös beszédcsoportba vonhatja össze.

- A közvetlen összeköttetés
  Amennyiben a beszédcsoport tagjai a hálózat lefedettségi területén kívül (pl. egy barlangban, stb.) tartózkodnak, közvetlen rádiókapcsolat (Direct Mode Operation, DMO) segítségével továbbra is tudnak egymással beszélni. Ilyenkor a készülékekbe kifejezetten erre a célra programozott frekvencián és csoportparaméterekkel folyik a forgalom. DMO üzemben a rádiók hatótávolsága tipikusan néhány száz métertől néhány kilométerig terjed, attól függően, hogy nyílt vagy zárt térben, milyen tagoltságú terepen, stb. használják őket.
  Léteznek olyan rádiók is, amelyek egy időben képesek hálózati és közvetlen összeköttetésre is. Ha ezek a rádiók mind a lefedetlen területen lévő más készülékek, mind a TETRA hálózat hatósugarában vannak, képesek a közvetlen összeköttetést használó rádiókat átjátszóként a hálózati forgalomba is bekapcsolni.
- Az egyéni hívások
  A TETRA rendszerben az egyéni hívások a más vezeték nélküli hálózatokban (pl. GSM) megszokott módon áll a felhasználók rendelkezésére.
- Az azonnali hívások
  A TETRA rendszer lehetővé teszi az úgynevezett azonnali (instant vagy expressz) hívásokat is. Ilyenkor a hívott fél (aki ebben az esetben csak egy másik TETRA felhasználó lehet) számának beütése után a hívó a beszédváltó gomb megnyomásával indítja a hívást. A hívott előfizetőnek nem kell a hívást fogadnia, a kapcsolat azonnal kiépül. A hívást ezután már bármelyik fél befejezheti a hívásmegszakító gomb megnyomásával.
- A duplex és fél duplex hívások
  A hagyományos telefonhálózatokban megszokott beszélgetések teljes duplex módon történnek: mindkét fél egyszerre beszélhet és hallgathatja is a másikat.
  Maga a TETRA infrastruktúra támogatja ezt a fajta kommunikációt, de előfordulhat, hogy egyes rádióterminálok egyéni hívásnál is csak a csoporthívásoknál szokásos fél duplex üzemmódban képesek működni. Ekkor a hívás indítása és fogadása a már leírt módon történik, de a beszélgetésnek egyszerre csak az egyik résztvevője beszélhet, az, amelyik a beszédváltó gombot éppen nyomva tartja.
- Az áramköri csoportok
  A TETRA rendszerben a más hálózatok felé irányuló, illetve onnan fogadott hívások kezelésében fontos szerepe van az úgynevezett áramköri csoportoknak. Egy-egy áramköri csoport tetszőleges számú, a társszolgáltatói vagy alközponti hálózatokhoz kapcsolódó fizikai interfészt fog össze
- A Rövid adatszolgáltatás
  A TETRA szabvány az adatalapú alkalmazások támogatására háromféle megoldást kínál: vonal-, illetve csomagkapcsolt adatátvitelt, valamint az úgynevezett rövid adatszolgáltatást (Short Data Service, SDS).
  A TETRA hálózatok rövid adat szolgáltatása műszaki megvalósítását tekintve hasonlít a GSM rendszerek SMS szolgáltatásához, de annál sokrétűbben használható.
- A jelátvitel kódolása és technikája

A TETRA digitális rádiórendszer, ami azt jelenti, hogy a továbbítandó beszéd-, jelzés-, és adatforgalom digitalizált formában kerül továbbításra a rádiócsatornán. A digitális rádióinterfész teszi lehetővé, hogy egy időben négy TETRA felhasználó forgalmazhasson ugyanazon a frekvencián, szélsőséges rádiós körülmények között is elfogadható hangminőséggel.
A TETRA rendszerben a digitalizált hangot ACELP (Algebraic Code-excited Linear Prediction) beszédkódoló áramkör kódolja, és nagymértékben tömöríti. A kódolás után az eredetileg kb. 104 kb/s hanginformációból 4,567 kb/s lesz. További előny, hogy mivel a kódoló emberi beszédre optimalizált, ezért háttérzajt és más, a kommunikációt zavaró hangokat nem visz át, így a TETRA rendkívül jól használható beszédkommunikációra még nagyon zajos környezetben is.

- A hálózat felügyelete és üzemeltetése
  A TETRA hálózatok üzemeltetése logikailag két részre bontható: a hálózati infrastruktúra műszaki üzemeltetésére, illetve az operatív felügyeletre, a felhasználói szervezetek, felhasználók, beszédcsoportok, és az ezekhez kapcsolódó jogosultságok adminisztrálására. Biztonsági megfontolásokból azonban szükséges, hogy ez a két funkció fizikailag is elkülönüljön egymástól. Kivételt képezhetnek ez alól az egy, vagy nagyon kevés felhasználó szervezetet kiszolgáló helyi TETRA hálózatok, ahol előfordulhat, hogy a rendszer konfigurálásához, felügyeletéhez szükséges eszközöket integrálják a diszpécserállomással.
  Magyarországon a NOKIA berendezési kerültek alkalmazásra, illetve a NOKIA ezen üzletágát, 2006. nyarán az EADS megvásárolta, és a továbbiakban a szállítást folytatta. A tulajdonos változás nem járt a szállítandó központok, mobil egységek változtatásával.
- A mobil egységek
  A közbeszerzési kiírásnak megfelelően az első időszakban szállított berendezések a NOKIA termékei. A Nokián kívül még számos gyártó foglalkozik a TETRA hálózatban használható készülékek gyártásával, ilyenek pl.: EADS, Motorola, Sepura, Selex Communacations (OTE), Cleartone Communication Systems, Teltronic, DeTeWe, Niros, amelyek a későbbiekben szintén, mint készülék beszállítók jöhetnek szóba, mivel a kiírt tender a rendszer beüzemelése után nem írja elő a felhasználó szervezeteknek, hogy kitől, illetve milyen gyártmányú készülékek szerezhetők be.[9]

A hálózat mindaddig jól használható, amíg a központok és az átjátszók működőképesek. Általánosan elmondható, hogy egy korszerű, minden tekintetben bővíthető rendszerről van szó.

## A hálózat kiépítése

Magyarországon a központhálózat négy központból és 227 bázisállomásból áll. Az országos lefedettséget alapvetően ezek biztosítják, de 5 mobil bázisállomás beiktatásával lehetőség van a nagyobb rendezvényeken a kapacitás átmeneti növelésére, és a hagyományos módon nehezen lefedhető területeken is működő zavartalan kommunikációra katasztrófa esetén, a készenléti szervek számára. A magyar rendszer 42 ezer készülék kezelésére alkalmas. Ennek eredményeként 11 készenléti szerv tudott bekapcsolódni a TETRA technológiájú hálózatba. A rendszer országos kiépítésével Európa egyik legkorszerűbb és létszámarányában legkiterjedtebb készenléti rádiórendszere valósult meg.

A világon hozzávetőlegesen 650 helyen működik TETRA rendszer, de csak nálunk történt meg ezidáig, az összes készenléti szerv bevonása a rendszerbe. Mivel a rádiórendszer szabványa európai uniós ajánlás, így alkalmas arra, hogy a schengeni egyezményhez tartozó országok rendvédelmi szerveinek együttműködését is támogassa. A TETRA technológiájú

rádiókommunikációs rendszer számos előnye mutatkozik meg a régi, analóg rendszerrel szemben. A TETRA szabvány szerint épült EDR jelentősen javítja az érintett szervek belső híradását, lehetővé teszi a szervek egymás közötti hatékony kommunikációját. [10]

## Rendszerértékelés

A magyar hálózat központjai úgynevezett szövevényes rendszerben vannak kiépítve. Ez a rendszer négy központig lehetséges, e szám felett hierarchikus felépítés szükséges. A magyar központrendszer előnye, hogy mindegyik központ az összes többivel összeköttetésben van, tehát ha az egyikben üzemzavar lép fel, a többi át tudja venni a feladatát.
A TETRA rendszer előnyei az analóg rendszerrel szemben, elsősorban az adatbiztonság, az elérési sebesség, és az egységek közötti közvetlen kapcsolat terén jelentős.

- Az adatbiztonság a titkosítás eredményeképpen végponttól végpontig biztosított.
- Az elérési sebesség a kapcsolási idő rövidsége, illetve a közvetlen hívások terén rendkívül rövid, néhány milliszekundum.
- A különböző szervezetek közötti kapcsolat korábban a diszpécserközpontokon keresztül volt esetlegesen megoldható, a TETRA egyik, a véleményem szerint legjobb tulajdonsága, ezen probléma megoldása.
  A rendszer, folyamatosan konfigurálható, az egyes beszédcsoportokba rendezett felhasználók, egy központi terminál segítségével, más csoportokhoz kapcsolhatók, vagy hozzájuk lehet rendelni más felhasználókat. Ennek eredményeképpen, a különböző készenléti szervezetekhez tartozó felhasználók közvetlenül tudnak egymással kommunikálni, ha az adott feladat ezt megkívánja.

A mobil készülékek a tapasztalatok alapján egy napos használatot újratöltés nélkül kibírnak, minőségük megfelelő. A telepített berendezések, gondolok itt elsősorban a gépjárművekbe szerelt egységekre, műholdas helymeghatározóval felszereltek, ezért a diszpécser nyomon tudja követni az egységek mozgását.
A készülékek képesek bizonyos esetekben átjátszóként is működni, tehát egy készülék, amely lefedettségi területen kívül üzemel, és hatókörén belül van egy másik készülék, amely már hálózaton belül van, képes a hálózati kommunikációra.
Véleményem szerint a készenléti szervek kommunikációja a TETRA rendszer segítségével, nagymértékű fejlődésen ment keresztül.

Az ismertetett rendszerek, képesek kiszolgálni az ország katasztrófák bekövetkezésekor igényelt kommunikációs feladatait, hatékonyan tudnak működni, de, egy közös, hátrányos tulajdonsággal rendelkeznek. Ez az infrastruktúra sérülékenysége. Abban az esetben, ha egy országos, vagy akár még nagyobb katasztrófa következik be, amely a rendszer átjátszó állomásait, központhálózatát lerombolja, vagy használhatatlanná teszi, a kommunikáció minden esetben, hosszabb – rövidebb időre megbénul. Ennek kiküszöbölésére jelenleg egyedül a műholdas kommunikáció képes. Magyarországon jelenleg a Magyar Honvédség rendelkezik bérelt műholdas csatornával, amelyet a külföldi kontingensekkel való kapcsolattartásra használnak.[11] A katasztrófavédelem egy műholdas csatorna segítségével, nagyobb biztonságú kommunikációra lenne képes, hiszen ez esetben, csupán a készülékek, és a mobil berendezések energia ellátásáról kellene gondoskodnia. A megvalósítás akadálya, a költségekben rejlik. A bérelt műholdas csatorna rendkívül költséges, de hosszú távon, érdemes megfontolni ennek alkalmazását, a kommunikáció biztonsága érdekében.

## Irodalomjegyzék:


1. www.continuitycentral.com/feature0397.htm; Letöltés ideje: 2007. 11. 21.
2. www.katasztrofavedelem.hu/tartalom.php?id=1; Letöltés ideje: 2007. 12. 9.
3. Dr. habil. Horváth László: Az országvédelem szervezeti rendszere ZMNE Egyetemi jegyzet Budapest, 2005.
4. Belügyminisztérium ágazati szintű informatikai stratégiája (BM szám: 63-470/99. ); Budapest, 1999.;
5. Dr. Fekete Károly: A magyar köztársaság kommunikációs infrastruktúrája Egyetemi jegyzet ZMNE EKK Nyt. Szám: 952/525
6. Máté József: A katasztrófavédelem 2007. évi főbb projektjei Kommunikáció 2007. konferencia ZMNE 2007. október 17.
7. Kovács Zoltán–Kovács Tibor–Vincze Árpád: Vegyi monitoring és térinformatika Hadtudomány XV. Évf. 2005. junius
8. Máté József: Az EDR rendszer bevezetésének katasztrófavédelmi feladatai, Katasztrófavédelem folyóirat – 2006 június
9. TETRA ( veszélyhelyzeti szolgálatok ) Kormányzati Frekvenciagazdálkodási Hivatal ( szám: 31/1. ); Budapest, 1996.;
10. www.sg.hu/cikkek/50263/elkeszult a tetra rendszer Letöltés ideje: 2007. 12.10.
11. Németh András: Szolgáltatásalapú műholdas hírközlés veszélyhelyzeti felhasználási lehetőségei; Kommunikáció 2007. ZMNE 2007.

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Körmendi Krisztina**
Protan ZRt.
kormendi@dcs.vein.hu

**Solymosi József**
Zrínyi Miklós Nemzetvédelmi Egyetem, egyetemi tanár
solymosi.jozsef@zmne.hu

# A VILLAMOSENERGIA-KRÍZIS KEZELÉS SZABÁLYOZÁSA MAGYARORSZÁGON

***Absztrakt***

*A villamosenergia-rendszer működtetése, villamosenergia-ellátás biztosítása szabályozásának alapja Magyarországon a villamos energiáról szóló 2007. évi LXXXVI. Törvény (Továbbiakban VET). A VET 170. § (1) bekezdésének 23. pontja alapján a Kormány a villamosenergia-rendszer illetve a villamosenergia-ellátás jelentős zavarának minősülő helyzet szabályait, valamint az ilyen helyzet esetén alkalmazandó intézkedések szabályait, továbbá a rendszerhasználók jogait és kötelezettségeit „a villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről" szóló 285/2007. (X. 29.) Kormányrendeletben (Továbbiakban: Rendelet) állapítja meg. A Rendelet előírja a rendszerirányítási tevékenység engedélyese számára az ún. Krízisterv elkészítését, ami részletezi a rendeletben meghatározott intézkedésekre vonatkozó szabályokat. A cikkben áttekintjük a VET és a Rendelet előírásaiban foglalt, villamosenergia-krízissel kapcsolatos alapvető fogalmakat; krízishelyzet kezeléssel kapcsolatos feladatokat, felelősségeket, hatásköröket, a krízishelyzet kezelésében alkalmazandó intézkedéseket, eszközöket és lehetőségeket.*

*The legislation for the power system and supply in Hungary is based on the LXXXVI. act of 2007. about the Electricity (hereafter: The Electricity Act). With the authorization of the Electricity Act the Government established the statutory order No. 285/2007 (hereafter: The Order), which contains the criteria of large scale failures situations affects the reliability of the electricity system or the continuity of the electricity supply, the actions should take if such situation occures, as well as the rights and responsibilities of the system users. The Order prescribes for the System Operator to create a „Crisis Management Plan", which specifies the rules of procedures for the necessary actions defined in the Order.*

*This article outlines the basic concepts regarding to electricity-crisis, the main tasks, roles and responsibilities in crisis management, necessary actions, tools and possibilities to manage crisis, based on the prescriptions of the Electricity Act and the Order.*

***Kulcsszavak**: villamosenergia-rendszer, villamosenergia-ellátás, villamosenergia-krízis, villamosenergia-krízis kezelés, Krízisterv ~ power system, electricity supply, electricity crisis, electricity crisis management, Crisis Management Plan*

# BEVEZETÉS

Ebben a rövid közleményben áttekintjük a villamosenergia-krízissel kapcsolatos alapvető fogalmakat, a krízis esetén teendő intézkedések hazai szabályozásának a rendszerét, a kríziskezeléssel kapcsolatos feladat és hatásköröket, valamint a krízis megelőzését és következményeinek enyhitését célzó intézkedéseket. A szabályozási rendszer összefoglaló bemutatásán túl e helyen nem térünk ki annak a más államok szabályozó rendszereivel történő összehasonlító vizsgálatára, sem a megtörtént események, illetve a rendszer gyakorlatok alapján szerzett tapasztalatok értékelésére, és a rendszer esetleg célszerűnek mutatkozó, korszerűsítési lehetőségeinek az értékelő elemzésére.

# A SZABÁLYOZÁS RENDSZERE

Magyarországon a villamos energiáról szóló 2007. évi LXXXVI. Törvény (Továbbiakban VET) határozza meg a villamos energiával, villamosenergia-rendszerrel, villamosenergia-ellátással kapcsolatos alapvető jogosultságokat és kötelezettségeket.

A VET 170. § (1) bekezdésének 23. pontja alapján a kormány a villamosenergia-rendszer illetve villamosenergia-ellátás jelentős zavarának minősülő helyzet szabályait, valamint az ilyen helyzet esetén alkalmazandó intézkedések szabályait, továbbá a rendszerhasználók jogait és kötelezettségeit kormányrendeletben állapítja meg.[1]

Ez a kormányrendelet a villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről szóló 285/2007. (X. 29.) Kormányrendelet (Továbbiakban: Rendelet).

E rendelet vezeti be, a jelentős zavar, a válsághelyzet veszélye, valamint a válsághelyzet (együttesen villamosenergia-krízis) fogalmát, határozza meg azon kritériumokat, mely alapján egy esetlegesen kialakuló helyzet jelentős zavarnak, válsághelyzet veszélyének vagy válsághelyzetnek minősül. A Rendelet továbbá meghatározza az alapvető feladatokat, felelősségi és hatásköröket a villamosenergia-krízis megelőzése és következményeinek enyhítése tekintetében. [2]

A Rendelet előírja a rendszerirányítási tevékenység engedélyese számára az ún. Krízisterv elkészítését, melyet a Magyar Energia Hivatal (továbbiakban: Hivatal) hagy jóvá.

Az EU irányelveknek való megfelelés érdekében a villamosenergia-szektort érintő változások (teljes piacnyitás, közüzem megszűnése stb.) következtében az új modellre vonatkozó új VET 2008.01.01-ével lépett hatályba. A változásoknak megfelelően a korábbi

azonos című 281/2002. Kormányrendeletet a 285/2007. Kormányrendelet váltotta fel szintén 2008.01.01. hatállyal. A cikk készítésekor a Hivatal 90/2005 számú határozatával jóváhagyott Krízisterv hatályos.

## VILLAMOSENERGIA-KRÍZIS FOGALMA

A Rendelet által használt fogalomértelmezésben a villamosenergia-krízis fogalomkörébe tartozik, így a Rendelet előírásai alkalmazandók a villamosenergia-rendszer jelentős zavara (továbbiakban jelentős zavar), villamosenergia-ellátási válsághelyzet veszélye I. és II. fokozat (továbbiakban válsághelyzet veszélye) valamint villamosenergia-ellátási válsághelyzet (továbbiakban: válsághelyzet) esetén. [2]

A VET 138. § (1) bekezdése szerint: *"A **villamosenergia-rendszer jelentős zavará**nak minősül 139. §. –ban meghatározott, a villamosenergia-ellátási válsághelyzetet el nem érő mértékű **üzemi hiba**, amelynek során a villamosenergia-rendszer erőműveiben vagy közcélú hálózatain olyan, **a villamosenergia-ellátási szabályzatokban meghatározott esemény** következik be, amely a villamos energia **termelését, termelési készségét, átvitelét, elosztását, szolgáltatását vagy felhasználását jelentősen korlátozza vagy megszünteti**, illetőleg a villamosenergia-rendszer **üzembiztonságát, szabályozhatóságát vagy együttműködő képességét súlyosan veszélyezteti**." [1]*

A Rendelet 16.§ (1) pontja szerint: *"A **válsághelyzet veszélye I. fokozat**ának minősül, ha a folyamatos villamosenergia-ellátást veszélyeztető olyan **tartós erőművi és import teljesítményhiány** jelentkezik, amikor a villamosenergia-rendszer **erőművi tartaléka**[1] 10%-ra csökken; vagy országos szinten a **tüzelőanyag-készlet** olyan mértékben **csökken**, hogy a **villamosenergia-ellátás folyamatossága** 3 napon belül **veszélybe kerülhet** a villamos energia **forrásoldal és a fogyasztás egyensúlyának hiánya** miatt." [2]*

A Rendelet 16.§ (1) pontja szerint: *A válsághelyzet veszélye II. fokozatának minősül, ha a villamos energia folyamatos ellátását veszélyeztető olyan tartós erőművi és import teljesítményhiány jelentkezik, amikor a villamosenergia-rendszer erőművi tartaléka 7%-ra csökken, vagy országos szinten a tüzelőanyag-készlet olyan mértékben csökken, hogy a villamosenergia-ellátás folyamatossága 2 napon belül veszélybe kerülhet a villamos energia forrásoldal és a fogyasztás egyensúlyának hiánya miatt. [2]*

A VET 139. § (1) pontja értelmében: "*Villamosenergia-ellátási válsághelyzetnek (a továbbiakban: válsághelyzet) minősül a külön törvényben meghatározott szükséghelyzetet*[2]*, illetve veszélyhelyzetet*[3] *el nem érő mértékű, **a személyeket, vagyontárgyaikat, a természetet, a környezetet, illetőleg a felhasználók jelentős részének ellátását közvetlenül veszélyeztető villamosenergia-ellátási zavar**. Válsághelyzetet különösen a következő események válthatnak ki:*

*a) tartós erőművi, illetőleg a határon keresztül beszállított villamos energia hiánya,*

---

[1] Rendelet 1.§ 2. *erőművi tartalék:* a rendszerirányítási tevékenység engedélyese által a wattos teljesítmény központi szabályozása keretében percenként figyelt tartalék kategóriák közül a maximális, időkorlát nélküli forgótartaléknak és az összes indítható gép maximális szabályozási teljesítmény határának az összege, az import villamos teljesítmény figyelembevételével;

[2] 1949. évi XX. Törvény A MAGYAR KÖZTÁRSASÁG ALKOTMÁNYA. 19.§ (3) i)

[3] 1996. évi XXXVII. Törvény a polgári védelemről. 2.§ (2)

*b) tartós elsődleges energiaforrás hiány,*

*c) az ország vagy országrész villamosenergia-ellátásában több napon át hiányt okozó környezetszennyezés, illetőleg vezetékek üzemszünete,*

*d) a felhasználók ellátásának zavara." [1]*

A fenti meghatározások értelmében a jelentős zavar nem más, mint - valamilyen üzemi esemény által kiváltott - üzemi hiba, melynek következtében a villamosenergia termelés, átvitel, elosztás, szolgáltatás vagy felhasználás **jelentősen** korlátozottá válik vagy megszűnik; illetve a rendszer üzembiztonsága, szabályozhatósága, együttműködő képessége – végeredményben a felhasználók villamosenergiával való ellátása - **súlyos** veszélybe kerül. A felhasználók jelentős részének ellátását közvetlenül veszélyeztető zavar pedig már válsághelyzetnek minősül.

A VET-ben megfogalmazott válsághelyzetet válthat ki tartós erőművi illetve import villamosenergia hiány valamint tartós elsődleges energiaforrás hiány. Az erre történő felkészülés érdekében a Rendelet bevezeti a - a válsághelyzetet megelőző - válásghelyzet veszélye I. és II. fokozatának minősülő állapotot, mely állapot meghatározását a villamosenergia-rendszer erőművi tartalékának és a rendelkezésre álló rendszerszintű tüzelőanyag-készlet mennyiségéhez köti.

A villamosenergia-rendszer Üzemi Szabályzata (továbbiakban: Üzemi Szabályzat) értelmében üzemi esemény fogalma alatt a villamosenergia-rendszer (továbbiakban VER) üzemében bekövetkező állapotváltozást vagy beavatkozást kell érteni. Az allábiakban áttekintjük az üzemi események - állapotváltozások vagy beavatkozások – Üzemi Szabályzatban tárgyalt típusait.

1. Üzemi hiba, azaz olyan **nem tervezett** üzemi esemény (változás vagy beavatkozás), mely a tervszerű üzemmenetben (termelés, átvitel, elosztás, kereskedés) **nem szándékolt változást** eredményez. Az Üzemi Szabályzat az üzemi hibán belül megkülönbözteti a következő kategóriákat: ***üzemzavar***, ***tüzelőanyag készlet csökkenés***, felhasználói kikapcsolódás, rövid idejű hálózati zavar, egyéb üzemi hiba. [4]

   Melyek közül az utóbbi három nem tartozik a jelentős zavar fogalomkörébe, tekintettel arra, hogy az ilyen események által okozott felhasználói ellátás-kiesés csak a hibát okozó felhasználót érinti (felhasználói kikapcsolódás) vagy az időtartama a 3 percet nem haladja meg (rövid idejű hálózati zavar) vagy nem okoznak felhasználói kikapcsolódást illetve (üzembiztonsági) határérték-túllépést (egyéb üzemi hiba). [4]

   Az *üzemzavar* fogalom meghatározása gyakorlatilag azonos a VET-ben szereplő jelentős zavar fogalom meghatározással. Az Üzemi Szabályzat szerint az üzemzavar lehet:

   - villamosenergia rendszer szintű, vagy rendszer üzemzavar; amikor a bekövetkező üzemi hiba következtében felhasználói korlátozás válik szükségessé, nagymértékű forráskiesés, a rendszer részrendszerekre bomlása lép fel vagy az üzembiztonsági szint tartósan lecsökken; [4]

   - erőművi üzemzavar, azaz az erőművekben fellépő olyan üzemi hiba, mely a villamosenergia-termelést, átadást korlátozza, megszünteti vagy a menetrend tartását lehetetlenné teszi; [4]

- rendszerszintű koordinációt igénylő hálózat üzemzavara, azaz olyan – az átviteli hálózaton vagy a rendszerszintű koordinációt igénylő elosztóhálózaton fellépő – üzemi hiba, mely az átviteli- vagy az átviteli hálózat üzemét befolyásoló elosztó hálózat főberendezéseinek rendelkezésre állását korlátozza, megakadályozza és 3 percet meghaladó felhasználói kieséssel jár. [4]

A *tüzelőanyag készlet csökkenés* fogalma olyan eseményt jelent, mely következtében az erőművek tüzelőanyag készlete jogszabályban[4] meghatározott normatív energiahordozó készlet szint alá csökken. [4]

2. A **tervezett üzemi esemény** az üzemeltető szándékának megfelelően bekövetkező esemény (tartalékban állás, próbaüzem vagy tervszerű kikapcsolás) [4]

3. Az **egyedi, különleges, átmeneti állapot beállítása vagy létrejötte** szintén előre megtervezett módon kerül végrehajtásra illetve megy végbe. Ilyen esemény a korlátozás (beleértve mind a Rendelet szerinti hatósági-; mind az automatikák által megvalósított önműködő vagy kézzel indítható üzemzavari korlátozást); a nemzetközi együttműködési céllal kialakított, előre megtervezett irányüzemi vagy szigetüzemi különleges üzemállapot; a próba, mérés; és a zárlatkorlátozás miatti üzemállapot. [4]

4. **Rendkívüli üzemi esemény**nek kell tekinteni a villamosenergia-termelés, átvitel, elosztás, kereskedelem folyamatát veszélyeztető munkabalesetet, tűzesetet, erőszakos cselekményt (bombariadó, terrorcselekmény), károkozást, időjárás okozta eseményeket, természeti csapást, tüntetést; az automatikus illetve a rendszerirányító vagy hatóság által elrendelt korlátozást valamint a más országokban kialakult kaszkádbomlás hatására bekövetkező kieséseket, határérték túllépéseket, szigetüzemi-, irányüzemi leválásokat.[4]

A fentiek értelmében jelentős zavar illetve válsághelyzet kialakulásához alapvetően rendszerszintű, erőművi vagy hálózati üzemzavar bekövetkezése valamint a tüzelőanyag készlet csökkenése, villamosenergia-termelés és import hiány vezethet.

Megjegyzendő, hogy egy esetleges üzemzavar abban az esetben minősül jelentős zavarnak, súlyosabb esetben válsághelyzetnek - vonatkoznak kezelésére a VET és a Rendelet kríziskezeléssel kapcsolatos előírásai – amennyiben a bekövetkezett üzemi hiba (vagy hibák együttese) a villamosenergia-termelés, átvitel, elosztás, szolgáltatás, felhasználás folyamatára; a villamosenergia rendszer üzembiztonságára jelentős korlátozó hatást gyakorol, esetleg azokat meg is szünteti (jelentős zavar) illetve ha a felhasználók jelentős részének ellátását közvetlenül veszélyezteti (válásghelyzet).

Értelmezésünk szerint a jelentős zavar illetve válsághelyzet a felhasználók villamosenergia-ellátásának folyamatosságát közvetlenül veszélyezteti illetve megszüntetheti; a válsághelyzet veszélye az ellátás folyamatosságának veszélyeztetettségét, megszűnésének lehetőségét jelzi előre. Ennek megfelelően eltérő intézkedések szükségesek az üzemzavar, jelentős zavar illetve válsághelyzet valamint a válsághelyzet veszélye állapotok kezelésére.

[4] 44/2002. (XII. 28.) GKM rendelet az 50 MW és annál nagyobb teljesítményű erőművek energiahordozó-készletének legkisebb mértékéről és a készletezés rendjéről

# VILLAMOSENERGIA-KRÍZIS KEZELÉSÉBEN RÉSZTVEVŐ SZERVEZETEK, HATÁSKÖRÖK ÉS FELADATOK

A Rendelet értelmében a krízis kezelésében – beleértve mind a megelőzés, felkészülés és elhárítás feladatait – részt vesz: [2]

- valamennyi villamosenergia-ipari engedélyes (engedélyköteles villamosenergia-ipari tevékenységet végző szervezetek);

- az államigazgatási szervek közül a Gazdasági és Közlekedési Minisztérium, a Környezetvédelmi és Vízügyi Minisztérium, a Magyar Energia Hivatal, az Országos Katasztrófavédelmi Főigazgatóság és a Kormányzati Koordinációs Bizottság;

- a Kormány.

A jelentős zavar megelőzése, következményeinek csökkentése és az elhárítás irányítása valamint válsághelyzet veszélye esetén a védekezés irányítása az átviteli rendszerirányítási tevékenység engedélyesének (továbbiakban: rendszerirányító) feladata. Válsághelyzetben a védekezést a Kormány irányítja. A megelőzést és a védekezést a rendszerirányító illetve a hatóságok elsősorban piacszabályozó eszközökkel biztosítják. [2]

Krízis megelőzése és az ellen való védekezés a villamosenergia-ellátási szabályzatok[5] előírásainak valamint a megelőzés tekintetében a rendszerhasználók[6] között érvényben levő szerződésekben foglaltak betartására alapul. [2] A VET értelmében azonban a rendszerhasználók, az általuk megkötött szerződésekben foglalt jogoktól és kötelezettségektől függetlenül, a villamosenergia-rendszer jelentős zavara esetén kötelesek az átviteli rendszerirányító, és az elosztó hálózati engedélyes utasításait végrehajtani és az ebből fakadó terheket viselni. [1]

Ugyanakkor ezek az utasítások az egyenlő elbánás elvén és az indokolatlan megkülönböztetés tilalmán kell hogy alapuljanak és csak a szükséges és indokolt mértékig okozhatnak terheket a rendszerhasználóknak. Továbbá az utasítások kiadásakor a társadalmi-gazdasági kár minimalizálására kell törekedni. [2]

# INTÉZKEDÉSEK KRÍZIS MEGELŐZÉSÉRE ÉS KEZELÉSÉRE

Krízis megelőzésére és következményeinek enyhítésére a Rendelet előírja: [2]

1. krízis előtt és ideje alatt teendő intézkedések kidolgozásáért felelős Krízis Munkabizottság működtetését;

2. krízis esetén foganatosítandó intézkedéseket részletező Krízisterv kidolgozását;

3. krízis esetén elrendelhető fogyasztói korlátozás rendjét szabályozó Rotációs Kikapcsolási Rend (továbbiakban: RKR) kidolgozását.

---

[5] Üzemi Szabályzat, Kereskedelmi Szabályzat, Elosztói Szabályzat

[6] VET 3.§ 50. *Rendszerhasználó:* olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező gazdasági társaság, aki (amely) a közcélú hálózathoz villamos energia betáplálása, illetve vételezése céljából közvetlenül, vagy közvetve kapcsolódik; (mj.: az engedélyesek és felhasználók)

A Krízis Munkabizottságot (továbbiakban: KM) az átviteli rendszerirányító hozza létre, elnöke az átviteli rendszerirányító vezérigazgatója, tagjai a termelői, elosztói, kereskedői és egyetemes szolgáltatói engedélyesek, az átviteli rendszerirányító és a paksi atomerőmű képviselői. A KM munkájáról tájékoztatást kap, abban részt vehet a gazdasági és közlekedési miniszter, a környezetvédelmi és vízügyi miniszter, a Kormányzati Koordinációs Bizottság titkárságának vezetője, az Országos Katasztrófavédelmi Főigazgatóság főigazgatója és a Hivatal elnöke illetve azok megbízottja. [2]

A KM Rendeletben meghatározott feladatai közül jelen cikk keretei között az alábbiakat emeljük ki:

1. Villamosenergia-ellátási szabályzatok véleményezése [2]

A villamosenergia-ellátási szabályzatok közé a villamosenergia-rendszer működésére vonatkozó Üzemi Szabályzat, a belföldi és nemzetközi villamosenergia-kereskedelem és a szervezett piac működésének főbb szabályait tartalmazó Kereskedelmi Szabályzat és az elosztó hálózat működésére vonatkozó Elosztói Szabályzat tartozik. [1]

Ezen szabályzatokat a rendszerirányító illetve az elosztói szabályzat esetén az elosztói engedélyesek dolgozzák ki az engedélyesekkel és a felhasználókkal (a szabályzati bizottságok útján) egyeztetve, valamint a Magyar Energia Hivatal hagyja jóvá. [1]

A KM feladata az villamosenergia-ellátási szabályzatok véleményezése a Hivatal számára annak szempontjából, hogy a szabályzatok a krízis elkerülésére és enyhítésére megfelelő műszaki, gazdasági előírásokat tartalmaznak-e. [2] A Krízisterv előírja a Szabályzati Bizottságok számára, hogy a krízis-kezeléshez kapcsolódó, a Rendeletben illetve a Krízistervben foglalt előírásokat építsék be a szabályzatokba. [3]

2. Javaslattétel

a) a termelői és kereskedői engedélyesek feladatainak meghatározására az ellátás folymatosságát veszélyeztető villamosenergia illetőleg tüzelőanyag hiány fellépése esetén illetve

b) a rendszerirányító és az elosztóhálózati engedélyesek feladatira a felhasználói kikapcsolások megelőzése illetve előkészítése vonatkozásában.

Ha a villamosenergia hiányából adódóan megbomlik a villamosenergia-termelés és fogyasztás egyensúlya, akkor az egyensúly helyreállítása érdekében a villamosenergia-termelést és importot kell fokozni; ha ez – a szükséges mértékben - nem lehetséges a felhasználást kell korlátozni.

Jelentős zavar és válsághelyzet veszélye esetén a termelés és import fokozására valamint a fogyasztói terhelés korlátozására vonatkozó előírásokat a Krízistervnek kell tartalmaznia. [2]

3. Információs rendszer előkészítése az állami szervek, a rendszerhasználók és a társadalom tájékoztatására

A Rendelet értelmében a felhasználói kikapcsolásokkal illetve ezek előrejelzésével kapcsolatos tájékoztatás módját és rendjét a Krízistervnek kell tartalmaznia. [2]

A társadalom krízishelyzetre történő felkészítése – tájékoztatók, takarékossági felhívások kiadásával - az illetékes államigazgatási szervek és az engedélyesek közös feladata. [2]

Az információs rendszer rendszerirányító által történő működtetése krízis esetén a rendszerszintű tüzelőanyag és teljesítmény helyzet illetve annak várható alakulása felmérésére is szolgál. [2]

4. A villamos energia szervezett piacán folyó tranzakciók végrehajtásának a válsághelyzeti állapot megszüntetéséig történő felfüggesztése rendjének kialakítása.[2]

A rendszerirányító válsághelyzet veszélye II. fokozata esetén köteles a villamosenergia szervezett piacán folyó tranzakciókat a válsághelyzet veszélye megszűnéséig felfüggeszteni. [2]

5. Krízisterv és RKR véleményezése

A Krízisterv kidolgozása a rendszerirányító, illetve saját működési területükre lebontva az elosztói engedélyesek feladata. Az RKR-t a rendszerirányító a hálózati engedélyesekkel együtt dolgozza ki. A Krízistervet és az RKR-t a Hivatal hagyja jóvá. [2]

A Rendelet 7. §-ában a Krízisterv kötelező tartalmi elemeiként meghatározott, és az egyes krízishelyzetek esetén előírt intézkedések közül jelen cikk keretében az alábbiakat emeljük ki:

1. Állami szervek, a társadalom, a rendszerhasználók és az engedélyesek tájékoztatása (krízis esetén)

Jelentős zavar valamint válsághelyzet I. és II. fokozata esetén a védekezés irányítása az átviteli rendszerirányító feladata. A rendszerirányító jogosult illetve köteles a meglévő polgári jogi szerződések keretein belül - az érintett engedélyesek bevonásával - a piacgazdasággal és a villamosenergia-ellátási szabályzatokkal összhangban álló utasításokat adni és intézkedéseket kezdeményezni a rendszeregyensúly helyreállítása érdekében. (Pl. az üzembiztonsági szolgáltatások és rendszertartalékok igénybevétele, nemzetközi kisegítés kérése, export-import menetrend módosítása, villamos erőművek fokozott igénybevétele, feszültségcsökkentés stb.). Az utasítások kiadásának módját valamint a végrehajtás technikai szabályait a villamosenergia-ellátási szabályzatok tartalmazzák. [2]

Jelentős zavar valamint válsághelyzet veszélye esetén a megtett intézkedésekről, azok hatásairól a rendszerirányító köteles a gazdasági és közlekedési minisztert valamint a Magyar Energia Hivatl elnökét tájékoztatni. [2]

2. A villamosenergia-termelés és import fokozása

A villamosenergia-rendszerben fellépő hiány pótlására, jelentős zavar és válsághelyzet veszélye I. fokozata esetén, a rendszerirányító jogosult illetve köteles a villamosenergia-termelés és import fokozását kezdeményezni a termelői és kereskedői engedélyesek erre történő felhívásával. A felhívás rendjét a Krízistervnek kell tartalmaznia. [2]

Megjegyzendő, hogy az import villamos energia behozatalára csak a kiosztott határkeresztező kapcitás mértékéig van lehetőség, így az import növelése csak a rendelkezésre álló határkeresztező kapcitás mértékéig lehetséges.

A termelés fokozásával kapcsolatosan megemlítendő a VET 4. § 3. pontjában foglalt rendelkezése, melynek értelmében a rendszerirányító - a legkisebb költség elvének figyelembevételével - bármikor igényelheti bármely üzemeltetésre alkalmas termelő berendezés hálózatra kapcsolását, ha annak indítási és üzemeltetési költségeit vállalja. Amennyiben a rendszerirányító a költségeket vállalja a termelői engedélyes az erőmű indítását nem tagadhatja meg. [1] Tehát krízis esetén - amennyiben a szükséges tüzelőanyag rendelkezésre áll valamint az erőműben az adott helyzet szempontjából megfelelő időn belül a termelés elindítható – továbbá az erőműindítás költsége az adott krízishelyzet kezelésére alkalmas egyéb intézkedések költségénél alacsonyabb, a rendszerirányító elrendelheti az erőmű indítását. [2]

3. Felhívás módját a villamos energiával való takarékosságra és annak jelentőségére,

Jelentős zavar és válsághelyzet veszélye II. fokozat esetén a rendszerirányító, valamint válsághelyzetben a Kormány önkéntes terheléscsökkentésre kérheti fel a fogyasztókat. A felhívás módját a Krízistervnek kell tartalmaznia. [2]

Esetleges krízis esetén a villamosenergia-rendszerben fellépő teljesítményhiány következtében megbomlott rendszeregyensúly helyreállítását elősegíti a felhasználói terhelés csökkenése. A felhasználó terhelés csökkenthető fogyasztói korlátozással, a fogyasztók kényszerű kikapcsolásával; ám a kényszerű korlátozás szükséges mértéke csökkenthető akár el is kerülhető amennyiben a felhasználók villamosenergia fogyasztásukat önkéntes módon– pl. a nagy fogyasztású háztartási berendezések használatának mellőzésével - az általuk megválasztott mértékben és időtartamban csökkentik.

4. A felhasználói terhelés csökkentése a villamos energia forrásoldal (termelés + import) és fogyasztás egyensúlyának megőrzése céljából

Jelentős zavar valamint válsághelyzet veszélye esetén fellépő teljesítményhiány kezelésére, a rendszeregyensúly megőrzése érdekében, a rendszerirányító kezdeményezi a saját hatáskörben történő, a termelő, kereskedő és felhasználó közötti szerződéseken alapuló terhelésszabályozást, terheléscsökkentést. Az automatikák által végzett illetve elrendelhető üzemzavari korlátozás 6 órát meghaladó időtartamban nem alkalmazható. Ha a korlátozás időtartama a 6 órás időtartamot meghaladja, akkor a rotációs kikapcsolási rendet (továbbiakban: RKR) kell alkalmazni. Válsághelyzet veszélye II. fokozata esetén a rendszerirányító utasítja az elosztói engedélyeseket az RKR előkészítésére. [2]

5. A válsághelyzet esetén követendő eljárási rend forgatókönyve

Azon eseményeket, üzemzavarokat; melyek válsághelyzetet válthatnak ki, a válsághelyzet várható időtartamát és következményeit valamint a helyreállítás érdekében tett intézkedéseket a rendszerirányító jelenti a gazdasági és közlekedési miniszternek és a Hivatal elnökének. A Kormányt a gazdasági és közlekedési miniszter tájékoztatja. [2]

Válsághelyzet esetén a védekezés irányítása a Kormány feladata. Válsághelyzetben a Kormány: [2]

- terheléscsökkentésre szólíthatja fel a felhasználókat;
- előírhatja az egyes tüzelőanyagok felhasználásának csökkentését, tilalmát vagy más tüzelőanyagok felhasználását, vásárlását;

- a megtett intézkedésekről a tömegkommunikáció útján tájékoztatja a közvéleményt;
- a korlátozó intézkedésekről tájékoztatja az Európai Bizottságot és a tagállamokat;
- A 30 napot meghaladó válsághelyzetről tájékoztatást ad az Országgyűlésnek.

Válsághelyzetben a rendszerirányító: [2]

- elrendelheti a hálózati engedélyeseknek a felhasználói terhelés csökkentését az előkészített RKR útján;
- köteles információs rendszert működtetni a rendszerszintű tüzelőanyag- és teljesítményhelyzet és várható alakulásának felmérésére;
- eltérő jogszabályi rendelkezés hiányában a jelentős zavar kezelésének szabályai szerint jár el.

A válsághelyzet megszűnését követően a rendszerirányító elrendeli a felhasználók visszakapcsolását és erről jelentést ad a gazdasági és közlekedési miniszternek valamint a Hivatal elnökének. A Kormány hatályon kívül helyezi a válsághelyzetben hozott intézkedéseit. [2]

# ÖSSZEFOGLALÁS

A cikkben áttekintettük a villamosenergia-krízis esetén teendő intézkedések szabályozásának rendszerét, a krízissel kapcsolatos alapvető fogalmakat, a kríziskezeléssel kapcsolatos feladat és hatásköröket, valamint a krízis megelőzését, és következményeinek enyhítését célzó intézkedéseket.

A szabályozás alapja 2007. évi LXXXVI. törvény a villamos energiáról, mely 170. § (1) bekezdésének 23. pontja alapján a kormány a villamosenergia-rendszer illetve villamosenergia-ellátás jelentős zavarának minősülő helyzet szabályait, a 285/2007 (X.29) kormányrendeletben állapította meg. A rendszerirányító a kormányrendelet 7. § (1) a) pontja szerinti tartalommal kidolgozta a Krízistervet, mely a villamosenergia-krízis megelőzésére és következményeinek enyhítésére szolgáló intézkedéseket tartalmazza. AKrízistervet a Hivatal 90/2005. számú határozatával hagyta jóvá. A Krízisterv előírásait a villamosenergia-ipari engedélyeseknek be kell építeniük a villamosenergia-ellátási szabályzatokba, belső utasításaikba, eljárásrendjeikbe; ez a láncolat biztosítja a VET-ben, illetve a Rendeletben foglalt előírások érvényre juttatását.[3]

A VET, a Rendelet és a villamosenergia-rendszer Üzemi Szabályzatában foglalt fogalomértelmezések alapján bemutattuk az üzemi hiba, üzemzavar, jelentős zavar, válsághelyzet, válsághelyzet veszélye, és villamosenergi-krízis fogalmakat valamint áttekintettük a krízis megelőzése érdekében és esetén alkalmazandó intézkedéseket.

A krízis megelőzése érdekében valamint a krízishelyzetre történő felkészülés keretében a Rendelet előírja a rendszerirányító számára Krízis Munkabizottság működtetését, a Krízisterv és a Rotációs Kikapcsolási Rend kidolgozását.

Villamosenergia-krízis esetén a Rendeletben foglalt előírásokat kell alkalmazni. Jelentős zavar és válsághelyzet veszélye esetén a védekezés irányítása a rendszerirányító feladata.

Krízis esetén a rendszerirányító jogosult illetve köteles az ellátási szabályzatokkal összhangban utasításokat adni, gondoskodni a rendszerhasználók, az illetékes állami szervek és a társadalom megfelelő tájékozattásáról; kezdeményezni a villamosenergia-termelés és import fokozását valamint a szükséges mértékű terheléscsökkentést (fogyasztói kikapcsolásokat); továbbá takarékossági felhívásokat kibocsátani.

Válsághelyzet esetén a védekezés irányítása a kormány feladata. Válsághelyzetben – ha a Rendelet vagy más jogszabály ettől eltérően nem rendelkezik – az engedélyesek alapvetően a jelentős zavar szabályai szerint járnak el.

Ebben a rövid közleményben nem tértünk ki a hazai szabályozásnak a más államok szabályozó rendszereivel történő összehasonlító vizsgálatára, sem a megtörtént események, illetve a rendszer gyakorlatok alapján szerzett tapasztalatok értékelésére, és a rendszer esetleg célszerűnek mutatkozó, korszerűsítési lehetőségeinek az értékelő elemzésére. Ezek a nagyon fontos területek mélyreható elemzést igényelnek, és a további vizsgálatokat egy külön tanulmányban tervezzük közzétenni.

## HIVATKOZÁSOK


[1] 2007. Évi LXXXVI. törvény a villamos energiáról. Magyar Közlöny, 2007/86 (2007) 6354-6409

[2] 285/2007. (X. 29.) Korm. Rendelet a villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről. Magyar Közlöny, 2007/146 (2007) 10261-10268

[3] A Magyar Energia Hivatal 90/2005. számú határozata. (2005. április 15.) http://www.eh.gov.hu/gcpdocs/200505/902005_krzis_mavir_2005_04_12.pdf (letöltés ideje: 2008.02.28.)

[4] A villamosenergia-rendszer Üzemi Szabályzata. (Jóváhagyta a Magyar Energia Hivatal 87/2008. számú határozata, 2008.02.13.) http://www.mavir.hu/domino/html/www/mavirwww.nsf/vAllPages/pUzemiSzabalyzat_WEB?OpenDocument (Letöltés dátuma: 2008.02.28)

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Kovács Judit**
BMF Kandó Kálmán Villamosmérnöki Kar
kovacs.judit@kvk.bmf.hu

**Tolvaj Balázs**
ZMNE Katonai Műszaki Doktori Iskola
tolvba@freemail.hu

**Huszár András**
PTE ÁOK Igazságügyi Orvostani Intézete
andras.huszar@aok.pte.hu

# BIOETIKA ÉS AZ EMBERI TÉNYEZŐ

## AZ EMBERI TÉNYEZŐ BIOETIKAI ALKALMAZÁSI LEHETŐSÉGÉNEK NÉHÁNY KÉRDÉSE

***Absztrakt***

*Az emberi tényezővel kapcsolatos kutatások eredményei széles körben felhasználhatóak. Egy ilyen alkalmazhatósági terület a bioetika, illetve katonai bioetika. A bioetika definiálása, és az emberi tényező szerepének megfogalmazása után néhány olyan példa kerül bemutatásra, amelyek esetén az emberi tényező bioetikai alkalmazása lehetséges. Az egyik ilyen terület az emberekkel való kísérletezés, a másik pedig néhány konkrét katasztrófa, illetve katasztrófa-típus elemzése az emberi tényező szempontjából.*

*The results of the research of the human factor may be applied for several fields of science. One of this possible scope is bioethics including military bioethics. After the definition of bioethics and the framing of the role of the human factor, some examples are shown for the bioethical application of the human factor. One of these examples is experimentation with humans. The other one is the analysis of some catastrophes with respect to the human factor.*

***Kulcsszavak:*** *bioetika, emberi tényező ~ bioethics, human factors*

## BEVEZETÉS

A **bioetika** olyan témákat foglal magában, mint az élet és halál definíciója, az abortusz, a mesterséges megtermékenyítés, a klónozás, az állat-, és emberkísérletek, a szervátültetés vagy az eutanázia. A bioetika a biológia és az orvostudomány etikai kérdéseivel foglalkozó, a természet és társadalomtudományokon alapuló interdiszciplináris tudomány, s mint ilyen, az ember kulcsfontosságú szerepét figyelmen kívül nem hagyhatja, illetve fő célja is az emberiség túlélésének szolgálata.
Az **emberi tényező** szerepe általánosan három fő csoportra bontható bármely esemény (baleset, veszélyhelyzet, katasztrófa) kialakulásával kapcsolatban. Az ember lehet okozója, elszenvedője, illetve megakadályozója egy adott eseménynek.
A bioetika az embert elsősorban, mint az események elszenvedőjét tekinti, míg az emberi tényezővel kapcsolatos kutatások leginkább az emberi hibák vizsgálatát tűzik ki célul. Az alábbiakban a bioetika két olyan területéről lesz szó, ahol az emberi tényezővel kapcsolatos eredmények felhasználhatók. Az egyik ilyen terület az emberekkel való kísérletezés, a másik pedig a katonai bioetika területét érintő katasztrófák elemzése, és a bioterrorizmusnak mint egyes katasztrófák előidézőjének vizsgálata.

## BIOETIKA

A bioetika szó a különbözõ vallási, politikai, kulturális, és tudományos csoportok számára más és más tartalommal bír. A bioetika legáltalánosabb definíciója szerint a bioetika a biológia és az orvostudomány etikai kérdéseivel foglalkozó, a természet és társadalomtudományokon alapuló interdiszciplináris tudomány. A bioetika olyan témákat foglal magában, mint az élet és halál definíciója, az abortusz, a mesterséges megtermékenyítés, a klónozás, az állat-, és emberkísérletek, a szervátültetés vagy az eutanázia.
A katonai bioetika olyan különböző problémákat vizsgál, mint például az emberekkel való kísérletezések során történő visszaélések, a katonai környezetszennyezés, a biológiai fegyverekkel kapcsolatos etikai problémák, illetve a bioterorizmus elleni küzdelem etikai kérdései. A katonai bioetika alapelve -a bioetika alaptörvényének megfelelően- az élet határtalan tisztelete. Az emberiség túlélési esélyeit tekintve az etika forradalma az egyik legjelentősebb tényező. A tudományos eredmények önmagukban nem vethetnek véget a környezetszennyezés és az emberi tevékenység következtében támadó katasztrófáknak, csak az emberi etika forradalmával együtt, amely elengedhetetlenül szükséges. A tudományban való túlzott bizakodás és az etika figyelmen kívül hagyása még az eddig ismerteknél is nagyobb katasztrófákat idézhet elő.
A Föld egységes, dinamikus egyensúlyban működő rendszer, amely bármelyik paraméterének változására az összes többi paraméter megváltoztatásával reagál. Hosszabb távon a katonai erők fő feladata egy globális világban az lehet, hogy összehasonlíthatatlan technológiai és katonai fölényüknél fogva kordában tartsák és blokkolják az ezen világhoz nem csatlakozott erők militánsainak a bioetika szűkebb és tágabb elveivel ellentétes törekvéseit. A globális világ korszakában a globális bioetika adhat választ a döntéshozók felelősségére [1].

## AZ EMBERI TÉNYEZŐ SZEREPE

Az emberi tényező szerepe általánosan három fő csoportra bontható bármely esemény (baleset, veszélyhelyzet, katasztrófa) kialakulásával kapcsolatban. Az ember lehet elszenvedője, okozója, illetve megakadályozója egy adott eseménynek.

**Az ember mint szenvedő alany**

A katonai bioetika által vizsgált problémák mindegyikében az ember az elsődleges szenvedő alany. Éppen ezért, legyen szó akár az emberekkel való kísérletezések során történő visszaélésekről, a katonai környezetszennyezésről, a biológiai fegyverekkel kapcsolatos etikai problémákról, illetve a bioterorizmus elleni küzdelem etikai kérdéseiről, a bioetika tudománya mindig az ember érdekeit tartja szem előtt.

Sok esetben azonban az ember nem pusztán szenvedő alanya, hanem okozója is az eseményeknek. Az emberi tényezővel kapcsolatos kutatások leginkább az emberi hibák vizsgálatát tűzik ki célul.

**Az ember mint az események okozója - az emberi hiba**

Azon okok között, amelyek potenciális veszélyekből akut veszélyhelyzetet válthatnak ki, minden esetben megtalálható az emberi tényező. Az összefüggések elég következetes feltárása még a műszaki okok mélyén is emberi mulasztásokat mutat ki. A megközelítés módjától függően különböző tanulmányok a hibák 45-80%-át emberi tevékenységre vezetik vissza.
Rankin és Krichbaum kutatásai alapján az utóbbi két évtizedben az emberi tényező szerepe a balesetek bekövetkezésében drámai emelkedést mutat, elérve akár 70-80 %-os arányt is, függetlenül a technológiai körülményektől [2].
Az emberi hibák kategorizálása sokféleképpen történhet. Az alábbiakban kétféle csoportosítást mutatunk be.
Az **emberi hiba** általános fogalom, amely magában foglal minden olyan helyzetet, amelyben a mentális vagy fizikai cselekvések megtervezett sorozata nem éri el előre eltervezett szándékozott célját és ez a kudarc nem tulajdonítható valamilyen rendkívüli véletlenszerű körülménynek [3]. Az ASME 2000 szabvány értelmében az **emberi hiba** belső emberi hibamechanizmusok következményeként létrejövő emberi beavatkozási hiba. Az emberi hiba fogalmával szabadon leírható bármely nem optimális emberi beavatkozás. Az emberi hibák két nagy csoportja: a **hibás emberi beavatkozás** és a **szükséges emberi beavatkozás elmulasztása**. Az emberi hiba mint az elvárt és a megvalósult tevékenység vagy viselkedés eltérésének következménye, három csoportba sorolható: **elvétés**, **kihagyás** és **tévedés**. A hibák egy külön kategóriája a (szándékos) **veszélyeztetés**, amelynél nem engedélyezett, tiltott, nem helyénvaló tevékenységet végeznek. A bioetika szempontjából ez a legfontosabb, illetve leggyakrabban előforduló típus. Számottevő szerepet kaphatnak még a **rejtett hibák**, amelyek időben és térben gyakran távol vannak a bekövetkezett eseménytől, és ezért nehezen azonosíthatók [4]. Az **emberi hibajelenség** meghatározott emberi beavatkozás hibája. Az emberi hibához képest ilyenkor több különböző ok vezethet a hibaeseményhez. A hibajelenség érinthet berendezéseket, ekkor **meghibásodás**ról beszélünk, és folyamatokat, amikor is **zavarállapot** következik be. Az olyan hibajelenség, amely elfogadhatatlan következményekhez vezet, a **kritikus hiba**.
Az emberi hibák egy másik elképzelhető csoportosítása az emberi beavatkozási hiba és a kialakult veszély időrendi sorrendjétől függ. Ezek alapján az úgy nevezett **A-típusú emberi beavatkozás hibája**: olyan hiba, amelyet a kezdeti esemény előtt végrehajtott emberi beavatkozás során követnek el, elsősorban a berendezések és rendszerek rendelkezésre állásával kapcsolatban( például a karbantartási tevékenységgel kapcsolatban). A **B-típusú emberi beavatkozás hibája** olyan hiba, amely közvetlenül kezdeti eseményt okoz. A **C-típusú emberi beavatkozás hibája** pedig olyan hiba, amelyet az üzemzavar vagy baleset elhárításánál végrehajtott emberi beavatkozások során követnek el [5].

Az emberi hibák csoportosítása után ejtsünk szót egy fontos, és sokszor figyelmen kívül hagyott tényről: az ember sok esetben képes lehet egy-egy szerencsétlen esemény kialakulását megakadályozni, illetve következményeit mérsékelni.

**Az ember mint a szerencsétlen esemény bekövetkezésének megakadályozója**

Azok a nézetek, amelyek szerint „csak az nem hibázik, aki nem dolgozik", „az ember a leggyengébb láncszem a rendszerben", vagy „az ember által végzett folyamatokat automatizálni kell", túlságosan leegyszerűsítik az emberi hibák kiküszöbölésének kérdését. Az ember képes helytállni előre nem várt helyzetekben, képes olyan megoldásokra, amelyek a veszélyhelyzetek káros következményeit mérséklik. Az emberi beavatkozás nélkül több veszélyhelyzet válthatna ki valós balesetet. A biztonságra törekvő viselkedés nem a hibák és a tévedések kizárását jelenti, hanem legfőképpen a megelőzés irányába történő elkötelezettséget[6].

Az alábbiakban a bioetika néhány olyan területét mutatjuk be, ahol az emberi tényezővel kapcsolatos kutatási eredmények felhasználhatók. Az eseményeket okozó emberi hibákat kategorizáljuk, és javaslatot teszünk az eredmények bioetikai felhasználására.

## AZ EMBEREKKEL VALÓ KÍSÉRLETEZÉS

Pasternák Alfréd kiemeli, hogy az emberekkel való kísérletezés legelrettentőbb példája a náci koncentrációs táborokhoz fűződik. A kísérletek (az eutanázia-programok mellett) külön hangsúlyt érdemelnek. Részint azért, mert ez az egyetlen terület, ahol az orvosok nem hivatkozhattak kényszerítő körülményekre: a kísérleteket önszántukból végezték. Másrészt, mert a kísérletek utólagos elemzése révén fogalmazták meg azt az etikai törvénytárat, amelyet alapjában véve ma is iránymutatónak ítél a tudományos orvosi világ.
A kísérletek egy része a hadsereg részére történt: ezek közé sorolhatók a malária, tífusz, hipotermia stb. kísérletek. Ideológiai célokat szolgáltak a különböző sterilizációs kísérletek, antropológiai vizsgálatok, s nem utolsó sorban a hírhedt auschwitzi tábororvos, Jozef Mengele, ikreken végzett vizsgálatai. Végül egyes náci orvosok „tudományos" érdeklődését kielégítő, egyéni kísérleteit is ide sorolhatjuk. Az egyik náci orvos például meztelenre vetkőztetett, éhező foglyokon a tűző nap tartós hatását vizsgálta. Egy másik orvos, a fokozatos vérveszteség vizsgálatára vénákat nyitott meg foglyokon, és megvárta, mérte a halál bekövetkeztét. Mások egyes endokrin mirigyek átültetésével a homoszexualitás gyógyításán kísérleteztek [7].
A fenti események az emberi tényező szempontjából elemezve egytől-egyig a szándékos veszélyeztetés kategóriájába sorolhatók.

A második világháborúban győztes négy hatalom katonai bíróságának a háborús főbűnösöket elítélő tárgyalása után, 1946-47-ben, Nürnbergben került sor az ún. „orvosperre", amely a náci orvosok holokausztban végzett tevékenységét volt hivatva tárgyalni.
A tárgyalások tanulságaként a bíróság a hippokratészi kötelezettséget nem találta elegendőnek az orvosi kísérletek alanyainak védelmében. Ehhez a kísérleti alanyok emberi jogainak védelmét szolgáló külön etikai törvénytár megalapozását tartotta szükségesnek. A Nürnbergi Kódexben [8] tíz vezérelvet fogalmaztak meg, mindegyikük középpontjában a kísérleti alany állt. A tíz alapelv a következőkben foglalható össze:
1. A kísérleti alany teljes tájékoztatása és a kísérlethez való önkéntes hozzájárulása elengedhetetlen.

2. A kísérlet eredménye a társadalom számára hasznos és más módon el nem érhető kell, hogy legyen.
3. A kísérleteket állatkísérletek előzzék meg.
4. Azok nem okozhatnak sem fizikai, sem mentális ártalmat.
5. Nem vezethetnek a kísérleti alany halálára vagy megnyomorítására.
6. Esetleges veszélyük nem haladhatja meg a várható pozitív eredmény értékét.
7. Az esetleges ártalom kezelésére előre fel kell készülni,
8. A kísérleteket csak tudományosan kellően felkészült kutatók végezhetik
9. Az alany kívánságára a kísérletet bármikor azonnal abba kell hagyni.
10. Ha a kísérlet közben, annak folytatását a kutató veszélyesnek tartja, azt azonnal be kell szüntetnie.
A Nürbergi Kódex magán hordozta a rebound jelenséget, azaz jóval szigorúbbra sikeredett, mint ahogy azt az általános etikai normák megkövetelték volna [1].
A Helsinki Nyilatkozat (WHO 1964.) a Nürbergi Kódex helyett kevésbé szigorú szabályozású. Az emberi tényező szempontjából egy lényeges pontja még így is kiemelendő:
”Emberi alanyokkal történő orvosi kutatás kizárólag tudományosan képzett személyek vezetésével, klinikai háttérrel rendelkező egészségügyi személyzet felügyelete alatt végezhető. A felelősség mindig az orvosilag képzett személyé, sohasem a vizsgálat alanyáé, még akkor sem, ha az alany hozzájárulását adta.[9]”

Az emberi hibák nagy arányának, illetve széleskörű elterjedésének okán a fenti alapelv minden kísérletnél betartandó, nem kizárólag a vizsgálati alany, hanem a vizsgálat tudományos hitelességének érdekében is.

A különböző katasztrófák elemzésekor az emberi tényező szintén kiemelt szerephez jut. Bizonyos katasztrófák bioetikai kérdéseket is felvetnek. A katasztrófák csoportosíthatók természeti, illetve civilizációs katasztrófaként, amelyek néhány alcsoportja a bioetikát és az emberi tényezőt is érinti.

## KATASZTRÓFÁK

A katasztrófa a szükséghelyzet vagy a veszélyhelyzet kihirdetésére alkalmas, illetőleg a minősített helyzetek kihirdetését el nem érő mértékű olyan állapot vagy helyzet, amely emberek életét, egészségét, anyagi értékeiket, a lakosság alapvető ellátását, a természeti környezetet, a természeti értékeket olyan módon vagy mértékben veszélyezteti, károsítja, hogy a kár megelőzése, elhárítása vagy a következmények felszámolása meghaladja az erre rendelt szervezetek előírt együttműködési rendben történő védekezési lehetőségeit és különleges intézkedések bevezetését, valamint az önkormányzatok és az állami szervek folyamatos és szigorúan összehangolt együttműködését, illetve nemzetközi segítség igénybevételét igényli [10].

### Geológiai eredetű katasztrófák

A természeti katasztrófák közé sorolható geológiai katasztrófák közül a bioetika és az emberi tényező szempontjából is kiemelt szerephez jut a tsunami, amelynek egyik legsúlyosabb veszteségekkel járó eseménye 2004-ben történt.
2004. december 26-án, Hawaii idő szerint 14 óra 59 perckor 9-es erősségű földrengés rázta meg az Indiai-óceán fenekét a szumátrai Banda Aceh kikötővárostól alig több mint 5 km-re. A tengerfenék kb. 2 métert emelkedett és hatalmas lökést adott a víznek. A keletkező hullámok,

elsősorban a Bengáli-öbölben (de nem csak ott), szinte példátlan pusztítást okoztak. Mintegy 300 ezer ember meghalt vagy eltűnt.[11]
Az emberi tényező szempontjából fontos kiemelni, hogy az ilyen mértékű veszteség megelőzhető lett volna megfelelő jelző- és riasztórendszer megléte esetén. Az igazság azonban az, hogy az Indiai-óceáni Tsunami Riasztó-rendszer kiépítéséről csak 2005. januárjában döntöttek, és 2006. óta működik. Ebben az esetben tehát a szükséges emberi beavatkozás elmulasztásáról van szó, tekintve, hogy hasonló rendszer a Csendes-óceánon 1949 óta működik.

**Biológiai eredetű katasztrófák**

A biológiai eredetű katasztrófák közül az emberi tényező szempontjából jelentős, és komoly bioetikai kérdéseket felvető katasztrófa-típusok a következők: az emberi hiba okozta biológiai katasztrófa, azaz gondatlanság vagy szakszerűtlenség következtében a laboratóriumokból, kutatóintézetekből kiszabaduló károkozók által előidézett fertőzés vagy járvány, illetve a szándékosan előidézett biológiai katasztrófa, azaz háború esetén, illetve terrorista akció során, mesterségesen keltett fertőzés vagy járvány, illetve a növényzet vagy az állatvilág elpusztítása.
Az 1994-es Surat-i pestisriadó esetén az emberi tényező akkor kerülhet szóba, ha elfogadjuk azt a verziót, amely bioterrorizmusként tekinti a katasztrófát, ekkor ismét a szándékos veszélyeztetés a kiváltó ok.
Ken Alibek könyvében azonban, amelynek magyar fordítása a „Biohalál" címet kapta (az eredeti, „Biohazard" cím biológiai veszélyt, illetve biológiai kockázatot jelent, amiből jobban látszana az összefüggés az emberi tényezővel mint kockázati tényezővel), beszámolók olvashatók tesztekről és szivárgásokról, laborbeli balesetekről és katasztrófákról is a KGB fenyegetések és gyilkosságok mellett [12, 13].

***Biológiai fegyverek – bioterrorizmus***

Szándékosan előidézett, és az előidéző számára kívánatos – emiatt az emberi tényező szempontjából talán a legnagyobb kockázatot jelentő - biológiai katasztrófát okozhat biológiai fegyverek bevetése és a bioterrorizmus.

A biológiai fegyverek eredetileg olyan kórokozó anyagok, amelyeknek élő szervezetekre van szükségük ahhoz, hogy szaporodjanak és romboló hatásukat kifejtsék A toxinok megjelenésével e definíció kissé módosult. A toxinok mikroorganizmusok vagy többsejtű állati vagy növényi szervezetek által termelt mérgező anyagok, melyek hatásukat élő szervezetekben fejtik ki, viszont nem szaporodnak, és mintegy átmenetet képeznek a vegyi fegyverek felé.
Az 1972-ben aláírt és 1975-ben életbe lépett Biológiai Hadviselési Konvenció elítélte a biológiai fegyverek fejlesztését, birtoklását és támadó célú alkalmazását, védelmi célú kutatásukat azonban nem korlátozta. A biofegyverek fejlesztése során a fő cél olyan anyag létrehozása, mely könnyen hozható aeroszol formába és ebben az állapotban kellően stabil.
A biológiai fegyvereket a bőrön át, a gyomor-bél rendszeren keresztül és injekcióval is be lehet juttatni a szervezetbe, de nem olyan hatékonyan, mint a tüdőn keresztül, aeroszol útján. Ebből a szempontból meghatározó tényező a tüdő felülete (kb. 100 $m^2$) valamint az, hogy az ember kénytelen lélegezni. Légzőmaszkok használata természetesen hatásos védelmet jelenthet, ennek azonban csak katonai szempontból van jelentősége. Egy terrortámadás során a célszemélyek nem sejtik, hogy biofegyverrel kerültek érintkezésbe, mert azok szagtalanok és láthatatlanok. Védőfelszerelés pedig aligha van a kezük ügyében.

Egy epidemiológus szerint: "Nem az a kérdés, hogy a terroristák bevetnek-e majd fertőző ágenseket ártatlan polgárok meggyilkolására, hanem az, hogy erre mikor és hol kerül sor." [14].
Nagyon fontos kiemelni, hogy a szándékos veszélyeztetés mellett egyéb emberi hibák is előtérbe kerülhetnek, amikor biológiai katasztrófáról, illetve bioterrorizmusról beszélünk, s ezért az emberi tényezővel kapcsolatos kutatások eredményeinek széleskörű bioetikai felhasználása is lehetséges.

## Ipari katasztrófák

Az ipari katasztrófák két olyan alcsoportját tekintjük át a következőkben, ahol az emberi tényező szerepe különösen jelentős, és ahol bioetikai szempontból is súlyos kérdések vetődnek fel.
Az első ilyen csoport a veszélyes anyagok kiáramlása, azaz az ipari, mezőgazdasági üzemekben tárolt, előállított vagy felhasznált mérgező, maró, tűz- vagy robbanásveszélyes, illetve fertőző anyagok jelentős mennyiségben történő szabadba jutása.
A másik csoport a radioaktív anyagok szabadba jutása, azaz az atomerőművekben, kutató- vagy egészségügyi intézményekben tárolt, előállított vagy felhasznált sugárzó anyagok kiszabadulása.
Az alábbiakban a fentiekre vonatkozó konkrét példákat láthatunk, amelyek az emberi tényező fontos szerepére, illetve bioetikai alkalmazásának lehetőségére hívja fel a figyelmet.

### *Vegyi katasztrófák*

A vegyi katasztrófák, illetve vegyi terrorizmus esetén semmiképpen nem hagyható figyelmen kívül az emberi tényező. Jó példa erre az 1984-es Bhopal-i katasztrófa. 1984. december 2-án éjjel az Indiában található Bhopal városában lévő, a Union Carbide nevű multinacionális cég rovar- és gyomirtó szereket és egyéb vegyi anyagokat előállító vegyi üzeméből mérgező gáz szabadult ki. Mind az okok, mind a következmények tekintetében a cég hivatalos álláspontja erősen eltér az érintett túlélőkétől. Az azonban biztosan megállapítható, hogy akár szándékos károkozásról volt szó (ami a cég véleménye [15]), akár a biztonsági előírások durva megsértéséről (ami az „Igazságot Bhopalnak Nemzetközi Kampány” álláspontja [16]), a katasztrófát az emberi tényező okozta.
A bioetika szempontjából is igen jelentős egy-egy ilyen vegyi katasztrófa elemzése, amely a biztonság kérdését ezáltal etikai kérdéssé teheti.

### *Nukleáris katasztrófák*

A XX. század második felében történt nagyobb reaktorbalesetek, illetve katasztrófák elemzésekor egyértelműen kiderül: a kiváltó okok az esetek többségében az emberi tényezőre vezethetők vissza [17]. Ezt mutatja az 1. sz. táblázat.

Mint a táblázatból is látható, a nukleáris balesetek kialakulásánál az emberi tényező szerepe kiemelkedően magas. Ennek következtében ezen a területen folyik az emberi tényezővel kapcsolatos kutatások döntő többsége. A kutatások eredménye azonban széles körben –így a bioetika területén is-felhasználható.

1. táblázat: Reaktorbalesetek és katasztrófák kiváltó okai

| Esemény éve | Esemény helyszíne | Esemény következménye | Esemény kiváltó oka |
|---|---|---|---|
| 1952. | Chalk River (Canada) | fűtőelemolvadás | **Operátori hiba** |
| 1957. | Windscale-i reaktor (Anglia) | tűz | **Operátori hiba** |
| 1979. | Three-Mile Island-i atomerőmű (USA) | fűtőelemolvadás | **Operátori hiba** |
| 1983. | Ciudad Juarez (Mexikó) | radioaktív szennyezés | **Tévedés**ből vashulladékként értékesítettek terápiás sugárforrást |
| 1986. | Csernobili atomerőmű (SZU) | robbanás, radioaktív szennyezés | **Sorozatos emberi hibák (tervezési hiányosságok, előírások durva megsértése)** |
| 1987. | Goiania | környezetszennyezés | **Emberi tájékozatlanság** |
| 1999. | Tokai Mura-i uránfeldolgozó | szabályozatlan láncreakciók | **Előírások megsértése** |

## ÖSSZEFOGLALÁS

A cikk az elméleti megközelítésen túl konkrét példákat is mutatott arra, hogy az emberi tényezővel kapcsolatos vizsgálatok és kutatási eredmények felhasználhatók a bioetika egyes területein is, ezáltal segítve az élővilág, az emberiség és a Föld túlélését.

## FELHASZNÁLT IRODALOM


[1] www.zmne.hu/tanszekek/ehc/konferencia/april2001/huszar1.html 2008-01-20

[2] W. Rankin, L. Krichbaum, Human Factors in Aircraft Maintenance, Integration of Recent HRA Developments with Applications to Maintenance in Aircraft and Nuclear Settings, June 8-10, 1998, Seattle, WA, USA.

[3] James Reason & Alan Hobbs: Managing Maintenance Error- A Practical Guide, Ashgate Publishing Company, 2003

[4] James Reason: Managing the Risks of Organizational Accidents, Ashgate Publishing Company, 2004

[5] OAH 3. 11. sz. Útmutató, Verzió száma: 1. 2006. szeptember

[6] NEA (2003): Nuclear Regulatory Challenges Related to Human Performance ISBN: 92-64-02089-6, OECD, Paris

[7] www.matud.iif.hu/06apr/08.html 2008-01-20

[8] Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No.10, Vol. 2, pp. 181-182. Washington, D.C.: U.S. Government Printing Office, 1949

[9] World Medical Association. World Medical Association Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects [Online]. Ferney-Voltaire Cedex, France. www.wma.net/e/policy/b3.htm 2008-01-20

[10] 1999. LXXIV. Törvény (a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről)

[11] Czelnai Rudolf: Tsunami, Természet Világa, 136. évfolyam, 4. szám, 2005. április

[12] Ken Alibek, Stephen Handelmann: Biohalál Ármádia Könyvkiadó 1999. (ISBN 963 85996 5 0)

[13] Juhász László mk. őrnagy, Dr. Huszár András ro. alezredes. Biohalál és bioetika Gondolatok Ken Alibek: Biohalál című könyve kapcsán www.zmne.hu/tanszekek/vegyi/docs/fiatkut/jl0607_2.htm

[14] M. Kolb, P. Langmann, K. Fleischer: A biológiai terrorizmus tüdőgyógyászati szemszögből, Orvostovábbképző Szemle XII. évfolyam, 5. szám (2005)

[15] www.bhopal.com 2008-01-20

[16] www.bhopal.net 2008-01-20

[17] www.zmne.hu/tanszekek/vegyi/personal/Balesetek 2007-03-18

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Kuti Rajmund**
Zrínyi Miklós Nemzetvédelmi Egyetem
r.kuti@vivamail.hu

**Földi László**
Zrínyi Miklós Nemzetvédelmi Egyetem
foldi.laszlo@zmne.hu

# A BEÉPÍTETT VÍZKÖDDEL OLTÓ RENDSZEREK ÚJABB ALKALMAZÁSI LEHETŐSÉGEINEK FELTÁRÁSA

***Absztrakt***

*Az elmúlt években a beépített tűzoltó rendszerek rendkívüli fejlődése tapasztalható a világban. A fejlődés nem kerülheti el hazánkat sem, így nálunk is egyre több új berendezés kerül telepítésre. Ilyen eszközök többek között a stabil vízköddel oltó rendszerek is. Ezek a berendezések a legrégebben használt oltóanyagnak, a víznek speciális felhasználását teszik lehetővé, melyeknek eredményes használatával lecsökken az oltási idő, és gyakorlatilag megszűnnek a másodlagos, úgynevezett vízkárok, melyek több tízmilliós értéket tesznek ki évente „csak" Magyarországon. Ezek az eszközök még nem terjedtek el hazánkban, mindössze pár darab áll szolgálatban. Ezeket a berendezéseket, működési elvüket, felhasználásuk rendkívüli előnyeit mutatjuk be cikkünkben. Ezzel az írással fel kívántuk hívni a figyelmet arra, hogy mekkora szükség van a modern tűzoltó-technika, illetve a környezetbarát anyagok használatára és a szakmailag igényes, alapos és a gyakorlatban is végrehajtható másodlagos károkozás nélküli tűzoltásra.*

*There is a significant development of built-in fire extinguisher systems all over the world in the past few years. This development can clearly be seen also in our country, so more and more up-to-date fire extinguishing equipment has been set up in Hungary. One of these new technologies is the water fog fire extinguisher system. This new equipment uses the special abilities of the oldest fire extinguishing material, water, and in a unique way practically decreases the extinction time, eliminates all the secondary damages emanated from the traditional use, which mean some ten million forints of damages yearly in Hungary. These systems haven't spreaded in our country yet, only few pieces installed and in use currently. We would like to introduce these devices in this paper, their operation principles, and advantages of their use. In addition, we would like to raise attention to the need of modern fire extinguishing equipment,*

*use of environmental friendly material, and the importance of the adequate, professional and practically adoptable extinction methods without causing secondary damages.*

***Kulcsszavak:*** *vízköd, oltóhatás, beépített vízköddel oltó rendszer ~ water fog, extinguishing efficiency, built-in water fog fire extinguisher*

## Bevezető

A XX. század végén fokozatosan előtérbe kerültek a környezetvédelmi szempontok a tűzoltás területén is. Miután a világ államainak többsége elfogadta az ózonromboló gázok korlátozásáról szóló megállapodásokat, új tűzoltási technológiák kutatására, fejlesztésére és gyakorlati bevezetésére került sor az utóbbi években. Így születtek meg a beépített vízködös oltórendszerek, melyek a legrégebben használt oltóanyagnak, a víznek speciális felhasználását teszik lehetővé. Vajon miként lehet a vízzel oltást hatékonyabbá tenni, úgy hogy ne jelentsen veszélyt az emberre, a környezetre, a védett objektumokra, tárgyakra?
A fenti kérdésre próbálunk választ keresni az alábbiakban.

## A víz oltóhatásai, a vízköd jellemzői

Mielőtt rátérnénk a vízköddel oltó berendezések bemutatására, szót kell ejtenünk a víz oltóhatásairól, ugyanis a vízköddel történő oltás során ezek közül egyszerre több is érvényesül.
Az oltóhatás olyan feltételek létrehozása, amelyek megakadályozzák, vagy gátolják az égést és feltételeinek kialakulását. Néhány esetben, ahol a víz, mint oltóanyag használata nem megengedett, a víz legtöbb esetben kiváló oltóanyag. Felhasználásának jelentősége abból adódik, hogy optimális körülmények között egy időben több oltóhatást képes kifejteni. Kísérletek sora bizonyítja, hogy a tűz oltásakor a klasszikus oltóhatások közül a hűtőhatás és a fojtóhatás érvényesül kisebb-nagyobb arányban, de a vízköddel oltásnál fontos megemlíteni az ütőhatást és az inhibíciós oltóhatást is.
Nézzük röviden az oltóhatások lényegét:

### Hűtőhatás:

A hűtőhatást a víz fő oltóhatásának tekintjük. Ez a hatás „Az égő anyag lehűtéséhez szükséges úgy, hogy a tűz fészkében és annak környezetében a hőmérsékletet az égő anyag gyulladáspontja alá csökkentsük”[1], illetve megelőzzük, hogy ezt az értéket elérje.

A hűtőhatást két részre bonthatjuk. Az egyik az égő anyag lángjának hűtése, a másik az égő anyag felületének hűtése. Az első rész a vízcseppeknek a lángzónába való behatolása alatti hőlekötésből áll. Ennek következtében a gyúlékony gázok lehűlnek, a hősugárzás csökken, a tűz továbbterjedése erősen korlátozódik. Így megkönnyíti az utána következő vízcseppek tűzfészekhez való jutását. Az oltóhatás második része az égő anyag hőjének elvonásából áll. Ezt hatékonyan úgy lehet megvalósítani, ha a teljes felületet vízcseppekkel fedjük le.
A lángzónába jutó víz először forráspontig melegszik, majd gőzzé alakul, végül a gőz, a lángzóna hőmérsékletéig melegszik, miközben elhagyja azt. E folyamat során 4760 kJ energiát von el egy kilogramm víz. Fontos megjegyezni, hogy ez csak elméleti érték, a gyakorlatban különféle veszteségek miatt, csak kb. 2200 kJ a kilogrammonként elvont hő.

A víz hőelvonó képességét növelni lehet, ha a zárt víztömeg helyett kisebb vízcseppecskék felhőjét juttatjuk az égő anyagokra. Alkalmazásakor jobban hasznosítható az oltóanyag, a megfelelő nyomáson történő porlasztásnak köszönhetően jelentősen csökkenthető a vízkár és a tűzoltást hatékonyan végre lehet hajtani. A tűzoltó technikai eszközök fejlődésének köszönhetően a vízköddel oltó berendezésekkel manapság az oltáshoz legoptimálisabb vízcseppeket is elő lehet állítani. Az alábbi táblázat a stabil vízzel oltó berendezésekkel, adott mennyiségű vízből előállítható vízcseppek tulajdonságait mutatja be.

*1. sz. táblázat: A stabil vízzel oltó berendezésekkel előállítható vízcseppek tulajdonságai*

| | Cseppméret (átl. µm) | Felület arány | Párolgás (másodperc) | Cseppszám |
|---|---|---|---|---|
| Sprinkler | > 1000 | 1 | 1 | 1 |
| Vízpermet | 300 | 10 | 0,1 | 40 |
| Vízköd | 50 | 400 | 0,003 | 8000 |

A táblázatból kitűnik, hogy ha kisebb mennyiségű vízből több cseppet állítunk elő, nagyobb lesz a fajlagos felület így azonos oltási eredményhez kevesebb víz elég.

### **Fojtóhatás** (kiszorító vagy inertizáló oltóhatás)

A víz elpárolgásakor igen figyelemre méltó a térfogat-növekedés.
A 100 °C-os vízgőz sűrűsége 0,598 kg/m$^3$ .
A víz sűrűsége 10 °C-nál 999,6 kg/m$^3$.
999,9 / 0,598 = 1675, azaz ha 1kg víz elpárolog, térfogata az eredeti térfogat 1675-szöröse lesz, kerekítve 1700-szorosára terjed ki.
A fojtóhatás lényege, hogy a hő hatására a vízből fejlődő vízgőz az éghető, vagy égő anyagot gőzfelhőbe burkolja, és ez által csökkenti a tűzhöz áramló oxigén mennyiségét, az ott lévőt pedig kiszorítja. Ha a vízgőz mennyisége a kb. 35%-ot eléri, az égés megszűnik.
A vízcseppek nagysága is nagyban befolyásolja, hogy a cseppek mennyi ideig képesek a levegőben lebegni, és fojtó hatásukat kifejteni. Ezért az optimális szemcsenagyság meghatározása igen fontos.

### Ütőhatás

A nagy erővel érkező víz, az égő anyagról leszakítja a lángokat és ez által megbontja az égő felületet, a tűzfészket. A kötött sugár szakadásmentes, viszonylag kis átmérőjű és nagy sebességű vízsugár. Nagy ütőerő és nagy hatótávolság jellemzi. A tűz fészkének megbontására alkalmas. Kötött sugarú oltóvíz adagolásnál a víz szinte hatástalanul halad át a lángzónán, ezért gyenge áramú gáztüzek oltására nem alkalmas. Legfontosabb hatása, a hűtőhatás nem tud érvényesülni, mert a tűzzel érintkező vízfelület kicsi és a kontaktidő túl rövid. Ez az oltóhatás a vízköddel oltókra kisebb mértékben jellemző.

### Inhibíciós oltóhatás

Porlasztás hatására a vízmolekulákról ionok válnak le. A keletkező negatív és pozitív töltésű ionok rekombinálódnak[1] az égésben résztvevő ionokkal és szabad gyökökkel. Ezek a rekombinációk megszakítják az égés láncreakcióját. Az inhibíciós oltóhatás a porlasztás függvényében érvényesül, vízköddel oltásnál jelen van.

[1] Az ellentétes töltésű részecskék egyesülése semleges képződménnyé.

Az előbbiek alapján megállapíthatjuk tehát, hogy a vízköddel oltás során előállított finom vízpára a hő hatására az égéshez szükséges három feltételből kettőt (oxigén, égéshő) minimalizál. Megkíméli ugyanakkor a harmadik feltételt, az éghető anyagot, hiszen az éppen a védett objektum!

## Milyen elven működnek a vízköddel oltó rendszerek?

A vízköddel oltó rendszerek definiálása és leírása az egyetlen nemzetközileg elfogadott szabványban az NFPA 750-ben történik. Az NFPA az amerikai tűzvédelmi mérnökök szövetsége, az általuk kiadott szabványok lefedik a tűzoltás valamennyi területét. A vízködös oltórendszerekről ez a szabvány a következőket mondja ki:

"Vízköd rendszer egy vízellátó, illetve vízellátó és atomizáló anyagellátó rendszerhez kapcsolt, tűz ellenőrzése, elnyomása, vagy oltása céljából vízköd kibocsátására alkalmas egy, vagy több szórófejjel felszerelt elosztó hálózat, amely bizonyítottan képes a minősítésének és a szabványoknak megfelelő teljesítmény követelmények kielégítésére”[2].

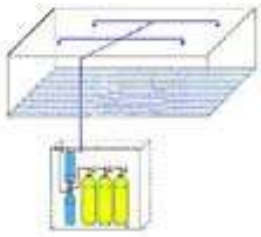
A szabvány szerint kis-, közepes- és nagynyomású vízködös oltórendszereket különböztetünk meg. A kisnyomású rendszerek munkanyomása kisebb, mint 12,5 bar, a közepes nyomású rendszerek nyomástartománya 12,5 és 34,6 bar közé esik, a nagynyomású rendszerek üzemi nyomása pedig nagyobb, mint 34,6 bar [3].

A vízköddel oltó berendezések lényege, hogy a speciális szivattyúkkal, vagy inert gázzal, illetve sűrített levegővel közép, vagy nagynyomású vizet állítanak elő, amelyet speciális fúvókákon átvezetve vízködöt képeznek.

A vízködös rendszerekkel az oltás két fázisban történik. Az első fázis a nagynyomáson előállított vízköd kiváló hőelvonó képességét használja ki. Az apró cseppekre bontott víz nagy felületet alkot, amely elvonja a hőt az égéstől. Ezzel egy időben az apró cseppek megkötik az égés körül kialakuló forró gázokat, megakadályozva ezzel a tűz továbbterjedését. Ez a fázis a tűzelnyomás. A következő fázis az oltás. Ehhez a kis cseppeket elégséges számban be kell juttatni az égéstérbe. A bejutott cseppek, a hő hatására a méretükkel fordítottan arányos idő alatt párolognak el, tehát a kisebb cseppek gyorsabban, a nagyobbak lassabban. A víz párolgásakor vízgőzzé alakul. Az égéstérben bekövetkezett térfogat növekedés kiszorítja az oxigént és ez a fojtó-inertizáló hatás oltja ki a lángot. Az inhibíciós oltóhatás több-kevesebb mértékben mindkét fázisban jelen van.
A nagy lánggal égő tüzek sok oxigént fogyasztanak, az elégetett levegő miatt jelentősebb a gázcsere hatásuk. Ezeknél a nagyobb cseppek is bejutnak az égéstérbe és – ha lassabban is – gőzzé válnak. A gond a kis lánggal égő, vagy alacsonyabb hőmérsékletű tüzek oltásánál jelentkezik. Ekkor az égéshő felhajtó ereje nagyobb a légbeszívó hatásnál és az égéstérbe csak azok a cseppek jutnak, melyek megfelelő mozgási energiával rendelkeznek és legyőzik a felhajtó erőt. A cél, hogy minél kevesebb vízzel oltsunk. Ehhez gyorsan párolgó kis cseppek nagyszámú jelenléte szükséges, de hogy a kis tömegű cseppek megfelelő energiával rendelkezzenek, a sebességüket meg kell növelni. A hatékony vízködös rendszerek a szórófejnél létrehozott nagy nyomással „lövik be” a cseppeket a lángtérbe. A vízköddel oltó berendezések mobil és stabil kivitelben készülnek. Jelen írásban csak a stabil vízköddel oltókkal, azon belül is a legelterjedtebb nagynyomású berendezésekkel foglalkozunk.

## A nagynyomású stabil vízköddel oltók jellemzői, felhasználási lehetőségeik

A nagynyomású vízköddel oltó rendszer a tiszta (szűrt) vizet alakítja át finom köddé 80-200 bar közötti nyomáson. A stabil vízköddel oltó berendezések esetében a nagynyomású víz előállítása kétféle módon történhet. Az egyik lehetőség a nagynyomású inert gáznak (nitrogén), vagy sűrített levegőnek, mint meghajtó anyagoknak a vízbe vezetése. Az alábbi ábrán a gázzal működtetett vízköddel oltó rendszer látható.



*1. sz. ábra: A gázzal működtetett vízköddel oltó rendszer*

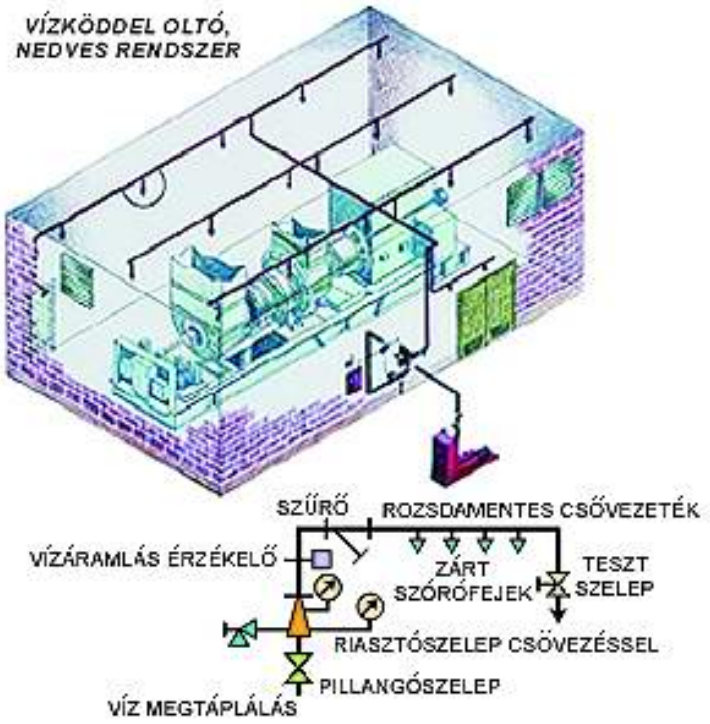
A másik megoldás, a külső energiaforrástól teljesen független gázhajtású, vagy dízelmotoros speciális szivattyúkkal, illetve külső energiaforrástól függő elektromos szivattyúkkal. A szivattyúk 25-800 l/perc teljesítménnyel dolgoznak, a rendszer méretét optimálisan lehet alakítani. A következő ábrán egy dieselmotoros szivattyú látható.


*2. sz. ábra: Dieselmotoros szivattyú*

A víz magas nyomáson történő porlasztása azt eredményezi, hogy a hűtőfelület lényegesen nagyobb, mint a hagyományos, pl. sprinkler rendszerekben. Ez az erős hűtőhatás nem csak a tűzoltásban előnyös, hanem azért is, mert elvonja a sugárzó hőt, így óvja az ott tartózkodó személyeket és vagyontárgyakat. A vízködpajzs hatékonyan védi az épületszerkezetet, falakat, ajtókat, homlokzatokat. Az elpárolgó ködcseppek az oxigént is eltávolítják a tűztől. Előnyei a többi berendezéshez képest: környezetbarát, emberre veszélytelen, egyenletes, választható ködcseppméret, kisebb vízmennyiség is hatékonyan olt, a vízkár szinte elenyésző, egyszerű felépítés, könnyű telepíthetőség, a rendszertechnika helyigénye igen csekély, füstelnyelési képesség nagy, elektromos helyiségekhez is alkalmazható.

Hátránya: a nagynyomású berendezések drágábbak, ezáltal az üzemeltetés költségei is nőnek, nagyobb tűzterhelések esetén kevésbé hatékony, mert az intenzív huzat, a gázcsere elviszi a vízködöt, megszüntetheti az oltóhatást.

A következő ábrán egy stabil vízköddel oltó rendszer felépítése látható.




*3.sz. ábra: Beépített vízköddel oltó rendszer felépítése*

A berendezések alkalmazása hazánkban még gyerekcipőben jár, mindössze néhány helyre került beépítésre hasonló rendszer, azonban tőlünk nyugatabbra rendkívül széles körben terjedtek el.
Felhasználási lehetőségeik a következők lehetnek.

- Műemlék épületek, múzeumok, levéltárak;
- Számítógépközpontok, elektronikus adatfeldolgozó és szerverszobák;
- Kábelcsatornák védelme;
- Ipari alkalmazások, dizel aggregátok, gázturbinák, különféle forgácsoló gépek védelme;
- Konyhák, ipari olajsütő berendezések védelme;
- Laboratóriumok;
- TV stúdiók;
- Hajók, tengeri olajfúró berendezések védelme;
- Alagutak védelme.

A fentiekből kitűnik, hogy a berendezések rendkívül széles körben, az ipartól kezdve szinte a gazdaság minden területén felhasználhatóak és kutatások folynak további felhasználási lehetőségek után.

## Összegzés

A környezetbarát, gyors, hatékony, vízkármentes, káros élettani hatás nélküli oltás rendkívüli előnyeivel rendelkező vízköddel oltó berendezések előtt óriási jövő áll. A fejlesztés és megvalósítás területén már több magyar cég is komoly eredményeket ért el.
A vízköddel oltó berendezések új megoldást kínálnak a tűzvédelemben, a gázzal oltó és sprinkler rendszerek pozitív tulajdonságait összesítve.

Reményeink szerint sikerül felhívnunk a figyelmet a berendezések rendkívüli előnyeire és hozzájárulhatunk ennek a környezetbarát, gazdaságos oltási technika elterjedéséhez hazánkban.

## Felhasznált Irodalom


1. Kuncz Imre: A tűz és oltóanyagai BM Könyvkiadó, Budapest 1976, 124. p.
2. NFPA 750 Szabvány, USA
3. Nádor András: Vízködös oltórendszerek - nem árt ismerni, mit miért választunk http://www.vedelem.hu/tanulmanyok

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Nagy Rudolf**
Zrínyi Miklós Nemzetvédelmi Egyetem
rudolf.nagy@katved.hu

**Halász László**
Zrínyi Miklós Nemzetvédelmi Egyetem
halasz.laszlo@zmne.hu

# MONITORING ÉS LAKOSSÁGI RIASZTÓ RENDSZER ÉS A KRITIKUS INFRASTRUKTÚRA-VÉDELEM ÖSSZEFÜGGÉSEI

***Absztrakt***

*A lakosságvédelem mint a következménykezelés egy kiemelt szegmense igen szorosan kötődik a monitoring-rendszerekhez. Nem képzelhető el tehát olyan veszélyes létesítmény, amelynél a környező települések védelme megfelelően realizálódhat a lakosság tájékoztatását szolgáló eszközök, illetőleg a veszély jelenlétét azonosítani képes ellenőrző rendszerek hiányában. Feltételezhetően ehhez hasonlóan lehet a kritikus infrastruktúra-védelem érdekében majdan felállítandó környezeti ellenőrző rendszerek működését, szerepét is meghatározni. Ezért kívánja a szerző ráirányítani az olvasó figyelmét a SEVESO létesítmények környezetében kiépítendő MoLaRi rendszer és létfontosságú infrastruktúrák védelmének kapcsolódási pontjaira.*

*Protection of the population as one of the main segments of consequence management is strongly connected to the monitoring system. Therefore the realisation of the adequate protection of the settlements around dangerous institutions can not be imagined without the means of public information and the systems capable of identifying the presence of danger. Supposable the definition of the role and function of the environmental monitoring system to be established for critical infrastructure protection can be similar to that. That is why the author would like to focus the readers' attention to the connection points between the critical infrastructure protection and the MoLaRi-system to be established around SEVESO institutions.*

***Kulcsszavak:*** *kritikus infrastuktúra-védelem, következmény-kezelés, biztonsági irányítási rendszer, monitoring rendszer, lakosság-tájékoztatás ~ critical infrastructure protection, consequence management, safety management system, monitoring system, public information*

## Bevezető

Az Országos Katasztrófavédelmi Főigazgatóság (OKF) koordinálása mellett kidolgozott Kritikus Infrastruktúra Védelem Nemzeti Programjának Korány által határozatban történő jóváhagyása új fázis kezdetét jelenti valamennyi érintett szakmai feladataiban. Az eddigi szakmai elemzéseinkre támaszkodva úgy vélem a hivatásos katasztrófavédelmi szervek létfontosságú infrastruktúra-elemek kapcsán kidolgozandó megelőzési és reagálási eljárásainak fókuszában az üzemzavarok lakosságvédelmi következményeinek kezelése kell, hogy álljon.

A fentiekből kiindulva jelen közleményben a kritikus infrastruktúra körébe tartozó veszélyes ipari létesítmények súlyos baleseti hatásai hatékony kezelését - az OKF üzemeltetésében - támogató Monitoring és Lakossági Riasztó (MoLaRi) rendszer ezen szerepét és a kialakítása követelményeiben e szempontból meghatározó tényezőket kívánom az érdeklődők elé tárni, elkerülendő azonban a reagálás egyéb szakmai összefüggéseinek mélyreható elemzését.

A kritikus infrastruktúra és védelmének kérdése az utóbbi időben egyre gyakrabban vetődik fel szakmai, és tudományos körökben. Újszerű, kissé talán rejtélyesen hangzó elnevezése - az infrastruktúrák idesorolható részének - sokakban, olykor még az elsődlegesen nyelvi előképzettségüknek köszönhetően nemzetközi téren ezzel mélyrehatóbban foglalkozókban is valamiféle különleges, eddig soha nem látott dolog képzetét ébresztik. Elég azonban a védelmi igazgatásban jártas, nagy tapasztalatú szakemberekkel csak néhány szót váltani a témáról és máris feltárul előttünk a tény, miszerint bizony nem is olyan új keletű ez a fogalom.

Meggyőződhetünk erről, ha felütjük a Hadtudományi Lexikont az *állóképesség*ére vonatkozó címszónál, és figyelmesen áttanulmányozzuk az ott leírtakat. Igaz ugyan, hogy ellenséges támadásról illetve ipari és természeti katasztrófák közvetlen és másodlagos hatásaival szembeni ellenálló képességről olvashatunk, de egyebek mellett itt is az állam, a lakosság számára létfontosságú üzemek, gazdálkodó szervezetek működőképességének megőrzése a cél a megelőzés eszköztárának kiaknázásával és védelmi intézkedések bevezetésével. [1]

Összevetve a fentebb említetteket a kritikus infrastruktúra védelmének (továbbiakban: KIV) Amerikai Egyesült Államok beli koncepcióját megalapozó első hívatalos dokumentumban rögzítettekkel, jelentős hasonlóságokat fedezhetünk fel.

A Clinton elnök által 1996-ban aláírt 1301012 számú elnöki rendelettel állították fel a KIV-ért felelős Elnöki bizottságot. Az e testület általi értelmezés alapján ide soroljuk az „Adott nemzeti infrastruktúrákat, amelyek olyan mértékben létfontosságúak, hogy működésképtelenné válásuk vagy megsemmisülésük az Egyesült Államok védelmi képességének vagy gazdasági potenciáljának gyengülését okozhatja.” [2]

A NATO Polgári Védelmi Bizottsága szerint például e fogalomkör *„Azokat a létesítményeket, szolgáltatásokat és információs rendszereket jelenti, amelyek olyan létfontosságúak a nemzetek számára, hogy működésképtelenné válásuknak vagy megsemmisülésüknek gyengítő hatása lenne a nemzet biztonságára, a nemzetgazdaságra, a közegészségre, a közbiztonságra és a kormány hatékony működésére.”* [3]

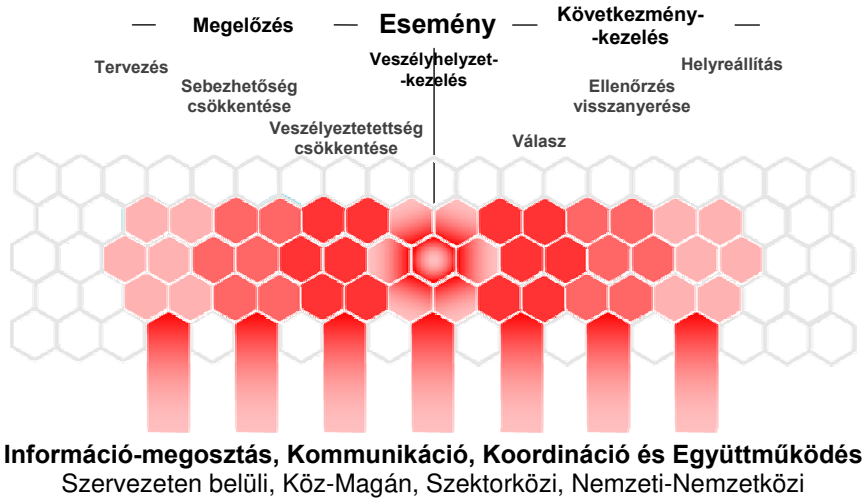
A Közösség dokumentumaiban szinonim kifejezésként használt létfontosságú infrastruktúrák definíciója alapján ezek „*olyan eszközök, vagy azok részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, ideértve az ellátási láncot, az egészségügyet, a biztonságot, valamint az emberek gazdasági és társadalmi jólétét is”*. [4]

## A következménykezelés jelentősége a kritikus infrastruktúra-védelemben

A kritikus infrastruktúrák tehát a modern társadalom létfeltételét képezik. Ebből kiindulva megfogalmazhatjuk a védelmük érdekében végzett tevékenység, a KIV-ének célját is. Miért látom ennek szükségét: tehetjük fel a kérdést.

Az utóbbi időben az infrastruktúrák vonatkozásában jelentkező biztonsági kihívások intenzív nemzetközi válaszlépések megtételére sarkallta az Európai Unió döntéshozóit és érintett intézményeit. A megszülető elvek a nemzeti szinten alkalmazott eljárásokra építve szándékozik egységes fellépést megvalósítani. Ez a folyamat gyakorlati eredményeket hozó szakaszba terelte az eddigi hazai, jórészt csak elméleti síkon folyó gondolkodást.

Az OKF aktív szerepvállalásával több szakmai fórumon felvetődött a KIV fogalmának hazai értelmezése. Némelyek szerint a KIV, csupán magának a vizsgált infrastruktúrának a létét, működését hivatott garantálni és nem tartozik e kérdéskörbe a szolgáltatás-kiesés jelentette következmények kezelése. Azonban a rendszerszemléletű megközelítést valló, tapasztalt szakemberek egyetértenek abban, hogy a cél meghatározza a feladatok körét is, és ehhez megkerülhetetlenül hozzátartozik a bekövetkezett üzemzavarok, sérülések hatásainak a kezelése is. Jól szemlélteti ezt a védelmi feladatok ütemezésének - a NATO Felsőszintű Polgári Veszélyhelyzeti Tervezési Bizottsága (SCEPC) megbízásából a KIV koncepcióját 2003-ban kidolgozó - NATO Polgári Védelmi Bizottsága (CPC) által történő felvázolása. Ezt mutatja be az 1. számú ábra.




1. ábra
Fázisok a kritikus infrastruktúra-védelemi intézkedésekben [5]

Leszögezhető tehát, hogy a létfontosságú infrastruktúrák védelmében nem az adott hálózat, rendszer működésének káros behatásoktól való önmagáért való megóvása a cél, hanem az általa betöltött funkciónak a társadalom számára történő biztosítása. Jól rávilágít erre, ha a figyelmünket egyes veszélyhelyzetek, krízis szituációk vagy technológiai zavarok esetén a kiesett szegmens pótlására tervezett másodlagos tartalékforrásokra, illetve alkalmazott szükségmegoldásokra irányítjuk. Hisz ennek kapcsán, a hiányzó szolgáltatás, erőforrás rendelkezésre állásának a fenntarthatóságát kell elérni.

Példaként említhetjük a mobil vízellátó egységeket, amelyek az ivóvízhálózat hibájából eredő ellátási gondok ideiglenes megszüntetésére hívatottak. Ez is jelzi, hogy a hasonló következmények kezelésére készülni kell a KIV területén. Persze ez az érintett üzemeltetők, tulajdono-

sok számára, akik elsődleges felelősségükből adódóan a gyakorlatban találkoznak ezekkel a problémákkal - és nem csak az író-, tárgyalóasztal mellett frissen szerzett ismeretek birtokában, avagy a szakmai elveket valamiféle prekoncepciótól vezérelve figyelmen kívül hagyva keresik a „helyes" módszereket – nyilvánvaló csakúgy, mint a védelmi szféra és abban is kiemelten a lakosságvédelemére hivatott OKF szakemberei számára.

A *kritikus infrastruktúra védelmének célja* tehát a fentiekből kikövetkeztethető módon nem más, mint:

- ~ a mutatkozó működési zavar vagy fizikai károsodás megelőzésére, elhárítására való felkészülés, illetve
- ~ a sérülés bekövetkeztekor a káros hatások csökkentése, a sérült szegmensek működésének helyreállítása. [6]

E megállapítások fényében keresve választ az alapkérdésre, a *kritikus infrastruktúra védelme*, mint *az ország mindennapi életkörülményeinek fenntartását, így az állam, a gazdaság szereplői, valamint a lakosság részéről jelentkező igények biztosításához szükséges létfontosságú infrastruktúrák lehető legnagyobb biztonsággal és magas fokú koordináció mellett történő működtetésének megvalósítását szolgáló intézkedések összessége* fogalmazható meg.

Visszautalva a bevezetőben használt terminológia szerinti állóképesség fogalmára, tartalmára és összevetve azt az előző bekezdés lényegi mondanivalójával látható, hogy a jelenlegi megközelítés jelentős eltéréseket is mutat. Ezek pedig nem elsősorban a társadalmi-gazdasági berendezkedés hozta változásokra értendők. Sokkal fontosabb, hogy a rendelkezésre állás biztosításának nem elsősorban a minősített időszakok jelentette helyzetben kialakuló szükségességét hangsúlyozza, hanem a mindennapok létfeltételeiről szól.

**a.)** E látásmód helyénvalónak ítélhető, ha vizsgáljuk a globális biztonságpolitikai kihívások:

~ kábítószer-kereskedelem;
~ nemzetközi terrorizmus;
~ nemzetközi szervezett bűnözés;
~ vallási, etnikai ellentétek;
~ túlnépesedés;
~ környezetszennyezés;
~ civilizációs és természeti katasztrófák;
~ migráció

modern társadalomat érintő veszélyeit. Kitűnhet ezekből, hogy többségük oly módon léphet elő veszélyhelyzet előídézőjévé, hogy közben minősített helyzet kihirdetésére nem kerül sor. Ez adódhat a jogszabályi feltételek hiányából vagy a rendkívüli jogrend kínálta plusz erőforrások, különleges eljárási mechanizmusok szükségtelen voltából.

**b.)** Eltérés még, hogy új infrastruktúrákat nevez meg, mint a bankszektor, info-, és telekommunikációs rendszerek. A sajátos technikai, illetve technológiai környezet ezeknél már nem teszi lehetővé a hagyományos válaszintézkedésekkel történő hatékony ellenállás kifejtését a nem kívánt eseményekkel szemben, legfeljebb csak az új eljárások kiegészítésében kaphatnak szerepet. E tekintetben még egy dolog nagyon fontos. Ezek a rendszerek bizony azok közé tartoznak, amelyek mindenféle előzmény nélkül és megdöbbentően nagyszámú véletlen, de leginkább szándékosan generált veszélyeztető behatással kell, hogy megbirkózzanak. A közelmúlt Észtország béli eseményei (a túlterhelt infokommunikáció lebénította az erre épülő többi rendszert is) is igazolásul szolgálhatnak erre, és bizony minősített helyzet bevezetése ezek kapcsán nem is igen képzelhető el.

**c.)** A szakemberek számára is meglehetősen komoly fejtörést okozó tényező az infrastruktúrák kölcsönhatása. A rendszerek és a hálózatok olyannyira egymásba fonódnak, hogy működésük összehangolása illetőleg egymásra gyakorolt hatásuk elemzése nélkül bizony ki-

terjedt, súlyos következményekre kell felkészülnünk még a társadalmi kihatásokat is ideértve. Példa erre az utóbbi években az Amerikai Egyesült Államokat illetve Európát sötétbe borító villamosenergia-ellátó rendszer zavara.

Elkerülhetetlen tehát az ez irányú intézkedések összehangolása, és persze nemcsak egy-egy létesítmény vagy hálózat üzemeltetőjének felelősségi körében, de a közigazgatás és a magánszféra, a szektorfelelős ágazatok között, illetve nemzetközi szinten is. Összhang megteremtése értelemszerűen csak ott lehetséges, ahol ennek valamilyen paralel kapcsolódási lehetősége megvan. Másik lényeges eleme a jól funkcionáló hálózat létrehozásának az alulról történő építkezés. Különösen igaz ez a tagállami szintet nézve az Európai Unióban.

A *szabályozás a létfontosságú infrastruktúrákkal kapcsolatos tevékenység terén* hazánkban akárcsak az Európai Unió tagállamainak többségében *jelenleg hiányzik a jogrendszerből*, ahogy napjainkig az Európai Uniónak jogrendszerében sem került meghatározásra ez a feladatkör.

A 2004. évi madridi terrortámadásosokat követően az Európai Tanács a kritikus infrastruktúrák védelmét szolgáló átfogó stratégia kialakítására kérte fel a Bizottságot. Ennek keretében a Bizottság előbb közleményt fogadott el „A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben" címmel, majd Zöld Könyvben fogalmazta meg a Kritikus Infrastruktúra Védelem Európai Programjának (EPCIP) általános célkitűzésit. [7]

Közösségi szinten megkezdődött az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló tanácsi irányelv kidolgozása. A Közösség célkitűzése szerint ez az irányelv a fontos infrastruktúrák védelmét célzó meglévő nemzeti programok kiegészítésére szolgál. Ahhoz, hogy ez így legyen Magyarországon is, hazánknak el kell fogadnia a saját nemzeti programját.

Hazánk kritikus infrastruktúra védelmének átfogó rendszere – összhangban az EU több tagállamát érintő infrastruktúrák védelmének megközelítésével – csak valamennyi veszélyforrás és azok kockázatainak számbavételével alakítható ki. Ez - akárcsak a katasztrófák bekövetkeztekor - kockázatelemzésen kell, hogy alapuljon. Szükséges ezért *a védelem integrált megközelítése az összveszélyeztetettség szemléletével*. Az *OKF a KIV Nemzeti Programja kimunkálásának tevőleges résztvevőjeként és első helyi felelőseként* is ezen elvek érvényre juttatásával *igyekszik megteremteni a* Közösség várhatóan hamarosan megszülető KIV programjához, továbbá a kritikus infrastruktúrák európai figyelmeztető és információs hálózatához (CIWIN) történő *kapcsolódás feltételeit*.

A kritikus infrastruktúrák védelméről szóló nemzeti program kiemelt jelentőséget tulajdonít a megelőzés, felkészülés illetve a következmény kezelés végrehajtásának. A terrorcselekmények prioritása mellett a hazai kritikus infrastruktúra védelem valamennyi veszélyforrást számításba veszi, ezért a Kormányzati Koordinációs Bizottság (KKB) 2003. óta végzett veszélyhelyzet-kezeléssel kapcsolatos tevékenységét továbbra is célszerű folytatni.

## Monitoring rendszerek szerepe a védelmi intézkedések bevezetésében

Az egyes veszélyes átalakulási folyamatok megkerülhetetlen beiktatásával üzemelő vagy adott rendkívüli helyzetben súlyos környezeti kockázatot magában rejtő, különleges fizikai paraméterek mellett működő létesítmények *üzembiztonságának megteremtése* szigorú üzemeltetési szabályok betartását, illetőleg műszaki paraméterek megtartását garantáló ellenőrző és riasztó rendszerek meglétét indokolja.

Az ezen folyamatokat kísérő kockázatok egy része az alkalmazott technológia üzemviteli eltéréseiből és a felhasznált anyagok esetleges változásaiból adódóan kisebb zavarokat eredményezhetnek. Ezek olyan események, melyeknél a kezelőszemélyzet a folyamatot továbbra is

teljes biztonsággal irányítani tudja, illetve azok elhárítására is képes az élet- és vagyonbiztonság veszélyeztetése és külső segítség nélkül. Az ehhez szükséges intézkedéseket a technológiai, illetve kezelési utasításban rögzítik, ezekre az érintetteket felkészítik. A kisebb üzemzavar – bár nem kívánatos – elég gyakorinak mondható, ezért nem tekinthető rendkívüli eseménynek. [8]

Ugyanakkor az ilyen jellegű történések sem mindig kezelhetők a monitoring rendszerek folytonos éber felügyelete hiányában, mert ezek némelyike a beavatkozás tartós elmaradása okán kezelhetetlen kiterjedt rendkívüli eseménnyé fajulhat. Ahhoz, hogy ne kelljen tétlen szemlélőként és a környezet kiszolgáltatottságának tudatában - a következmények kedvező alakulásában bízva - figyelnünk a fejleményeket, megfelelő balesetelhárítási struktúrát kell felállítani. Ez az úgynevezett biztonsági irányítási rendszer, a benne foglaltatott funkcionális elemekkel és infrastruktúrával - köztük a monitoring rendszerekkel - felelős a rendkívüli események[1] kezeléséért.

A kockázatelemzések megmutatják, hogy egy bekövetkező rendkívüli esemény során szükségessé váló veszélyhelyzet-, és következmény-kezelése a *biztonsági irányítási rendszer* részéről, milyen képességeket és kapacitásokat igényel. A védelemnek a beépített berendezések legalább olyan fontos részei, mint a kárelhárító szervezetek. [9] Paramétereik együtt alapozzák meg a beavatkozás milyenségét és döntik el, hogy a biztonsági irányítási rendszer eséllyel tud-e szembenézni a veszéllyel.

A megfelelő erőforrásokkal rendelkező biztonsági irányítási rendszer eredményes fellépésének záloga a szükséges *időelőny* és a *hiteles információ* megléte. Ennek elérésében és generálásában jutnak szerephez a monitoring rendszerek. Ezek e funkcióik betöltése révén válnak a kritikus infrastruktúra részévé, hiszen mára már olyan komoly infokommunikációs rendszerekként garantálják az üzemfolytonosságot és a rendszerfelügyeletet, ami a biztonság különféle dimenzióiban létfontosságú. A *monitoring rendszerek* az informatikai hálózatok mellett a másik olyan technológia, amely átfogja a kritikus infrastruktúrák nagy részét. Emiatt komoly figyelmet szentelnek az energetikában, a vízgazdálkodásban, a közlekedésben és a vegyiparban alkalmazott monitoringrendszereknek. [10]

Az egyes a szektorokban az üzemfolytonosságban beálló veszélyes helyzetek kapcsán a gyors beavatkozás csak akkor kecsegtethet pozitív eredménnyel - feltételezve a szakértelem meglétét és operatív alkalmazásának képességét - ha az az elháríthatatlan esemény bekövetkeztéig rendelkezésre álló időn belül megtörténik.

Szakaszokra bontva egy baleseti folyamatot láthatjuk, hogy az események láncolatában elsőként az *érzékelés* az, amely elindítja az egymást követő lépések sorozatát. Itt már mutatkozhat némi időveszteség, ha a változások detektálása valamiféle integrálási eljárás vagy szakaszos működés eredménye, amennyiben a szenzor kiesésével nem számolunk. Gondolhatná bárki: Hisz akkor egyszerű a megoldás folyamatos működésű, valósidejű információt generáló eszközöket kell alkalmazni. Ez valóban nagyban megkönnyítené az érzékelés kérdését, azonban sok olyan meghatározandó paraméter lehetséges, amelyek értelmezése csak valamely más egységhez viszonyítva lehetséges. Ilyenek lehetnek például a gyakoriságra, az eloszlásra vagy az elnyelődésre utaló mutatók. Érthető tehát, ha rögzítjük ennek az időveszteség kalkulálásának szükségességét. Megjegyzendő, hogy a legoptimálisabb érzékelési feltételek mellett is jelentkezhetnek, illetve jelentkeznek olyan kiiktathatatlan tényezők, mint a folyamatokat kísérő tehetetlenség általi, vagy az érzékenység jelentete

[1] Tóth Tamás – Tóth Szabó József szerint [8], 179 oldal: Rendkívüli eseményen értjük azt a hírtelen fellépő, váratlan, ismert vagy ismeretlen eredetű eseményt, amely már a keletkezése pillanatában vagy a későbbiek során olyan súlyos lehet, hogy: a helyszínen lévő kezelő-személyzet nem tudja a helyzetet befolyásolni, az esemény veszélyezteti a kezelő, illetve a mentő személyzet testi épségét; az esemény az adott berendezésekben jelentős anyagi károkat okoz, vagy ilyen károk keletkezhetnek; egy vagy több személy súlyos, életveszélyes vagy halálos sérülését okozza.

késleltetés. Mindemellett az érzékelők által rögzített *adatok feldolgozásához*, valamint az így keletkezett információk továbbításához szükséges idővel is számolni kell, amikor az ellenintézkedések megtételére rendelkezésre álló időt kívánjuk meghatározni.

A legritkább esetben fordul elő, hogy a beavatkozó erők és eszközök települési helye, elhelyezése egybeesik a beavatkozást kívánó esemény bekövetkezésének helyével. Ezért az időszámvetésekben az erőforrások riasztására, mobilizálására, kárhelyre történő kijuttatására és beavatkozására is időt kell biztosítani. Ha tehát mindezen időveszteségek ellenére van még némi idő, amely az eszkalációig rendelkezésre áll, úgy lehetőség van az ellenőrzés visszanyerésére.

Az időelőny megszerzése mellett a *pontos helyezetkép* alkotása is nélkülözhetetlen, mert térben és időben, illetőleg minőségében, mennyiségében azonosított információk birtokában lehet csak szakmailag megalapozott operatív intézkedéseket hozni. A nagy érzékenységű, megfelelő specifikációval és infokommunikációs képességgel rendelkező korszerű monitoring rendszereknek rendeltetésűk szerint ezen igények kiszolgálásának is eleget kell tenniük.

A veszélyek érzékelése és az azokról megbízható adatokat szolgáltató funkcionális egységek mellett a biztonsági irányítási rendszernek - mint azt a működési mechanizmusának vázlatos áttekintéséből láthattuk - a hatékonyság növelése és ez által az elháríthatatlan környezeti veszélyek csökkentése céljából részét kell képezzék a riasztást és tájékoztatást megvalósító elemeknek is.

A *riasztás és tájékoztatás* feladatai szoros összefüggést mutatnak, mivel az előbbi csak egy a felkészítési folyamat egymásra épülő ismereteinek elsajátítását követően begyakorlott tevékenység végrehajtására hív fel. A riasztás azt jelenti, hogy az érintettek a riasztás (szervezeti és technikai) rendszere útján információkat kapnak a fenyegető veszélyekről. Azonban az általános metódusok alapján végzett feladatok nem minden esetben elégítik ki az aktuálisan kialakuló helyzet által diktált elvárásokat. Az adaptált eljárások, magatartási formák eléréséhez szükség van a részletes tájékoztatásra, melyben meghatározzák a helyzettől függő teendőket. [11]

A Nemzeti Katasztrófavédelmi Stratégia[2] céljainak elérését szolgáló MoLaRi rendszer integrálva magába az ezirányú képességek kialakítását célzó törekvéseket, eredményesen járul hozzá veszélyhelyzet-kezelés, reagálás és beavatkozás feltételeinek javításához. A hivatásos katasztrófavédelem szakmai felelősségében továbbfejlesztendő monitoring rendszer a hazai ökológiai infrastruktúra[3] átalakulásának tekintetében is jelentős.

Komoly szerepet játszik a területfejlesztés egyik legfontosabb célja, a megfelelő életminőséghez szükséges környezeti állapotjellemzők fenntartásában és javításában. Különösen a környezett havária jellegű szennyezésével veszélyeztetett térségekhez tartozó SEVESO II. irányelv hatálya alá eső veszélyes ipari üzemek körzetében. Megjegyzendő azonban, hogy e monitoring rendszer elsődleges feladata azanban a lakosságvédelem kiszolgálása.

## A MoLaRi rendszer szerepe a külső védelmi feladatok megalapozásában

A KKB 2007. I. félévi rendes ülésén elfogadta az OKF főigazgatójának beszámolóját a kriti-

[2] A Tervezet a szükséges szakmai és közigazgatási eljárások folyamán minden fórumon támogatást kapott, hatályba léptetése azonban jogtechnikai akadályok miatt várat magára.

[3] VÁTI Magyar Regionális Fejlesztési és Urbanisztikai Kht., Az infrastruktúra szerepe a területi fejlődésben, a térszerkezet és az infrastruktúra fogalmai, [12], 25. oldal:
Dr. Kőszegfalvi György felosztási rendszerét alapul véve a települések természeti és művi környezetéhez kapcsolódó infrastruktúrákat jelenti.

kus infrastruktúra védelem hazai helyzetéről, valamint jóváhagyta a további feladatokra vonatkozó javaslatokat. A feladatok megvalósulásának folyamatában első jelentős eredményként 2007. júliusában elkészült a kritikus infrastruktúrák védelméről szóló Nemzeti Programot (továbbiakban: KIVNP) megalapozó hazai Zöld Könyv. E dokumentum összhangban a EPCIP-nak általános célkitűzéseivel a központi államigazgatási szervek feladatának tekinti - a védelem nemzeti keretjogszabályon és programon nyugvó feltételének kialakításaként - az *üzemeltetői biztonsági terv* hatósági jóváhagyását. [13]

Az EPCIP az *állandó biztonsági intézkedések* nélkülözhetetlen eszközének tekinti azon technikai rendszereket, amelyek egyebek mellett, el kell lássák a monitoring, riasztási és tájékoztatási funkciókat. [7]

Lévén, hogy az *alsó és felső küszöbértékű veszélyes ipari üzemek* valamennyi, eddig napvilágot látott elemzés alapján részét képezik a kritikus infrastruktúrának. Ezért várhatóan az ilyen üzemek esetében az OKF a lakosság és a környezet magas fokú védelme érdekében továbbra is köteles lesz ellenőrizni az üzemeltetői biztonsági terv monitoring, riasztási és tájékoztatási feladatait érintő tartalmának megvalósulását. Minden bizonnyal a KIVNP-ban meghatározott feladatok realizálásában majdani ágazati felelősséggel bíró más központi államigazgatási szervek részére is hasznosak lesznek a veszélyes ipari üzemek környezetében kiépítendő MoLaRi rendszer üzemeltetési tapasztalatai. *Jelentősége* mindenekelőtt a súlyos következményekkel járó eseménysorok *megelőzésében*, illetőleg a *következmény-kezelés* terén kiemelkedő.

A megelőzés céljait elsősorban a kockázatokra és a súlyos baleseti eseménysorokra kiterjedő felkészülés feladatai végrehajtása és a műszaki biztonsági követelmények maradéktalan teljesítése szolgálják. Az üzemeltető felelősségi körében összeállítandó védelmi tervek, a rendszerbeállított veszélyhelyzeti beavatkozó és riasztó eszközök, illetve rendszeres ellenőrzésük lehetőséget adnak az esetlegesen bekövetkező balesetek keltette veszélyek mérséklésére, leküzdésére és kezelésére. A *belső védelmi terv*ben[4] szereplők *végrehajtására rendeltetett* szervezetrendszer a *biztonsági irányítási rendszer*, amely egyébként szorosan kötődik az alaptevékenység irányítási struktúrájához, megelőzve a vezetés hatékonyságát rontó - az esetleges feladat-, és hatásköri nézeteltérésekből fakadó - tisztázatlan irányítási kérdések felmerülését. A jogalkotó szándékával is egyező elv a vonatkozó norma [15] 1. mellékletének 1.9.2. pontjában is rögzítésre került: „Az üzemeltető a biztonsági irányítási rendszert beépíti a veszélyes ipari üzem általános vezetési rendszerébe."

A *biztonsággal kapcsolatos irányítás* a *kockázat megállapítását*, valamint az adott *kockázat* meghatározott szintű *csökkentésére* irányuló *intézkedések meghozatalát* és *végrehajtását foglalja magában*. Krízishelyzetben, amíg a súlyos üzemzavar okozta nem kívánt következmények az üzemeltető által felügyelt infrastruktúrális rendszeren kívül nem éreztetik hatásukat, addig az elsődleges beavatkozást az üzemeltető által szervezett biztonsági irányítási rendszernek kell végrehajtania. Ehhez a kockázatot jelentő tényezők és az azt befolyásoló körülmények megállapítását, mérését és ellenőrzését végző rendszer - mint amilyen a MoLaRi is - nem nélkülözhető.

A monitoring rendszerek által szolgáltatott információk felhasználhatósága nem csak a korábban már részletezett elvi funkciók megvalósítását biztosító műszaki paraméterektől függ. A rendszer stacioner részeinek felállítása megköveteli a telepítés tervezett helyszínének összevetését a veszélyanalízis alapján kapott kockázatra vonatkozó értékekkel és az ott uralkodó átla-

[4] 1999. évi LXXIV. Törvény [14] 3. § a) bekezdés:
A veszélyes anyagokkal kapcsolatos súlyos balesetek kialakulásának megelőzését, a balesetek elhárítását, következményeinek mérséklését szolgáló intézkedések megtételét, az értesítési, riasztási, felkészítési feladatok veszélyes ipari üzemen, veszélyes létesítményen belüli végrehajtásának rendjét, feltételeit szabályozó üzemeltetői okmány.

gos környezeti feltételekkel. A MoLaRi rendszer eddig létesített részegységei[5] is ezen általános elvi, szakmai és ebből eredeztethető műszaki követelmények figyelembe vételével kerültek rendszerbe állításra.

E rendszernek az érintett létesítményre adoptált, szakmai szempontok érvényesítését szolgáló eszköze az úgynevezett *üzemi monitorozási terv*.

**a.)** A katasztrófavédelmi feladatoknak e problémakörhöz köthető szegmensében a leglényegesebb tartalmi elemek az alábbiak:

~ létesítmény és környezete;
~ az abban felhasznált anyagok;
~ rangsorolt hatásterületek;
~ veszélyes anyagok terjedési tulajdonságai;
~ monitoring végpontok telepítési helyeinek diszlokációja,

amelyeket meg kell jeleníteni az üzemi monitorozási tervben is.

A lakosság védelmét igénylő veszélyhelyzetekben az információszükséglet kielégítésére és a megfelelő automatizmusok beindítására szolgáló rendszer *elvárt műszaki, létesítési követelményei* - a fentiekben említett tervek tartalma által is befolyásolva - a következők:

~ az érzékelők jelzési és riasztási szintjeinek követniük kell a védelmi tervek életbe léptetését előíró feltételeket;
~ a szabadba jutó anyag terjedését illetően a lehetséges legkedvezőtlenebb feltételek bekövetkeztében kialakuló, és ez által a lehető legnagyobb koncentrációt feltételező, legkisebb felhőszélességgel kell számolni;
~ a monitoring végpontok az esetlegesen lakosságot veszélyeztető mérgezőanyag-felhő feltételezett útjába kell, hogy essenek;
~ az érzékelőkkel történő lefedettség a mérgezőanyag-felhő bármely terjedési útvonala esetben biztosítsa a detektálást;
~ a mérgező felhő valós beérkezési idejének meghatározása, lehetőleg megkettőzött végponttelepítéssel, a település veszélyes létesítményhez legközelebb eső határán;
~ az érzékelők megsemmisülésének a kizárása a robbanási zónákon kívülre telepítéssel;
~ a talaj menti meteorológiai adatok rögzítését végző érzékelők telepítésénél figyelembe kell venni az épületek ezekre gyakorolt befolyását;
~ a műszerek beállításakor a kalibrációs sajátosságokra figyelemmel kell lenni. [17]

**b.)** A MoLaRi működése szükség szerint a külső védelmi tervek foganatosítandó *intézkedéseinek életbe léptetését* is maga után vonhatja.

Az OKF-t *a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 18/2006. (I. 26.) Korm. rendelet* hatósági jogkörrel ruházza fel, és mint ilyen a súlyos balesetek megelőzése, az ellenük való védekezés érdekében az engedélyezési eljárás, illetve felügyeleti tevékenysége során vizsgálja a veszélyek csökkentését szolgáló biztonsági irányítási rendszer működőképességét, valamint az ezzel szorosan összefüggő külső védelmi terv végrehajtási feltételeinek meglétét is. A hatósági vizsgálatnak el kell döntenie, hogy a veszélyhelyzeti irányítás és a védekezéssel kapcsolatos infrastruktúra alkalmasak-e a balesetből fakadó elhárítási feladataik ellátására.

A hatósági tevékenység a védelmi képesség megteremtése kötelezettségének teljesítésén túl el kell érje, hogy ezen létesítmények üzemeltetői és a külső védelmi feladatokat irányító önkormányzati vezetők eleget tegyenek a lakosságtájékoztatás jogszabályi

[5] Vass Gy. - Máté J.: A MOLARI a megvalósulás útján [16]:
Országosan 20 veszélyes ipari üzem környezetében 360 monitoring és 565 riasztó és tájékoztató végpontot fog magába foglalni.

elvárásainak.

**c.)** A MoLaRi rendszernek harmadik fő eleme a *települések lakossága riasztását és tájékoztatását* szolgáló rendszer, melynek alapvető feladata a monitoring alrendszer vegyianyag-specifikus mérőszondái generálta jelzések alapján a veszélyeztetettségi övezetben lévő települések polgármesterei részére a külső védelmi tervekben megfogalmazott lakosságvédelmi rendszabályok eredményes végrehajtását biztosító riasztás és tájékoztatás. [18]

A lakosság riasztásásának három összetevője van, melynek keretében:

- ~ normál időszakban tájékoztatást kell adni a veszélyeztetettség mibenlétéről, a *lehetséges következményekről*, az egyére nézve kockázatot jelentő ártalmakról, a védekezés lehetőségeiről, illetőleg a követendő magatartási szabályokról tájékoztató kiadványok, lakossági fórumok és egyéb eszközök útján;
- ~ második fázisban a lakosság figyelmét fel kell hívni a *bekövetkezett esemény okozta veszélyre* alapvetően a kiépített szirénarendszeren keresztül;
- ~ a helyzettől függő *konkrét teendőkről* pedig részletes tájékoztatást a közszolgálati média ad. [19]

A tájékoztatási tevékenységének támogatása a hivatásos katasztrófavédelmi szervek szakmai munkályában prioritást élvez lévén az a *polgári védelemről szóló 1996. évi XXXVII. Törvény* meghatározásában polgári védelemi feladat a lakosságot veszélyhelyztető helyzetekben. A feltételek biztosítása az újonnan rendszerbe álló MoLaRi végpontok esetében igényli a helyi önkormányzatokkal való szoros együttműködést az üzemi alrendszerek kiépítése és a települési helyszín kijelölése vonatkozásában. A tájékoztatás, felkészítés alanyai közül ezért elsők maguk az önkormányzati vezetők, mint települési polgári védelmi parancsnokok és e feladat egyszemélyi felelősei. Felkészítésükben az OKF területi és helyi szervei működnek közre hasznosítva a meglévő tapasztalatokat.

## Következtetések

A MoLaRi rendszer már felállított végpontjainak működtetéséből levont szakmai következtetések hatékonyan egészíthetik ki a lakosságvédelmi feladatok megoldásában elsajátított ismereteket. A MoLaRi rendszer beállításával nyert információk integrálása adalékul szolgálhat a KIV szükség szerint létrehozandó, a következménykezelés, valamint településbiztonság céljait megvalósító monitoring rendszereinek kialakításához is.

Ez alapján elmondható, hogy a MoLaRi rendszer nem csak a tájékoztatás veszélyhelyzetben végzendő feladatainak sikeres megoldásához járul hozzá, hanem rendeltetésszerű alkalmazásával nagyban javítható a lakosságvédelem települési feladatainak hatékonysága a következményekre való gyorsabb és adekvátabb reagálás által.

## Irodalomjegyzék


[1] Hadtudományi Lexikon I. kötet, Magyar Hadtudományi Társaság, Budapest, 1995, 37. o.

[2] Executive Order 13010 - Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138. pp 37347-37350.

[3] NATO Senior Civil Emergency Planning Committee (SCEPC), Civil Protection Committee, Critical Infrastructure Protection Concept Paper EAPC(SCEPC)D(2003)15;

[4] Tanács irányelv-javaslat, az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről COM(2006) 787, Európai Közösségek Bizottsága, Brüsszel, 2006. december 12.;

[5] Critical Infrastructure Protection in a NATO/EAPC Civil Emergency Planning context, Presentation tool, Civil Protection Committee, 2007. szeptember, 25. o.;

[6] Nagy Rudolf: A kritikus infrastruktúra védelme és annak katasztrófavédelmi aspektusai a terrorizmus tükrében, Kard és Toll, 2006/3, 56 – 64. o.;

[7] Zöld Könyv a kritikus infrastruktúra védelmének európai programjáról" Európai Közösségek Bizottsága, Brüsszel, 2005. november 17. COM(2005) 576 final;

[8] Tóth Tamás – Tóth Szabó József: Munkavédelem a vegyiparban, Műszaki Könyvkiadó, Budapest, 1981, 179. o.;

[9] Ipari biztonsági kockázatkezelési kézikönyv, KJK-KERSZÖV Jogi és Üzleti Kiadó Kft., Budapest, 2004, ISBN 963 224 816 3 207. o.;

[10] Industrijska bezbednost – hrestomatija – prevod i priređivanje, Univerzitet u Beogradu, Klub Studenata Fakultet Bezbednosti, Beograd, januar 2007., 65. o., http://www.ksfb.org.yu /materijali.php, (Letöltve: 2007. 01. 01.);

[11] Ipari biztonsági kézikönyv, KJK-KERSZÖV Jogi és Üzleti Kiadó Kft., Budapest, 2003, ISBN 963 224 716 7 123. o.;

[12] Az infrastruktúra szerepe a területi fejlődésben, a térszerkezet és az infrastruktúra fogalmai, VÁTI Magyar Regionális Fejlesztési és Urbanisztikai Kht., Területfejlesztési Igazgatóság, Elemző és Értékelő Iroda, 2004. február; 25. o. http://www.terport.hu/download.php?ctag=download&docID=4911, (Letöltve: 2007. 01. 01.);

[13] Előterjesztés-tervezet a Kormány részére a Kritikus Infrastruktúra Védelem Nemzeti Programjáról, Önkormányzati és Területfejlesztési Minisztérium, Budapest, 2007., 22. o.

[14] A katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV. Törvény;

[15] 18/2006. (I. 26.) számú Kormányrendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről;

[16] Vass Gyula - Máté József: A MOLARI a megvalósulás útján, Katasztrófavédelem 2006. április, ISSN 1586-2305, 2. o.;

[17] Vass Gyula: MOLARI: rendszer meteorológiai vegyi monitoring eleme, Katasztrófavédelem 2006. április, ISSN 1586-2305, 3. o.;

[18] Máté József: MOLARI: a lakossági riasztó és tájékoztató rendszer, Katasztrófavédelem 2006. április, ISSN 1586-2305, 6. o;

[19] Szakál Béla: Polgári védelem, Jegyzet, Szent István Egyetem, Ybl Miklós Műszaki Főiskolai Kar, Tűzvédelmi és Biztonságtechnikai Intézet, 2005., 40. o.;

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Gyarmati József**
Zrínyi Miklós Nemzetvédelmi Egyetem
gyarmati.jozsef@zmne.hu

# SMART, A TÖBBSZEMPONTÚ DÖNTÉSI PROBLÉMA EGY EGYSZERŰ MEGOLDÁSA[1]

***Absztrakt***

*A cikk egy többszempontú döntési módszert mutat be, amely olyan szemléletes elemzési eljárással rendelkezik, ami lehetővé teszi felhasználását a K+F és a haditechnikai eszközök beszerzésének döntéselőkészítési folyamatában.*

*This article describe a multi-attribute utility process, witch have an illustrative analyst methods. We could use this method in a development and research, and suit for preparation of acquisition of weapon systems.*

***Kulcsszavak:*** *többszempontú döntési módszer ~ multi-attribute utility process*

## BEVEZETÉS

A haditechnikai eszközök értékelése és összehasonlítása egy un. többszempontú döntési probléma [1]. A döntéselmélet e döntési osztály modellezésére több módszerrel is rendelkezik. Ezeket a módszereket a szakirodalom széles körben tárgyalja. A leggyakrabban használt és a legkorszerűbb eljárások alkalmazására mutat be példákat az [1] irodalom. Az [1] és a [6] példákon keresztül mutatja be, hogy haditechnikai eszközök összehasonlításakor ezen módszerek használatával kapott rangsorok valamit pontszámok a módszerek alkalmazásának minőségétől függően jelentős szórással rendelkezhetnek. A többszempontos döntéselmélet tehát igazoltan alkalmazható a haditechnikai eszközök összehasonlítására viszont minden esetben tudatában kell lenni annak, hogy a kapott eredmények pontossága önmagában ismeretlen. Ilyen esetben nagy jelentőséggel bírnak azon matematikai és statisztikai eljárások, amelyek a kapott eredmények pontosságára vonatkozólag adnak becsléseket, vagy az eredmények további elemzését vagy értelmezését teszik lehetővé.

Az eredmények pontosságára vonatkozólag a [9] irodalom mutat be egy érzékenységvizsgálatot, amely egy hiperbolikus programozás segítségével az alternatívákat értékelő pontértékekhez olyan intervallumokat rendel, amely kifejezi a súlyszám változás

[1] Ez a cikk a Bolyai János Kutatási Ösztöndíj támogatásával készült.

pontértékre gyakorolt hatását. Az [1] tüzérségi tűzvezető rendszerekre valamint terepjáró tehergépkocsik többszempontú döntési modelljére alkalmazza az érzékenységvizsgálatot. A [7] és a [8] az egyes eredmények vagy részeredmények elemzésére, valamint a döntési modell kialakítására mutat be további módszereket.

A SMART (Simple Multi-Attribute Rating Technique, Egyszerű Többszempontú Skálázási Technika) nem tekint vissza régi múltra, először a 70-es évek végén publikálták [2]. A módszer első modellje, ahogy az a nevében szerepel rendkívül egyszerű, amely egyszerűség miatt az [5] a „naiv" módszerek közé sorolja. Az eljárást többször módosítják a szerzők, amelyek során olyan elemzési lehetőségeket is kap [3], [4], amelyek a katonai-műszaki terület számára is érdekessé és használhatóvá teszik az eljárás. A módszert és annak elemzési lehetőségeit jelen cikk a [3] szerint mutatja be. A módszer ismertetésének a célja a jól használható elemzési eljárás gyakorlati példán keresztül történő bemutatása.

## AZ ELJÁRÁS MATEMATIKAI MODELLJE

A döntési modell két pontértékkel értékeli az alternatívákat. A döntési modell nem csupán egy pontszámokat rendel az egyes alternatívákhoz, hanem két pontszámot, amelyeket egy koordináta rendszerben ábrázolva, lehetőséget ad a döntéshozók számára a döntési probléma alaposabb elemzésére. Az eljárás döntési modelljét az (1) és a (2) egyenletek mutatják.

Az (1) egyenlet szerinti $y_j$ a $j$-edik alternatíva hasznosságát jelző szám. A hasznosság értékének számítása során $y_j$ pontszámban a költség jellegű tulajdonságok nem szerepelnek. A költség jellegű szempontokat az $x_j$ változóban pontozza az eljárás. A két pontszám segítségével lehetőség nyílik az eszközök képességeinek és a velük járó költségeknek a külön-külön pontozására.

| | $A_1$ | $A_2$ | $\cdots$ | $A_n$ | |
|---|---|---|---|---|---|
| $C_1$ | $u(a_{11})$ | $u(a_{12})$ | $\cdots$ | $u(a_{1n})$ | $w_1$ |
| $C_2$ | $u(a_{21})$ | $u(a_{22})$ | $\cdots$ | $u(a_{2n})$ | $w_2$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ | |
| $C_m$ | $u(a_{m1})$ | $u(a_{m2})$ | $\cdots$ | $u(a_{mn})$ | $w_n$ |
| | $y_1$ | $y_2$ | $\cdots$ | $y_n$ | |

(1)

$$y_j = \sum_{i=1}^{n} w_j u_j\left(a_{ij}\right)$$

ahol: $C_i$ az $i$-edik szempont;
$A_j$ a $j$-edik alternatíva;
$a_{ij}$ a $j$-edik alternatíva $i$-edik szempont szerinti értéke;
$u_i$ az $i$-edik szempont hasznossági függvénye;
$w_i$ az $i$-edik szempont fontosságát kifejező súlyszám.

A döntési modell összegzése szerint az alternatívák szempontonkénti hasznosságának súlyszám szerint súlyozott átlaga az alternatíva $y_j$ pontértéke az (1) egyenletben.

| | $A_1$ | $A_2$ | $\cdots$ | $A_m$ |
|---|---|---|---|---|
| $F_1$ | $a_{11}$ | $a_{12}$ | $\cdots$ | $a_{1n}$ |
| $F_2$ | $a_{21}$ | $a_{22}$ | $\cdots$ | $a_{2n}$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ |
| $F_m$ | $a_{m1}$ | $a_{m2}$ | $\cdots$ | $a_{mn}$ |
| | $x_1$ | $x_2$ | $\cdots$ | $x_n$ |

(2)

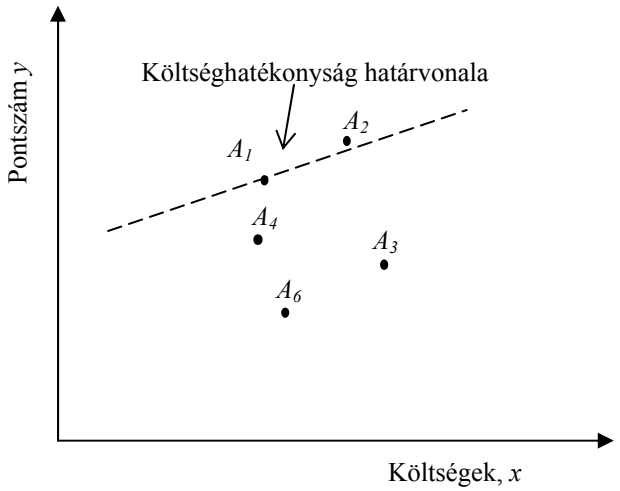
$$x_j = \sum_{i=1}^{m} a_{ij}$$

ahol: $F_i$ az $i$-edik költségösszetevő.

A költség szerinti pontszám gyakorlatilag meggyezik az összköltséggel, amit az $x_j$ mutat a (2) egyenletben.

Az alternatívákhoz hozzárendelt $\{x_j ; y_i\}$ pontszámokat egy koordináta rendszerben kell ábrázolni a (3) egyenlet szerint, ahol az abszcisszán vannak feltüntetve a költségösszetevők.

$$A_i \rightarrow \{x_i ; y_i\} \tag{3}$$




1. ábra

Az (1), (2), (3) egyenletek által leírt döntési modell alapján az eredményeket az 1. ábra szerint kell ábrázolni. A döntési modell ezen változata alapvetően abban különbözik a többi többszempontú döntési modelltől, hogy a költségeket külön ábrázolja, így lehetőség nyílik az eszközök eredő hasznosságának és a költségeinek az összevetésére. Meghatározható, hogy a nagyobb hasznosság eszközönként mekkora összegbe kerül, más megfogalmazásba lehetőség nyílik egy un. fajlagos hasznosság megállapítására, amit az 1. ábrán a költséghatékonyság vonala jelöl ki. Az eredmények értelmezésekor a pontértékeket nem csak egymáshoz hanem ehhez a vonalhoz képest is értékelhetők. Meghatározható vagy eldönthető, hogy egy

hasznosabb alternatíva mennyire éri meg a vele járó többletköltségeket. Az elemzés eredményeként nem feltétlenül a leghasznosabb alternatíva kiválasztására van lehetőség hanem a költséghatékonyság tekintetében a legkedvezőbb kiválasztására. Az 1. ábrán a leghasznosabb az $A_2$ . Az $A_1$-el összevetve viszont megállapítható hogy ez utóbbi hasznossága némileg alacsonyabb viszont ezt lényegesen kisebb költséggel éri el, ennek megfelelően az összességében legkedvezőbb az $A_1$ alternatíva.

## AZ ELJÁRÁS LÉPÉSEI

### 1. A döntéshozó azonosítása

A döntéselmélet döntéshozó fogalma nem egyezik meg a Honvédelmi Minisztériumban használttal. A döntéshozón katonai területen azt a személyt értik, amelyik a végső döntéseket meghozza vagy az engedélyeket kiadja. A döntéselméletben pedig mindazon személyek, akik érintettek a döntések következményeivel vagy részt vesznek a döntési modell kialakításában. Ennek megfelelően a döntéshozó megnevezés helyett helyesebb a szakértő kifejezés használata.

A szakértők mindazon személyek, akik valamilyen szinten érintettek a döntések következményeiben. Amennyibe a döntési probléma több haditechnikai eszköz kiválasztása, akkor a szakértők az eszközt üzemeltetők, vagyis használók és az eszközt üzembentartók, vagyis a karbantatást a javítást és egyéb logisztikai tevékenységet végzők köréből kerül ki. Ilyen meggondolások szerint a szakértők egy löveg esetében tüzér, fegyverzeti, és logisztikusi szakmai számú személyek közül kerülhetnek ki. A szakértők közé sorolhatók azon személyek, akik az eszközt ugyan nem üzemeltetik de az alkalmazás előnyeit és hátrányait közvetlenül élvezik. Az előbb bevezetett löveg példa esetében ez az elöljáró szervezet parancsnokságát jelentheti.

A döntéselmélet a döntéshozók számát tekintve megkülönböztet egyszemélyi és az un. csoportos döntéseket. Az előbbiek alapján kijelenthető, hogy katonai értelemben a haditechnikai eszközök összehasonlításakor, minden esetben csoportos döntésről beszélhetünk. A csoportos döntések a döntéselmélet egy összetettebb problémakörét taglalják, ugyanis nem egy szakértői véleményből, hanem több szakértő valamilyen módon összesített véleményéből kell kiindulni. Az eredő vagy modális vélemények meghatározására katonai példákat mutat be a [7].

### 2. Az alternatívák azonosítása

A döntési modellek ezen osztálya alkalmazható minden olyan esetben, ahol az alternatívákat nem egy hanem több következményértékkel lehet jellemezni és ezen következmények a modell szerint 1 valószínűséggel realizálódnak. Katonai döntések esetében a modell alkalmazhatósága széles körű, hiszen még egyes harcászati szintű probléma döntés-előkészítésében is felhasználnak bizonyos naiv módszereket. A cikk a módszert olyan aspektusból vizsgálja, hogy haditechnikai eszközök összehasonlító elemzésére hogyan és milyen eredményességgel alkalmazható, tehát az alternatívák haditechnikai eszközök. Kiválasztásuk alapvetően a döntés környezetétől függ. A döntési környezeteket az [1] 44-48 oldalán azonosítja. A döntés környezete az összehasonlítás célját határozza meg, ami lehet beszerzés, előzetes felmérés, döntés előkészítés, vagy meglévő eszközök közüli kiválasztás egy feladatra akár kivonásra is.

Az alternatívák meghatározásakor minden esetben a döntéshozói célokból kell kiindulni, miszerint: Melyek lehetnek azok az eszközök, amelyek a kitűzött célokat teljesíteni képesek?

Ha a döntési cél egy ellenséges eszköz képességeivel való összemérés akkor az alternatívákat ezen célt kielégítő eszközcsoport lesz a megoldás.

### 3. A szempontok meghatározása

Az alternatívákat meghatározó szempontrendszer kialakítása lényegében az általános törvényszerűségek szerint történik. A haditechnikai eszközök szempontrendszerének kialakításának törvényszerűségeit a [10] és a [11] tartalmazza. A SMART esetében viszont mindenképpen meg kell határozni költség jellegű szempontokat is, hiszen ezek függvényében lesz ábrázolva a többi szempont szerint számított hasznosság.

A SMART módszertan a szempontok meghatározását fastruktúra keretében javasolja, ahol a kiindulás a döntéshozók fő célja, majd ezen célok teljesítéséhez szükséges képességeket bontja a fa ágain keresztül az un. levélszempontig, amely teljesítésének a szintje már közvetlenül mérhető. A kiindulást követően a szempontokat két csoportba sorolja, ezek: hasznosság; költség, amely két főszempontot méri az (1) és a (2) egyenlet.

Haditechnikai eszköz esetében ez az elv nem minden esetben alkalmazható, hiszen a döntéshozó célja a hasznosságot tekintve egyként nem fogalmazható meg katonai értelemben inkább cél és követelményrendszerről lehet beszélni. A szempontrendszer kialakítása ennek megfelelően a [10] és a [11] szerint javasolt, avval a kiegészítéssel, hogy a költségeket egy külön főszempontba kell csoportosítani.

### 4. A szempontok hasznossági függvényeinek definiálása.

A hasznossági függvények feladata, hogy a szempont által leírt képesség betöltési minőségének döntéshozói (szakértői) hasznosságát határozza meg. Ha a szempont például a páncélátütő-képesség, akkor a hasznossági függvénye megadja hogy az egyes eszközök ezen képessége mekkora például egy 1-től 10-ig terjedő skálán.

A SMART a hasznossági függvényeit a szakértői értékítéletek segítségével javasolja meghatározni. A megoldás menete:

a) határozzuk meg azt az értéket vagy eszközt, amely a maximális hasznosságot jelenti számunkra, ezt pontozzuk 100-ra;

b) határozzuk meg azt az értéket vagy eszközt, amely a minimális, vagyis 0 hasznosságot jelenti számunkra, ezt 0-val pontozzuk;

c) a két szélső érték alapján határozzuk meg azt az értéket vagy eszközt, amely a maximálishoz képest fele hasznosságot jelenti számunkra, ezt pontozzuk 50-re;

d) a középső és a maximális hasznosság alapján határozzuk meg azt az értéket, amely hasznosság szempontjából a kettő között helyezkedik el, ezt pontozzuk 75 re;

e) a minimális és a közepes hasznosságok alapján keressük meg azt az értéket, amely hasznosság szempontjából a kettő között helyezkedik el és ezt pontozzuk 25-re.

A skálát tetszőlegesen finomíthatjuk, megfelelő matematikai apparátus segítségével a meghatározott pontokhoz függvényt lehet simítani. A módszer kitűnően alkalmas a hasznossági függvény linearitásának az ellenőrzésére.

Katonai gyakorlatban használható hasznossági függvényeket definiál a [10], a definíciók matematikai alapjait az [5] 67-95 oldalán közli.

## 5. Súlyszámok számítása

A többi többszempontú döntési modellhez hasonlóan a szempontok különböző fontosságát a SMART figyelembe veszi. A súlyszámok meghatározására közvetlenbecslést javasol, de célszerűbb ennél pontosabb eljárás például az AHP vagy a Guilford féle páros összehasonlítás használata. A két módszer katonai alkalmazására az [1] 67-72 oldalán mutat be példát.

A súlyszámok meghatározásakor miden esetben figyelembe kell venni, hogy csoportos döntésről van szó. A súlyszámrendszernek tükröznie kell a teljes csoport értékrendjét. Az egyes szakértők súlyszámaiból átlagértékek számításának problémájával a [7] foglalkozik.

## 6. Az alternatívák pontértékeinek számítása

Az egyes alternatívák szempontonkénti hasznosságét a 4. pontban definiált hasznossági függvények segítségével kell meghatározni, majd ezen hasznosság értékek (1) és (2) szerinti súlyszámok szerint súlyozott átlagát kell számítani. A (2) egyenletben nem szerepelnek súlyszámok, amit a költség típusú szempontok speciális tulajdonságai miatt el lehet hagyni. A költségek esetében a kiadások nagysága természetes módon súlyozza magát. A különböző költségtípusok azonos skálán vannak mérve ezért összeadhatók. A költségek tekintetében a fő cél egy reális összköltség számítása, amely tartalmazza az alternatívákkal kapcsolatban felmerülő összes költségeket, például, beszerzés; fenntartás; egyéb kiadások.

## 7. pontértékek ábrázolása

Az ábrázolás a (3) hozzárendelési szabály szerint az 1. ábra alapján történi. Az ábrázolás által lehetőség nyílik egy költség-haszonosság elemzésre. A két szempont egymáshoz viszonyított arányai alapján megállapítható az 1. ábra „költséghatékonysági határvonala”, amely révén mérhetővé válik a képességnövekedés gazdaságossága.

## 8. Érzékenységvizsgálat

Ahogy az a bevezetésben említve lett a többszempontú döntési modellek eredményei ismeretlen szórásssal rendelkeznek, vagyis nincs ismeret a számított pontérték pontosságárra vonatkozólag. A SMART ezért egy érzékenységvizsgálatot javasol. Az érzékenységvizsgálat lényegében egy szempont súlyszámát változtatja 0-tól a maximáli értékig és ezen érték mint független változó függvényében ágrázolja az alternatívák pontértékeinek a változását. Az eljárás érzékenységvizsgálata egyszerre egy szempont súlyszámának az $y_i$ pontértékekre gyakorolt hatását mutatja. Az érzékenységvizsgálat az alternatívák $y_i$ pontértékeit egy függvény segítségével fejezi ki, ahol a független változó a vizsgált szempont súlyszáma értelmezési tartománya pedig 0 – 100.

$$y_i\left(w_p^*\right)=\sum_{j=1}^{n} w_j^* u_j\left(a_{ij}\right), w_p^* \in [0,100], w^*{}_j = \frac{w_j}{\sum_{j=1}^{n} w_j - w_p}\left(\sum_{j=1}^{n} w_j - w_p^*\right) \qquad (4)$$

ahol: $w_p^*$ a vizsgált súlyszám eredeti értéke.
$w_p$ a vizsgált súlyszám, a független változó.

A számítás matematikai modellje meglehetősen egyszerű, amely lehetővé teszi hogy irodai programcsomag segítségével is elvégezhető legyen a számítás. Hátránya viszont hogy egyszerre csak egy szempont súlyszámának változását veszi figyelembe. Az összes

szempontra vonatkozó görbesereg vizsgálata már viszonylag kevés szempont esetében is kezelhetetlenül sok információt nyújt, ezért az érzékenységvizsgálatot célszerű az a [9] modellje szerint is elvégezni.

## TEHERGÉPKOCSIK ÖSSZEHASONLÍTÁSA

Ebben a pontban a cikk egy gyakorlati példát mutat be, amely az [1] 75 oldalán található összehasonlítás adataira támaszkodik. A példa során az előző fejezet pontjai szerint kerül bemutatásra a SMART alkalmazás. A példa adottsága miatt az 1. pont vagyis a döntéshozó azonosítása nem kerül bemutatásra.

### 2. Az alternatívák azonosítása

Az alternatívák 5-8 tonna hasznos teherbírású terepjáró tehergépkocsik. Hat alternatíva van ezek megnevezésére a reklám elkerülése miatt nem kerül sor, az alternatívákat az $A_1$ , $A_1$ … $A_6$ szimbólumok jelölik.

### 3.-4.-5.-6. A szempontok, súlyszámok és hasznossági függvények meghatározása

1. táblázat

| | **$A_1$** | **$A_2$** | **$A_3$** | **$A_4$** | **$A_5$** | **$A_6$** | **u** | **paraméter** | **w** |
|---|---|---|---|---|---|---|---|---|---|
| VSE[2] [-] | 65 | 105 | 84 | 76 | 108 | 116 | max. | min 50 | 25 |
| Teljesítmény dotáció [kW/t] | 11,3 | 13,6 | 17,8 | 13,4 | 13,4 | 13,3 | max. | min 10 | 15 |
| Hasznos teher [t] | 5015 | 5800 | 7598 | 7120 | 7900 | 6000 | max. | min 5000 | 24 |
| Lengéskényelem [h] | 2 | 4 | 2 | 2,2 | 1,3 | 2 | max. | – | 23 |
| Rakfelület [$m^2$] | 12 | 12,15 | 10,56 | 12,23 | 11,5 | 9,28 | max. | – | 12 |
| Ár [1 000 000 Ft] | 17 | 24 | 28 | 26 | 26 | 28 | min | – | – |

Jelen pontban foglaltak az [1] 75 oldala szerint a 1. táblázat ismerteti. A 1. táblázatban első három szempontjához paraméterek vannak megadva, amelyek hasznosság szempontjából azt jelentik, hogy a szakértők értékrendje alapján ezen értékekhez van 0 hasznosság rendelve. A legnagyobb hasznosságot a legkedvezőbb paraméter jelenti. A hasznos teher tekintetében ez a **$A_5$** alternatíva, amely 7900 kg hasznos tömeggel rendelkezik. A hasznosság számítása e két érték alapján történik lineáris interpolációval. Példaképpen az **$A_3$** alternatíva hasznossága teherbírás tekintetében az (5) egyenlet szerint számítandó. A lengéskényelem és a rakfelület szempontjainál a szakértők nem határoztak meg paramétereket, ebben az esetben a 0 hasznosságú adat a legkisebb. A hasznosságok számítása a (5) alapján történik értelemszerűen. Az ár esetében nincsen meghatározva hasznossági függvény ezt a szempontot a módszer külön tengelyen ábrázolja.

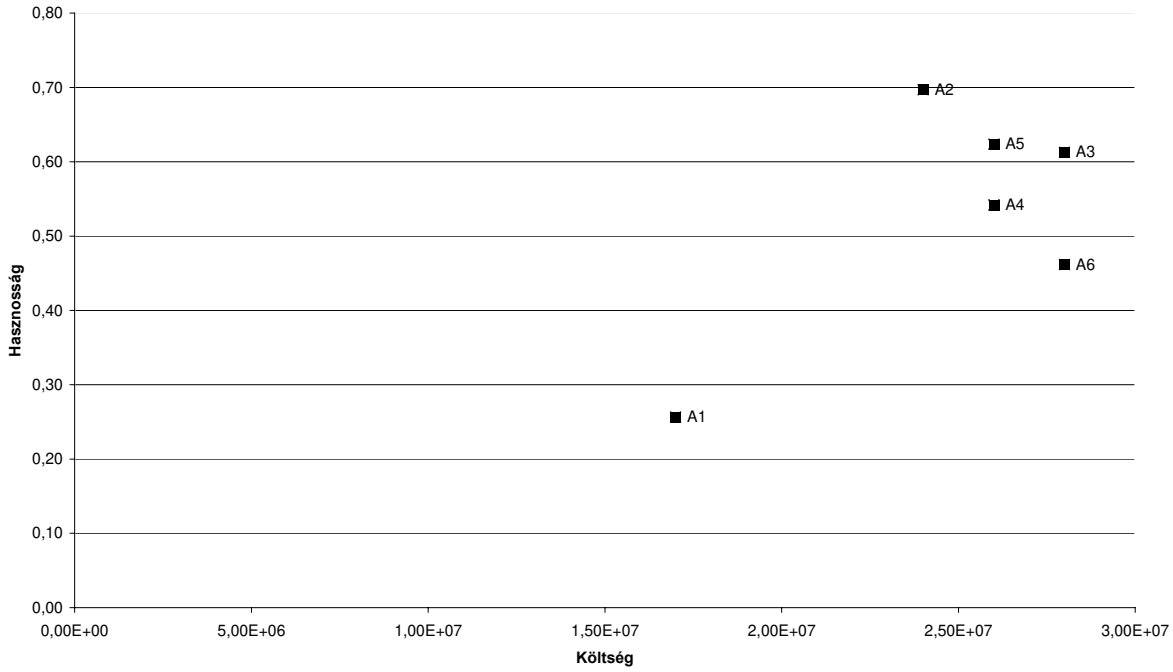
$$u_3(a_{33}) = \frac{7598 - 5000}{7900 - 5000} = 0{,}8958 \qquad (5)$$

A 2. táblázatban látható, hogy az ár szempontjának nincs súlyszáma. Mivel ennek a szempontnak az ábrázolásban külön tengelye lesz ezért itt nem is kell súlyszám, az ár jelentőségét a koordináta rendszerbe történő ábrázolás majd a költséghatékonyság határvonalának az iránytangense adja meg a szakértői értékítéletek szerint.

### 7. pontértékek ábrázolása

[2] Vehicle Slope Elevation a jármű terepjáróképességét kifejező mutató.

A koordináta rendszerbe történő ábrázolást a 2. ábra mutatja. Az ábra elemzését megelőzően meg kel állapítani, hogy az [1] több döntési modell alkalmazásán keresztül az $\mathbf{A_1}$ alternatívát




2. ábra

jelölte ki legkedvezőbbnek. A 2. ábra szerint viszont az $\mathbf{A_2}$ a leghasznosabb és az $\mathbf{A_1}$ hasznosság tekintetében lényegesen elmarad az $\mathbf{A_2}$ alternatívához képest.. Az $\mathbf{A_1}$ elsőségét az [1] vélhetőleg a kedvező ára miatt állapította meg. Az $\mathbf{A_6}$ alternatívákat egyértelműen ki lehet zárni, hiszen sem, költség sem pedig hasznosság tekintetében nem mutat kedvező tulajdonságokat. A költséghatékonyság határvonala alatt helyezkedik el, a vonaltól, a legnagyobb távolságra, tehát a hasznossága és a vele járó költségek ebben az esetben a legkedvezőtlenebbek.

$\mathbf{A_1}$ alternatíva nagyon kedvező áron, de nagyon alacsony hasznosságot kínál, ez tehát egy nagyon olcsó, de a többi szempont szerint kevés előnnyel rendelkező választás. Az $\mathbf{A_1}$ kiválasztása inkább szükségmegoldás lehet, leszámítva azt az esetet, ha az általa kínált hasznosság eléri a szakértők által követelt minimális szintet. Ebben az esetbe az $\mathbf{A_1}$ alternatíva optimális lehet. Ami még mellette szól, figyelembe véve a költséghatékonyság határvonalát megállapítható, hogy a hasznosság és a költség között kedvező az arány. Az alacsony hasznosságú alternatívák költség tekintetű preferálásához szükséges követelményeket a [11] részletesen taglalja.

Az elemzéshez a továbbiakban az $\mathbf{A_2}$-$\mathbf{A_5}$ alternatíva marad. Ahogy azt az előzőekben meg lett állapítva a legkedvezőbb az $\mathbf{A_2}$ viszont az említett alternatívák között nagyon kicsi a távolság ezért érdemes egy érzékenységvizsgálatot is elvégezni.

## 8. Érzékenységvizsgálat

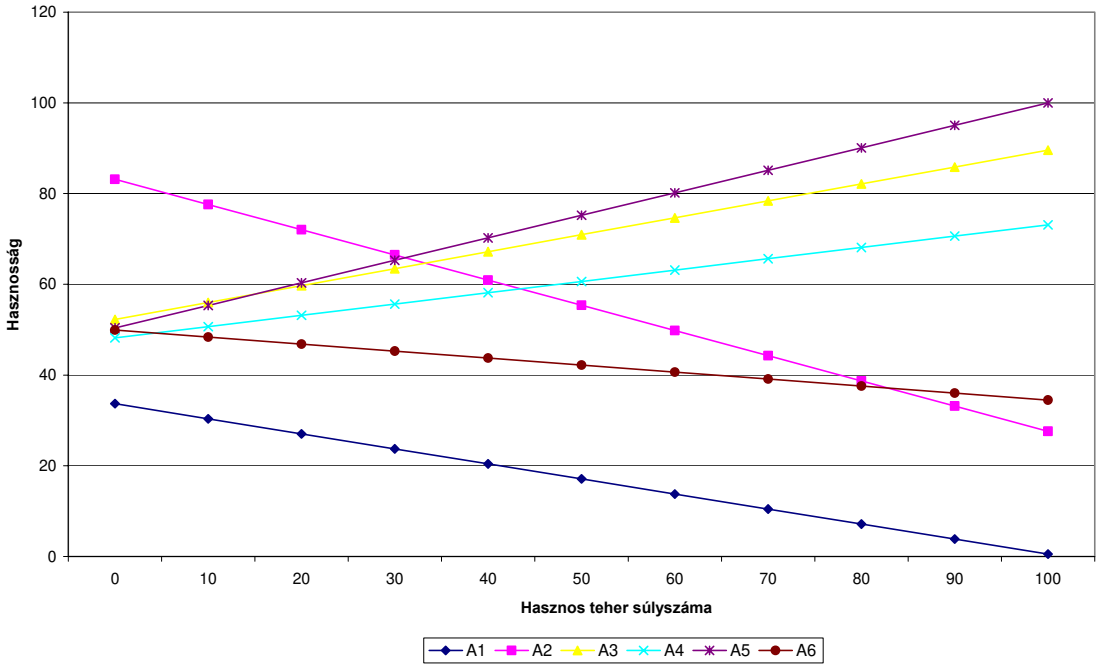
Az érzékenységvizsgálat során az kell megvizsgálni, hogy a súlyszámok milyen mértékű változása okozhatja az $\mathbf{A_2}$-$\mathbf{A_5}$ alternatívák közötti rangsor megváltozását. A rangsorfordulást, vagyis $\mathbf{A_2}$ hátrább sorolását két eset idézheti elő. Egy olyan szempont súlyszámának növekedése ahol $\mathbf{A_2}$ kedvezőtlenebb, mint $\mathbf{A_3}$-$\mathbf{A_5}$, vagy egy olyan szempont súlyának a csökkenése ahol $\mathbf{A_2}$ kedvezőbb mint $\mathbf{A_3}$-$\mathbf{A_5}$. Az 1. táblázat szerint ezek a hasznos teherbírás és

a lengéskényelem szempontjai lesznek. A két szempont érzékenységvizsgálatát a 3. és a 4. ábra mutatja.

A 3. ábra a hasznos teher súlyszám változásának hatásait mutatja a hasznosságértékekre. A hasznos teher eredetileg megállapított súlyszáma: $w_3 = 0{,}24$ . A 3. ábra szerint $\mathbf{A_2}$ hasznossága a $w_3$ növekedésével csökken és $\mathbf{A_3}$-$\mathbf{A_5}$ hasznosságai pedig nőnek**.** A rangsor megváltozása $w_3 = 0{,}31$-nél történik. Százalékos arányban ez azt jelenti, hogy: 0,31/0,24=1,29 , vagyis a súlyszám 29%-os növekedése esetében $\mathbf{A_2}$ elsősége megszűnik. Kérdés, hogy ez a 29% jelen esetben kicsi vagy nagy, elképzelhető ilyen mértékű pontatlanság vagy nem? A választ erre a kérdésre a szerint lehet megadni, hogy milyen módszerrel lett meghatározva a súlyszám, közvetlen becslés estén elképzelhető ilyen pontatlanság, de egy korszerű súlyozásra is használható módszer például AHP esetében nem.

A 4. ábra a lengéskényelem szempontjára végzi el az előzőhöz hasonló vizsgálatot. Az eredeti súlyszám: $w_4 = 0{,}23$, a rangsorfordulás itt a súlyszám csökkenésekor várható, ami az ábra szerint $w_4 = 0{,}16$ értéknél következik be. Százalékos formában kifejezve: 0,23/0,16=1,44, vagyis 44%-os csökkenés esetében következik be. Ekkora pontatlanság a súlyszámok közvetlen becslésekor szintén előfordulhat, de magasabb skálaszintű eljárások esetében nem.

Összességében megállapítható, hogy min a két esetben az $\mathbf{A_2}$ és az $\mathbf{A_5}$ alternatíva rangsora változik először, tehát a választást ezen kettő közé lehet szűkíteni, jelen esetben a súlyszámokat az [1] AHP segítségével határozta meg, tehát kijelenthető, hogy az $\mathbf{A_2}$ elsősége biztos. A módszer érzékenységvizsgálata viszont egyszerre csak egy súlyszám változásainak a hatását veszi figyelembe a többihez képeset ezért ellenőrzésképpen a [9] szerinti érzékenységvizsgálat is el lett végezve. Az eredményeket az 5. ábra mutatja. Az érzékenységvizsgálat elvégzésekor a súlyszámok ±20%-os változása volt feltételezve.




3. ábra

Az 5. ábra szerint az $\mathbf{A_1}$ $\mathbf{A_4}$ és $\mathbf{A_6}$ alternatívákat egyértelműen ki lehet zárni. A rangsor itt nem változhat olyan mértékben, ami a legelső alternatíva változását jelentené. Az $\mathbf{A_3}$ alternatíva sávja és az $\mathbf{A_2}$ között látható némi eltérés, de ez nagyon csekély, valamint a 2. ábra

szerint $\mathbf{A_3}$ rendelkezik a legmagasabb költséggel, ezért ez is kizárható, mint optimális alternatíva.

Két alternatíva marad az $\mathbf{A_2}$ és az $\mathbf{A_5}$. Az 5. ábra szerint a súlyszámok ±20% változása esetében fennáll e kettő rangsorának változása, viszont a 2. ábra szerint a költséghatékonyság határvonalától, bármely iránytangens esetében $\mathbf{A_5}$ kedvezőtlenül helyezkedik el, ezért az optimális választás az $\mathbf{A_2}$.

## IRODALOM


[1] Gyarmati J.: Többszempontos döntéselmélet alkalmazása a haditechnikai eszközök összehasonlításában, ZMNE, PhD értekezés, 2003.

[2] Edwards, W.: How to use multiatribute utility measurement for social decision making IEEE Transaction System,Man, and Cybernetics, SMC-7, 326-340, 1977

[3] Goodwin, P. & Wright, G. (2001) Enhancing strategy evaluation in scenario planning: a role for decision analysis Journal of Management Studies 38(1) pp. 1-16.

[4] Cavalcante, Cristiano A.V.; da Costa, Ana Paula C.S.; Filho, Adiel T. de Almeida Multicriteria decision making on selection of decision analysis software. From: Journal of Academy of Business and Economics | Date: 3/1/2005 http://www.encyclopedia.com/doc/1G1-149213906.html

[5] Temesi, J.: A döntéselmélet alapjai, Aula, 2002, 120-121.

[6] Gyarmati, J.,: A haditechnikai eszközök összehasonlításának módszertana, Katonai Logisztika, 12. évf. 2. szám 148-194. p. 2004.

[7] Gyarmati J.: A nehézpuskát jellemző szempontok fontosságát kifejező súlyszámok számítása és statisztikai vizsgálata, Haditechnika, 2006/2, 11-16.

[8] Gyarmati J.: Műszaki berendezések vizsgálta faktoranalízis segítségével, Alkalmazott Matematikai Lapok 23 (2006), 73-83.

[9] Rapcsák, T., Többszempontú döntési problémák AHP modellek, Egyetemi oktatáshoz segédanyag, Budapesti Közgazdaságtudományi és Államigazgatási Egyetem MTA Számítástechnikai és Automatizálási Kutatóintézetében kihelyezett Gazdasági Döntések Tanszék.

[10] Gyarmati, J.: Haditechnikai eszközök összehasonlítása közbeszerzési eljárás során, Hadmérnök I. Évfolyam 2. szám - 2006. szeptember

[11] Gyarmati, J.: Döntési modell kialakítása közbeszerzési eljárás során Hadmérnök, . Évfolyam 3. szám - 2007. szeptember

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Fürjes János**
Zrínyi Miklós Nemzetvédelmi Egyetem
furjes.janos@chello.hu

# KORSZERŰ RÁDIÓFELDERÍTÉS KIHÍVÁSAI AZ INFORMÁCIÓS MŰVELETEKBEN

***Absztrakt***

*Az új biztonságpolitikai helyzetben számos új kihívás és veszély jelent meg, amelyek természetszerűleg új védelmi megoldásokat, eszközöket és rendszereket követelnek a védelmi szférától is. A megfelelő válaszlépések magukba kell, hogy foglalják azokat a korszerű, az információs technológia által nyújtott új lehetőségeket, amelyek a távközlés, a személyi kommunikáció, a radartechnika, az adatátvitel, a navigáció és más elektronikai berendezések, rendszerek révén ma már jelen vannak mindennapjainkban.*
*A szerző bemutatja az információ szerepét a hadviselésben, valamint a rádióelektronikai felderítés kihívásait napjainkban.*

*New risks and challenges have appeared in the new security policy situation, which require new defense answers, solutions, systems and assets. These answers must include the up to date, high-tech technology provided by information revolution such as communications, radar technology, data transmission, navigation and other everyday used electronic devices.*
*In this paper the author describes the role of information in the modern warfare, and the new challenges of SIGINT.*

***Kulcsszavak**: információ, információs műveletek, rádióelektronikai felderítés ~ information, information operations, SIGINT*

## Bevezetés

A hidegháború befejezésével és a kétpólusú világrend felbomlásával egy teljesen új gazdasági és politikai világrend épült ki. Ez az új magántőkén alapuló gazdasági-politikai világrend, a globalizáció nevet kapta. Az új gazdasági-politikai berendezkedésre történő áttérés, ha nem is teljesen békés úton, de globális fegyveres konfliktus nélkül zajlott le. Az új világrend nem a politikai (szocialista – kapitalista) szembenállás folytatását, hanem az Amerikai Egyesült Államok kiemelkedésének, gazdasági és katonai egyeduralkodásával egypólusú világrend

kialakulását eredményezte. [1] A globális fegyveres konfliktusok kialakulásának esélye egyre kisebb, bár az újra talpra álló Oroszország néha meglepő, olykor barátságtalan lépéseket tesz, amelynek komolyságát felmérni pontosan nem lehet. Ezen erőfitogtatások mögött inkább gazdasági presszió gyakorlása és nem katonai erők alkalmazása húzódik. Sokkal komolyabb kihívásként kell értékelnünk a helyi (gazdasági, vallási, etnikai) konfliktusok kezelésének kérdését, illetve az igazán komoly kihívást jelentő terrorizmus elleni küzdelmet. Azt is látnunk kell, ahogy azt Irak és Afganisztán példája mutatja, a fegyveres konfliktus lezárását követően a tevékenység nem ér véget. Az elhúzódó béketeremtő, békefenntartó (gazdasági újjáépítő) feladat sokkal nagyobb erőforrás-igényű, mint az azt megelőző fegyveres harc. Az elhúzódó katonai, civil jelenlét megköveteli a harctámogató és harcbiztosító erők hangsúlyosabb jelenlétét.
Az új biztonságpolitikai helyzetben számos új kihívás és veszély jelent meg, amelyek természetszerűleg új védelmi megoldásokat, eszközöket és rendszereket követelnek a védelmi szférától is. A megfelelő válaszlépések magukba kell, hogy foglalják azokat a korszerű, az információs technológia által nyújtott új lehetőségeket, amelyek a távközlés, a személyi kommunikáció, a radartechnika, az adatátvitel, a navigáció és más elektronikai berendezések, rendszerek révén ma már jelen vannak mindennapjainkban. [2]

## Az információ szerepe a hadviselésben

A XXI. századi harctevékenységekben megjelenik egy új technológia, melyet az információ források - és az információ szétosztási, illetve továbbítási képességek gyors ütemű növekedésével lehet jellemezni. Ez az új technológia az *információs technológia*, mely növeli a csapatok lehetőségét a helyzeti fölény elérésére, ugyanakkor az ellenséget is képessé teszi arra, hogy saját lehetőségeit kihasználja. A korszerű fegyveres küzdelemben az információ (az idő, tér és erő mellett) mindinkább előtérbe kerül. Az „információ folyam” kézben tartása lehetőséget nyújthat az erőviszonyok, a dinamikusan változó helyzet kézben tartására, valamint az információkra támaszkodva az ellenség megelőzésére, esetleges fölényének kiegyenlítésére, vagy a fölény megszerzésére. [3]
Az információ az egyik leglényegesebb alapja a *tudás alapú hadviselésnek*. Az információ képessé teszi a parancsnokokat, hogy koordinálják, integrálják és szinkronizálják a harctevékenység különböző funkcióit a harcmezőn. Az ellenség információs rendszerébe való beavatkozás jelentősen befolyásolhatja a helyzet felmérését, vagy megakadályozhatja, hogy a lényeges információkat felhasználja, ezáltal közvetlenül hozzájárul a sikeres harctevékenységhez. Ugyanakkor az ellenséges információs rendszerbe való beavatkozás mellett saját hasonló rendszerünk védelméről is gondoskodni kell.
A modern fegyverek jelentősen növelik a harctevékenység sikerét. E fegyverek hatása viszont nagymértékben függ az információk pontosságától. Az információs csatornák megszakítása, vagy magának az információ minőségének a lerontása (pl.: megtévesztéssel), jelentősen befolyásolják a nagypontosságú fegyverek és fegyverrendszerek hatékonyságát.
Az információs műveletek korunk egyik legújabb, a hadtudományok legdinamikusabban fejlődő területe, melynek tevékenysége az információs fölény kivívására irányul. A legfontosabb a tudásbeli fölény kivívása. Ehhez többet kell tudnunk a minket körülvevő eseményekről. Jobb érzékelők alkalmazására, megbízhatóbb hírszerzési információk beszerzésére, fejlettebb infokommunikációs eljárásokra és az információk hatékonyabb feldolgozására van szükség. Ennek birtokában képes a korszerű vezetés helyes és gyors döntések meghozására, amelyek alapvetően befolyásolják a harc és békeműveletek, valamint az “információs műveletek” kimenetelét, hiszen napjainkban a fejlett ipari társadalmak nem csak hagyományos háborúkat, hanem információs háborúkat is folytatnak és folytathatnak ellenfeleikkel szemben. Az információs hadviselésben a fő feladat az információ

megszerzése, annak minél gyorsabb és hatékonyabb feldolgozása az eredményes felhasználás érdekében, a szembenálló fél információs rendszerei működésének korlátozása, valamint a saját információ megfelelő védelme.

## A XXI. századi rádiófelderítés kihívásai

Az információs műveletekben a legnagyobb információszerző képességgel a rádiófelderítés bír. Ezen területen használt eszközök és eljárások fejlesztésének fontossága nyilvánvaló.
A rádiófelderítés (COMINT) a rádióelektronikai felderítés (SIGINT) egyik eleme, ugyanakkor e tevékenység megjelenik az elektronikai támogató tevékenységben is. Az elektronikai támogató tevékenység az elektronikai hadviselés egyik fontos összetevője.
„*Az elektronikai hadviselés azon katonai tevékenység, amely az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti, vagy megakadályozza az elektromágneses spektrum ellenség részéről történő használatát, és biztosítja annak a saját csapatok általi hatékony alkalmazást.”* [4]
Az elektronikai hadviselés szerves része mindenfajta katonai hadműveletnek és egyike az információs műveletek elemeinek. Az elektronikai hadviselés elősegíti az értékelő és döntéshozó folyamatot, hozzájárul a szervezéshez és hadműveleti irányításhoz, óvja a csapatokat az ellenséges tevékenységektől és biztosítja az elektronikai eszközeink működését a saját csapatok kisugárzó eszközeinek nem szándékos elektromágneses interferenciái mellett is. [5]
Az elektronikai támogató tevékenység hasonlóan az elektronikai felderítéshez, az ellenség által használt elektromágneses spektrumból nyeri információit, vagyis az elektromágneses és más kisugárzások jeleinek érzékelésével, azonosításával és azok felhasználásával kapcsolatos tevékenység. Az elektronikai támogatás fontos információkkal szolgál arról, hogyan használja az ellenség az elektromágneses és egyéb spektrumot. Az elektronikai támogatás érzékeli, azonosítja és felhasználja az ellenség szándékos (pl. rádióadás) és a nem szándékos (pl. kipufogó gázok infravörös hullámtartományú) kisugárzásait. A harcászati szintű elektronikai támogató rendszerek feladata a harci információk gyors lehetőleg azonnali megszerzése és továbbítása a helyi parancsnokok felé, ezzel biztosítva a minél gyorsabb és határozottabb reagálást, ezzel biztosítva az információs fölényen keresztül a vezetési fölény fenntartását. [6]
Napjaink kommunikáció berendezései által kisugárzott teljesítmény, az adaptivitásuknak köszönhetően, csak a minimálisan szükséges mértéket éri el. Felderítés szempontjából ez azzal a kellemetlen következménnyel jár, hogy az ellenőrzésünk alá vont területhez közel kell elhelyezni az érzékelőinket. Az alkalmazott multifunkciós berendezések miatt (pl. GSM/UMTS), az érzékelőknek (vevőknek) képesnek kell lenniük multispektrális (széles spektrumú) felderítés végrehajtására.
A felderítő berendezések nem önmagukban létező egységek, hanem egy bonyolult rendszer alkotóelemei. Az alkotóelemeknek olyan egymással mind fizikai, mind logikai kompatibilitással rendelkező berendezéseknek kell lenniük, amelyek biztosítják az integrálhatóságukat. A fejlesztésük során olyan jövőbe mutató architektúrális alappal kell rendelkezniük, amely hosszú évtizedekre meghatározza a fejlesztés irányát. Szerencsére a technika mai szintje mellett, olyan teljesítményű és bonyolultságú berendezések készíthetők, amelyek (a szabadon programozhatóságuk révén) tízéves távlatban megfelelő technológiai alapot nyújtanak ezen tevékenységek végrehajtásához. A nagymértékű integráció révén hatalmas számítási kapacitással bíró, mégis kis tömegű, kis fogyasztású berendezések állíthatók elő. A jelenlegi csúcskategóriájú hordozható számítógépek számítási kapacitása eléri az 1998-ban alkalmazott nagygépes architektúrák teljesítményét, fogyasztásukat és súlyukat tekintve század akkora értékkel. Elmondható, hogy mind a stacioner, mind a mobil eszközök egységes berendezés parkkal megvalósíthatóvá váltak.

A mobil technika alkalmazásánál (harcászati szinten) újabb problémák merülnek fel a hordozó eszköz kiválasztása tekintetében. Itt olyan mobil képességű eszköz alkalmazása válik szükségessé, amely minden tekintetben kiszolgálja a berendezések és a kezelőszemélyzet igényeit. A teherhordó, terepjáró képességen túl az álcázhatóság jelent kihívást, különösen a hadműveleti területen végrehajtott támogató műveletek során.
Az adatokhoz való hozzáférést a széleskörű technikai támogatás mellett sajnos meglehetősen sok tényező hátráltatja. Az egyik és legfontosabb ilyen tényező az idegen nyelvű környezet saját nyelvre történő lefordítása. Az elmúlt évtizedekben a hadseregek és titkosszolgálatok által képzett tolmácsok (fordítók) munkája nélkülözhetetlen volt. Kiképzésük az akkori feladatrendszernek megfelelően zajlott. Az elmúlt évtized során a megváltozott feladatrendszernek köszönhetően, nincs megfelelően képzett szaknyelvi személyzet. A fordítók munkáját nehezen lehet gépesíteni, bár rengeteg ígéretes próbálkozás folyik. Vannak egész fejlett automatikus nyelvi felismerő és fordító programok, amelyek kontrollálása mind a mai napig humán eszközöket igényel.
A kommunikációs és rádiótechnikai rendszerek fejlettsége olyan automata rendszer életre hívását követeli meg, amely nem csak a kommunikációs berendezések által kibocsátott jelek, hanem a rádiótechnikai (lokátorok, távirányítású robbantó szerkezetek, stb.) jeleinek vételére is alkalmasak. Külön feladatként jelentkezik ezen jelek osztályozása, és gyors felismerése, valamint harcászati körülmények között ezekre történő adekvát válasz zavarás kiadása. Itt a vevő (érzékelő) és a zavaró berendezések közötti nagysebességű vezérlő kapcsolat elengedhetetlen feltétele a gyors reagálásnak.
A keletkezett felderítő információk olyan formátumban kell rendelkezésre állniuk, amely a későbbi fúziós módon végrehajtott adatfeldolgozási mechanizmus számára elfogadható formátumot jelentenek. Kiváló példa erre az Egyesült Államok által használt ABCS (Army Battle Command and Control System), amely egységes adatbázisban kezeli a különböző szenzorok információit, így támogatva a döntéshozatali mechanizmust.
A megszerzett adatokat olyan nagy megbízhatóságú, nagy sebességű kommunikációs (informatikai) rendszeren kell továbbítani az adatfeldolgozó egységek felé, amely a továbbított információ védelmét is megfelelő szinten biztosítja. Itt a több úton kialakított kommunikációs utak kezelését is meg kell oldani.
A technikai lehetőségeinket figyelembe véve a hadászati felderítésben nem az adatokhoz (távközlési csatornákhoz) való hozzáférés jelenti a kihívást. Itt a nagyszámú párhuzamosan működő források közül, az informatívak kiválasztása jelenti a legfőbb feladatot. Ezen szelekció elvégezhető utólagosan, hosszas elemző munka végeredményeként, vagy a fúziós adatfeldolgozás eredményeként operatív segítséggel. A titkosított, vagy speciális átviteli jellemzőkkel bíró adatforrások esetén csak operatív együttműködéssel lehet tartalmi információkhoz jutni.

## A rádióelektronikai felderítés technikai kihívásai

A harcászati, hadászati kommunikációs berendezések követik a világban lezajlott folyamatokat, így döntő többségben digitális adásmódot alkalmaznak. A legnagyobb technikai kihívást ezen adásmódok vétele és azonosítása jelenti. A trendek figyelembe vételével, csak olyan berendezés alkalmazása képzelhető el, amely a legkorszerűbb szoftverrádiós technika alkalmazását valósítja meg. Napjaink vételtechnikájának meghatározó eleme a szoftverrádió technológia. Ez egy képesség technológia (enabling technology) amelynél az alkalmazott alapelvek a következőkben foglalhatók össze:

- a berendezés végső tulajdonságát az elkészített és implementált szoftver határozza meg;
- univerzálisan felhasználható elemekből épül fel;

- könnyen átprogramozható funkcionálisan tagolt blokkokból áll;
- hardveres módosítás nélkül továbbfejleszthető, ezáltal értékálló berendezés.

A szoftver rádió nem termék, hanem technológia, egyfajta készülék-építési filozófia, egy modell.

A megfelelően megtervezett és felépített vevő berendezések alkalmassá tehetők a kiterjesztett spektrumú és a különleges modulációs módok vételére is, pusztán szoftver fejlesztés révén.[1] Technikai kihívásként a berendezés elején történő tartományi konverzió végrehajtása. Itt az analóg front-end[2] fokozatnak olyan tulajdonsággal kell bírnia, amely a sávszélesség és dinamika előírásokat teljes mértékben kielégítik. A multispektrális alkalmazás miatt (minimálisan 20 MHz-6 GHz) egy megfelelő tuner egység kialakítása elkerülhetetlen. A tuner kettős kihívással kell szembenéznie. Egyrészről nagyon gyors frekvencia beállásúnak kell lennie, ugyanakkor rendkívül kis fáziszajjal kell rendelkeznie. A hopping felderítés[3] miatt a gyorsaság elengedhetetlen, míg az esetleges kis sávszélességű alkalmazások miatt a fáziszaj kritériumok szintén magasak. E kettős látszólag egymásnak ellentmondó specifikációnak megfelelni nem lehetetlen feladat (természetesen a hagyományos elvek alkalmazása itt nem lehetséges). A megfelelően kialakított tuner alkalmas lehet nemcsak a földi, de a távközlési mesterséges holdakon folyó kommunikáció vételére, amely napjainkban egyre gyakrabban kerül alkalmazásra (pl. INMARSAT, IRIDIUM). A megfelelően végrehajtott szélessávú tartományi konverzió révén, a kommunikációs eszközökön kívül, a rádiótechnikai (lokációs) berendezések vételére, analizálására is alkalmassá kell válnia az eszköznek, az igen gyors üzemmódú elektronikus nyaláb mozgatású rendszerek kezelését is megoldva. A következő nagyon fontos alapelem a mintavevő órajel stabilitása és minőségének kérdése. A legjobb minőségű átalakítók kiváló tulajdonságai kihasználatlanok maradnak korrekt órajel meghajtás nélkül. [7]

A digitalizálást követő jelfeldolgozási algoritmusok műveletigényének megbecslése és ennek kezelésére alkalmas hardver elem kiválasztása komoly tervező munka eredménye. Az algoritmusok műveletigényének meghatározására szerencsére egyre több és pontosabb módszer áll rendelkezésünkre. Az egyik legfontosabb és kikerülhetetlen eszköz a MATLAB környezet használata, amellyel blokk szintjén szimulálható és ellenőrizhető a fejlesztendő egységek korrekt működése. A megfelelően kiválasztott FPGA és DSP kombinációjával a digitális adásmódok kezelése széles tartományban megoldható. A számítási kapacitás fejlődésére jellemző, hogy 1972-ben a Cray-1–es 100 millió utasítás végrehajtására volt képes közel 2 tonnás súlyával. 1998-ban az IBM által fejlesztett nagygépes konfiguráció már 1 milliárd műveletet végzett másodpercenként, kb. 120 kg-os tömeggel. Jelenleg a csúcsot $10^{15}$–en (1 petaflop) műveletet végző szuperszámítógépek jelentik. Összehasonlításul egy korszerű laptop kb. 4 milliárd műveletet tud elvégezni, kiegészítő FPGA kártyával ez 300 milliárdra növelhető. Az áramköri elemek nagyfokú integrációja révén a teljes jelfeldolgozási folyamat egy hagyományos PC kivitelében megvalósítható. Mobil környezetben a PC-t egy laptop helyettesítheti. Amennyiben ezen tényezőket figyelembe vesszük, kijelenthetjük, hogy egy jól skálázható, mobil környezetben is teljes funkcionalitással használható berendezéshez jutunk.

---

[1] Ilyen különleges adásmód lehet például a vezeték nélküli hálózatok fizikai átvitelét jelentő COFDM (**C**oded **O**rthogonal **F**reuency **D**ivision **M**ultiplex) technológia. Itt egyszerre több ezer párhuzamosan működő csatorna egyidejű vételére és demodulálására van szükség. Ezt hagyományos vételtechnikai megoldásokkal fizikai képtelenség venni.

[2] A front-end fokozatok feladata a nagyfrekvenciás jel, ez akár 100 GHz is lehet, megfelelő sávszélességben, szintben és frekvenciában történő illesztése a tartományi konverter képességeihez. Ezek jelentik az utolsóelőtti analóg egységeket a szoftver rádiókban. Tulajdonképpen a tartományi konverterek (A/D átalakítók) képességeinek kiterjesztésére szolgálnak.

[3] A frekvenciaugratásos adások nem egy diszkrét vivő frekvencián viszik át az információt, hanem folyamatosan változtatva akár másodpercenként több ezer vivő frekvenciaváltást végezve. Ezek váltások lehető legkisebb késlekedéssel történő követése a hopping felderítés legfőbb kihívása.

Az energia ellátás és klimatikus előírások betartása ebben az esetben már nem jelent akkora kihívást, a hagyományos berendezésekhez képest. A miniatürizálás révén nem csak szárazföldi alkalmazásra nyílik lehetőség, hanem pilóta nélküli repülőgépek fedélzetén történő elhelyezésre.
Amennyiben a vételtechnikán túl zavaró tevékenység végrehajtására is szükség van, akkor meg kell valósítani a közvetlen vezérlést. A vevő és zavaró berendezések egymás közötti nagysebességű kommunikációja és vezérlése ezen cél elérésének záloga. Természetesen a zavaró berendezések hardver alapjait ugyanazon környezet valósítja meg, ezáltal a tervezés és gyártás ciklusideje jelentősen csökkenthető. Természetesen az adástechnikából adódó különbségeket leszámítva.[4]
Harcászati környezetben a tartalmi információk jelentősége nem túl nagy, mivel ezek analízisére, lefordítására az esetek többségében nincs idő és lehetőség. A hadászati szintű felderítésben a technikai paramétereken túl, a tartalmi adatok megszerzése a legfőbb cél. Itt a megfelelő szabványú adásmódokhoz történő hozzáférés megvalósítása és a megszerzett hatalmas mennyiségű információ feldolgozása képezi a legnagyobb technikai kihívást. Míg a mobil környezetben végzett felderítésnél a berendezések általában önmagukban kell, hogy biztosítsák a megfelelő infrastruktúrát az adott tevékenység elvégzéséhez, addig a hadászati szintű felderítésben hálózatba kapcsolt, egymással szoros kapcsolatban lévő berendezések üzemelnek. Ezen berendezések önmagukban csak bizonyos funkciókat valósítanak meg nagyon jó hatásfokkal, de a teljes funkcionalitáshoz szükséges az összeköttetésük biztosítása. Természetesen a harcászati szintű rendszereknek is képesnek kell lenniük egymással összekapcsolódva adatcserét végezni, de ez nem minden esetben kivitelezhető. Ilyen eset előfordulhat a kommunikációs rendszer zavarása miatt, vagy a megfelelő fedettség biztosítása érdekében végzett csak passzív tevékenység miatt. Amennyiben a kommunikációs összeköttetéseinket többféle módon kívánjuk biztosítani (tartalékolás miatt), akkor a csatornák közötti váltás vezérlését is meg kell oldani.
Tapasztalataim szerint az adatszerző munka során egyre kevesebb emberi erőforrás alkalmazására kell törekedni, mivel a rendszerek üzemeltetésében a leggyengébb láncszemet a humán oldal jelenti. Felgyorsult világunkban a szükséges, releváns, a döntések alapjául szolgáló, valóban reális információ megszerzésére rendelkezésre álló idő behatárolt, amíg maga az információtömeg, amelyből mindezeket ki kell választani, folyamatosan növekszik. Ennek megfelelően az adatok automatikus megszerzésére irányuló tevékenységek és az azokat megfelelő idő alatt információvá alakító eszközök, rendszerek és eljárások szerepe rendkívüli módon felértékelődik. [8]
Az elmúlt évtizedek során az adatszerző állomány létszámaránya egyre zsugorodott, vele párhuzamosan a feldolgozó állomány aránya viszont nőtt. Hazánkban már évekkel ezelőtt már igényként fogalmazódott meg egy automatizált adatszerző rendszer realizálására, azonban az akkor rendelkezésre álló technikai háttér miatt ez nem volt megvalósítható. Mára olyan képességű programozható logikai egységek állnak rendelkezésünkre, amelyekkel ezek megvalósítása már nem lehetetlen feladat. Az információszerzés szerves részét képezi a települési hely meghatározásának kérdése is. Ennek automatikus meghatározása szintén komoly feladat, amelyet ezen berendezéseknek szintén kezelniük kell. Itt a rádió-iránymérés megvalósítása és ennek térképen történő ábrázolása elengedhetetlen. Az iránymérés egyszerre több vételi csatorna (minimum 5-6 antenna és a teljes vételi lánc) kezelését jelenti. Megfelelő FPGA választással ez is kivitelezhetővé válik. A megkapott iránymérési adatok (több

[4] Az előállítandó zavaró jelek ugyanazzal a hardver környezettel (PC, DSP kártya, FPGA), készülhetnek, mint a vele párhuzamosan végrehajtott vétel. A kimenetén digitális analóg átalakítás után, pedig kisugárzásra kerülhetnek, így nem kell „csak” az analóg egységeket külön legyártani. A két egység közötti kommunikáció gyorsasága ebben az esetben nem kétséges.

iránymérő állomás esetén), a domborzati viszonyoknak megfelelően megjeleníthetővé vállnak térképen is.[5]
Harcászati szintű rádióelektronikai felderítés (elektronikai támogató műveletek) végzése közben a kisugárzások észlelésének gyors felismerése és ezekre történő adekvát válasz megadása jelenti a kihívást. A gyors és automatikus felismerés után, gyors reakció kell, hogy következzen, zavarás, lefogás, vagy egyszerű tudomásul vétel (pl. saját erők kisugárzása esetén). Hadműveleti szinten a keletkezett nagy mennyiségű információhalmaz feldolgozása jelenti a nehézséget. Míg harcászati szinten a tartalmi adatok megismerésére általában nincs lehetőségünk (és nem is kell erre törekednünk), addig a hadműveleti szinten ezekre az információkra van leginkább szükségünk. E kettős funkcionalitás egy egységben történő megvalósítása a mai technológiai szinten megvalósíthatóvá vált.
A tartalmi adatokhoz való hozzáférés manapság elképzelhetetlen operatív segítség nélkül. A rendszernek képesnek kell lennie ezen HUMINT forrásból származó adatok kezelésére és alkalmazására. Ki kell alakítani egy olyan adatbázis rendszert, amely képes ezen adatok automatikus relációjának kezelésére, az összadatforrású felderítés megvalósítására. Ezen automatizált rendszer kialakításának nincs technikai, technológiai akadálya.

## Összegzés, következtetések

Az eddigiekben a rádióelektronikai felderítés és az elektronikai támogatás eljárásbeli és technikai kihívásaival foglalkoztam. Az automatikusan végrehajtott rádióelektronikai felderítés, illetve az elektronikai támogatás technikai kiszolgálása a mai technikai lehetőségekkel elérhetővé vált. Olyan rendszer kifejlesztése, amely e kettős célnak megfelel elérhető közelségbe került. Kutató munkám fókuszában az említett kettős funkciójú rendszer kifejlesztésének technikai lépései állnak.
A fent leírtak alapján, felhasználva eddigi tapasztalataimat, egy olyan hardver és szoftver rendszer megalkotását tűzöm ki célul, amely alkalmas a lehető legtöbb jelenleg alkalmazott és a jövőben várható átviteli rendszer monitorozására, a megszerzett információ számítógépen történő rögzítésére, illetve a forrás adatbázisban történő elhelyezésére, mind harcászati, mind hadműveleti szinten, ezzel a fúziós adatfeldolgozási technikára épülő katonai információs rendszer alapját képezve.

## Irodalomjegyzék


[1] Dr. Haig Zolt, Dr. Várhegyi István: Információs Műveletek II. kötet. Egyetemi jegyzet, ZMNE 2004.

[2] Dr. Haig Zsolt, Dr. Kovács László, Dr. Vass Sándor, Dr. Ványa László: A 21. század kihívásai az elektronikai hadviseléssel szemben, Tanulmány, ZMNE 2008. június 3.

[3] Dr. Haig Zolt, Dr. Várhegyi István: Információs Műveletek II. kötet. Egyetemi jegyzet, ZMNE 2004.

[4] Dr. Haig Zolt, Dr. Várhegyi István: Információs Műveletek II. kötet. Egyetemi jegyzet, ZMNE 2004.


[5] A települési hely valószínűségét súlyozni kell a domborzati viszonyokkal. Így egy forrás a magaslati ponton nagyobb valószínűséggel található, mint egy völgy közepén. Ezen valószínűségi számítások elvégzéséhez elengedhetetlen valamilyen domborzati adatbázis használata.

[5] Dr. Haig Zolt, Dr. Várhegyi István, Dr. Kovács László: Információs Műveletek tartalma. CD-ROM, ZMNE 2005.

[6] Dr. Haig Zolt, Dr. Várhegyi István: Hadviselés az információs hadszíntéren, Zrínyi, 2005.

[7] Fürjes János: Nagy sávszélességű jelfeldolgozás kihívásai, Hadmérnök 2008 február, ZMNE 2008

[8] Kovács László: Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a magyar honvédségben. Doktori (PhD) értekezés, ZMNE 2003.

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Kerti András**
Zrínyi Miklós Nemzetvédelmi Egyetem
kerti.andras@zmne.hu

# KATONAI INFOKOMMUNIKÁCIÓS RENDSZERSZERVEZÉS

***Absztrakt***

*Jelen cikk a hazai infokommunikációs szakterületet jogi (normatív) szabályozatlanságának kérdéskörével foglalkozik. A szerző kísérletet tesz az ok-okozati összefüggések feltárására, amelyen keresztül javaslatot tesz a NATO szabályozási elveihez illeszkedő nemzeti rendszer kialakítására. A felvetett szisztéma moduláris felépítéséből adódóan rugalmasabban biztosíthatja az egyre gyakoribb változások révén kialakuló kihívásoknak való megfelelést.*

*This article deals with the legally uncontrolled nature of the field of infocommunication in Hungary. The author tries to reveal the cause and effect connections and by doing this he comes up with a proposal to create a national system which fits into the NATO regulation principles. The suggested system has a modular structure, thus it could be more suitable to meet the challenges arising from the more and more frequent changes - in a more flexible way.*

***Kulcsszavak:*** *Infokommunikáció, híradás, rendszerszervezés, szervezési elvek ~ infocommunication, communication, system management, organizational principles*

## BEVEZETÉS

Az elmúlt 4-5 évben nagyon sok jó publikáció, doktori értekezés látott napvilágot a híradás és infokommunikáció területéről, azonban ezek a publikációk mindegyike valamilyen részterületet érintett. Például, a rádióhíradás jövőjéről, a vezetékes technológiáról, vagy éppen a vezetékes technológia kiváltásának lehetőségéről. Nem született publikáció viszont a híradás, infokommunikációs hálózat szervezési elveiről. Ezt a hiányt azért is érzem nagynak, mert a *„Szakutasítás a szárazföldi csapatok híradás szervezési elveire” (HÍR/126)*[1] hatálytalanítása óta nincs egy a szakterületet átfogó teljes szabályzat, vagy a mostani szóhasználatot követve doktrína érvényben. Bár 1993 –ban kiadták az azóta is érvényben levő ÁLT 210 informatikai szabályzatot, jelenleg ez is elavultnak tekinthető, valamint a kiadás

évszámából következik, hogy abban a időszakban még nem sokan foglalkoztak a számítógépes hálózatokkal, az ÁLT 210 kifejezetten csak az egyedi gépekre vonatkozik.

Természetesen ez nem azt jelenti, hogy a híradó beosztású katonák nem tudják ellátni a feladatukat, és a munkájuk eredményességét a különböző missziók jól működő híradása is jelzi. Mindazon által úgy gondolom, hogy szükség lenne egy új „híradó szabályzatra", illetve a végbe ment technikai változásokat figyelembe véve egy „infokommunikációs szabályzatra".

*Mielőtt azonban megvizsgálnánk azt, hogy mit tartalmazzon egy ilyen szabályzat, meg kell vizsgálni azt is hogy ennek a „szabályzatnak" a felépítését és viszonyát a más dokumentumokhoz, szabályzatokhoz.*

Ahhoz, hogy egy ilyen szabályzatot ki lehessen dolgozni meg kell vizsgálnunk milyen változások mentek végbe az elmúlt időszakban.

## Végbement változások

A viszonyítási időszaknak a jobb híján Hír/126 kiadásának évét választottam, mivel véleményem szerint minden szabályzat és utasítás a megjelenése pillanatában kezd elavulni. Ebből a feltevésből kiindulva minden szabályzót folyamatosan, meghatározott periodicitással felül kell vizsgálni.[1] Tehát a meglátásom szerint ezért az utolsó jól szabályozott év a szabályzat kiadásának éve, amiért is bázis évnek választottam.

A híradás megszervezéseinek elveire hatással levő tényezők közül a lejátszódott változások jellegüket tekintve az infokommunikációs technikai eszközök egész világon végbement korszerűsödésével kapcsolatosak, de ugyanolyan szinten figyelembe kell vennünk szervezeti változásokat is.

***A szervezeti változások***

A szervezeti változások vizsgálatakor a legszembetűnőbb változás a Magyar Honvédség létszámcsökkenése. A jelenlegi állapot[2] alapján a létszám a kezdeti időpontnak kb. csak a 15 %-a. Ezzel együtt a csapatok, szervezetek száma is radikálisan lecsökkent.

Természetesen ez a változás csak azért jöhetett létre, mert megváltozott a feladatrendszer is. Ma már mindenki előtt ismert tény, hogy a bázisévnek tekintett időszakban a hadsereg feladata alapvetően támadó jellegű volt, nem kevés országon belüli karhatalmi szereppel.

Ma Magyar Honvédség szerepét és feladatainak irányelveit a Magyar Köztársaság nemzeti biztonsági stratégiájából tudhatjuk meg:

*„Az ország katonai biztonságának legfőbb garanciája az Észak-atlanti Szerződés Szervezete keretében folytatott szövetségi együttműködés. Magyarországnak rendelkeznie kell a NATO keretei között folytatott kollektív védelemhez és a szövetségesek kollektív védelméhez szükséges katonai képességekkel, valamint a szövetségesek részvételével zajló válságkezelő és békefenntartó műveletekben és a katasztrófa-elhárításban való részvételhez szükséges képességekkel. Magyarországnak képesnek kell lennie az Európai Unió keretében folyó*

[1] Ez a felül vizsgálat a HÍR/126 esetében is megtörtént, de a felülvizsgálat eredményeként megalkotott szabályzat tervezet nem lett bevezetve.
[2] 2008. január.

*válságkezelő tevékenységben való részvételre is. A Honvédségnek rendelkeznie kell rugalmasan alkalmazható, expedíciós műveletekre is igénybe vehető, a szövetséges erőkkel együttműködni képes, gyorsan telepíthető és fenntartható erőkkel, amelyek földrajzi korlátozás nélkül alkalmazhatók a válságövezetekben. ... A cél egy működési filozófiájában új, a vállalt szövetségi kötelezettségeket teljesíteni képes, finanszírozható, képességalapú és az Észak-atlanti Szerződés Szervezetén belül tudatosan szakosodott haderő kialakítása, ... Az ezzel kapcsolatos célokat és feladatokat a nemzeti katonai stratégiában kell rögzíteni".*[3]

A fenti szervezeti változások természetesen a vezetési rendszer változásait is magukkal hozták addig amíg a bázis időszakban a vezetési rendszer többszintű volt(ho-k hdt-k, Hds-ek), jelenleg ez a vezetési rendszer háromszintű a vezérkar, középszint, csapat szint.[4]

***Szövetségi rendszer változása***

A szövetségi rendszerünk változása is nagy hatással volt a híradás helyzetére, mert addig, amíg a VSZ-ben minden feladatra, így a híradásra is igaz, hogy nagyon központosított, felügyelt munka folyamat volt, addig ezekben a NATO úgymond ajánlásokat fogalmaz meg.

A VSz-ben attól függetlenül, hogy melyik országban gyártották a különböző eszközöket, azok szinte teljesen egyformák voltak. Ugyanez elmondható a szervezésről is, a Vsz tagállamaiban a híradófőnökök munkarendje teljesen megegyezett, sőt a 80-s évek végén a híradó szolgálatok megnevezését is egységesítettük még megnevezés szintjén is. [2]

Ma a NATO tagországok a fegyvereiket, berendezéseinket annál a vállalatnál szerzik be ahol akarják, és olyan elvek szerint alkalmazzák, ahogy nekik tetszik, ha a az eredmény megfelel a követelményeknek. A híradórendszerek egymással összekapcsolhatóságát a különböző STANAG-okban lefektetett szabványok adnák. Tehát elvben minden rendben, de azt hogy a gyakorlat más, a különböző végrehajtott gyakorlatok[5] és missziók híradási problémái a jelzik.

***A technikai jellegű változások***

Az országgyűlés 2007 őszén elfogadta a LXXIV. törvényt [3] a műsorterjesztés és a digitális átállás szabályairól, ami véleményem szerint azért volt lehetséges, mert a sokat emlegetett távközlési és informatikai hálózatok technikai konvergenciájának megvalósulása lezárult a polgári életben. Ugyanerre az eredményre jutunk, ha azt vizsgáljuk, hogy a nagy távközlési és média cégek már egy csomagban, egy szolgáltatásként –egy vezetéken- kínálják a telefon, Internet, televízió szolgáltatásukat.

Ugyan ez a konvergencia folyamat a NATO-ban is elindított egy út keresést amelynek neve NNEC.

Akarjuk vagy nem a jövő alapvető információ továbbító katonai hálózata az IP alapú lesz, kifejezetten igaz ez az állandó jellegű hálózatokra.

[3] A jelenlegi tudásom szerint a katonai stratégia még nincs elfogadva.
[4] A HM SZMSZ alapján
[5] Pl. a COMMIT, Combined Endeavor

## Infokommunikációs doktrína, stratégia vagy más?

Az általam a bevezetőben szükségesnek ítélt „infokommunikációs szabályzat” megalkotásakor az első probléma már az elnevezéssel kezdődik, mind az infokommunikációs, mind a szabályzat szempontjából.

Annak ellenére, hogy a tudományos élet és a szakmai szerveztek is jól ismerik az „infokommunikációs” kifejezést, a mindennapi életben ez nem honosodott meg, sokkal inkább az „információs” kifejezés a használatos mint például információs társadalom, információs stratégia. A HM SZMSZ, amely leír különböző felelősségeket, különböző kidolgozandó okmányokra, sem említi az „infokommunikációs” jelzőt, hanem informatikai, információtechnológiai, informatikai és hírközlési szavakat emleget a kidolgozandó stratégiák megnevezésekor.

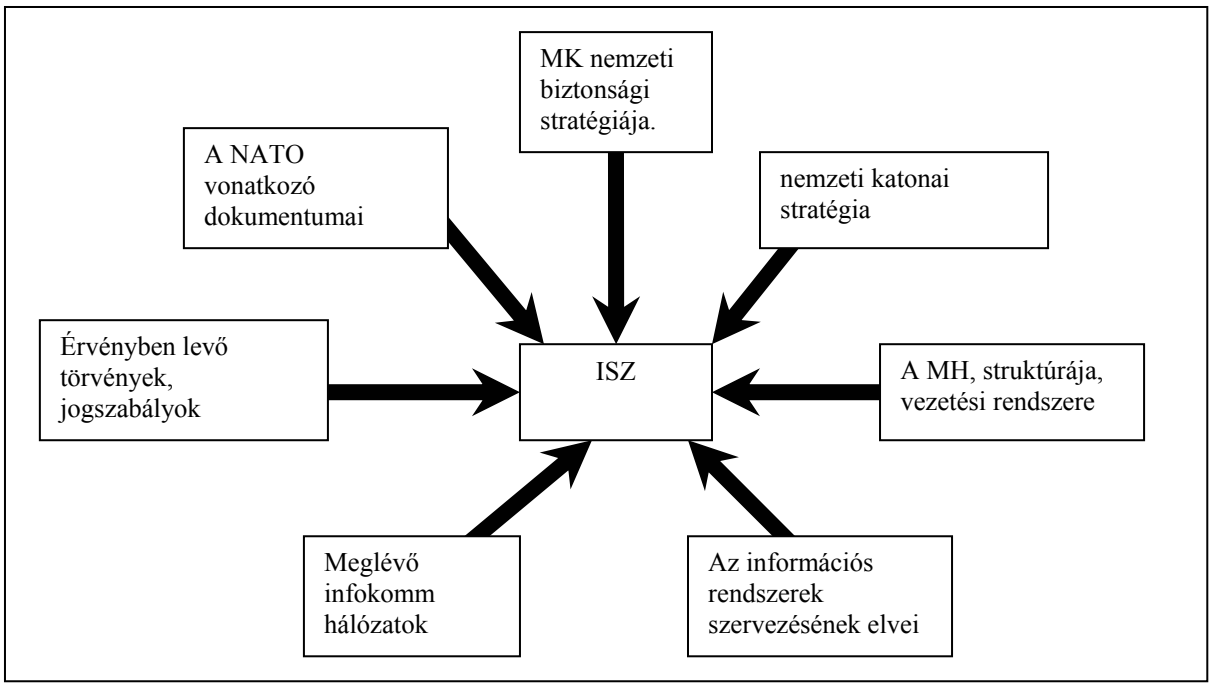
A „szabályzat” kifejezéssel is vannak bizonyos problémák, a magyar „katonai történelmi” nyelvben sokáig egyeduralkodó kifejezés volt, azonban mára már a NATO terminológiából átvett „doktrína”, „politika”, „irányelv” stb[6]. kifejezések hatására kiszorulóban van a használata. Ennek a kiszorulásnak az is az oka, hogy a régi szabályzataink szinte mindent mereven leírtak minimális eltéréseket engedve meg. Ez a felfogás a mai gyorsan változó korban nem célravezető.

Véleményem szerint azonban maga a névválasztás másodlagos sokkal inkább fontos a tartalom. Ahhoz azonban, hogy mit tartalmazzon és hogyan nézzen ki a szabályzónk, meg kell vizsgálnunk, hogy a kialakítására milyen tényezők hatnak, és milyen szerepet foglal el a szabályozási rendszerben (a továbbiakban egyelőre „Infokommunikációs Szabályzat (ISZ)”-ként fogom emlegetni.)

## Az „Infokommunkációs Szabályzat” kidolgozására hatással lévő főbb tényezők:

Az 1. ábrán láthatjuk, az „Infokommunikációs szabályzatra” hatással levő általam legfontosabbnak vélt okmányokat és tényezőket:

[6] A közöttük levő kapcsolatot viszont véleményem szerint nem teljesen szabályozott. Jelenleg 25/1997 HM utasítás a Magyar Honvédség belső szabályozó tevékenységének rendjéről, és a 93/2006 HM utasítás a szolgálati könyvek és a főnökségi kiadványok kiadásának rendjéről, szabályozza a témakört, de a kettő nincs összhangban egymással.




**1. ábra**

***A Magyar Köztársaság nemzeti biztonsági stratégiája.***

A Magyar Köztársaság Nemzeti Biztonsági Stratégiája [4] alapvetően nem katonai dokumentum, hanem az ország egészére vonatkozó biztonsági fenyegetéseket, az azokra adandó válaszokat megfogalmazó dokumentum. A katonai rész –amelyet fentebb már szinte szó szerint idéztem- a honvédség alkalmazásainak csak a legfontosabb elveit rakja le, amelyek a katasztrófavédelemben való részvétel, és szövetségi rendszereinken (NATO, EU) belüli szerepvállalás. A részletes feladatok kidolgozását a nemzeti katonai stratégiára bízza.

***Nemzeti katonai stratégia***

A nemzeti katonai stratégia a cikk írásakor nem jelent meg. Sok szaktiszttel beszélgetve azt tapasztaltam, hogy sokan arra a következtetésre jutottak, hogy a katonai stratégia kidolgozása előtt a szabályzatot nem lehet kidolgozni. Véleményem szerint a katonai stratégia megléte nagymértékben segítené a szabályzat kidolgozását, de nem feltétlenül szükséges hozzá. Egyrészt az MH fő feladatai, szervezete, az infokommunikációs hálózatok szervezésének elvei ismertek, amelyek alapján ki lehet dolgozni. Másrészt ugyan ezt bizonyítja, hogy a katonai stratégia megléte nélkül is meg lehetett szervezni a missziók, és gyakorlatok infokommunikációs hálózatait. Igaz ez felveti azt a kérdést, ha tudunk a szabályzat nélkül dolgozni, akkor az nem is kell. Meggyőződésem de igen is szükség lenne rá. Az általam javasolt, okmányok nagymértékben segítenék a napi munkát, egy fajta keretet biztosítanának az információs rendszer tervezéséhez, szervezéséhez és üzemeltetéséhez.

***A NATO vonatkozó dokumentumai***

Az általunk tervezendő hálózatoknak mindenféleképpen csatlakozniuk kell a szövetségi rendszerünkben szerepet vállaló többi ország fegyveres szervezeteinek hálózataihoz, illetve a NATO C4ISR rendszeréhez, ez viszont csak akkor valósítható meg, ha tisztában vagyunk a követelményekkel.

### *Meglévő infokommunikációs hálózatok*

A Magyar Honvédség már rendelkezik egy kialakított infokommunikációs hálózattal, amelyet a MH pénzügyi helyzetének megfelelően folyamatosan korszerűsítenek. Minden kialakításra kerülő (tábori) híradó és informatikai hálózatot valamilyen formában csatlakoztatni kell ehhez, ezért ez nagymértékben befolyásolja lehetőségeinket, és messzemenően figyelembe kell vennünk mindenféle tervezési és szervezési feladatnál.

### *A Magyar Honvédség, struktúrája, vezetési rendszere*

„…azoknak a kollektíváknak és törzseknek, amelyek útján korunkban a parancsnok összegyűjti az információkat és hatalmát gyakorolja, nagyszerűen egymásba illeszkedő és simán működő gépezetnek kell lenniük.” [5] Eisenhower tábornok szavai ma is épen olyan időszerűek mint amikor 1948-ban papírra vetette őket. Akarjuk vagy nem, de az infokommunikációs hálózatok szerepe az, hogy ezeknek a „gépezeteknek” a munkáját segítse, közöttük a megfelelő, a kor színvonalán álló információ, adat áramlást biztosítsa. Ebből kifolyólag az infokommunikációs hálózatok felépítésére vonatkozó alapvető rendező elv a Magyar Honvédség strukturális felépítése és az ebből következő vezetési rendszere.

### *Érvényben levő törvények, jogszabályok*

Ma Magyarországon jogrend uralkodik, ami azt jelenti, hogy az életünket különböző törvények és jogszabályok irányítják, semmilyen hivatalos irat, iromány nem lehet ellentétes a jogszabályokkal, és a kidolgozásukkor, az irat tárgyával kapcsolatos jogszabályoknak meg kell felelni. A honvédelmi miniszter is a Magyar Honvédség életét különböző jogszabályokkal irányítja. Az „Infokommunikációs Szabályzat (ISZ)” kidolgozásakor is sok jogszabályt kell figyelembe venni.

### *Az információs rendszerek szervezésének elvei*

Mielőtt kitérnék arra, hogy a fent vázolt változások milyen hatással lehetnek az infokommunikációs hálózat tervezésére, nézzük meg milyen kapcsolatokkal kell rendelkeznie, egy feladatát végző katonai alakulatnak, szervezetnek. Ehhez egy elképzelt missziós feladatot végrehajtó szervezet infokommunikációs kapcsolatait veszem alapul.

Könnyen belátható, hogy ebben az esetben a következő összeköttetéseket kell megszervezni:

- Az elöljáró parancsnoksággal
- A Magyarországon levő elöljáró parancsnoksággal,
- Az alárendelt szervezetekkel
- Az együttműködő illetve szomszédos alakulatokkal, szervezetekkel
- A helyi polgári szervekkel

Továbbá természetesen ki kell alakítani a vezetési pontok belső infokommunikációs rendszerét is.

A fenti séma alkalmazható az összes esetben, csak a különböző feladatok végrehajtásakor, más és más összeköttetések kapnak nagyobb hangsúlyt, illetve kisebb szerepet.

Ahhoz azonban, hogy ezt a kapcsolati rendszert ki lehessen alakítani, sok tényezőt kell figyelembe venni, ezek:

- A vizsgált alakulat szervezeten belül elfoglalt helye.
- A végrehajtandó feladat.
- A földrajzi környezet.
- A saját technikai lehetőségeink.
- A parancsnok elhatározása a feladat végrehajtására.
- Az elöljáró híradó szervezet híradó utasítása, a vezetés rendszere.

## Az „Infokommunikációs Szabályzat" felépítése és tartalma

A fenti felsorolásból látszik, hogy az ISZ kidolgozása nem egyszerű feladat, ha mindent aprólékosan ki akarunk dolgozni, maga az iromány méreteivel egy több kötetes irodalmi művel vetekedne. Ha ehhez még figyelembe vesszük, hogy fenti tényezők közül több is időről-időre változik, azokat felülvizsgálják, mire elkészül az ISZ, addigra dolgozhatjuk is át. Véleményen szerint, ebből kiindulva mindenképpen egy többfokozatú szabályzó rendszert kell kialakítanunk.

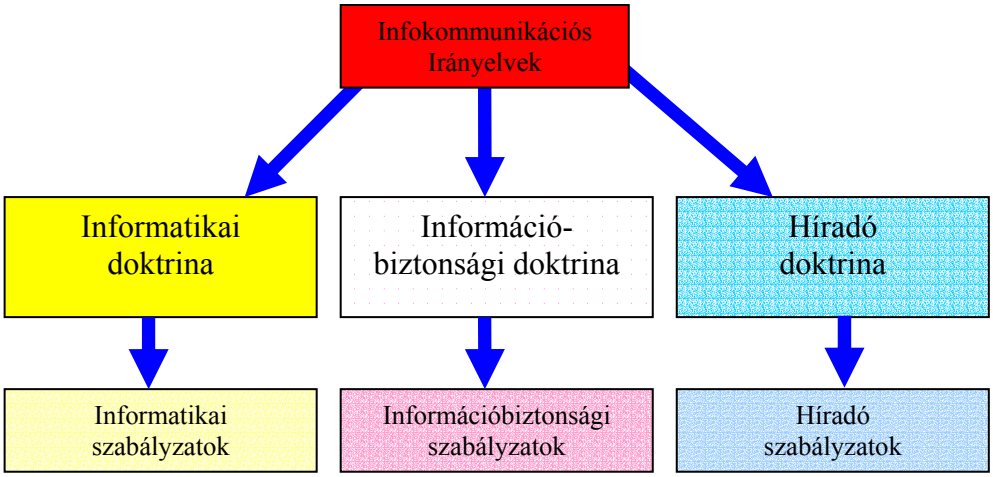
A szabályzó rendszer legfelső szintű alkotó eleme egy rövid, 4-5 oldalas, nem csak a szakemberek számára készül, hanem mindenki által érthető, a teljes infokommunikációs rendszert átfogó irányelveit tartalmazó dokumentum kell hogy legyen. Ennek a dokumentumnak a neve Infokommunikációs Irányelvek (II) lehetne. A tartalmára pedig a következő a javaslatom:

- Az II célja, időbeli és szervezeti hatálya.
- Az infokommunikációs rendszer tervezésének, szervezésének, irányításának rendje.
- A kidolgozandó dokumentumok, azok elkészítésének rendje.
- Az infokommunikációs rendszer részterületeinek egymáshoz való viszonya.
- A felülvizsgálat rendje.

Az II mellékleteként szerintem, meg kell adni azoknak a dokumentumoknak az elérhetőségét, amelyek szükségesek lehetnek az infokommunikációval foglalkozók számára. Ilyenek lehetnek a különböző törvények, és jogszabályok, illetve segédletek. Az utolsó pontban említett felülvizsgálat rendje a manapság tapasztalható gyors változások miatt szükséges.

A szabályzó rendszer középső szintjét az infokommunikációs rendszer alkotó elemeinek irányelvei, doktrínái kell hogy képezzék. Melyek ezek a részterületek? Elsőre egyértelmű, hogy az informatika, és a távközlés (híradás), azonban véleményem szerint van egy harmadik részterület is, amelyre mindig is nagy figyelmet fordított mindkét részterület, azonban különálló részterületként csak mostanában kezd kibontakozni, ez pedig az Információbiztonság vagy az Információszavatolás (IA, Information Assurance). Egyértelmű, hogy a három részterület egymással szoros összefüggésben van, és éppen ezért nem lehet ezeket egymástól függetlenül kialakítani. Ezeknek a részterületeknek a tatalma részterületenként más és más, ezeket a szakterület felelősöknek kell kialakítani.

A harmadik szintje a szabályzó rendszernek, amikor az előző kettő szabályozóra alapozva kialakítjuk a részterületek részterületeinek az előírásait. Ezek a részterületek a –teljesség igénye nélkül- híradóknál a rádiós, a műholdas, stb. összekötetések megszervezésének szabályzatai, az információvédelem tekintetében a fizikai, személyi, elektronikus, stb. biztonsági szabályzatok. A 2. ábra szemlélteti az általam elképzelt szabályozási rendszert:




**2. ábra**

A szabályzó rendszer második és harmadik szint kidolgozása meghaladja ennek a cikknek a terjedelmét és véleményem szerint egy teljes „infokommunikációs törzs”-re lenne szükség hozzá, ezért ebben a cikkben nem foglakozom vele.

## Összegzés

Az hogy egy szabályzó rendszer megalkotása a mai Magyar Honvédségben mennyire nem egyszerű feladat azt Szenes Zoltán szavai is mutatják: ”A szervezeti változások, a technikai fejlesztések miatt a már kidolgozott dokumentumok is több tekintetben elavultak. A minisztérium és parancsnokságok gyakori átszervezése miatt a doktrínaíró csoportok nem tudtak stabilizálódni, fordításra, kiadásra nem volt elég forrás.” [6]

Ennek ellenére, mindenképpen úgy ítélem meg, hogy egyre inkább szükség van az infokommunkáció részterületeit egy egységes rendszerként kezelő szabályzórendszer kidolgozására, amelynek messzemenőkig figyelembe kell venni a NATO követelményeket, illetve a hazai objektív feltételeket.

Az általam javasolt rendszer nagymértékben hasonlít a NATO szabályozási rendszeréhez (Policy, Directives, Guidance), és moduláris rendszere miatt, biztosítaná, hogy az egyes összetevőket érintő változások esetén, csak a rész doktrínákat, illetve szabályzatokat keljen átalakítani, ami az egész rendszert nem érintené.

## Felhasznált irodalom

1. Szakutasítás a szárazföldi csapatok híradás szervezési elveire (HÍR/126)

2. ÚTMUTATÓ a hírközpontok hadműveleti-technikai szolgálat megszervezésére és ellátására Hír/348

3. 2007. évi LXXIV. Törvény a műsorterjesztés és a digitális átállás szabályairól.

4. 2073/2004. (III. 31.) Korm. Határozat A Magyar Köztársaság nemzeti biztonsági stratégiája. Internet letöltés 2007-11-18:

http://www.mfa.gov.hu/kum/hu/bal/Kulpolitikank/Biztonsagpolitika/Nemzeti_biztonsagi_strategia.htm

5. Dwight D. Eisenhower: Keresztes háború Európában Budapest Zrínyi kiadó 1982

6. Szenes Zoltán: Magyar Honvédség a NATO-ban. Mit várhatunk Rigától? Hadtudomány 2006/4 Internet letöltés. http://www.zmne.hu/kulso/mhtt/hadtudomany/2006/4/2006_4_6.html

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Gábri Máté**
Zrínyi Miklós Nemzetvédelmi Egyetem
gabrimate@ippimail.com

# A CYBERBŰNÖZÉS ÚJ HAJNALA - OROSZ ÜZLETEMBEREK A VILÁGHÁLÓN

***Absztrakt***

*Már az internet születése előtt „divat" volt a telefonos hálózatok feltörése pusztán szórakozásból, vagy egy-egy távolsági hívás kedvezményes lebonyolítása miatt. A világháló segítségével a kártékony szoftverek terjedése és terjesztése előtt új dimenziók nyíltak, illetve a távoli hálózatok elérhetővé váltak a kíváncsi szemek számára. Mindezidáig az interneten folyó bűnözői tevékenység jelentős részét az egyéni szórakoztatás, valamint az egyszemélyes, esetleg kis létszámú csoport haszonszerzési szándéka tette ki. Napjainkban megfigyelhető, hogy komoly gazdasági és politikai érdekeltséggel bíró szervezetek jelennek meg a cyberbűnözők között. Jelen írás egy ilyen esetet kíván bemutatni az elmúlt másfél év eseményei alapján.*

*People liked to hack into the telephone networks before the internet was borne to make trunk calls cheaper. The malicious code or software could spread farther and faster with the World Wide Web, and the networks became more accessible for the curious eyes. Until recently crime on the internet was like a hobby for some enthusiasts, or money making for individuals or a small group. However, nowadays groups with economic and political interests are appearing behind cyber-crime. This paper's aim to describe such a group based on events in the last one and a half years.*

***Kulcsszavak:*** *cyberbűnözés, spam, Russian Business Network, botnet ~ cyber-crime, spam, Russian Business Network, botnet*

## BEVEZETÉS

A világháló hasznos és jó dolog. Végtelen sok funkcióját, szolgáltatását, lehetőségeit felsorolni szinte lehetetlen, azonban erre nincs is szükség, hiszen a fontosabbakat nap, mint nap használjuk: információ-keresés, csevegés, levelezés, böngészés. Kis gyakorlattal pillanatok alatt megtalálhatunk bármit az interneten, unaloműzőként pedig beszélgethetünk, levelezhetünk ismerőseinkkel vagy akár új barátokat szerezhetünk. Ez a kellemes és egyben hasznos időtöltés azonban nem veszélytelen, és hogyha nem vagyunk kellően tudatosak, és nem figyelünk eléggé, akkor könnyen áldozatul eshetünk a világhálón egyre inkább terjedő,

otthoni felhasználókat célzó bűnözésnek.

Az internet robbanásszerű fejlődése az ezredforduló környékére tehető, amikor a szélessávú, percdíj nélküli internet elérhetővé vált a lakosság szélesebb rétegei számára. Egyre nagyobb igény mutatkozott a meglévő szolgáltatások fejlesztésére, újak bevezetésére, majd ezek segítségével jutott el közvetlenül szinte minden emberhez a világháló. Új dimenzió nyílt meg a szolgáltatói szektor számára, tele kiaknázatlan lehetőségekkel, melyre természetesen a bűnözői körök is szemet vetettek. A folyamatosan frissülő, bővülő otthoni felhasználói tábor kétségkívül ideális célpontot jelent a rossz indulatú személyek, szervezetek számára.

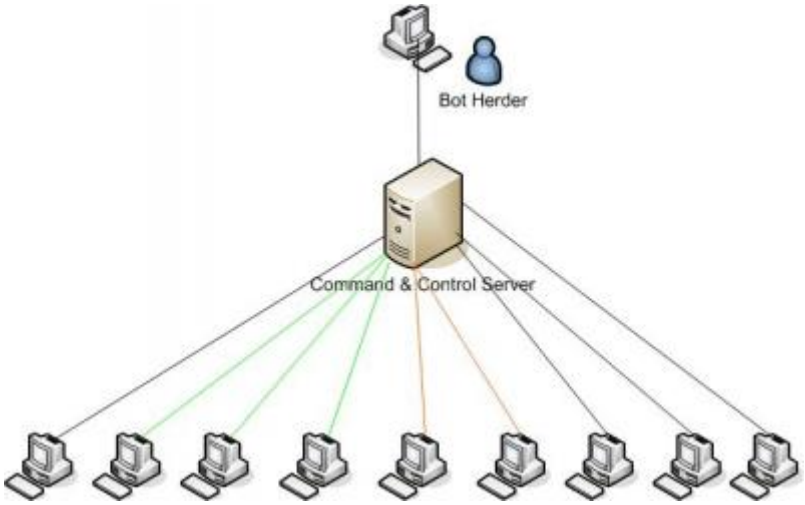
Az otthoni felhasználó alapvetően jóhiszemű, hiszen egy fizetős szolgáltatást használ, ezért eleinte nem gyanakszik, illetve nem feltétlenül van tisztában az interneten előforduló fenyegetésekkel. Éppen ezért kevesebb, vagy éppen semmilyen figyelmet nem fordít számítógépe és internetforgalma biztonságára, és minden megjelenő tartalmat jóindulatúnak minősít. A kártékony kódok, programok ezt a helyzetet használják ki azokon a szolgáltatásokon keresztül, melyeket napi rendszerességgel használunk. Ilyenek például e-mailben terjedő vírusok vagy a sűrűn látogatott weboldalakba beillesztett kódrészletek, melyek tartósan megfertőzhetik a látogató számítógépét, vagy információkat – például a látogatott weboldalon megadott felhasználónév és jelszó, bankszámlaszámok és PIN-kódok, a számítógépen tárolt jelszóadatbázis, stb. – juttathatnak el a kód készítőjéhez. A sor szinte a végtelenségig folytatható, hiszen a lista kimeríthetetlen, és nap, mint nap újabb módszerekkel bővül.

Cikkemben egy olyan gazdasági szervezetet szeretnék bemutatni, amely végtermékként legális tevékenységet, szolgáltatást folytat, azonban jövedelmét mégis a világhálón megtalálható illegális forrásokból szerzi.

## A *Storm* féreg

A tavalyi év elején egy újabb, kártékony e-mail melléklet jelent meg az interneten, ami a *Storm Worm* (Storm féreg) névre hallgatott. Ugyanakkora figyelmet kapott, mint a naponta több tucatnyi megjelenő más káros program, tehát szinte semmit. A programocska júniusban kezdett feltűnni a különféle informatikai biztonsággal foglalkozó híroldalak hasábjain, illetve a technikai fórumokon. Ekkor derült fény arra, hogy az eddig csendben terjedő „élősködő” a megfertőzött gépeket egy úgynevezett bot-hálózatba csatolja[1] *(lásd: 1. ábra: A botnet felépítése)*.

1 A bot-hálózat, vagy ismertebb nevén *botnet*, olyan „zombi” gépekből álló internetes hálózat, melyet egy másik hasonló zombi gép, vagy egy személy irányít és használ fel illegális cselekedetekre.




*1. ábra: A botnet felépítése*

A több tízezres „géppark” már szép eredménynek mondható egy botnet esetén, amivel napi több százezer spam[2] küldhető, vagy komoly *DDoS*[3] támadás indítható internetes kiszolgálók ellen. Pesszimista becslések szerint a *Storm* worm által megfertőzött gépek száma 250 ezer és 1 millió közé tehető[1], míg mások szerint elérte a 10 milliót [2] is.

A hagyományos botnetek vezérlése egy központi webszerveren, vagy IRC-csatornán keresztül történik. Ez a kapcsolat könnyen felderíthető és blokkolható akár az internetszolgáltató, akár a helyi hálózati infrastruktúrában található csomagszűrők által. A *Storm* készítői ezért egy másik, decentralizált vezérlési formához nyúltak. Az alkalmazott protokoll a *peer-to-peer* nevet viseli, és itt nem egy központi kiszolgálóról gyűjtik be az információt a kliensek, hanem mindegyik kliens csak két másikat lát, az egész hálózatot nem. Természetesen megfelelő idő alatt ez a felépítés is visszakövethető lenne, azonban itt nem néhány tucat, hanem több százezer gép kapcsolatáról beszélünk. Ebben a *peer-to-peer* hálózatban is található néhány vezérlő gép, ahonnan a parancsok kiindulnak. A támadók, hogy elrejtsék ezeket a klienseket, az úgynevezett *fast-flux* eljárást használják. Minden egyes géphez több (akár több ezer) IP címet rendelnek, melyeket folyamatosan cserélnek, így a kiinduló parancsok, kapcsolatok mindig más kiindulási címet mutatnak és szinte lehetetlen visszakövetni, hogy fizikailag hova mutatott az adott cím[3]. Mintha ez még nem lenne elég, a *Storm* Worm egy meglehetősen egyszerű védelmi mechanizmussal is rendelkezik. Amikor észleli, hogy a hálózati adminisztrátorok behatolás észlelő[4] eszközökkel vizsgálják a gépeket, akkor *DDoS* támadást indítanak az ellenőrzést végző gép ellen.

A kezdetekben a *Storm* bot saját magát terjesztette spamekkel, azonban a több százezres infrastruktúra már sokkal nagyobb lehetőségeket rejt magában. A hálózat egy részét *DDoS* támadásokra használták, míg más részét bérbe adták személyeknek, cégeknek, akik kéretlen e-mailek küldésére használták a megfertőzött gépeket. Szeptember 9-én 280 ezer fertőzött gépről tudtak biztosan, amelyek aznap összesen 2,7 milliárd spamet küldtek szét az

2 Kéretlen e-mail. Olyan levél, melyet a címzett szándéka ellenére kapott.

3 Distributed Deniel of Service, vagyis elosztott szolgáltatás-megtagadási támadás. A „hagyományos” szolgáltatás-megtagadási támadás precízebb formája, ugyanis itt nem egy, hanem több számítógép vesz részt. A támadást indító számítógépek csatlakozási kérelmet (TCP SYN csomag) küldenek a szolgáltatást nyújtó szervernek, az visszaküldi a kérés nyugtázását és a saját kapcsolatfelépítési kérelmét, amire azonban már nem kap választ. A kiszolgáló 30 másodpercig nyitva hagyja a kapcsolatot a beérkezési kérelemre várva és ez idő alatt a memóriában le van foglalva a kapcsolat számára bizonyos hely. Elosztott támadás esetén másodpercenként akár több tízezer kérés érkezhet, ami könnyen használhatatlan állapotba juttattatja a szervert, így a valódi kapcsolatot igénylő kliensek számára elérhetetlenné válik a szolgáltatás.

4 IDS, Intrusion Detection System.

interneten, ami körülbelül 4%-a volt a teljes spam forgalomnak. [4]

A *Storm* féreg ráadásként egy úgynevezett *rootkit*-et is telepített az áldozat gépére, melynek segítségével egy támadó azonnal rendszergazdai jogosultságot szerezhetett a gépen. Eleinte külön meghajtóként települt, így viszonylag könnyebb volt felderíteni és eltávolítani, azonban később már meglévő rendszermeghajtókba – mint például a hálózat egy protokolljáért felelős tcpip.sys, vagy a cdrom.sys – települt, megnehezítve az ártalmatlanná tételüket [5].

## Illegális szolgáltatás, legálisan?

A kártékony programokat, vezérlő szoftvereket valahol tárolni kell, a legtöbb esetben az internet-szolgáltatók tárhelyét használják e célra. Amint az illetékes szolgáltató arról értesül, hogy szerverein káros anyagokat tárolnak, azonnal törli azt, egyebet sajnos nem tehet.

Az orosz **Russian Business Network** (továbbiakban RBN) elsősorban tárhelyszolgáltató, azonban más internetes tevékenységet is folytat. Ügyfelei számára garantálja, hogy a tartalmat nem törlik, illetve szervereik védve vannak a különféle *DDoS* támadásoktól. Természetesen ezt a „szolgáltatást" meg kell fizetni. Egy átlagos méretű tárhely körülbelül hat-tízszerese a hagyományos szolgáltatók által kiszabott díjnak. A kapcsolatfelvétel nem hivatalos formában történik: fórumokon, levelezőlistákon keresztül lehet elérni az üzemeltetőket és a kívánt tárhelyet, illetve egyéb szolgáltatásokat megigényelni.[6] A jelenlegi jogszabályok – főleg az Orosz Föderációban – nem kényszerítik az internet-szolgáltatókat a kártékony tartalmak eltávolítására, így az RBN zavartalanul működtetheti webszervereit.

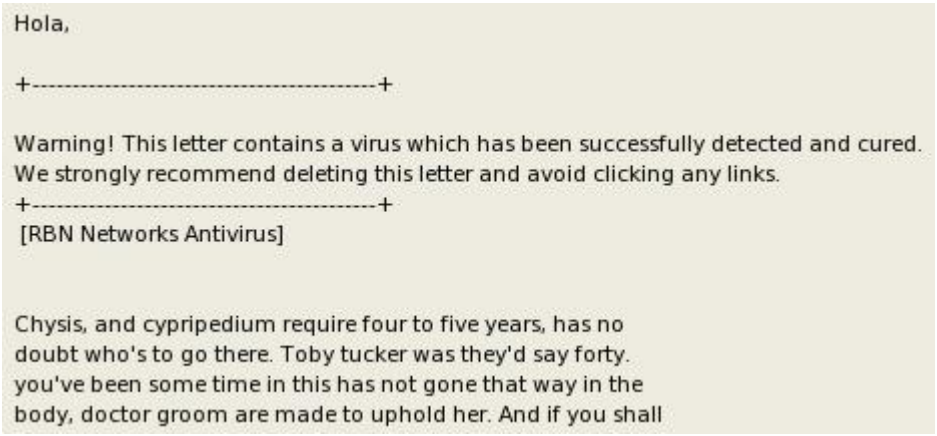
Az RBN természetesen nem csak tárhelyszolgáltatással foglalkozik. Bevezette az egyik legdivatosabb alvilági módszert, a védelmi pénz szedését. Az eljárás egyszerű: *DDoS* támadással megbénítanak egy gépet, vagy akár egy teljes hálózatot, majd felkeresik az üzemeltetőt, és egy tetemesebb havi összegért garantálják a szolgáltatások védelmét. [7] Emellett aloldalakon keresztül eladásra kínálnak rendszer- és hálózati feltörést segítő szoftvereket. A felhozatal teljesen vegyes, és található néhány igazi „gyöngyszem" is, például grafikus felületű, fejlesztői támogatást élvező termékek. Ilyen az *Mpack* nevű eszköz, mellyel tetszőleges, weboldalba épülő kódokat lehet készíteni, melyek megfertőzik a látogatók gépét, majd egy webes felületen keresztül a támadó adatokat – elsősorban internetes banki tranzakcióknál használt információt – lophat az áldozat számítógépéről. A szoftver körülbelül 700 dollárba kerül, ami magában foglal egy éves támogatást, illetve lehetőség van kiegészítők vásárlására is. [8] Az *Mpack* leglátványosabb megjelenése a *Bank of India* honlapjának megfertőzése volt. [9] A honlapba egy 3 soros kódot [10] ültetett a támadó, ami kártékony programok tucatjait telepítette a látogatók számítógépére.

Nyár végére a két legkiterjedtebb botnet a *Storm* és az *Mpack* által megfertőzött hálózatok voltak. Olyannyira elterjedtek, hogy a készítők egymást kezdték támadni „cyberhadseregeikkel". A többszázezres gépparkok *DDoS* támadásai olyan mértékű internet-forgalmat generáltak, hogy egyes szolgáltatók be tudták mérni a főbb vezérlőgépeket és az érintett hálózatot egyszerűen lekapcsolták a világhálóról.

Novemberben a teljes RBN hálózat eltűnt az internetről, egyrészt a leválasztás miatt, másrészt, pedig a tulajdonosok állították le a szervereket. [11] Nem sokkal később Kínában és Tajvanon vélték felfedezni az RBN nyomait. [12] A Spamhaus.org adatbázisa szerint [13] széles IP tartományokat regisztráltak, azonban aktív használatuk elmaradt. Feltételezett megjelenésük nagy nyilvánosságot kapott szakmai körökben, így kiemelt figyelemmel illették az adott IP tartományokat az informatikai biztonsággal foglalkozó szervezetek. Ennek hatására ismét „sátrat bontottak" és eltűntek a világhálóról. Feltételezhetően ismét felbukkannak majd, azonban jóval elővigyázatosabbak lesznek. Több mint valószínű, hogy ezúttal a világ különböző pontjain, több internet-szolgáltatónál elosztva fognak megjelenni, hogy felderítésük nehezebb legyen.

### Miről mesél egy spam?

Vélhetően jelen cikk szerzője is kapott egy, az RBN létezésére utaló nyomot. A *2. ábrán* egy spam látható, amit feltehetően az RBN-en keresztül kézbesítettek. A törzsszöveg gyakorlatilag lényegtelen, csak a megszólítás utáni kiemelt rész a fontos, ami figyelmeztet minket, hogy a levél vírust tartalmaz, azonban a kereső szoftver ezt sikeresen felfedezte és hatástalanította, majd javasolja a levél törlését, és azt tanácsolja, hogy egyetlen linkre se kattintsunk. Ami a legérdekesebb az az, hogy mindezt az *RBN Networks Antivirus* szoftvere végezte, a levél szerint. Gyanítom az e-mail míg elérte a laptopomat semmilyen szűrésen nem esett át, mégpedig azért, mert a figyelmeztetés ellenére nem tartalmazott semmilyen linket, mellékletet és a számítógépemen futó víruskereső sem talált semmi gyanúsat. Ebből arra következtetek, hogy a figyelmeztetést az RBN hálózatot használó spammer, vagy az általuk készített spamküldő szoftver beilleszt egy ilyen, vagy ehhez hasonló automatikus üzenetet a címzett megnyugtatására.


Hola,

+----------+

Warning! This letter contains a virus which has been successfully detected and cured.
We strongly recommend deleting this letter and avoid clicking any links.
+----------+
[RBN Networks Antivirus]

Chysis, and cypripedium require four to five years, has no
doubt who's to go there. Toby tucker was they'd say forty.
you've been some time in this has not gone that way in the
body, doctor groom are made to uphold her. And if you shall

*2. ábra: Spam az RBN-től*

A levél forrása *(lásd: 3. ábra: RBN spam forrása)* mutatja, hogy a helyi gépen futó spam- és vírusszűrő nem találta gyanúsnak.[5] A spam-et küldő SMTP szerver feltehetően egy fertőzött olasz irodai szerver, mégpedig azért, mert statikus IP címmel rendelkezik[6], azonban a címhez nem tartozik regisztrált domain név *(lásd: 4. ábra: A spammer név szervere)*[7], valamint MX rekord *(lásd: 5. ábra: A spammer MX rekordja)*. A bejegyzett és megfelelő IP címre mutató MX, valamint PTR rekord elengedhetetlen a hiteles e-mail küldéshez. Sajnos a fogadó szerverek többsége nem ellenőrzi ezek meglétét, elősegítve a spam-ek terjedését.

5 X-Virus-Flag: no és X-Spam-Status: No jelölés.

6 Több, mint valószínű, hogy a szervert internet átjáróként használja egy vállalkozás és azért kapott fix címet, mert a szolgáltatóknál az üzleti előfizetéshez ez jár.

7 Nincs bejegyzett név szerver és az IP címet a szolgáltató által biztosított igen hosszú és kacifántos név oldja fel. (host88-32-static.43-88-b.business.telecomitalia.it)

```
X-Virus-Flag: no
Return-Path: <lichenology@gampot.com>
X-Spam-Checker-Version: SpamAssassin 3.2.4 (2008-01-01) on notebook
X-Spam-Level:
X-Spam-Status: No, score=0.0 required=5.0 tests=HTML_MESSAGE autolearn=ham
        version=3.2.4
X-Original-To: info@duosol.hu
Delivered-To: m5070@royalty.hu
Received: from host88-32-static.43-88-b.business.telecomitalia.it (host88-32-static.43-88-b.business.telecomitalia.it [88.43.32.88])
        by royalty.hu (Postfix) with SMTP id D404338245
        for <info@duosol.hu>; Mon, 17 Mar 2008 15:39:38 +0100 (CET)
Date: Mon, 17 Mar 2008 14:41:50 +0000
From: "Clarkin Burel" <lichenology@gampot.com>
X-Mailer: The Bat! (3.0.2.2) Professional
Reply-To: Clarkin Burel <lichenology@gampot.com>
X-Priority: 3 (Normal)
Message-ID: <9372130529.20080317143724@gampot.com>
To: <info@duosol.hu>
Subject: valle
```

*3. ábra: RBN spam forrása*

```
notebook scout3r # host -t NS host88-32-static.43-88-b.business.telecomitalia.it
host88-32-static.43-88-b.business.telecomitalia.it has no NS record
```

*4. ábra: A spammer név szervere*

```
notebook scout3r # host -t mx host88-32-static.43-88-b.business.telecomitalia.it
host88-32-static.43-88-b.business.telecomitalia.it has no MX record
```

*5. ábra: A spammer MX rekordja*

Tovább kutattam a rejtélyes spammer gép után és még érdekesebb információra találtam, amivel korábbi feltételezésemet támaszthatom alá, miszerint a küldő gép egy fertőzött irodai szerver. A kiszolgálón futtatott operációs rendszer nagy valószínűséggel Microsoft Windows Server valamelyik verziója és a világháló felé nyitott szolgáltatások is ezt mutatják *(lásd: 6. ábra: A spammer szerver adatai)*. Ami még érdekes lehet az a PPTP, ami a VPN megvalósítások egyik változata, mely a Microsoft termékeiben is megtalálható. Sajnos ez a protokoll hemzseg az ismert biztonsági résektől ezért használata erősen ellenjavallt. [14]

A tárgyalt kiszolgálón futó verzió például támadható érvénytelen TCP fejléc beállításokkal. A támadó ezt kihasználva egyetlen egy, jól megszerkesztett csomaggal lekapcsolhatja a cél tűzfalát, teljes és nyitott hozzáférést szerezve a géphez *(lásd: 7. ábra: PPTP sebezhetőség)*.[8] Az elemzés utolsóként egy Webmin nevezetű szolgáltatást vélt felfedezni, azonban ez csak UNIX alapú rendszereken érhető el. Rövid keresés után egy hálózati adatmentő szoftverre bukkantam, ami alapértelmezett beállításként a 10.000-es TCP portot használja Windows alatt. Feltételezem ehhez hasonló futhat a kiszolgálón.

Látható, hogy SMTP (25-ös TCP port) szolgáltatás nem fut a gépen, így e-mail szerver nem lehet a kiszolgáló. Ebből is csak arra tudok következtetni, hogy a spam-et, vagy spam-eket küldő kártékony szoftver feladatát befejezve inaktív állapotba került, hogy majd egy későbbi időpontban ismét levélszeméttel áraszthassa el a világhálót.

8 A hibakeresés a Nessus (http://www.nessus.org) nyílt forrású szoftverrel készült.

```
notebook scout3r # nmap -sS -sV -O host88-32-static.43-88-b.business.telecomitalia.it

Starting Nmap 4.20 ( http://insecure.org ) at 2008-03-18 22:31 CET
Interesting ports on host88-32-static.43-88-b.business.telecomitalia.it (88.43.32.88):
Not shown: 1687 closed ports
PORT      STATE    SERVICE       VERSION
67/tcp    filtered dhcps
135/tcp   filtered msrpc
136/tcp   filtered profile
137/tcp   filtered netbios-ns
138/tcp   filtered netbios-dgm
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1723/tcp  open     pptp?
3389/tcp  open     microsoft-rdp Microsoft Terminal Service
10000/tcp open     http          Webmin httpd
Device type: general purpose
Running (JUST GUESSING) : Microsoft Windows 2003|2000|XP (97%)
Aggressive OS guesses: Microsoft Windows 2003 Server SP1 (97%), Microsoft Windows 2000 Server SP4 (90%), Microsoft Windows 20
00 SP4 (90%), Microsoft Windows XP SP2 (90%), Microsoft Windows XP SP2 (firewall disabled) (90%), Microsoft Windows 2000 SP3
(89%), Microsoft Windows 2000, SP0, SP1, or SP2 (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

OS and Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 143.657 seconds
```

*6. ábra: A spammer szerver adatai*

**Security Issues and Fixes: host88-32-static.43-88-b.business.telecomitalia.it**

| Type | Port | Issue and Fix |
|---|---|---|
| Vulnerability | pptp (1723/tcp) | The remote system appears vulnerable to an invalid Options field within a TCP packet. At least one vendor firewall (Symantec) has been reported prone to such a bug. An attacker, utilizing this flaw, would be able to remotely shut down the remote firewall (stopping all network-based transactions) by sending a single packet to any port.<br><br>See also :<br><br>http://www.eeye.com/html/Research/Advisories/AD20040423.html<br><br>Risk factor : High<br>CVE : CVE-2004-0375<br>BID : 10204<br>Other references : IAVA:2004-A-0010, OSVDB:5596<br>Nessus ID : 12216 |
| Informational | pptp (1723/tcp) | Synopsis :<br><br>A VPN server is listening on the remote port.<br><br>Description :<br><br>The remote host is running a PPTP (Point-to-Point Tunneling Protocol) server. It allows users to set up a tunnel between their host and the network the remote host is attached to. |

*7. ábra: PPTP sebezhetőség*

### Következtetések

Az RBN amellett, hogy számos „újítást” vezetett be az internetes bűnözés módszerei közé, kitűnő példával szolgál arra, hogy a világháló történései komoly nemzeti és nemzetközi biztonsági kérdéseket vetnek fel.

Az RBN nem egy kedvtelésből káros programokat író fiatalok kis csoportja. Fő profiljuk a szolgáltatás, ami a jelenlegi jogi környezetben teljesen legális, függetlenül a tartalomtól. Teljes körű infrastruktúrát biztosítanak a kártékony szoftverek terjesztéséhez, fejlesztéséhez, illetve elérhetővé teszik végfelhasználók számára.

Az amerikai hatóságok nyomoztak az RBN és a *Storm* féreg alkotói után, Oroszország azonban nem volt hajlandó együttműködni, így nem jártak sikerrel. Egyes feltételezések szerint azért sem, mert az RBN-nek szoros kapcsolatai vannak a vezető politikai körökkel. [15]

Ahhoz, hogy a cyber-bűnözést hatékonyan tudjuk kezelni, nemzetközi együttműködésre és megfelelő jogharmonizációra lenne szükség.[9]

Egy jól szervezett, komoly pénzügyi és szakmai tőkével rendelkező csoportosulás igen komoly veszélyt jelenthet egy adott ország informatikai és információs infrastruktúrájára. Elképzelhető, hogy az RBN is segédkezett az Észtország elleni informatikai támadásban, hiszen az több mint valószínű, hogy Oroszországból indult ki, és pont egy olyan időszakban, amikor az RBN erejének tetőpontján volt. A támadásban használt eljárás – elosztott szolgáltatás-megtagadási támadás – abszolút az RBN profiljába illik, és megfelelő eszközök álltak rendelkezésre, hogy sikeresen véghezvigyék.

A támadások kifinomultabbak, szervezettebbek, ugyanis a tét igen komoly, a lebukás esélye pedig ezzel egyenes arányosságban nő. A célpontok eleinte az egyszerű otthoni felhasználók, azonban ahogy nő a rendelkezésre álló infrastruktúra és a világháló feletti befolyásoló képesség, úgy változik a célpontok jellege, típusa és ezzel együtt emelkedik a várható nyereség is.

Egy gazdasági alapon, kvázi legálisan működő, profitorientált bűnöző szervezet elleni harc rendkívül nehéz. A csoporthoz közeli személyektől szinte lehetetlen információt szerezni, hiszen az anyagi tényező erősebb, mint a „jót cselekedni” tudat.

Elengedhetetlen, hogy az ilyen internetes bűncselekményeket rugalmasan, nemzetközi együttműködéssel és a lehető legrövidebb idő alatt képesek legyünk lereagálni.

## Felhasznált irodalom


- *Hálózati biztonság.* Tom Thomas, Panem, Budapest 2005.
- *Information Warfare*. Winn Schwartau, Thunder's Mouth Press 1996.
- *Information Warfare and Security*. Dorothy E. Denning, Addison-Wesley 1999.


## Internetes hivatkozások


[1]. http://www.networkworld.com/news/2007/080207-black-hat-storm-worms-virulence.html?page=1

[2]. http://blog.washingtonpost.com/securityfix/2007/10/the_storm_worm_maelstrom_or_te.html

[3]. http://www.darkreading.com/document.asp?doc_id=129304

[4]. http://blog.washingtonpost.com/securityfix/2007/10/the_storm_worm_maelstrom_o


9 Gábri Máté, *Információs biztonság, azaz a biztonság hatodik dimenziója.* Hallgatói Közlemények, XI. évf. 2. szám

r_te.html
[5]. http://en.wikipedia.org/wiki/Storm_Worm
[6]. http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html
[7]. http://www.networkworld.com/news/2008/021908-researcher-russian-hosting-network-runs.html?page=1
[8]. http://blog.washingtonpost.com/securityfix/2007/06/the_mother_of_all_exploits_1.html
[9]. http://www.theregister.co.uk/2007/09/01/bank_of_india_website_takeover/
[10]. http://sunbeltblog.blogspot.com/2007/08/breaking-bank-of-india-seriously.html
[11]. http://www.theregister.co.uk/2007/11/08/rbn_offline/
[12]. http://it.slashdot.org/article.pl?sid=07/11/09/1957239&from=rss
[13]. http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=ROK7829
[14]. http://www.schneier.com/pptp-faq.html
[15]. http://blog.washingtonpost.com/securityfix/2008/01/unhappy_birthday_to_the_storm.html

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Gyányi Sándor**
Budapesti Műszaki Főiskola
gyanyi.sandor@kvk.bmf.hu

# CYBER-TÁMADÁSOK ELLENI VÉDEKEZÉS ÉS A VÁLASZCSAPÁSOK LEHETŐSÉGEI

***Absztrakt***

*A számítógépes hálózatok egyre nagyobb szerepet töltenek be a mindennapi életben, az államigazgatásban, a banki szektorban és nem utolsó sorban a fegyveres erőknél is. A térnyeréssel párhuzamosan a számítógépes támadások száma is növekszik, új bűnözői és terrorista csoportok is fokozzák jelenlétüket, egyre több állam kezdi el – bevallottan vagy titkoltan – hadseregét felkészíteni a virtuális térben folytatandó műveletek végrehajtására. A technológia fejlődését azonban nem kíséri a gondolkodásmód, a jogszabályi háttér és a nemzetközi jog ilyen irányú fejlődése, így a cyber támadások vizsgálata, a tettesek utáni kutatás során sokszor adódhatnak vitás, nehezen értelmezhető helyzetek. Igyekeztem a virtuális térben folyó és a hagyományos tevékenységek közötti hasonlóságokat bemutatni, analógiákat keresni a kétféle tevékenység között.*

*Nowadays computer networks are playing more and more important part in our everyday life, in the government, in monetary sector and last but not least in armed forces. Together with the extension the number of attacks is increasing. There are new groups of criminals and terrorists appearing, more and more governments start to prepare (either admittedly or in secret) their armies for carrying out operations in cyber space.*
*However, the development of technology is not followed by the development of thinking, of law background and of international law, so investigation of cyber attacks and searching for criminals often bring about controversial situations.*
*I tried my best to show the similarities between virtual and convential activities and to look for analogies between them.*

***Kulcsszavak**: információs terrorizmus, cyber támadások, botnet ~ information terrorism, cyber attacks, botnet*

## Bevezetés

A modern katonai műveletek során egyre nagyobb szerepet kap a harcoló egységek informatikai támogatása, az információs fölény kivívása. A tendencia az, hogy – költséghatékonysági okokból - a hadseregek a polgári életben alkalmazott informatikai technológiákat igyekeznek rendszeresíteni, természetesen a különleges követelmények figyelembe vételével. Ezek a rendszerelemek azonban széles körben használt technológiákat tartalmaznak, amiket jól ismernek a polgári élet szakemberei, így a potenciális támadók („harcosok") köre is jelentősen kibővült. Egy jövőbeli, közel azonos technikai fejlettségű hatalmak közti katonai incidens fontos helyszíne lesz a virtuális tér (Cyber-space), emiatt fontos az ilyen „hadszíntéren" folyó műveletek előzetes felmérése, a várható veszélyhelyzetek megismerése. Érdekes gondolatmenet a virtuális és a valódi harchelyzetek, eszközök párhuzamba állítása, és ebből kiindulva egy ilyen konfliktus értékelése.

## Párhuzamok

A virtuális hadszíntéren lényegesen egyszerűbb bármilyen akciót elindítani, mint a valódi helyszíneken. Nem szükséges a haditechnika felvonultatása, a harcolókat itt a számítógépes hálózatok végpontjai helyettesítik. A mai nyilvános informatikai hálózatok (és itt leginkább az Internetre kell gondolni) alacsony költségek mellett jelentős adat mozgatását teszik lehetővé fizikailag egymástól nagy távolságokra levő végpontok között. Az Internetre bárki csatlakozhat, a mai technikai fejlettség mellett a szegényebb, katonailag jelentéktelenebb államok, militáns csoportok vagy akár magánszemélyek is komoly eszközparkot képesek felvonultatni. Az informatikai támadásokkal szemben ráadásul a fejlettebb infrastruktúrával rendelkező országok sokkal sebezhetőbbek, mint egy fejletlenebb hátterű ország, emellett az ilyen támadások elkövetőit azonosítani is rendkívül problémás.
A támadásokban – akár áldozatként, akár támadóként – szereplőket három nagy csoportba sorolhatjuk (természetesen a szereplők alatt az általuk birtokolt, használt infrastruktúrát kell érteni):

- önállóan tevékenykedő magánszemélyek;
- csoportok, szervezetek;
- államok.

Ha ebből összeállítjuk a lehetséges támadó-célpont kombinációkat, akkor többnyire csak kriminalisztikai szempontból érdekes változatokat kapunk. A magánszemély-magánszemély, magánszemély-szervezetek, szervezetek-magánszemély, szervezetek-szervezetek kombinációkra rengeteg ismert példát lehet felhozni, az ilyen támadások fő motivációja általában az anyagi haszonszerzés. Az igazán érdekes párosítások a következők:

- magánszemély támad államot;
- állam támad magánszemélyt;
- szervezet támad államot;
- állam támad szervezetet;
- állam támad másik államot.

A „magánszemély támad államot" kategória való világbeli analógiája a magányos merénylő lehetne, azonban egy elszigetelten működő magánszemély által sikeresen végrehajtott, a célpontnak, és csak a célpontnak komoly károkat okozó informatikai támadás nehezen kivitelezhető. Voltak komoly pusztítást végző – általában számítógépes vírusok vagy férgek

által végrehajtott – akciók, azonban ezek egyike sem állami infrastruktúrát támadott. Az első világméretű pusztítást okozó, magát az Interneten terjesztő számítógépes malware a 2000. május 4-én elszabadult „I love you” nevű féreg volt, amely az agresszív terjedésével több komoly levelező rendszert is időszakosan működésképtelenné tett. Szerzőjeként egy Onel de Guzman nevű Fülöp-szigeteki diákot azonosítottak, akit azonban a helyi törvények szerint nem lehetett elítélni, mivel a Fülöp-szigeteken a számítógépes víruskészítés nem számított bűncselekménynek [1].

Az előző kombináció ellentéte, az „állam támad magánszemélyt” nem túl valószínű forgatókönyv, bár sokan az állam túlzott érdeklődését az állampolgárok privát dolgai iránt is támadásnak tartják. Egyfelől a hatalom a pozitív szándékait hangsúlyozza, a minél több információ begyűjtésével könnyebben derítheti fel a különböző bűnözői vagy – napjainkban egyre nagyobb nyilvánosságot kapó – terrorista csoportok szándékait, terveit. Másfelől az állampolgárok félelme is érthető, mivel könnyű az orwelli „1984” világába képzelni magunkat.

A „szervezet támad államot” a legvalószínűbb, előbb-utóbb biztosan bekövetkező esemény. A különböző szélsőséges csoportok, terrorszervezetek bizonyítottan előszeretettel használják az Internetet egymás közti titkos kapcsolattartásra, propagandaanyagok terjesztésére, toborzásra. Az ilyen tevékenység különösen erős Nagy-Britanniában és a szintén jelentős iszlám közösséggel rendelkező Németországban [2]. Az említett funkciók használata mellett komoly esély van arra is, hogy a szervezési feladatok segítése mellett fegyverként is felhasználják majd az informatikai hálózatokat. Iszlám ideológiákat követő hackerek komoly mennyiségű weboldalt támadtak meg és törtek fel sikeresen, helyeztek el rajta propaganda jellegű üzeneteket. Ezek az akciók azonban általában kevésbé gondosan védett informatikai rendszereket értek, és a támadások ezen típusa ellen hatékony óvintézkedések tehetők. Az infrastrukturális feladatokat ellátó rendszereket veszélyeztető legkomolyabb módszer az elosztott túlterheléses (DDoS – Distributed Denial of Service) támadás, amely ellen hagyományos módszerekkel nehéz védekezni. A DDoS támadás során egy időben, nagyszámú internetes végpontról végzik a célpont megbénítására szolgáló adatcsomagok küldését, emiatt a támadó végpontok – vagy legalább az általuk generált adatforgalom – semlegesítése nem megoldható. Az elkövető számára az egyetlen nehézséget a szükséges mennyiségű, hálózatra kötött számítógép megszerzése jelenti. Erre automatizált megoldást kínálnak a számítógépes vírusok, férgek és trójai alkalmazások, amelyek segítségével átvehető egy fertőzött számítógép feletti uralom. A háttérben zajlanak a „fegyverkezési verseny” folyamatai, szinte elképzelhetetlen mennyiségű számítógépet vonnak uralmuk alá különböző szervezetek, amelyeket aztán hálózatba szerveznek, divatosan elnevezéssel zombie hálózatokat (botnet) alakítanak ki. Ezeket a botneteket valószínűleg bűnözői csoportok hozzák létre, legfontosabb alkalmazási területük a kéretlen elektronikus levelek küldése, azonban a megfelelő ellenszolgáltatásért cserébe az ilyen kapacitások bérelhetők is tőlük. Ez azt jelenti, hogy akár egy terrorcsoport is képes azokat felhasználni saját céljainak megvalósítására, csak a megfelelő anyagi háttérre van szükségük.

Ha egy állam egy szervezet ellen követ el informatikai támadást, akkor a logika szabályai szerint annak megelőző jellegűnek kell lennie. A támadónak kellő indokokkal, bizonyítékokkal kell rendelkeznie, a támadásnak a veszélyforrással arányosnak kell lennie, amennyiben a fegyveres konfliktusokra érvényes szabályokat próbáljuk rájuk alkalmazni. Az ellentámadás indokoltsága és különösen a módszere sok vitás pontot tartalmaz, amelyekkel érdemes behatóbban foglalkozni.

Az „állam támad másik államot” kategória túllép a civil szféra határain, hiszen ez két szuverén hatalom közti fegyveres konfliktusnak is tekinthető, amelyet nem halálos fegyverekkel vívnak. A legfrissebb ilyen esetként sokan a 2007. májusi észtországi szerverek ellen elkövetett DDoS támadást tekintik, jóllehet az orosz állam szerepe nem bizonyított az akcióban. Az észt szakemberek sok olyan végpontot azonosítottak, amelyek orosz állami hivatalokban működtek, azonban ezek a végpontok lehettek fertőzött gépek is, amelyek egy botnet tagjaként vették ki részüket a támadásból. Az államok közti cyber támadások rengeteg jogi problémát is felvetnek, amivel mindeddig keveset foglalkoztak a döntéshozók. Kína már az 1990-es évek elején kialakította saját, cyber hadviselésre szolgáló katonai infrastruktúráját. 1999-ben a Kínai Néphadsereg két ezredesének nyilatkozata szerint egy Tajvan miatti USA-Kína incidens esetén kínai hackerek képesek lennének lerombolni az USA polgári informatikai infrastruktúráját [3]. A kínaiak mellett természetesen más országok (Franciaország, Oroszország, Nagy-Britannia, Izrael) is rendelkeznek kifejezetten katonai jellegű informatikai támadások végrehajtására kiképzett állománnyal. Érdekes módon az Egyesült Államok Légiereje (USAF) csak 2007-ben hozta létre saját, Cyber Command nevű egységét, amelynek feladata a virtuális térben felvenni a harcot a potenciális támadókkal.

## Lehetséges konfliktusok

A társadalom informatikai függőségének növekedésével párhuzamosan a kockázatok is növekednek. Egy jól kivitelezett támadás a társadalom kritikus informatikai infrastruktúráinak időszakos leállását vagy meghibásodását is okozhatja, amivel az állampolgárok mindennapi életét nehezíthetik meg, aláásható a pénzügyi, államigazgatási rendszerekbe vetett hitüket, szélsőséges esetben, pedig fizikai sérülést is okozhatnak. Az államoknak kötelességük polgáraikat megvédeni, ami igaz a virtuális térben kivitelezett támadások esetére is. A legnagyobb problémát az idegen államokból érkezett támadásokra adott reakciók jelentik, itt ugyanis a diplomáciai és nemzetközi jogi szabályok akadályozhatják az alkalmazható módszereket. Ha sikerül egy idegen államot egy informatikai támadás kiinduló pontjaként azonosítani (ami nem triviális feladat), akkor három különböző lehetőség jöhet szóba [8]:

- a kiinduló ország illetékeseivel felvenni a kapcsolatot, és közösen leállítani a támadást;
- a kiinduló ország illetékeseinek tudta nélkül felderíteni a támadót és megpróbálni letiltani hozzáférését (a hozzáférést biztosító szolgáltató segítségével);
- a kiinduló ország illetékeseinek tudta nélkül semlegesíteni a támadót.

Az első megoldás fő problémája az együttműködés hivatalos folyamatának hosszadalmas volta. Míg egy támadás elindításához néhány másodperc is elegendő, a hivatalos szervek kapcsolatfelvételéhez ennél lényegesen több idő szükséges. Figyelembe véve a szervereken képződő naplók mennyiségét és a szükséges rendszernaplók számát (egy támadó általában több feltört rendszer közbeiktatásával csatlakozik a tényleges akciót végző végpontokhoz, így tényleges címének felderítéséhez több végpontot is meg kell vizsgálni), a hivatalos csatornák közbeiktatásával kevés esély mutatkozik a valódi elkövető azonosítására. A második változat esetében diplomáciai gondot okozhat az, hogy bár a hírszerzést általánosságban nem tiltja a nemzetközi jog, egy külföldi ország ügynöke által elkövetett kémkedést a legtöbb ország jogrendszere szankcionálja. A harmadik eset a legveszélyesebb, egy idegen államban elkövetett, nem bejelentett akció akár háborús helyzethez is vezethet, természetesen csak elméleti síkon maradva. Mindhárom esetben még kényesebbé válhat a helyzet, ha a támadás kiindulási pontjaként azonosított országról kiderül, hogy az ottani végpont csak egy korábban

uralom alá vont (tehát szintén áldozat) végpont, amit az elkövető proxy-ként használt céljaihoz. Ha a tettes egy harmadik államból – vagy extrém esetben a célpont országból - kezdte akcióját, akkor az ellentevékenység komoly presztízsveszteséget okozhat mindegyik félnek.
Ha előfordulna az az alacsony valószínűségű eset, hogy a támadóról minden kétséget kizáróan bebizonyítható, hogy egy idegen állam megbízásából tevékenykedett, akkor az incidens akár komolyabb következményekkel is járhat. Az eddig napvilágra került esetek egyikében sem sikerült minden kétséget kizáróan felfedni az elkövető kilétét, jóllehet sejtések vannak ez ügyben. A sort 1999-ben, a Pentagon hálózata ellen elkövetett adatlopási akció nyitotta. Az események felderítésére indított "Moonlight Maze" [9] kódnevű FBI akció felderítette, hogy a támadók sikeresen bejutottak a Pentagon routereibe - hálózati útválasztóiba - és az adatforgalmat 8 másik olyan végponton vezették keresztül, amelyet könnyen lehallgathattak. A támadás szisztematikus volt, nem véletlenszerű adatokra vadásztak, a támadást elkövető végpontok közül, pedig sikerült azonosítani egy Moszkvától 30 kilométerre található internetes szervert. Az orosz érintettséget a szakértők azzal is igyekeztek bizonyítani, hogy az akciók mindig moszkvai idő szerint 8:00 és 17:00 között, tehát munkaidőben történtek. Természetesen az orosz hatóságok tagadták érintettségüket az ügyben. A következő, nagy port kavaró esetet a nyomozók által Titan Rain [10] névre keresztelt kínai hackercsoport követte el, több fontos amerikai katonai beszállító ellen. A nyomozás során kínai végpontokig sikerült a nyomokat visszakövetni, de természetesen a kínai szervek nem vállalták a felelősséget.
Ha az a helyzet állna elő, hogy egy állam egy másik kritikus infrastruktúráját megtámadta, akkor a megtámadott ellentevékenységéhez jelenleg nem állnak rendelkezésre kiforrott eljárások. A nem cyber támadások esetén az ENSZ alapokmányának [11] VII. fejezete ad útmutatást, érdemes megvizsgálni ennek alkalmazhatóságát. A 41. cikkely rendelkezik a nem fegyveres erők felhasználásával foganatosítható rendszabályokról: *"A Biztonsági Tanács határozza meg, hogy milyen fegyveres erők felhasználásával nem járó rendszabályokat kíván foganatosítani abból a célból, hogy határozatainak érvényt szerezzen és felhívhatja az Egyesült Nemzetek tagjait arra, hogy ilyen rendszabályokat alkalmazzanak. Ilyeneknek tekintendők a gazdasági kapcsolatok, a vasúti, tengeri, légi, postai, távírói, rádió és egyéb forgalom teljes vagy részleges felfüggesztése, valamint a diplomáciai kapcsolatok megszakítása."*

Az angol nyelvű változatban az "egyéb forgalom" eredetileg "other means of communication" kifejezésként szerepel, ami "a kommunikáció egyéb formája" értelmű. Vagyis, ha a Biztonsági Tanács a nem katonai jellegű beavatkozás mellett dönt, akkor a támadó fél valamennyi kommunikációs lehetőségét (beleértve az Internethez hozzáférést is) korlátozhatják. Ha ezek az intézkedések nem hoznak eredményt, akkor a 42. cikkely szerint: *"Ha a Biztonsági Tanács úgy találja, hogy a 41. cikkben említett rendszabályok elégtelenek, vagy elégteleneknek bizonyulnak, úgy légi, tengeri és szárazföldi fegyveres erők felhasználásával olyan műveleteket foganatosíthat, amelyeket a nemzetközi béke és biztonság fenntartásához, vagy helyreállításához szükségesnek ítél. Ezek a műveletek az Egyesült Nemzetek tagjainak légi, tengeri és szárazföldi hadereje által foganatosított tüntető felvonulásból, zárlatból (blokád) vagy egyéb műveletekből is állhatnak."*

Ennek értelmében az ENSZ felügyelet alatt akár fegyveres akcióvá is eszkalálódhat egy virtuális konfliktus, aminek – bár elméleti lehetőség van rá – valószínűsége napjainkban csekély. A Biztonsági Tanács tevékenységére eddigi fennállása során még a komoly fegyveres konfliktusok esetén sem a gyorsaság és az egyetértés volt a jellemző. Talán emiatt, az 51. cikkely biztosítja az államok számára az önvédelem jogát: *"A jelen Alapokmány egyetlen rendelkezése sem érinti az Egyesült Nemzetek valamelyik tagja ellen irányuló*

*fegyveres támadás esetében az egyéni vagy kollektív önvédelem természetes jogát mindaddig, amíg a Biztonsági Tanács a nemzetközi béke és a biztonság fenntartására szükséges rendszabályokat meg nem tette. A tagok az önvédelem e jogának gyakorlása során foganatosított rendszabályaikat azonnal a Biztonsági Tanács tudomására tartoznak hozni és ezek a rendszabályok semmiképpen sem érintik a Biztonsági Tanácsnak a jelen Alapokmány értelmében fennálló hatáskörét és kötelességét abban a tekintetben, hogy a nemzetközi béke és biztonság fenntartása vagy helyreállítása végett az általa szükségesnek tartott intézkedéseket bármikor megtegye."*

A fegyveres támadás kifejezés kiterjesztése a cyber támadásokra egy újabb érdekes problémát vet fel: mi számít fegyvernek egy támadás során? Ha olyan eszközre gondolunk, amely segítségével képes a fegyver használója emberéletben kárt okozni, akkor érdemes elgondolkodni egy olyan – filmekben előszeretettel bemutatott - számítógépes támadáson, amely segítségével egy atomerőmű vezérlését teszi tönkre a behatoló, ezzel az erőmű leállását vagy túlterhelését okozva. De példát lehetne hozni egyéb kritikus infrastruktúrára is, és bár nem túl valószínű egy tisztán informatikai eszközökkel végrehajtott ilyen jellegű támadás, de egyéb akciók támogatásaként teljesen valószerű.

A továbbiakban tekintsük át a cyber támadások során alkalmazott módszereket, illetve a megelőzés vagy az ellencsapás lehetőségeit.

## Felderítés

Egy számítógépes hálózat mindig vonzza a rosszindulatú embereket, akik valamilyen motiváció miatt szeretnének bizalmas információkat szerezni, a hálózat erőforrásait uralni, erkölcsi és anyagi kárt okozni, a hálózat működését lehetetlenné tenni. A számítógépes hálózatok sikeres megtámadásához alapvető fontosságúak a célpont részletes műszaki paraméterei, amit – jó esetben – a rendszer adminisztrátorai igyekeznek titokban tartani. Ha a támadó nem ismeri a védvonalakon (tűzfalakon) belül elhelyezkedő célpontok paramétereit, nem sok esélye van célja elérésére. A szükséges információ megszerzésére több lehetőség is adódik:

- a célrendszert használók hibáit, jóindulatát kihasználva begyűjteni a hálózati sajátosságokat (egyes alrendszerek elérhetősége, bejelentkezési jogosultságok), tehát az emberi tényezőre építeni;
- fizikai hozzáférést szerezni az adott rendszerben, vagyis a rendszernek helyet biztosító épületekben hírszerzést folytatni;
- a számítógépes hálózaton keresztül speciális alkalmazások futtatásával begyűjteni a szükséges adatokat.

Az első két módszer veszélyeket hordoz magában, hiszen a támadónak meg kell jelennie a helyszínen, emberekkel kell találkoznia, ami könnyen lebukáshoz vezethet. Nehezíthetik az elkövető dolgát emellett a nyelvi nehézségek, etnikai különbözőségek is. Emiatt a harmadik, tisztán technikai megközelítés a leggyakoribb, széles körben rendelkezésre álló segédprogramok könnyítik meg az információszerzést.
Egy informatikai rendszer támadása három fő kategóriába sorolható:

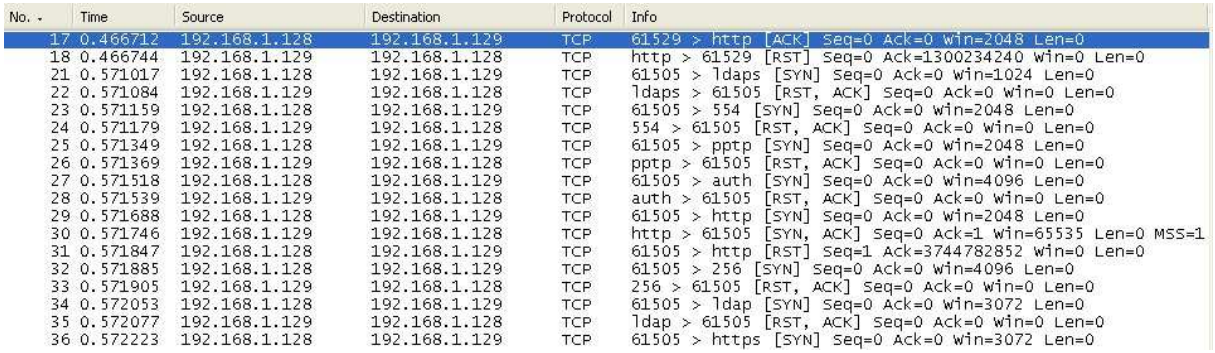
- lehallgatás;
- uralom átvétele;

- az üzemszerű működés lehetetlenné tétele.

A három módszer közül a lehallgatás megvalósítása csak speciális feltételek mellett (fizikai hozzáférés a célpont belső hálózatához, a rendszer valamelyik eleme feletti ellenőrzés megszerzése) vihető végbe. A rendszer feletti uralom megszerzése hosszadalmas, aprólékos munkát igényel, és szükséges hozzá valamilyen üzemeltetői hiba (helytelen rendszerkonfiguráció, a rendszer valamelyik elemének hibája, felhasználói gondatlanság). Az üzemszerű működés lehetetlenné tétele egy DoS vagy DDoS támadás segítségével könnyen végrehajtható, ha megvannak hozzá a szükséges eszközök. Egy rendszer sikeres megtámadásához a támadónak először fel kell mérnie a célpont sajátosságait:

- a célpont informatikai hálózatában üzemelő végpontok címeit;
- az ismert végpontok sajátosságait (operációs rendszer, szolgáltatások elérhetőségei);
- a végpontokon futó szolgáltatások esetleges hibáit;
- a rendszert használók adatait, esetleges hozzáférési jogosultságait.

Mindezt persze úgy kell elvégezni, hogy a célpontot üzemeltetők ne szerezzenek tudomást a készülő akcióról. A végpontok címeinek felmérése az Interneten viszonylag egyszerű. Az Internet hálózati protokolljaként a már nem túl fiatal IP (Internet Protocol), annak is a v4 verziója szolgál - bár létezik már egy korszerűbb, kevesebb sérthetőséggel rendelkező v6 változat is, annak elterjedése még várat magára. Az IPv4 minden hálózati végponthoz egy 32 bites azonosítót rendel, amely két részből áll össze: hálózati cím (ami a célpont hálózatát azonosítja) és végpont cím (amely a megcímzett hálózaton belül jelöli ki a végpontot). Az internetes címek kiosztása nem egyenként történik, hanem nagyobb egységekben, címtartományba szervezve. A címtartományok mindig csupa „0” értékű végpontbitekkel kezdődnek, és csupa „1” értékű végpontbitekkel érnek véget, a címtartományok egyediségének biztosítása céljából a tartományokat központilag tartják nyilván, és ugyanabba a címtartományba tartozó címeket nem osztanak ki két tulajdonosnak. Ezek a nyilvántartások bárki számára elérhetők, az európai IP címtartományokról például a http://www.ripe.net weboldalon lehet információt kérni. A keresés segítségével meghatározható az a tartomány, amelyben a célhálózat egyes elemei elhelyezkedhetnek, ezután már csak a tartományon belüli címeket kell ellenőrizni. A végpontok működőképességének ellenőrzésére egyszerűbb esetben elegendő a legtöbb operációs rendszerben „ping” névre keresztelt parancs használata, amely ICMP Echo Request üzeneteket küld a célpont számára, majd a válaszul kapott ICMP Echo Reply üzenetek beérkezését jelzi a kérést kiadó felhasználónak. Mivel az Echo Request üzenetre válaszoló végpontok könnyen elárulják a felderítést végzőnek létezésüket, ezért sok rendszergazda szűri az ilyen típusú üzeneteket. Ilyenkor tesznek jó szolgálatot a portszkennerek, amelyek speciális csomagok elküldésével és a válaszok elemzésével képesek a végponton üzemelő TCP vagy UDP módszerrel kommunikáló szolgáltatások felderítésére. A legismertebb és talán a legsokoldalúbb ilyen eszköz az „nmap” névre hallgató segédprogram, amely ingyenesen elérhető, akár forráskóddal együtt. Sokoldalú képességei nem csak a nyitott, de a külvilág irányába csomagszűrési beállításokkal lezárt szolgáltatások felderítése mellett az operációs rendszer hozzávetőleges megállapítására is alkalmasak. Az nmap népszerűsége és elterjedtsége akkora, hogy az Internetre kötött végponton néhány percenként megjelenik egy ilyen típusú felderítést végző program. Ha a szkennelés működését megvizsgáljuk, akkor látható, hogy a specifikus csomagok nem okoznak jelentős hálózati forgalmat, egyetlen port felderítése mindössze 114 byte adatforgalmat generál.



| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 17 | 0.466712 | 192.168.1.128 | 192.168.1.129 | TCP | 61529 > http [ACK] Seq=0 Ack=0 Win=2048 Len=0 |
| 18 | 0.466744 | 192.168.1.129 | 192.168.1.128 | TCP | http > 61529 [RST] Seq=0 Ack=1300234240 Win=0 Len=0 |
| 21 | 0.571017 | 192.168.1.128 | 192.168.1.129 | TCP | 61505 > ldaps [SYN] Seq=0 Ack=0 Win=1024 Len=0 |
| 22 | 0.571084 | 192.168.1.129 | 192.168.1.128 | TCP | ldaps > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0 |
| 23 | 0.571159 | 192.168.1.128 | 192.168.1.129 | TCP | 61505 > 554 [SYN] Seq=0 Ack=0 Win=2048 Len=0 |
| 24 | 0.571179 | 192.168.1.129 | 192.168.1.128 | TCP | 554 > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0 |
| 25 | 0.571349 | 192.168.1.128 | 192.168.1.129 | TCP | 61505 > pptp [SYN] Seq=0 Ack=0 Win=2048 Len=0 |
| 26 | 0.571369 | 192.168.1.129 | 192.168.1.128 | TCP | pptp > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0 |
| 27 | 0.571518 | 192.168.1.128 | 192.168.1.129 | TCP | 61505 > auth [SYN] Seq=0 Ack=0 Win=4096 Len=0 |
| 28 | 0.571539 | 192.168.1.129 | 192.168.1.128 | TCP | auth > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0 |
| 29 | 0.571688 | 192.168.1.128 | 192.168.1.129 | TCP | 61505 > http [SYN] Seq=0 Ack=0 Win=2048 Len=0 |
| 30 | 0.571746 | 192.168.1.129 | 192.168.1.128 | TCP | http > 61505 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1 |
| 31 | 0.571847 | 192.168.1.128 | 192.168.1.129 | TCP | 61505 > http [RST] Seq=1 Ack=3744782852 Win=0 Len=0 |
| 32 | 0.571885 | 192.168.1.128 | 192.168.1.129 | TCP | 61505 > 256 [SYN] Seq=0 Ack=0 Win=4096 Len=0 |
| 33 | 0.571905 | 192.168.1.129 | 192.168.1.128 | TCP | 256 > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0 |
| 34 | 0.572053 | 192.168.1.128 | 192.168.1.129 | TCP | 61505 > ldap [SYN] Seq=0 Ack=0 Win=3072 Len=0 |
| 35 | 0.572077 | 192.168.1.129 | 192.168.1.128 | TCP | ldap > 61505 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0 |
| 36 | 0.572223 | 192.168.1.128 | 192.168.1.129 | TCP | 61505 > https [SYN] Seq=0 Ack=0 Win=3072 Len=0 |

1. ábra: nmap portszken csomagjai

A tapasztalt támadók ráadásul hosszabb idő alatt, kis intenzitással végzik az ilyen feladatot, emiatt a rendszeradminisztrátor számára láthatatlan lesz ténykedésük. Néhány ritka kivételtől eltekintve a port letapogatás a végpont működését sem veszélyezteti, így az ilyen tevékenység nehezen minősíthető támadásnak. A célpont üzemeltetője – még ha tudomására is jut egy ilyen akció – semmilyen ellentevékenységet sem tud kifejteni (maximum olyan eljárásokat alkalmazhat, amik meghamisítják a felderítés eredményét).
Ha szolgáltatások adatait ismeri a támadó, a következő lépés a szolgáltatás verziószámának meghatározása, ennek ismeretében lehet valamilyen meglevő programozási hibát találni, aminek felhasználásával hozzáférés szerezhető. Természetesen erre is léteznek segédprogramok, azonban lényegesen egyszerűbb, „csendesebb” módon is meghatározhatók a kívánt paraméterek. A legtöbb szolgáltatást megvalósító program a kapcsolat létrejötte után egy üdvözlő szöveget küld a kliensnek (banner), és bár a lehetőség adott a szöveg eltüntetésére vagy kevesebb kényes információt tartalmazó módosítására, a legtöbb adminisztrátor nem veszi a fáradságot erre. Például egy SMTP szerver verziószámának lekérdezéséhez elegendő a célpont 25-ös TCP portjára csatlakozni egy egyszerű telnet alkalmazással:

```
telnet célpont 25

220 ESMTP Sendmail 8.13.4/8.13.4/Debian-3sarge3; Mon, 26 May 2008 20:38:11
+0200
```

A válasz árulkodó: a szerveren egy Sendmail nevű alkalmazás végzi az elektronikus levelek továbbítását vagy kézbesítését, előzékenyen még az operációs rendszer típusát (Debian Linux) is elárulja. Mivel a lekérdezés gyakorlatilag megegyezik egy levelező kliens tevékenységével, ezért itt sem beszélhetünk bűncselekményről, a nagyszámú beérkezett kapcsolat között elvesznek az ilyen típusú próbálkozások.
Ha gondatlan a rendszeradminisztrátor, akkor a felhasználói nevek könnyen meghatározhatók az elektronikus levélcímből, a támadónak ezután már csak egy megfelelő jelszót kell találnia. Ha a felhasználó saját jelszavát nem eléggé körültekintően választotta meg, akkor megint csak a reménybeli behatoló dolgát könnyítette meg.
Hasonló példákat lehetne még sorolni, az ismertetett eljárásokból viszont így is kiderül az a tény, hogy bár minden támadás a felderítéssel kezdődik, azonban ezt a folyamatot nem könnyű észrevenni. Ha mégis sikerül felfedni, akkor sincs túl sok törvényes lehetőség az elkövető korlátozására (általában még személyazonosságának felderítésére sem).

## Passzív védekezés

Ha egy informatikai hálózat nem tartalmaz hibás, megtámadható elemeket, a rendszert használók kellően képzettek, vagyis minden ideális állapotban van, akkor nincs szükség védekezésre. Természetesen ez csak egy idealizált helyzet, hiszen minden rendszerben találhatók gyenge pontok, amiket egy kellően türelmes támadó képes kihasználni. Minden operációs rendszerben - akár a tűzfalakon futókban is - előfordulhatnak „0 napos sebezhetőségek" (0-day vulnerabilities), vagyis olyan programhibák, amelyeket még nem javítottak ki a rendszert fejlesztők. Az ilyen hibák ellen a leggondosabb rendszergazda is tehetetlen, mivel egy nem létező hibajavítást még ő sem tud telepíteni. A 0 napos sebezhetőségek egy támadónak kincset érnek, segítségével jelentős mennyiségű rendszert képes feltörni rövid idő alatt. Emiatt aztán az informatikai rendszerek folyamatos felügyeletet igényelnek, a támadás első jelére meg kell tenni a megfelelő ellenlépéseket. Az ellenlépések köre korlátozott, és csak akkor hajtható végre, ha a támadás ténye már bizonyított:

- a támadást - esetleg még csak a felderítést, ha a célpont ezt veszélyesnek ítéli - kezdeményező végpont elérésének korlátozása technikai eszközökkel (csomagszűrés hálózati szinten);
- a nemkívánatos tevékenységet végző végpont hálózati infrastruktúráját biztosító illetékes szervezet megkeresése és figyelmeztetése.

Mindkét megoldásban közös a probléma: a nemkívánatos végpontot megbízhatóan azonosítani, majd tevékenységét korlátozni kell. A végpont azonosítása látszatra egyszerű, mivel a rendszer naplóállományaiból kinyerhető az IP cím. Azonban az esetek döntő többségében a cím nem a tényleges támadóhoz tartozik, hanem egy proxy végpontként használt számítógéphez vagy pedig egy bárki által elérhető, névtelenül is használható hozzáférési ponthoz. A végpont tevékenységének korlátozása szintén gondokat okozhat. Példának okáért, egy üzleti tevékenységet végző weboldal a látogatói számára szolgáltatást nyújt. Ha ebből a szolgáltatásból egy személyt vagy egy csoportot kizár, akkor esetleg megszegi a saját szerződési feltételeit, ami miatt akár bíróságon is megtámadható.
A másik módszer szerint a megtámadott illetékese felveszi a támadó hálózati hozzáférését biztosító szervezettel a kapcsolatot és jelzi a támadás tényét. Az ilyen szervezet többnyire egy internet-szolgáltató, akinek erkölcsi feladata saját ügyfeleire ügyelni. Az általános gyakorlat szerint a szolgáltatók az „abuse@" kezdetű email címen fogadják az ilyen jellegű bejelentéseket. Az már egy teljesen más problémakör, hogy mekkora reakcióidővel dolgoznak (saját tapasztalataim szerint a 2 óra és a soha közötti intervallumon belül mozognak). A legtöbb esetben egy ilyen ügy véget ér azzal, hogy a szolgáltató ügyfelének gépén megtalálják a támadó által használt vírust vagy trójai alkalmazást és eltávolítják, a támadó pedig egy másik hálózatot igénybe véve rövidesen újra megjelenik a célpont hálózatának védvonalait vizsgálgatva. A nagyobb magyar internet-szolgáltatók szerződési feltételeit megvizsgálva azt tapasztalhatjuk, hogy foglalkoznak a hálózatukból kiinduló rosszindulatú akciók elkövetőinek korlátozásával. Az egyik megközelítés a T-Online ÁSZF-ben [4] található, és az ügyfél szolgáltatásának korlátozását helyezi kilátásban, ha az:
10.1.b.4 pont: „Az Előfizető a számára nyújtott szolgáltatást felhasználva jogosulatlan adatszerzésre, adatküldésre vagy más számítógépes rendszerekbe történő behatolásra tesz kísérletet illetve hajt végre…"
A UPC Magyarország ÁSZF [5] ezzel szemben nem részletezi a szankcionálandó tevékenységeket, hanem az Internet Szolgáltatók Tanácsa által kiadott hálózathasználati irányelveket fogadja el:

„A Szolgáltató elfogadja, és magára nézve kötelezőnek tekinti az Internet használata kapcsán kialakult és nemzetközileg elfogadott Hálózathasználati Elveket (AUP – „Acceptable Use Policy”), amelyek Magyarországon az Internet Szolgáltatók Tanácsa tesz közzé és vizsgál felül rendszeresen.”
A hálózathasználati irányelvek [6] megsértőivel szemben szintén a szolgáltatás korlátozását vagy a szolgáltatási szerződés felmondását helyezi kilátásba. Az ISzT irányelveiben részletesen szerepel minden tiltott tevékenység, beleértve az informatikai rendszerekbe történő behatolást és a túlterheléses (DoS) támadásokat is.
A külföldi hálózatok ügyfeleivel szemben azonban kétséges a fellépés eredményessége, egy rendszergazda gyakorlatilag a külföldi hálózat üzemeltetőire van utalva az ellenséges tevékenységet folytató ügyfelekkel szemben vívott harcában. Az ilyen esetekben lenne szükség állami felügyeletekre, akik a szolgáltatókat rákényszerítenék az együttműködésre és a hathatós segítség nyújtására.
Megállapíthatjuk, hogy bár a passzív védekezési módszerek fontos és elkerülhetetlen részei az informatikai rendszerek biztonságos üzemeltetésének, azonban hatékonyságuk nem a legmagasabb.

## Aktív védekezés

Az aktív védelem két területre osztásával a katonai fogalmakkal újabb párhuzam állítható fel: ezek az ellencsapás és a megelőző csapás fogalmai. Az ellencsapás cyber megfelelője tisztán technikai szinten is kivitelezhető, nem szükséges a politikai, diplomáciai kapcsolatrendszert felhasználni hozzá. A támadó által alkalmazott módszerek a célpont számára is elérhetők, amiket a támadó azonosítása után be is vethet. Azonban a célpontra is vonatkoznak a szabályok, a támadásra hivatkozva sem alkalmazhat illegális módszereket. Egy klasszikus példa erre az eset, ami 1998-ban az Electronic Disturbance Theater (EDT) nevű radikális politikai szervezet és a Pentagon között történt [12]. Az EDT által a Pentagon webszervere ellen alkalmazott támadási módszer egy DoS támadás volt, a támadó végpontok internetes böngészőjében egy JavaScript nyelven írt alkalmazás nagy sebességgel elkezdett weboldalakat lekérni a Pentagon szerveréről. Kellően sok böngészővel és megfelelő hálózati sávszélességgel ez a módszer jelentős terhelést okoz a kiszolgálónak. Ahogy a támadás ténye kiderült, a Pentagon szakemberei azonnal ellentámadásba lendültek. A támadó kliensekre töltöttek egy Java appletet (hostileapplet), amely a böngésző képernyőjén kávéscsészéket - a Java logója - és az "ACK" üzenetet jelenítette meg akkora mennyiségben, hogy a böngésző erőforrásai elfogytak, ami a támadó számítógép lefagyását idézte elő. Az EDT fontolóra vette a Pentagon perbe fogását a „Posse Comitatus”, egy 1878-as törvény alapján, amely tiltja a katonaság bevetését a belföldi törvények betartatása során.
A megelőző csapás fogalmát a virtuális térben értelmezve a „békeidőben” végzett felderítés és a felfedett potenciális veszélyforrások megszüntetése jelenti, amire érdemes több figyelmet szentelni.
Napjainkban a legnagyobb fenyegetést a gomba módra szaporodó és egyre több végpontot tartalmazó botnetek jelentik. A botnetek felelnek a legtöbb DDoS támadásért, a kéretlen reklámlevelek küldésében pedig szinte egyeduralkodókká váltak. A klasszikus, előzetes felderítésen alapuló, a célrendszer sebezhetőségeit kihasználó betörés kivitelezése egyre nehezebb, a legtöbb operációs rendszeren már megvalósított automatikus rendszerfrissítéseknek köszönhetően. A rendszerüzemeltetők is egyre gondosabbak lesznek, az informatikai biztonság fontossága lassan bevonul a köztudatba. A hagyományos, „kézműves” jellegű támadásokat sem szabad lebecsülni, hiszen ezekkel lehet a legnagyobb erkölcsi és anyagi károkat okozni, azonban a túlterheléses támadások ellen keveset tehet az

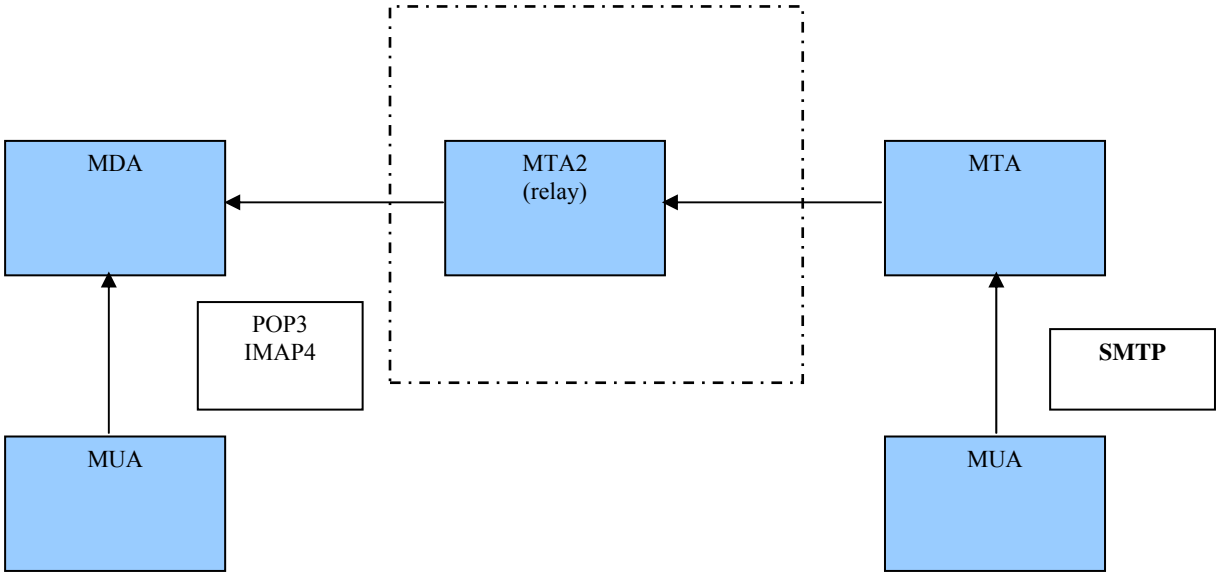
áldozat. Ha a támadás megindult, akkor már csak a kárenyhítés lehetséges, a túlterhelést okozó végpontok nagy száma miatt gyakorlatilag nem lehetséges egyedileg kitiltani az összeset. A nagyobb címtartományok kitiltása értelemszerűen korlátozza a nyújtott szolgáltatást legálisan igénybe vevők körét is.
A botnetek elleni küzdelemben fontos módszer lehet a megelőzés, a már megfertőződött végpontok – botok – felderítése és a szükséges ellenintézkedések megtétele. Egy botnet tag általában nyit a hálózat felé egy kommunikációs portot, amelyen keresztül várja az irányító számítógépektől az elvégzendő feladatot. Egyszerű feladat egy olyan alkalmazást készíteni, amely az Internetet (vagy csak a saját szűkebb környezetét) bejárva ellenőrzi az ismert botnet kliensek által megnyitott parancscsatornákat, majd ha ilyenre talál, akkor riasztást ad. Egy sikeresen elkapott és kivizsgált kliensből aztán már további információk nyerhetők a vezérlő, úgynevezett „command&control" végpontokról, így a teljes hálózat felgöngyölíthető. A gyakoribb botnet kliensek tesztelésére rendelkezésre is állnak ilyen alkalmazások, azonban a szélesebb körű, automatizált használattal szemben is lehet érveket felhozni:

- mivel ez az eljárás lényegében egy szűkített méretű portszkennelés, ezért – bár a cél nemes – az ilyen felderítést végző is az illegális tevékenység határait súrolja;
- az újgenerációs kliensek már szakítottak a hagyományos alá- és fölérendeltségi viszonyokon - a Command & Control struktúrával - és egyenrangú, Peer-to-peer hálózatként funkcionálnak (például a Storm Worm nevű [7]), emiatt az ilyen kliensek felderítése nem triviális;
- készíthetők olyan botnet kliensek, amelyek a felderítési szándékot érzékelve ellentámadást indítanak.

Egy másik, erkölcsileg sem támadható botnet kliens felfedési metódus az alábbi tényezőket használhatja ki:

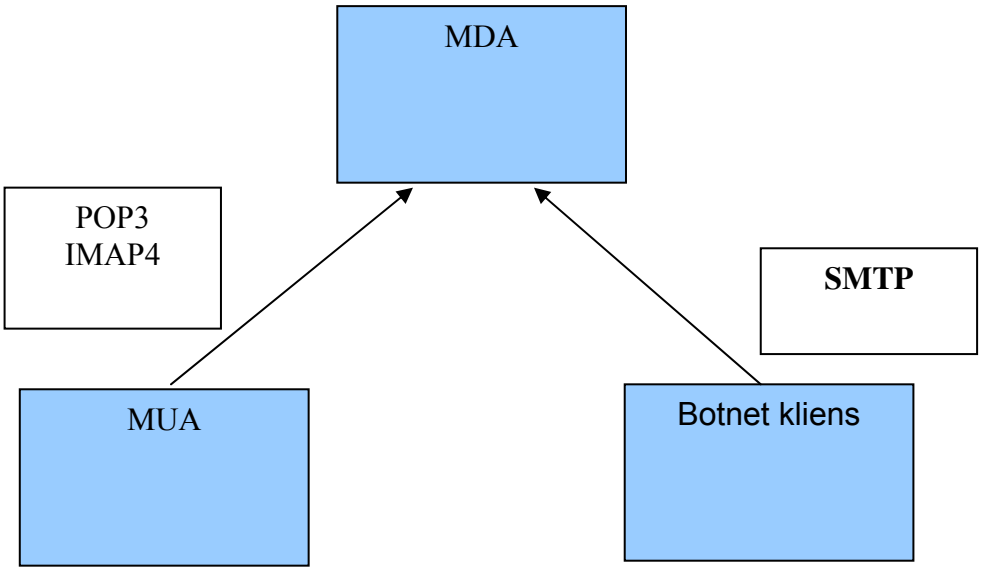
- a botnetek egyik legfontosabb feladata a kéretlen reklámlevelek (SPAM) küldése;
- a SPAM üzenetek túlnyomó többsége manapság botnet kliensektől származik;
- a SPAM a levelező szervereken viszonylag nagy megbízhatósággal szűrhető (95% feletti hatékonysággal);
- a levelező szerver a levél átvételekor ismeri a küldő végpont IP címét.

A metódus ismertetéséhez érdemes röviden áttekinteni az elektronikus levelek célba juttatásának menetét. A 2. ábra a folyamatban közreműködő elemeket mutatja be.




2. ábra: az elektronikus levelezés elemei

A levelet feladó a kliensprogram (Message User Agent – MUA) segítségével összeállítja a levelet, majd SMTP (Simple Mail Transfer Protocol) használatával elküldi a levelező szervernek (Message Transfer Agent – MTA). A levelező szerver megkeresi a címzett postafiókját kezelő másik levelezőszervert (Message Deliver Agent – MDA) és szintén SMTP használatával elküldi neki a levelet. A folyamatba közbenső szerverek is részt vehetnek (relay), ez főként nagyobb rendszerek esetén használatos. Az SMTP kezdeti verziója nem tartalmazott semmilyen hitelesítési folyamatot, ezért gyakorlatilag bárki küldhetett egy SMTP szerver számára levelet, amit az továbbított a címzett számára. Ekkor jelentek meg először a kéretlen leveleket küldők, akik könnyedén juttatták célba leveleiket az ilyen szerverek használatával. Később az SMTP szerverek a levéltovábbítási kéréseket (tehát az olyan levelek továbbküldését, amelyek címzettje nem a saját fennhatóságuk alá tartozik) már feltételekhez kötötték, például a küldőnek a szervert üzemeltető szolgáltató ügyfélkörébe kellett tartoznia, vagy egy jelszót kellett megadnia. A nem ezt a politikát követő SMTP szervereket feketelistára helyezik, ami azt jelenti, hogy a feketelistát figyelő más levelezőszerverek nem vesznek át leveleket tőlük.
Hamarosan megjelentek az olyan káros programok, amik saját SMTP továbbító mechanizmust tartalmaznak, azaz nem a szolgáltató SMTP szerverének küldik el a továbbításra a levelet, hanem közvetlenül a címzett postafiókját kezelő MDA számára.



3. ábra: közvetlen levéltovábbítás

Az első ilyen mechanizmust használó alkalmazások vírusok voltak, amelyek saját maguk terjesztésére használták a beépített SMTP motort. Napjainkban azonban már minden trójai program tartalmaz ilyen funkciót, vagyis a kéretlen levelek keresztül sem haladnak a botnet klienst futtató számítógép hálózati szolgáltatójának SMTP szerverén. Emiatt az ilyen levelek szűrése csak a címzett postafiókját kezelő szerveren (MDA) lehetséges, persze ha eltekintünk attól a valószínűtlen lehetőségtől, hogy az IP csomagok továbbítását végző útválasztók ismerjék fel a kéretlen leveleket.
Az MDA általában nem egyetlen címzett postafiókját kezeli, így komoly mennyiségű levél halad rajta keresztül. A levelek tartalmának vizsgálatára rengeteg termék áll rendelkezésre, víruskeresőktől kezdve a komolyabb szűrőprogramokig, amelyek a levelek szövegének statisztikai elemzésével öntanuló módon ismerik fel a kéretlen leveleket.
A SPAM minősítést kapott levelek feladója – pontosabban a feladó email címe – nem ismert, mivel mind a feladó neve, mind a feladó email címe hamisított. Ellenben az MDA rendelkezik egy fontos adattal: a számára a kéretlen levelet átadó végpont IP címével. A botnet kliensek hatékony felismeréséhez tehát elegendő a kéretlenként azonosított levelek küldőjének IP címét, valamint a küldés időpontját tárolni, és máris rendelkezésre áll egy lista a potenciális támadó végpontokról. Mivel a küldő gépek általában magánszemélyek otthoni gépei, ezért IP címeik nem tekinthetők állandónak. A legtöbb internet-szolgáltató ügyfelei számára nem biztosít kizárólagos használatú IP címeket, hanem rendszeres időközönként – tipikusan 24 óránként – megváltoztatja azt, ezért egy ilyen lista csak rövid ideig érvényes. A rövid érvényesség ellenére azért a végpontok azonosítására alkalmas, mivel az internet-szolgáltatók naplózzák az ügyfeleik számára kiadott címeket, így záros határidőn belül visszakereshető a fertőzött gép tulajdonosa.
A módszer hatékonyságának igazolására elvégeztem egy kísérletet. Olyan email címmel rendelkezem, amely nyilvánosan elérhető weboldalon szerepel, így már évekkel ezelőtt bekerült a SPAM küldők címlistájára. Ennek eredményeképpen napi több száz kéretlen levél érkezik a postafiókomat kezelő szerverre, amely szintén saját tulajdonú. 2008. április 25 és 2008. május 25 közti 30 napban azonosított 9904 kéretlen levelet összegyűjtöttem, majd egy egyszerű script segítségével kigyűjtöttem belőlük a küldő végpont IP címét, az eredményt pedig egy SQL táblába helyeztem. A feldolgozás eredménye az lett, hogy a 9904 kéretlen levelet 9117 különböző IP címről küldték, vagyis a legtöbb végpont nem fáradt azzal, hogy több kéretlen levelet is elküldjön. Az, hogy ez a szám ténylegesen hány fertőzött gépet és hány különböző botnetet jelent, ezzel a módszerrel persze nem lehet megállapítani. Fennáll

annak esélye, hogy ugyanaz a fertőzött gép több nap, különböző IP címekről is küldött levelet, bár ennek valószínűsége nem túl magas, figyelembe véve a SPAM küldés célpontjainak magas számát, illetve a botnetek roppant méreteit.
Látható, hogy egy viszonylag kis forgalmú levelező szerver és nem túl nagy mennyiségű levél vizsgálatával is komoly méretű, fertőzött gépekből álló hálózatokat lehet felfedni. Egy komolyabb forgalmú levelező szerver, amely naponta több százezer vagy akár millió elektronikus levelet vizsgál át, képes teljes botnetek feltérképezésére is. A folyamat automatizálásával megoldható lenne az IP címek szolgáltatók szerinti szétválogatása és a szolgáltatók illetékes szakembereinek értesítése is. Ha az internet-szolgáltatók felkészülnének – esetleg erre jogszabály kötelezné őket - az ilyen listák alapján az ügyfelek értesítésére vagy végső esetben a fertőzött ügyfél hozzáférésének korlátozására, akkor komoly pusztítást lehetne végbevinni a botnetek között, ami az Internet veszélyforrásait csökkentené.

## Összegzés

Igyekeztem bemutatni a virtuális és a valóságos térben végrehajtott támadások közti árhuzamokat, rámutatni az ilyen jellegű tevékenységek elleni fellépés problémáira. A jog jelenleg még nem készült fel a tényleges támadás és az ártalmatlan felderítés közti vékony határvonal kezelésére. Az Internetet sokan használják illegális tevékenységre, amelyekkel a tisztességes felhasználók érdekeit veszélyeztetik, a „békeidőben” végzett megelőző tevékenységek pedig nem kellően szabályozottak, szervezettek. Bemutattam egy egyszerűen használható felderítési mechanizmust, amelyekkel fertőzött számítógépek fedhetők fel.

# Irodalomjegyzék


[1] No 'sorry' from Love Bug author
http://www.theregister.co.uk/2005/05/11/love_bug_author/

[2] Terror Base UK

[3] Cyber catch-up
C4ISR Journal, March 2008 p: 20-21

[4] Általános szerződési feltételek a T-Online internet szolgáltatásra
http://www.t-online.hu/attached/20080411internet_aszf_20080411.pdf

[5] A UPC Magyarország Telekommunikációs Korlátolt Felelősségű Társaság
Internet-hozzáférési szolgáltatás nyújtására vonatkozó Általános Szerződési Feltételei
http://www.upc.hu/pdf/internet_ASZF_2008_0513.pdf

[6] Az ISzT által támogatott hálózathasználati irányelvek
http://www.iszt.hu/iszt/aup.html

[7] Storm Worm DDoS Attack
http://www.secureworks.com/research/threats/view.html?threat=storm-worm

[8] Gregory D. Grove, Seymour E. Goodman, Stephen J. Lukasik:
Cyber Attacks and International Laws
Survival, vol. 42, no. 3, Autumn 2000, pp.89-103

[9] Russians Seem To Be Hacking Into Pentagon
http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/10/07/MN58558.DTL

[10] The Invasion of the Chinese Cyberspies
http://www.time.com/time/magazine/article/0,9171,1098961,00.html

[11] Az Egyesült Nemzetek alapokmánya
http://www.menszt.hu/layout/set/print/content/view/full/186

[12] Civil Disobedience in Cyberspace
http://home.clara.net/heureka/gaia/elec-act.htm


*Az internetes források 2008. május 27-én elérhetők voltak.*

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Illési Zsolt**
Proteus Consulting Kft.
illesi.zsolt@proteus.hu

# BOTNETEK KIALAKULÁSA, HASZNÁLATUK, TRENDJEIK

***Absztrakt***

*Az internet fejlődésével, az információ- és a kommunikációs technológiák konvergenciájával új bűncselekmények jelentek meg. Ezen technikák egyike a „botnet", melynek hatására egyre több számítógép van kitéve a zombi gépek támadásának, illetve a zombivá válás fenyegetésének.*
*Jelen munka összefoglalja a botnetek fejlődését, azonosítja a lényeges ismérveit, elemzi a botnetek architektúráját és a főbb támadási módokat. A botnetek fejlődésnek elemzésekor a szerző előrevetíti azokat az irányokat, amelyek a botnetek struktúrájára, illetve az a támadási módszerekre jellemzők lehetnek a jövőben.*

*Expansion of the internet, the convergence of information and communication technology get new criminal techniques surfaced. One of these is botnet, which made unavoidable that more and more networked computers are under the attack or suffers from the attacks of zombie computers.*
*This paper summarises the evolution of botnets, identifies its main criteria, and analyses the architecture and main attack methods. In the trend analysis of botnet evolution, taking into consideration both attack methods and botnet architecture, the author highlights some possible directions of future enhancements.*

***Kulcsszavak**: internet, rosszindulatú szoftver, zombi, botnet ~ internet, malware, zombie, botnet*

## Bevezetés

Az internet térhódítása megállíthatatlan. A múlt század utolsó évtizedében viharos gyorsasággal terjedtek el a számítógépek és fejlődött a globális hálózat is. Ma már az élet minden területén ott vannak a számítógépek, az internethasználat természetes és nélkülözhetetlen.

Az informatika és a kommunikáció konvergenciájával a papír alapú irodák lassan eltűnnek, a nyilvántartások adatbázisokba, adattárházakba kerülnek, amelyeket már csak

számítógéppel lehet keresni, megtekinteni. Az ipari rendszerek irányítása is egyre inkább automatizált lesz, a termeléstervezés, a folyamatirányítás és az adminisztráció terhei és aprólékos részletei is a gépekre hárulnak. A gazdaság többi szereplője is számítógépfüggővé válik, nincs bank, repülésirányítás, de számvitel, sőt lassan levelezés sem számítógépek, hálózatok és internet kapcsolat nélkül. A kor követelményeihez igazodva az államigazgatás is, az állampolgár-barát állam az ügyfélkapukon keresztül egyre több szolgáltatást biztosít az interneten keresztül, és az államigazgatás feladatai közül is egyre többet számítógépesítenek.

E trend elől a katonai szervezetek sem tudnak kitérni. Az információs képességek fejlődésével a korszerű számítástechnikai megoldások, kommunikációs technikák is jelen vannak a korszerű haditechnikai megoldásokban. A tudás alapú hadsereg (Knowledge Based Army) a legkorszerűbb digitális technológiát használja felderítésre, kommunikációra, információs műveletekre, az adatok feldolgozására, a vezetési-döntési feladatok hatékonyságának növelésére, a harctevékenység támogatására.

A számítógépek egyre inkább felgyorsítják az ügyintézést, a folyamatirányítást, egyszerűbbé és kényelmesebbé teszik a mindennapokat. A technológiai fejlődéssel együtt azonban a bűnözés is fejlődött. A hagyományos bűnözés mellett megjelent a kiberbűnözés, a kiberterrorizmus is. Az új típusú bűnözés természetesen sajátos bűnelkövetési módszerekkel is rendelkezik, megjelentek a programozott és az információtechnológiához kapcsolódó egyéb fenyegetések, amelyeket a biztonsággal, információ biztonsággal vagy információs terrorizmussal foglalkozó szakembereknek is meg kell ismerniük, hogy felkészülhessenek az ellenük való védekezésre.

Dolgozatomban ezek közül az új technikák közül szeretnék egyet – a botneteket – bemutatni, feltárva a sajátosságait, ismertetve a felhasználásának módját és a fejlődésének lehetséges trendjeit.

## Botnetek fogalma, kialakulása

A botnet szó a robot és a hálózat (network) szavakból keletkezett informatikai zsargon, az együttműködő szoftver robotok számítógép hálózaton keresztül összekapcsolódó és együttműködő csoportját jelenti. Az ilyen szoftver robot hálózatok tudományos, mérnöki vagy például üzleti célokra is létre lehet hozni, és ezek főleg az elosztott, párhuzamos vagy többszálas számítások terén alkalmazhatók hatékonyan. A legitim felhasználás mellett a botnetek szolgálhatják az internetes alvilágot abban, hogy illegálisan pénzt vagy adatokat szerezzenek. A továbbiakban ezekkel, a bűnözők által működtetett botnetekkel foglalkozom.

A kiberbűnözők által menedzselt botneteket olyan internetes kapcsolattal rendelkező szoftver robotok, ún. zombi számítógépek alkotják, amelyeket a gépen futó valamely program sebezhetőségét kihasználva távolról megfertőznek, vagyis amelyekre valamilyen távoli menedzselésre is alkalmas rosszindulatú programot telepítenek a felhasználó tudta és akarata nélkül. Zombivá bármilyen internetre kötött programozható, memóriával és processzorral rendelkező eszköz válhat, tekintet nélkül arra, hogy milyen módon kapcsolódik az internetre vagy, hogy milyen technológiát képvisel, így PC-k, notebookok, PDA-k, mobiltelefonok is megfertőzhetők.

A botneteket az ún. pásztor (herder, botherder) irányítja, rendszerint valamilyen közbeiktatott számítógépen keresztül (Command and Control, vagy C&C szerver). [1] [2]

A botnetek kialakításának első lépése egy olyan program megírása, amely lehetővé teszi a sebezhető számítógépek megfertőzését és az azok feletti kontrol megszerzését. Ezek a programok rendszerint úgy vannak megírva, hogy sikeres fertőzés után további célpontokat keressenek (és fertőzzenek meg), illetve felvegyék a kapcsolatot a C&C szerverrel (és szolgálatra jelentkezzenek), vagy megnyissanak egy portot, amelyen keresztül lehetővé teszik,

hogy a pásztorok egy célzott portszkennelés során felismerhessék őket és átvehessék az uralmat. Ezeket a programokat a fejlesztőik egyre gyakrabban automatizált módon mutálják, vagyis úgy módosítják a program felépítését, kódját, hogy az ne érintse a programok funkcionalitását, azonban megnehezítse a víruskeresők számára a felismerést.

A botnet kliens természetesen a saját működést nem csak a víruskeresők elől, hanem a számítógép jogosult felhasználója elől különböző technikák alkalmazásával is eltünteti. Az álcázás során elrejtheti a futtatásához szükséges könyvtárakat, fájlokat, processzeket, vagy valamely jogosult program nevében futva ártalmatlannak tünteti fel magát.

A botnetek kialakítására és működtetésére a legtöbb esetben az Internet Relay Chat (IRC: RFC 1459 és RFC 2812) kliens-szerver alapú csevegő protokollt használják, de a botnetek fejlődésével egyéb protokollokat (pl. HTTP) vagy egyenrangú kapcsolatot biztosító (peer to peer vagy p2p) technológiára épülő megoldásokat is alkalmaznak már. Ezek a nem IRC alapú botnet kliensek általában megnyitnak egy portot, amelyen keresztül megszólíthatók és menedzselhetők.

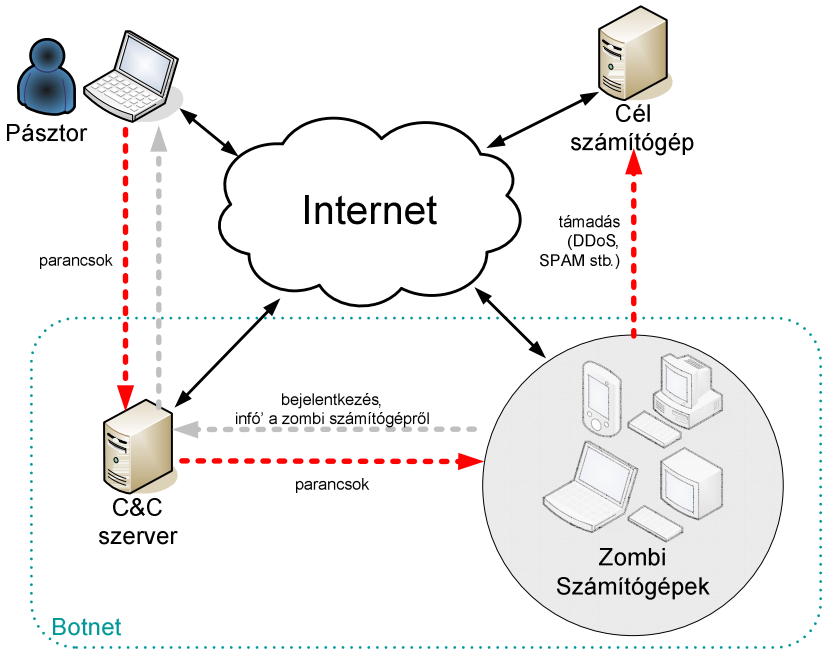
A megfertőzött gép általában nem marad passzív a megfertőzést követően, hanem a környezetében lévő számítógépeiket pásztázza, hogy van-e közöttük olyan, amelyet megfertőzhetne. Ennek az aktivitásnak a következményeként egyes becslések szerint az interneten lévő számítógépek akár fele is zombi számítógép lehet.

A pásztor feladata a fertőző kór megírása és szabadon eresztése után már „csak” annyi, hogy megtalálja és vezérelje a zombikat. A pásztorok azonban nem csak a számítógép felhasználókkal küzdenek a gép kontrolljáért, de egymás közt is rivalizálnak, hogy a mások által megfertőzött gépeket hogyan tudnák saját uralmuk alá hajtani. A több zombi ugyanis jelentősebb támadási potenciált, több adatot és nagyobb erőforrásparkot jelent.

A kontrollált gépekkel a pásztor rendszerint az IRC alapú C&C szerveren keresztül kommunikál, azonban arra is lehetőség van, hogy valamely zombi szervert a pásztor C&C szerverré nevezzen ki, és azon a gépen keresztül kommunikáljon a „nyájjal”.

A pásztor a zombi számítógépekről közvetlenül is letöltheti az azokon tárolt adatokat, illetve utasíthatja azokat valamilyen célpont megtámadására. A zombi-szerver, valamint a szerver-pásztor csatornát a protokollba ágyazott titkosítás védheti, így az egyszerű hálózati betörésfigyelő rendszerekbe épített mintafelismerő rutinok sem képesek minden esetben azonosítani a nemkívánatos kommunikációt.

A botnet sémáját és a működésének vázlatát a következő ábra mutatja be:




**1. ábra – A botnetek működési sémája** [szerk.: Illési Zsolt]

Az első botnetek az IRC hálózatok kialakulását követően jöttek létre. Az IRC kényelmi szolgáltatásainak bővülésével lehetővé vált a szerverek és a kliensek egyes feladatainak automatizálása. A szkriptekkel[1] automatizált kényelmi szolgáltatásokat nyújtó IRC kliensek voltak a botnetek előfutárai. A hackerek természetesen már korán felismerték az automatizmusokban rejlő lehetőségeket és felderítették a rendszerben rejlő sebezhetőségeket. A korai támadások egyszerűek voltak, és csak néhány parancs eredeti, a rendszer mély ismeretéről tanulságot tevő utasítás alkalmazásából állt.

A technológia elterjedésével nőtt a kliensek száma, de ezzel együtt nőtt a renitens felhasználók és a visszaélések száma és a támadások bonyolultsága. A támadók először gyerekes csínyként az IRC szerver, egyes felhasználók egymás gépei, illetve IRC kliensei felett vették át az uralmat és tevékenykedtek a nevükben, majd megjelentek a „keményebb játékosok", akik már rosszindulatúan vagy nyereségvágyból használták fel a tudásukat és okoztak kárt.

Az IRC operátorok természetesen ott voltak a „tűzvonalban" és a támadások szaporodásával ők is kivették a szerepüket: a rosszindulatú felhasználókat és a szerver szabályait megszegőket kitiltották a szerverről. A kizárt felhasználók természetesen visszavágtak: az első DoS (Denial of Service, azaz szolgáltatás-megtagadás) és DDoS (Distributed Denial of Service, azaz megosztott szolgáltatás-megtagadás) támadásokat az IRC szerverekkel szemben indították.

[1] A szkriptek (makrók, parancs, batch stb.) valamely programhoz kapcsolódó magas szintű programnyelven megírt parancsállományok, amelyek lehetővé teszik az alkalmazáshoz kapcsolódó funkciók automatizált, paraméterezett végrehajtását, adatstruktúrák manipulálását. A szkriptelésre példa a DOS/Windows rendszerekben alkalmazott batch, a Linux környezetben a shell programozás, de ilyen például az MS Office esetében a VBA (illetve a VBA makrók), Open Office környezetben a Python makrók.

Az IRC protokoll nyitott jellege egyébként is vonzotta a problémás elemeket és a rosszindulatú kódokat. Megindult az IRC sebezhetőségét és gyenge pontjait kihasználó eljárások és kódok fejlesztése, illetve a kliens gépek meghódításáért folytatott verseny.

A korai internet protokollok strukturális sebezhetősége egyébként is kedvezett a visszaéléseknek, például a spam elterjedésének oka is javarészt az SMTP gyengeségében keresendő.

Az IRC funkcionalitásának bővülése, az ezt használó felhasználók számának növekedése, illetve a megfertőzött számítógépek számának növekedése felkeltette az alvilág figyelmét is, elkezdték felfedezni az ebben rejlő lehetőségeket.

A botnetek kialakításának és felhasználásának az alvilág figyelme új fejeztet nyitott, ami az internet közössége számára több megfertőzött gépet, több problémát, a bűnözők számra komoly profitot jelent.

## Botnetek főbb felhasználási területei

Jelenleg a „csata" az operátorok, biztonsági szakemberek és a botneteket kialakító, felhasználó kiberbűnözők között még nem dőlt el. Az IRC folyamatos finomítása és a protokoll ismert sebezhetőségeinek kiküszöbölése az ismert támadási vektorok számát csökkenti ugyan, de a vírus, féreg és trójai programfejlesztők bevonása, a támadási módszerek finomodása újabb kiskapukat nyit meg a bűnözői körök előtt. [1]

A zombi számítógépeket a bűnözők többféleképp is felhasználhatják. A megfertőzött gépen lévő adatokat közvetlenül elérhetik, vagy a tömegben rejlő lehetőségeket felhasználva megtámadhatnak további meg nem fertőzött célszámítógépet. Ezeket a támadásokat a következőképp lehet csoportosítani:

- adat lopás;
- csalás;
- szolgáltatás megbénítás vagy blokkolás;
- rosszindulatú kód továbbítása.


**2. ábra – Támadások botnetekel és zombi számítógépekkel** [szerk.: Illési Zsolt]

Az adatlopás során elsősorban a zombi gépeken tárolt bankkártya adatokhoz, hitelesítési adatokhoz (felhasználónév, jelszó), személyes adatokhoz, üzleti titkokhoz férhet hozzá a támadó. Mivel a pásztor a felhasználó gépe felett teljesen átveszi az uralmat, a megszerzett adatokat letöltheti a saját vagy más számítógépére, módosíthatja, vagy törölheti azokat.

Egyes bot klienseknek külön az adatlopásra kifejlesztett rutinjaik vannak, amelyek szisztematikusan kutatnak a megfertőzött gépen dokumentumok, képek videók, bankkártya adatok, felhasználói azonosítókat és jelszavakat tartalmazó rendszerfájlok, vagy egyéb érzékeny adatok után.

A támadónak lehetősége van arra is, hogy a jogosult felhasználót megszemélyesítve jelenjen meg az internet közössége előtt és a felhasználók nevében kövessenek el csalást.

A jellemző elkövetési módot az internetes zsargon a clickfraudnak nevezi. A támadás alapja a kattintás alapú hirdetés (pay per click), vagyis egy olyan internetes üzleti modell, amelyben egy weblap tulajdonos és egy marketing cég megállapodnak abban, hogy a hirdető vagy marketinges cég a weblapok felületén megjelenő hirdetésekre történő kattintások alapján fizet a weblap tulajdonosnak (pl. Google AdSense) valamilyen előre megállapított összeget.

A csalás során a zombi gépek, valós IP cím, esetleg valós felhasználói adatok felhasználásával, szimulálják a felhasználói magatartást és a hirdetésekre kattintásokat. A kattintások számának növelésével a reklámstatisztikák használhatatlanná válnak, megzavarják a viselkedés-alapú hirdetések értékelését, így rontva egy-egy marketing kampány hatásfokát, továbbá a jelentősen megnövelt kattintások eredményeként többletköltséget is okoznak a hirdetőnek. A kattintási statisztikák szabálytalanságai aláássák a bizalmat is a szerződő felek között, és ennek eredményeként a hirdetési felületeket bérbeadók elveszthetik a beszerzési forrásaikat. [1]

A zombi számítógépek felhasználhatók szervergépek szolgáltatásának megbénítására úgy, hogy legitimnek látszó kérésekkel árasztják el a célszámítógépet, amely így nem lesz képes a valódi felhasználók igényeinek kielégítésére, és jelentősen megnő a válaszideje vagy megbénul (szolgáltatás megbénítás: DoS vagy Denial of Services). A zombik számának növelésével a támadások számát radikálisan növelni lehet ezáltal a célszámítógép szolgáltatásait sokkal nagyobb valószínűséggel lehet leállítani, illetve jelentősen meg lehet növelni a leállás időtartamát (DDoS). [1]

A támadók célja lehet valamely vetélytárs informatikai szolgáltatásainak (webhely, fájlmegosztás, internetes alkalmazás vagy e-szolgáltatás) tartós megbénítása. Esetenként a támadók „védelmi pénzeket” szednek olyan vállalkozásoktól, amelyeknek üzleti-kritikus alkalmazásai elsődlegesen az interneten keresztül érhetők el (pl. internetes fogadás). A támadó ilyen esetben demonstrálja, hogy képes megakasztani a kritikus alkalmazások működését, a megtámadott pedig ezt követően vagy üzleti modellt vált, vagy megpróbálja a sávszélesség, a szerverek kapacitásának növelésével védeni magát, vagy beadja a derekát és kifizeti a zsarolónak a váltságdíjat.

A támadó célszámítógép megbénítása nélkül, a kritikus adatfájlok titkosításával is ellehetetlenítheti a jogszerű használatot, illetve zsarolhatja a felhasználót, hogy váltságdíj vagy valamilyen fizetős szolgáltatás fejében (például gyógyszerkészítmény vásárlása legalább 50 USD értékben valamelyik orosz webáruházban) tegye újra lehetővé a kódolt adat hasznosíthatóságát. [3]

A zombi számítógépek felhasználhatók arra, hogy aktívan bővítsék a botnet „klienseinek” körét, és a hálózati kapcsolaton keresztül az ismert sebezhetőségeket kihasználva további számítógépeket keressenek és fertőzzenek meg (vírus, trójai programok stb. távoli telepítésével).

A zombik egyik legismertebb adattovábbítási funkciója a kéretlen levelek (spam) küldése. A kéretlen levelek „kék pirulákkal”, szépészeti beavatkozásokkal, legális és illegális termékekkel és szolgáltatásokkal bombázzák az internet közösségét. A statisztikák szerint a spam felel a legális internet forgalom jelentős részéért, komoly fejtörést és többletterhet róva az internet szolgáltatókra, levélszerver üzemeltetőkre és a levelezést folytató felhasználókra, hogy hogyan kezeljék a megnövekedtet adatforgalmat, illetve hogyan szűrjék ki a kéretlen levelek áradatából azokat a leveleket, amelyeket legitim céllal legitim felhasználók küldenek a címzettnek.

A botnetek jelenlegi adatforgalmának kisebbik része a felhasználói magatartások nyomon követése. A zombi gépek közvetlenül vagy közvetve személyes információkat

gyűjtenek (spyware), amelyek hozzájárulnak a spam kampányok címlistáinak kialakításához és finomhangolásához.

## Botnet trendek

A botnetek fejlődése nem állt meg. A támadók felismerték a védetlen felhasználói gépekben rejlő lehetőségeket. A pásztorok már nem csak maguknak gyűjtik a zombi gépeket, hanem megindult a botnetek kereskedelme is. Egyre nagyobb létszámú és egyre jobban szervezett botneteket lehet venni vagy bérelni spam küldésre, adatgyűjtésre, vagy a konkurencia működésének megzavarására. [4] [5] A kereskedelmi lehetőségek hatására a támadók köre kibővült, nem kell informatikai szakértőnek lenni, hogy egy botnet tulajdonosaként azt támadási célra felhasználja valaki. Több botnet egyidejű birtoklásával, pedig egymástól függetlenül, de egy időben vagy egy esemény bekövetkeztekor is elindíthatók a támadások, ezzel is növelve a támadás hatékonyságát és eredményességét.

Az eddig fegyverrel, bombával „dolgozó” terrorszervezetek:

- a zombi gépekből nyert adatok adatbányászati módszerekkel történő feldolgozásával a támadásaik előkészítéséhez nyerhetnek többletinformációt;
- a letöltött hitelesítési adatokat közvetlenül felhasználva a jogosult felhasználót megszemélyesítve, annak jogaival visszaélve tevékenykedhetnek informatikai rendszerekben;
- szolgáltatás megbénítással a kritikus infrastruktúrát vezérlő számítógépeket, informatikai rendszereket állíthatnak le;
- kéretlen levélszemétben széles körben reklámozhatják a céljaikat, toborozhatnak tagokat, gyűjthetnek pénzt és erőforrásokat.

A technológia fejlődésével várhatóan a támadó egyre inkább a névtelenség homályába fog süllyedni, például újabb és újabb C&C szerverek bevonásával az irányítási hierarchia szintek bővítésével, a kommunikációs csatornák következetes és hatékony titkosításával. A csatorna titkosítására használhatnak szabványos protokollokat (SSH), anonim kommunikációs csatornákat (onion routing), egyedi fejlesztésű kriptográfiai megoldásokat vagy ezek valamilyen kombinációját. Ezek alkalmazásával nem csak a támadó személyét egyre nehezebb felderíteni, hanem a botnetekhez tartozó zombikat és a botnet egyedei közötti kommunikációt is. A jövőben az IRC alapú vezérlés mellett egyre nagyobb szerephez jutnak az egyenrangú kliensekből álló botnetek, amelyben bármely gép rendelkezik a C&C szerver képességeivel, és a pásztor véletlenszerűen alakíthatja ki a feladathoz legjobban illeszkedő irányítási struktúrát.

A kliensek intelligenciájának növelésével a jövő botnetjei képesek lesznek elkerülni a felderítést, a csatornatitkosítás mellett, például a botnet kliens program polimorfikus kódolásával, a csatornák/portok szélesebb körének kihasználásával. Az intelligens botnet kliensek képesek lesznek az operátorok és a biztonsági szakemberek által állított csapdák (honeypot, kliens kód visszafejtés, beépülés) észlelésére és kijátszására. [6] [7]

A botnetek önvédelmi funkcióit a fejlesztők kiegészítik a „megelőző csapás” képességgel, így például a botnetek a felderítést érzékelve:

- viszont felderítést (sebezhetőségi vizsgálatot) és a feltárt gyenge pontok ellen célzott, vagy
- DDoS

támadást intéznek az ellen a számítógép ellen, ahonnan a felderítés indult.

A botnetek egy másik várható fejlődési iránya az elosztott párhuzamos számítások végzése. A hackerek már jelenleg is komoly eredményeket értek el a kriptográfiai kódok megfejtésének időproblémájának tárhely problémává konvertálásával kapcsolatban[2] [8] [9], illetve egyes csoportok már kísérleteznek a zombi gépekből kialakítható szuperszámítógépekkel [10]. Az elosztott párhuzamos számítások célja a kriptográfiai támadások mellett lehet például a begyűjtött adatok adatbányászati elemzés hatékonyságának növelése.

A bűnözők mellett a katonai szervezetek is felfigyeltek a botnetekben rejlő lehetőségekre. A honi informatikai infrastuktúra szerepének növekedése és külföldi hadseregek (pl. Kína) online jelenlétének megerősödése és az ebből adódó fenyegetés miatt az USA katonai vezetői egyre többet és egyre komolyabban foglalkoznak saját katonai célú botnet hálózat kifejlesztésével és működtetésével. A defenzív stratégiai megoldások mellett a „digitális szőnyegbombázás", az ellenséges országok, szervezetek internetes infrastruktúrájának megbénítása jelentős tényező lehet a modern stratégák eszköztárában. [11]

## Összefoglalás

Az internet térhódításával az informatika és a kommunikációs technikák-technológiák konvergenciájával elkerülhetetlen, hogy egyre több és több számítógép legyen kitéve a botnetek hatásainak. A hálózatba kötött gépeket vagy a zombivá válás, vagy a zombik támadása fenyegeti.

Dolgozatomban összefoglaltam a botnetek lényeges ismérveit, a rendszereztem lényeges támadási módszereket. A trendek elemzésénél kiemeltem azokat a fejlődési irányokat, amelyek a véleményem szerint a jövőben meghatározói lesznek ennek a támadási módszernek.

A botnetek fenyegetése ellen csak a jogalkotók, a gyártók, az internet szolgáltatók és a felhasználók együttesen tudnak hatékonyan fellépni.

A jogalkotóknak olyan normákat kell alkotniuk, amelyek megteremtik a támadók felderítésének és felelősségre vonásának kereteit, meghatározzák a gyártóktól, az internet szolgáltatóktól, az egyedi és szervezeti felhasználóktól, a szervezetvezetőktől elvárható gondosság szintjét. A jogalkotónak a követelmények támasztása mellett a rendvédelmi, igazságszolgáltatási, honvédelmi és egyéb államigazgatási szervek feladati ellátásához szükséges tárgyi, jogi és anyagi feltételekről is gondoskodnia kell. A botnetek elleni hatékony fellépéshez egy ország erőfeszítései nem elegendőek. A hazai jog mellett nemzetközi fellépésre is szükség van a határokon átívelő problémák megelőzésére, felderítésére és hatékony kezelésére.

A gyártóknak a jelenleginél hatékonyabb és hibatűrőbb biztonsági protokollokat és funkciókat kell beépíteniük a termékeikbe. Amennyiben a gyártók felelősség tehetők a biztonsági szempontból alkalmatlan termékek (egyedi vagy dobozos szoftver, hardverbe ágyazott program), úgy várhatóan több biztonságos termék jelenne meg a piacon. A biztonságosabb termék nem csak a felhasználónak jelent magasabb garanciát arra, hogy a rendszer az elvárásai szerint fog működni, de a termék környezetében működő társfelhasználóknak is kevésbé kéne tartaniuk egy hibás termék miatti fenyegetéstől.

Az adatbiztonsági, adatvédelmi és titokvédelmi törvények mellett néhány speciális szervezet (hírközlési szolgáltatók, pénzügyi szervezetek) számára a jogalkotó már most is

[2] Az ingyenes 400 MB-os szivárvány tábla segítségével 99%-os valószínűséggel törhetők fel az akár 14 karakter hosszú, betűket és számokat tartalmazó jelszavak, a 9GB-s pénzért beszerezhető változat, pedig már külön kezeli a kis és nagybetűket, valamint a speciális karaktereket is.

meghatároz olyan speciális feladatokat, amelyeket az informatikai rendszer védelmében meg kell tenniük. Azonban az informatikai szolgáltató (pl. szakértői-tanácsadó tevékenységet vagy kiszervezett informatikai üzemeltetést végző) szervezetek felelősségét, az ilyen szervezetektől elvárható személyi és tárgyi feltételeket is a jelenleginél részletesebben, például az építészek sajátos szakmai követelményeihez és jogosultságaihoz hasonlóan, kellene meghatározni ahhoz, hogy az internetes fenyegetettség szintje csökkenjen.

Az internet szolgáltatóknak a jelenleginél hatékonyabban kellene kontrollálniuk az általuk kezelt alhálózatba –be és kiáramló adatot a legális felhasználók tevékenységének tiszteletben tartása mellett.

Az egyéni felhasználóknak is el kell sajátítaniuk a biztonságtudatos számítógép és internet használat alapjait. Ebben az oktatás, az új fenyegetéseket és az elhárításukat tudatosító kampányok és a biztonságot is érdemben tárgyaló – és nem utolsó sorban érthető – dokumentáció nyújthat segítséget.

## Irodalomjegyzék


[1] Wikipedia: Internet bot, Zombie computer, Dosnet; Wikipedia, h.n., http://en.wikipedia.org

[2] Sándor Munk: Software robots (softbots), their characteristics, and military applications, ZMNE, h.n., 2001. http://www.zmne.hu/tanszekek/ehc/konferencia/april2001/munk.html

[3] David Emm: Focus on trojans – holding data to ransom, Network Security Volume 2006, Issue 6, June 2006, p 4-7

[4] Robert Lemos: Bot herder pleads guilty to 'zombie' sales, Security Focus, h.n., 2006. http://www.securityfocus.com/news/11370

[5] kdawson: US Bot Herder Admits Infecting 250K Machines, Slashdot, h.n., 2007. http://it.slashdot.org/article.pl?sid=07/11/10/2054234&from=rss

[6] Elia Florio and Mircea Ciubotariu: Peerbot: Catch me if you can, Symantec Security Response, Ireland, 2007. www.symantec.com/avcenter/reference/peerbot.catch.me.if.you.can.pdf

[7] John Canavan: The Evolution of Malicious IRC Bots, Symantec Security Response, h.n., 2005. www.symantec.com/avcenter/reference/the.evolution.of.malicious.irc.bots.pdf

[8] Index: Percek alatt fejti meg jelszavainkat az új hackerszerszám, Index, h.n., 2007. http://index.hu/tech/szoftver/passwd110907/

[9] http://ophcrack.sourceforge.net/

[10] Kristóf Csaba: A botnetek verik a szuperszámítógépeket, Computerworld, h.n., 2007, http://www.computerworld.hu/botnetek-verik-szuperszamitogepeket.html

[11] COL. CHARLES W. WILLIAMSON III: Carpet bombing in cyberspace, Why America needs a military botnet, 2008/05, http://www.armedforcesjournal.com/2008/05/3375884

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Kovács László**
Zrínyi Miklós Nemzetvédelmi Egyetem
kovacs.laszlo@zmne.hu

# AZ INFORMÁCIÓS TERRORIZMUS ELLENI TEVÉKENYSÉG KORMÁNYZATI FELADATAI

***Absztrakt***

*A kritikus információs infrastruktúráink magukban hordozzák annak a veszélyét, hogy ezeket olyan terroristatámadás éri, amelyek ezeken az információs rendszereken keresztül valósulnak meg, vagy pont azokat célozzák meg. Jelen írás arra keresi a választ, hogy milyen szerepe lehet a kormánynak abban, hogy ezeket az információs infrastruktúrákat a lehető leghatékonyabb védelemmel lássa el.*

*Our critical information infrastructures include the potential threats of terrorist attack. These systems could become targets of terrorist attack, or the raid will execute through these systems. The main aim this paper to identify the possible action taken by the government to protect our essential infrastructure.*

***Kulcsszavak:*** *kritikus információs infrastruktúra, terrorizmus, kormányzat ~ critical information infrastructure, terrorism, government*

## BEVEZETÉS

A kritikus információs infrastruktúrák sebezhetősége az egész társadalom számára rendkívül nagy veszélyt jelent. Amennyiben a terrorizmus kihasználja ezt a sebezhetőséget, akkor a 2001. szeptember 11-i támadások következményeinél hatványozottabban nagyobb károkat szenvedhetünk el.

A kritikus infrastruktúrák és azok azonosítása azonban korántsem egyszerű és nagyon sokszor nem is egyértelmű kérdés. A következő nehéz feladat, hogy a kritikus infrastruktúrákon belül megtaláljuk és azonosítsuk, melyek azok a rendszerek, amelyek kritikus információs infrastruktúrának tekinthetők. E kérdés jelentősége abban mutatkozik meg, hogy amíg a kritikus infrastruktúrák esetében a fenyegetések és a veszélyek jórészt a hagyományos támadások (robbantások, fizikai károkozások, stb.) kategóriájába sorolhatók,

addig a kritikus információs infrastruktúrákat ezektől a hagyományos veszélyektől merőben eltérő – az *információs térből*[1] érkező – veszélyek és kihívások fenyegetik.

Hazánkban a kritikus infrastruktúrák vonatkozásában a napokban jelent meg hivatalosan a várva várt, úgynevezett Zöld Könyv[2], amely a hazai kritikus infrastruktúra védelemről rendelkezik. Ez a dokumentum, illetve kormányhatározat már tartalmaz utalásokat és némi kategorizálást a kritikus információs infrastruktúrák vonatkozásában, ugyanakkor a fogalom meghatározása, azaz, hogy mit tekintünk kritikus információs infrastruktúrának, annak részletes felsorolása, osztályozása, valamint a védelem konkrét feladatainak leírása mindezidáig hivatalosan, kormányzati szinten nem történt meg.[3]

Jelen írás azokat a legfontosabb szempontokat igyekszik számba venni, amelyek elengedhetetlenül fontosak ahhoz, hogy a kormányzat és a piaci élet szereplői[4] koordináltan felkészüljenek a kritikus információs infrastruktúrák védelmére, illetve egy esetlegesen bekövetkező támadás esetén a következmények mielőbbi felszámolására.

## TÁMADÁSOK AZ INFORMÁCIÓS RENDSZEREKEN KERESZTÜL

Gyakran elhangzó kérdés, hogy amennyiben valóban fennáll az előbb említett információs infrastruktúra sebezhetősége, akkor mindezidáig miért nem következett be komolyabb támadás, amely ezeket a rendszereinket érte volna?

Ennek kiderítése meghaladja jelen írás terjedelmi korlátait és valódi célkitűzéseit is. Az azonban kijelenthető, hogy voltak már kisebb-nagyobb támadások, amelyek elsősorban az interneten keresztül történtek, vagy amelyek éppen annak működésképtelenné tételét próbálták meg elérni. Ezek közül a támadások közül azonban nem mindegyik került nyilvánosságra. Ugyanakkor a nyilvánossá vált támadások közül is számos esetben felmerült a bizonyíthatóság problémája. Mindezek mellett fontos megemlíteni, hogy néhány bekövetkezett információs támadást terrorista szervezetek, vagy az általuk felbérelt csoportok követték el. Ez pedig világosan előrevetíti annak lehetőségét, hogy a különböző terrorszervezetek a jövőben is élni fognak ezzel a hatékony – bár nem mindig egyértelműen „médiásítható” – fegyverrel.

A következőkben néhány bekövetkezett információs (informatikai) támadást mutatunk be nagyon röviden.

### Támadások

Nagyon sokáig az első és egyetlen cyberterrorista akcióként[5] aposztrofálták az LTTE (Tamil Eelam Felszabadító Tigrisei) nevéhez fűződő támadást, amely során 1997-ben a szervezet aktivistái spamekkel árasztották el a világ különböző országaiban működő srí lankai követségek e-mail postaládáit, válaszul néhány tagjuk bebörtönzésére. Az akció nagy kárt

[1] Információs dimenzióból

[2] A Kormány 2080/2008. (VI.30.) Korm. határozata a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.

[3] Általánosságban már több kutatócsoport is meghatározta, majd osztályozta ezeket a rendszereket, amelyek talán a kormányzati munka kiinduló alapjai is lehetnének.

[4] Mivel az infrastruktúrák jelentős része, így a kritikus infrastruktúrák és a kritikus információs infrastruktúrák többsége is gazdasági társaságok tulajdonában vagy üzemeltetésében van, ezért az világosan látszik, hogy azok védelme nem csak kormányzati, hanem közös – a tulajdonosokkal és az üzemeltetőkkel koordinált – tevékenységeket kell, hogy takarjon.

[5] Ezen a helyen azokat a támadásokat is cybertámadásoknak tekintettük, amelyeket hagyományos terrorszervezetek, vagy olyan csoportok, személyek követtek az interneten keresztül, amelyek terrortámadásnak minősíthetőek.

nem okozott, de felhívta a figyelmet az információs rendszerek sebezhetőségére, illetve arra a tényre, hogy a hagyományos terrorista szervezetektől sem áll távol az információs támadás.[1]

1997 júliusában e-mail bombatámadás érte az Institute for Global Communications (IGC) amerikai internetszolgáltatót, akik az Euskal Herria (Baszk Újság) honlapját tartották fenn. A támadás a honlap eltávolítását követelte. [2]

2000 márciusában a Japán rendőrség bejelentett, hogy több mint 150 rendőrségi gépjármű számítógépes rendszerében olyan kémprogramokat találtak, amelyeket többek között követésre, valamint adatlekérésre programoztak. A vizsgálat kiderítette, hogy a gépjárművek fedélzeti szoftvereit az Aum Shinryko terrorista csoporthoz köthető egyik vállalkozás fejlesztette. (Ez a terrorista a csoport követte el a Tokiói metróban, 1995-ben a 12 halálos, és több mint 6000 sérültet okozó szaringáz támadást). A szoftverek segítségével 115 rendőrségi gépjármű helyét követték, amelyek között több civil autó is volt. A további vizsgálatok rámutattak, hogy a csoport több mint 80 japán cég és 10 kormányzati szerv számára szállított szoftvereket korábban. Ezekbe a leszállított szoftverekbe trójai programokat telepíttettek egy későbbi terrortámadás elősegítésére. [3]

2002 októberében az internet legfontosabb infrastruktúrái ellen indult összehangolt támadás. Ekkor a 13 DNS[6] root szerver ellen követtek el DoS[7] illetve DDoS[8] támadásokat. Ez a fajta támadás 2007 februárjában megismétlődött. Szerencsére egyik esetben sem sikerült komoly fennakadást okozni a nemzetközi internet forgalomban, amely egyrészt annak köszönhető, hogy a 13 root szerver több mint 40 helyen tükrözve van. [4]

2003-ban román elkövetők megzsarolták az amerikai National Science Foundation-t (NSF), hogy eladják a szervezet feltört és így nagymértékben feltérképezett számítógépes hálózatának adatait, amennyiben nem kapnak megfelelő anyagi ellenszolgáltatást. Ez a hálózat irányította a Déli-sarkon lévő NSF által fenntartott kutatóbázis energiaellátását és fűtését. Miután bebizonyosodott a fenyegetés valódisága, le kellett választani a kutatóbázis hálózatát. [5]

2004-ben történt, a később Titan Rain-nek keresztelt támadás, amelynek során feltételezhetően kínai hackerek bejutottak az amerikai védelmi minisztérium számára is fejlesztő Lockheed Martin számítógépes hálózatába és onnan érzékeny adatokat szereztek meg. [6]

2007 áprilisában és májusában DDoS támadások érték Észtország számítógépes hálózatait. Az egyébként igen fejlett információs infrastruktúrával rendelkező, és az e-kormányzat területén komoly sikereket elért Észtország, a több mint kéthetes támadás során komoly anyagi károkat szenvedett, mert számos kormányzati, minisztériumi és több bank internetes oldala vált elérhetetlenné a támadások következtében. A támadások a tallinni orosz emlékmű elmozdítása után kezdődtek, és nagy részük többé-kevésbé beazonosíthatóan Oroszországban működtetett szerverekről indult. Az észt miniszterelnök az orosz kormányt tette felelőssé a támadások miatt. Oroszországot korábban Ukrajna és az Egyesült Államok is megvádolta hasonló támadások végrehajtásával, de Moszkva minden alkalommal határozottan tagadta részvételét az akciókban. Az online támadások alatt összesen 128 túlterheléses támadás történt, a legkomolyabbak öt-tíz órán át, több száz megabitnyi sávszélességen bombázták folyamatos adatlekérésekkel a megtámadott szervereket, addig amíg azok össze nem omlottak. Az észt hálózaton az adatforgalom esetenként órákon át a normális ezerszerese volt. Ehhez egyes források szerint valószínűleg az internetes alvilágtól kellett erőforrásokat bérelnie a támadóknak. Érdemes megjegyezni, hogy közel fél évvel a támadások után csak egyetlen támadót sikerült bizonyíthatóan azonosítani. Meglepő módon azonban ez a támadó egy észt fiatalember volt, akit a bizonyítékok alapján pénzbüntetésre ítéltek. [7]

[6] Domain Name Server
[7] DoS: Denial of Service, azaz túlterheléses támadás.
[8] DDoS: Distributed Denial of Service, azaz elosztott túlterheléses támadás.

## A cyber- és az információs terrorizmus

A fenti információs (informatikai) támadások tanulmányozása esetén nyilvánvalóan kitűnik, hogy a terrorista szervezetek is egyre inkább használják az információs rendszereket, magát az internetet, sőt támadásaikat azon keresztül is kivitelezhetik. Ennek kapcsán felmerül a cyberterrorizmus kérdése.

A témában a cyberterrorizmusra vonatkozó egyik legelső meghatározás az FBI úgynevezett cyber részlegének volt vezetőjétől – Keith Lourdeau-tól – származik: „*A cyberterrorizmus olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs lehetőségekkel úgy hajtanak végre, hogy azok rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében.*" [8]

Mindezek alapján az nyilvánvaló és jól következtethető, hogy a hagyományos terrorizmus, illetve a cyberterrorizmus közös, esetenként egymást kiegészítő, párhuzamos támadásai a legsebezhetőbb és nélkülözhetetlen információs infrastruktúráink ellen, beláthatatlan anyagi és humán károkat okoznának. Abban az esetben, amennyiben egy ilyen közös támadás, vagy az azzal való fenyegetés megjelenik, és azok valóban az információs rendszereinket célozzák, beszélhetünk *információs terrorizmusról*. Az információs terrorizmus definíciószerűen megfogalmazva: „*a cybertámadásokat és a hagyományos terrortámadásokat egyszerre alkalmazó olyan terrortevékenység, amely az információs infrastruktúrákat felhasználva, a kritikus információs infrastruktúra elleni támadásokkal próbálja meg célját elérni*." [9]

## A KRITIKUS INFRASTRUKTÚRA ÉS A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA MEGHATÁROZÁSA MAGYARORSZÁGON

Kutatók már korábban megállapították, hogy már a kritikus infrastruktúrák feltérképezése is meglehetősen nehéz és bonyolult feladat, mert „*ami kritikus* (infrastruktúra) *helyileg, az nem biztos, hogy kritikus az állam számára is. Ráadásul, erről gyakran még pontos információ sincs, hiszen jellemzően területi, vagy helyi szinten nem rendelkeznek szakszerű, tudományosan megalapozott kockázatértékeléssel."* [10]

Ugyanakkor, amennyiben a kritikus infrastruktúrák illetve a kritikus információs infrastruktúrák részleges, időleges, vagy akár teljes kiesése vagy leállása esetén megvizsgáljuk azokat a hatásokat, amelyek ennek következményeként fellépnek, akkor a következő kategorizálást tudjuk megtenni [11; 12]:

- Kiterjedés[9]: a kritikus infrastruktúra, illetve azok egyes elemeinek kiesése esetén jelentkező negatív hatás annak a földrajzi területnek nagysága alapján jellemezhető és osztályozható, amelyet a veszteség vagy az adott szolgáltatás megszűnése érinthet. Mivel infrastruktúráink több földrajzi régiót érintve egymással kapcsolatban vannak, több földrajzi régiót érintve, ezért ezt a kategóriát nemzetközi, nemzeti és regionális szintekre is fel lehet osztani.
- Nagyságrend: az infrastruktúra meghibásodásából vagy kieséséből fakadó hatás mértékét jelenti, amely a társadalom, a gazdaság és a kormányzat esetében jelenik meg. Ezt a következőképpen lehet értékelni: nincs hatás, minimális, mérsékelt vagy jelentős hatás. A nagyságrend megállapításához a következő szempontokat szükséges figyelembe venni:

[9] A kiterjedést sok esetben hatókörként is értelmezik, melynek tartalma megegyezik az itt leírtakkal.

- társadalmi hatás (népességre gyakorolt hatás): a szolgáltatás kiesése miatt érintett lakosság, azaz a szolgáltatást igénybe vevők száma;
- gazdasági hatás: a gazdasági veszteség jelentősége, illetve a termékek és szolgáltatások színvonalában mérhető negatív változás mértéke. Ebbe a hatásba tartozik az infrastruktúra fizikai sérüléséből, elvesztéséből fakadó közvetlen (azaz a sérült infrastruktúra értéke, annak pótlásának költsége) vagy a közvetett (pl. piacra gyakorolt negatív hatás) károk;
- környezeti hatás: az infrastruktúra működésképtelensége miatt bekövetkezett környezeti kár mértéke;
- politikai hatás: az állami intézmények iránti bizalom csökkenése, vagy az állami szervek működőképességének csökkenése;
- közegészségügyi hatás: áldozatok száma, betegségek, esetleges járványok, súlyos sérülések, stb. hatása;
- pszichológiai hatás: lakosság magatartásának megváltozása;
- kölcsönös függőségi hatás: azoknak az interdependáns rendszereknek, illetve elemeknek az elemzése és értékelése, amelyek az adott infrastruktúrát, az adott vagy tágabban kapcsolódó szektort, illetve a nemzeti és nemzetközi viszonylatban felmerülő függéseket meghatározzák, befolyásolják.

- Időbeli hatás: annak meghatározása, hogy az adott infrastrukturális rendszerrel, vagy rendszer-elemmel kapcsolatos veszteség mennyi idő elteltével fejt ki komoly hatást (azonnali, 24–48 óra, egy hét, stb.), illetve mennyi ideig tart ez a hatás.

A már említett hazai Zöld Könyv immár hivatalosan is meghatározza a kritikus infrastruktúra fogalmát: „*Kritikus infrastruktúra alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot feltárásában*.” [12]

Az 1. Táblázat bemutatja, hogy a hazai Zöld Könyv milyen ágazatokra és alágazatokra bontja a hazai kritikus infrastruktúrákat. Érdemes megjegyezni, hogy a kormányhatározat 2. melléklete felelősöket is hozzárendel – hasonlóan az USA ilyen irányú rendelkezéséihez[10] – a felsorolt ágazatokhoz.

Mielőtt a táblázatban felsorolt kritikus infrastruktúrákat kritikus információs infrastruktúra szempontból megvizsgálnánk, célszerű meghatározni, hogy mit is értünk a kettő különbségén. A kritikus infrastruktúra meghatározást már láthattuk. Ugyanakkor a kritikus információs infrastruktúra nem minden esetben egyezik meg a kritikus infrastruktúrával. A kritikus infrastruktúrák védelmére vonatkozó európai programról szóló Zöld Könyv szerint „*kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, internet, műholdak stb.)”*. [13]

[10] pl.: a Bush elnök által kiadott 7/HSPD-7 elnöki direktíva [14]

**1. Táblázat:** Kritikus infrastruktúra ágazati, alágazati és felelősi besorolás a hazai Zöld Könyv alapján [12]

| Ágazat | Alágazat | Felelős |
|---|---|---|
| I. Energia | 1. kőolaj kitermelés, finomítás, tárolás és elosztás<br>2. földgáztermelés, tárolás, szállítás és rendszerirányítás, elosztás<br>3. villamosenergia-termelés, átvitel és rendszerirányítás, elosztás | KHEM |
| II. Infokommunikációs technológiák | 4. információs rendszerek és hálózatok<br>5. eszköz-, automatikai és ellenőrzési rendszerek<br>6. internet, infrastruktúra és hozzáférés<br>7. vezetékes és mobil távközlési szolgáltatások<br>8. rádiós távközlés és navigáció<br>9. műholdas távközlés és navigáció<br>10. műsorszórás<br>11. postai szolgáltatások<br>12. kormányzati informatikai, elektronikus hálózatok | MeH EKK, KHEM |
| III. Közlekedés | 13. közúti közlekedés<br>14. vasúti közlekedés<br>15. légi közlekedés<br>16. vízi közlekedés<br>17. logisztikai központok | KHEM |
| IV. Víz | 18. ivóvíz szolgáltatás<br>19. felszíni és felszín alatti vizek minőségének ellenőrzése<br>20. szennyvízelvezetés és -tisztítás<br>21. vízbázisok védelme<br>22. árvízi védművek, gátak | KvVM |
| V. Élelmiszer | 23. élelmiszer előállítás<br>24. élelmiszer-biztonság | FVM |
| VI. Egészségügy | 25. kórházi ellátás<br>26. mentésirányítás<br>27. egészségügyi tartalékok és vérkészletek<br>28. magas biztonsági szintű biológiai laboratóriumok<br>29. egészségbiztosítás | EüM |
| VII. Pénzügy | 30. fizetési, értékpapírklíring- és elszámolási infrastruktúrák és rendszerek<br>31. bank és hitelintézeti biztonság | PM |
| VIII. Ipar | 32. vegyi anyagok előállítása, tárolása és feldolgozása<br>33. veszélyes anyagok szállítása,<br>34. veszélyes hulladékok kezelése és tárolása,<br>35. nukleáris anyagok előállítása, tárolása, feldolgozása<br>36. nukleáris kutatóberendezések<br>37. hadiipari termelés<br>38. oltóanyag és gyógyszergyártás | KHEM, HM, ÖM (OKF), IRM (OAH) NFGM |
| IX. Jogrend – Kormányzat | 39. kormányzati létesítmények, eszközök<br>40. közigazgatási szolgáltatások<br>41. igazságszolgáltatás, | IRM, ÖM, HM |
| X. Közbiztonság – Védelem | 42. honvédelmi létesítmények, eszközök, hálózatok<br>43. rendvédelmi szervek infrastruktúrái | IRM, HM, ÖM (OKF) |

Amennyiben ez utóbbi megfogalmazást elfogadjuk a kritikus információs infrastruktúrára vonatkozónak, akkor az előbbi táblázatból – azaz a hazai kritikus infrastruktúrák felsorolásából – jól látszik, hogy bár a *II. Infokommunikációs technológiák* ágazat, illetve az itt meghatározott alágazatok – információs rendszerek és hálózatok; eszköz-, automatikai és ellenőrzési rendszerek; internet, infrastruktúra és hozzáférés; vezetékes és mobil távközlési szolgáltatások; rádiós távközlés és navigáció; műholdas távközlés és navigáció; műsorszórás; postai szolgáltatások; kormányzati informatikai, elektronikus hálózatok – kritikus információs infrastruktúráknak tekinthetők, mégis számos más ágazatban is találhatunk olyan rendszert vagy elemet, amely kritikus információs infrastruktúrának minősül. Többek között ilyen rendszer vagy elem az *I. Energia* ágazatban több alágazatnál említett rendszerirányítás is.

Korábbi tanulmányok már többször – természetesen esetenként a vizsgálatot végző csoport szakmai kompetenciáját, vagy megközelítési módszereit tükröző módon, de többnyire egyöntetűen, illetve egymástól csak kis mértékben eltérve – megállapították, hogy hazánkban melyek minősülhetnek kritikus információs infrastruktúrák. Ezek közül a kritikus információs infrastruktúra-csoportosításokból kettőt kívánunk bemutatni.

Az első felosztás alapvetően az információs rendszereket – ezek közül is az egyik legsérülékenyebbeket, a számítógép-hálózatokat – vette alapul a felosztás megalkotásakor. E felosztás szerint a következők minősülhetnek kritikus információs infrastruktúrának:

- energiaellátó rendszerek rendszerirányító számítógép-hálózatai;
- kommunikációs hálózatok (vezetékes, mobil, műholdas);
- közlekedés szervezés és irányítás számítógép-hálózatai;
- pénzügyi-gazdasági rendszer számítógép-hálózatai;
- védelmi szféra riasztási, távközlési, számítógép-hálózatai;
- egészségügyi rendszer számítógép-hálózatai;
- kormányzati és önkormányzati információs rendszerek. [9; 15]

A másik bemutatandó felosztás már nem csak a számítógép-hálózatokat, hanem a tágabb értelemben vett infokommunikációs eszközöket és rendszereket helyezte a vizsgálat homlokterébe. Ennek megfelelően a Magyar Köztársaság kritikus információs infrastruktúrái közé tartoznak:

- informatikai rendszerek és hálózatok;
- automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
- internet szolgáltatás (infrastruktúra is);
- vezetékes távközlési szolgáltatások;
- mobil távközlési szolgáltatások;
- rádiós távközlés és navigáció;
- műholdas távközlés;
- műsorszórás;
- közigazgatási informatika és kommunikáció;
- a kritikus infrastruktúrák létfontosságú infokommunikációs rendszerei. [11]

A két felosztás – bár látszik a vizsgálati szempontok alapján a különbség – mégis nagyon sok hasonlóságot, sok átfedést tartalmaz.

Összességében tehát megállapíthatjuk, hogy számos kritikus infrastruktúra önmagában, vagy egyes részeiben és elemeiben is kritikus információs infrastruktúra, ugyanakkor a fenti két felosztást kiemelve a kritikus információs infrastruktúrák alapvetően infokommunikációs rendszerek. Ezek sérülékenysége – a hathatós védelmi intézkedések, ajánlások és szabályzók ellenére – igen magas. Tovább nehezíti a kérdést, hogy sok esetben ezek az infokommunikációs rendszerek azok, amelyek a már említett kritikus infrastruktúrák közötti interdependenciát jelentik, azaz pont ezek azok a rendszerek, amelyeken keresztül

infrastruktúráink összekapcsolódnak. Ez az összekapcsolódás lehet fizikai, de lehet logikai is, hiszen sok esetben az infokommunikációs rendszerek által összegyűjtött, feldolgozott, majd a megfelelő helyre eljutatott adat vagy információ jelenti a kapcsolatot.

Abban az esetben, amennyiben ezek az infokommunikációs rendszerek, azaz kritikus információs infrastruktúrák sérülnek – akár csak időlegesen, vagy akár csak lokálisan –, akkor az a kritikus infrastruktúrák működésére komoly negatív hatással van, azaz azok is működésképtelenné válhatnak.

Ennek megfelelően kijelenthető, hogy a kritikus információs infrastruktúrák jelentik azokat a kulcspontokat, amelyek védelme érdekében mindent meg kell tenni, azaz a kritikus infrastruktúrák védelem területén kiemelt helyen kell kezelni ezeket a rendszereket.

## A VÉDELEM KORMÁNYZATI FELADATAI

A már idézett EU Zöld Könyv szerint a kritikus információs infrastruktúra védelme: „a *tulajdonosok, üzemeltetők, gyártók és használók, valamint a hatóságok programjai és tevékenységei, melyek célja fenntartani a kritikus információs infrastruktúra teljesítményét meghibásodás, támadás vagy baleset esetén a meghatározott minimális szolgáltatási szint felett, illetve minimálisra csökkenteni a helyreállításhoz szükséges időt, valamint a károkat.*" [13]

Az EU a védelem érdekében különböző szervezeteket (hálózatokat és projekteket) is létrehozott, illetve a közeljövőben létre fog hozni. Ilyen szervezetek például:

- Kritikus Infrastruktúra Figyelmeztető Információs Rendszer (Critical Infrastructure Warning Information Network — CIWIN[11]);
- Európai Hálózati és Informatikai Biztonság Ügynökség (European Network and Information Security Agency — ENISA);
- Kritikus Információs Infrastruktúra Kutató Koordináció projekt (Critical Information Infrastructure Research Co-ordination — CI2RCO). [13]

A kritikus infrastruktúra illetve a kritikus információs infrastruktúra védelem nem új keletű feladat hazánkban sem. A védelemről már a terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004. (V.7) Korm. határozat, illetve annak módosításáról szóló 2046/2007 (III. 19.) Korm. határozat 1. sz. melléklet 2.3.1. pontja is rendelkezik, amely előírja a Kritikus Infrastruktúra Védelem Európai Programjának (EPCIP – European Programme for CIP) megközelítését tükröző, a különböző ágazati feladat- és hatáskörbe tartozó kritikus infrastruktúra védelmi tevékenységek közös keretrendszerbe foglalásáról, ágazatközi összehangolásáról szóló előterjesztés elkészítését. További lépések megtételét írja elő a katasztrófavédelemmel összefüggő 2007. évi feladatokról szóló 1/2007. (III.29.) Kormányzati Koordinációs Bizottság határozat 5. b) pontja, amely értelmében meg kell kezdeni a kritikus infrastruktúra védelem nemzeti programjának kidolgozását, elő kell készíteni a kritikus infrastruktúra védelem hazai koordinációjáról, feladatairól szóló kormány előterjesztést.

Mindezeket figyelembe véve született meg a hazai Zöld Könyv, azaz a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló kormányhatározat. A dokumentum alapján szükségessé válik az állami és a tulajdonosi feladatok szétválasztása, majd ennek megfelelően a konkrét védelmi tennivalók meghatározása. A Zöld Könyv a következő feladatokat határozza meg a kormány számára:

[11] A hazai Zöld Könyv meghatározza, hogy egy adott konkrét veszély megléte esetén az információknak, illetve a veszélyjelzéseknek a kritikus infrastruktúra tulajdonosok és üzemeltetők, illetve az állami szervek számára is rendelkezésre kell, hogy álljanak. Ezért meg kell vizsgálni azt, hogy a hazai veszélyjelző és jelentő informatikai és kommunikációs rendszer alkalmas-e arra, hogy a CIWIN-nel együtt tudjon működni.

- a nemzeti koordináló szerv és feladatainak meghatározása:
  a hatékonyság és a koherencia megteremtésére szükséges egy nemzeti koordináló szerv felállítása (pl.: Miniszterelnöki hivatalban), amely összefogja, irányítja és elősegíti az eltérő ágazatokban, illetve a kormány és a különböző tulajdonosok közötti kritikus infrastruktúra védelem feladatait;
- a kritikus ágazatok és az ágazati koordináló minisztériumok kijelölése;
- javaslattétel az európai szintű kritikus infrastruktúra elemek kijelölésére. [12]

A Zöld Könyv nem csak a kormány, hanem a központi államigazgatási szervek, illetve a különböző kritikus infrastruktúra elemek tulajdonosainak és üzemeltetőinek is meghatároz számos – a védelem területén igen fontos – feladatot. Ezek azonban többnyire általános, nagyvonalakban meghatározott tevékenységek.

Kritikus információs infrastruktúra szempontból elemezve a dokumentumot, elmondható, hogy a hazai Zöld Könyv nem határoz meg külön feladatokat a hazai kritikus információs infrastruktúrák védelmére, azokat mintegy a kritikus infrastruktúra védelembe érti. Ezt támasztja alá az is, hogy a kormányrendelet a kritikus infrastruktúrákat veszélyeztető tényezők között megemlíti *„a gazdasági, vagy politikai indítékból, kritikus informatikai rendszerek és hálózatok ellen elkövetett visszaélések, illetve cyber-támadások (cyber-terrorizmus, DDOS támadások, tömeges phising incidensek)”* [12] jelentette veszélyeket,[12] ugyanakkor ezekhez a veszélyekhez konkrét védelmi feladatokat nem rendel hozzá.

Mindezek alapján a hazai kritikus információs infrastruktúrák védelmének területén a következő kormányzati feladatok válnak szükségessé:

- meg kell határozni a kritikus információs infrastruktúra hazai fogalmát;
- az ágazati kritikus infrastruktúrák mellett meg kell határozni azokat az elemeket, amelyek kritikus információs infrastruktúraként jelentkeznek;
- fel kell tárni a hazai a kritikus információs infrastruktúrákat fenyegető konkrét veszélyeket;
- elemezni kell, hogy a feltárt veszélyforrások közül, melyik és milyen mértékben érinti a meghatározott kritikus információs infrastruktúrákat, illetve azok egyes elemeit;
- konkrét szimulációkat kell tervezni és szervezni az információs infrastruktúrák körében, amelyek alapján fel lehet tárni azokat a pontokat, kulcsfontosságú elemeket, amelyek a gazdaság, a társadalom és a kormányzat szempontjából létfontosságúak;
- meg kell határozni, és fel kell térképezni a hazai információs infrastruktúrák egymásra, illetve a kritikus infrastruktúrákra gyakorolt közvetlen és közvetett hatásait;
- meg kell határozni, és fel kell térképezni a hazai információs infrastruktúrák környező országok infrastruktúráira gyakorolt hatását;[13]
- a kormányzati koordináló szerv feladatait és résztvevőit ki kell egészíteni a kritikus információs infrastruktúra tulajdonosainak, üzemeltetőinek, illetve a hazai CERT-ek képviselőivel;
- meg kell vizsgálni, hogy alkalmas-e egy esetleges terrortámadás esetén a hazai információs és kommunikációs infrastruktúra a riasztás és a jelzés, majd a vészhelyzeti kommunikáció menedzselésére;
- a tudatos és biztonságos internet-, illetve infokommunikációs eszközhasználatának oktatása, az erre való lakossági felkészítés az eddiginél hatékonyabb és nagyobb szerepet kell, hogy kapjon.

[12] Érdemes megjegyezni, hogy a dokumentum informatikai rendszerek és hálózatokat említ ehelyütt, a tágabb értelemben vett információs rendszerek helyett.

[13] Ezt a feladatot előírja az Európai Bizottság 9403/08-as, az európai kritikus infrastruktúra azonosításáról és megjelöléséről, és azok védelmének növeléséről szóló határozata is. [16]

## ÖSSZEFOGLALÁS

Természetesen a fent megfogalmazott kormányzati feladatok önmagukban még nem hozzák meg a kívánt eredményt, azaz nem lesznek „sebezhetetlenek” a kritikus információs infrastruktúráink.

Az azonban teljes bizonyossággal látszik, hogy a védelem lehető legmagasabb szintűre emelése érdekében egy széleskörű, érdekközösségen alapuló összefogásra van szükség, amelyben a kormány mellett a különböző kormányzati szerveknek, a kritikus információs infrastruktúrák tulajdonosainak és üzemeltetőinek, valamint a társadalomnak is komoly szerepe és faladatai vannak.

Ugyanakkor a védelem megteremtése kormányzati és tulajdonosi oldalról sem történhet máshogy, csak koordináltan. E koordináció, pedig a hatékonyság maximalizálása érdekében centralizált kell, hogy legyen.

A védelem hármas célját, azaz a felkészülést a védelemre, a riasztás és jelzést, valamint a folyamatos és kiesés nélküli üzemeltetést, csak abban az esetben lehet megvalósítani, amennyiben a különböző résztvevők – kormány, kormányzati, vagy ágazati szervek, tulajdonosok, üzemeltetők, riasztást és az együttműködők közötti kommunikációt biztosító információs rendszert üzemeltetők – képviselői közösen vesznek részt a koordinációs szerv munkájában.

## FELHASZNÁLT IRODALOM:


[1] http://konfliktus.index.hu/sritigrisek.html (2008.06.10.)

[2] http://www.bbc.co.uk/politics97/news/07/0719/eta.shtml (2008.06.10.)

[3] http://fas.org/irp/threat/terrorism/sup2.pdf (2008.06.10.)

[4] http://index.hu/tech/biztonsag/hekk0207/ (2008.06.10.)

[5] http://www.fbi.gov/page2/july03/071803backsp.htm (2008.06.10.)

[6] http://www.time.com/time/magazine/article/0,9171,1098961,00.html (2008.06.10.)

[7] http://index.hu/tech/jog/eszt250108 (2008.06.10.)

[8] http://www.fbi.gov/congress/congress04/lourdeau022404.htm (2008.06.10.)

[9] Kovács László: Kritikus információs infrastruktúrák. Egyetemi jegyzet. ZMNE, 2007.

[10] Bukovics István–Vavrik Antal: Infrastruktúrák kockázata és biztonsága: kritikai problémaelemzés. Hadmérnök, 2006. december. http://zrinyi.zmne.hu/hadmernok/archivum/2006/3/2006_3_bukovics.html ISSN 1788-1919 (2008.06.10.)

[11] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Doktori értekezés. ZMNE, Budapest, 2007.

[12] 2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[13] Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final.

[14] Homeland Security Presidential Directive 7/HSPD-7, Washington, December 17, 2003.

[15] Haig Zsolt – Kovács László – Ványa László: Kritikus információs infrastruktúrák támadása, védelme. Dunaújvárosi Főiskola Közleményei, XXIX/1. ISSN 1586-8567

[16] European Council directive on the identification and designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection (9403/08).

*Jelen írás a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.*

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Varga Péter János**
Budapesti Műszaki Főiskola
varga.peter@kvk.bmf.hu

# A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK ÉRTELMEZÉSE

***Absztrakt***

*A szerző a cikkben bemutatja a kritikus infrastruktúrák és ezen belül a kritikus információs infrastruktúrák fogalmát a hazai és nemzetközi szakirodalom tükrében. Felvázolja a kritikus infrastruktúrák ágazatait és az ágazatok kapcsolatát a kritikus információs infrastruktúrákkal. Részletezi a kritikus információs infrastruktúrákon belül a támogató– és funkcionális információs infrastruktúrákat.*

*In this paper the author describes the critical infrastructure, defines critical information infrastructure in the mirror of both the national and international technical*
*literature. The author shows the branches of critical infrastructure, their relationships with critical information infrastructure, and in addition he distinguishes and defines supporting and functional information infrastructure.*

***Kulcsszavak:*** *infrastruktúra, kritikus infrastruktúra, kritikus információs infrastruktúra ~ infrastructure, critical infrastructure, critical information infrastructure*

## BEVEZETŐ

A föld népessége egyre nő, amely a szükségletek mennyiségi növekedését eredményezi. Ezek kielégítésének biztosításában nagy szerepet játszanak az infrastruktúrák, ezen belül is a kritikus információs infrastruktúrák. Ezzel kapcsolatban a következő kérdések merülnek fel:

- Mi az infrastruktúra?
- Mi a kritikus infrastruktúra?
- Mi a kritikus információs infrastruktúra?

## INFRASTRUKTÚRA FOGALMA

A fogalmak közül vizsgáljuk meg először az infrastruktúra fogalmát a különböző szakirodalmakban.

A Magyar Értelmező Kéziszótár meghatározása szerint az infrastruktúra olyan angolszász eredetű szó, amely jelentése „a társadalmi, gazdasági tevékenység zavartalanságát biztosító

alapvető létesítmények, szervezetek (pl. lakások, közművek, a kereskedelem, a távközlés, az oktatás, az egészségügy stb.) rendszere." [1]

A Magyar Larousse Enciklopédia meghatározása szerint az infrastruktúra „a társadalmi, gazdasági újratermelés zavartalanságát biztosító háttér. Legfontosabb elemei a közművek, az energiaellátás rendszere és a közlekedési, hírközlési hálózat (utak, vasutak, telefonhálózat, stb.) Az ún. lakossági infrastruktúrához tartozik a lakásállomány, a kereskedelmi és szolgáltatási hálózat, az egészségügyi, szociális, kulturális ellátás, az oktatás eszközei és intézményrendszere (kórházak, rendelőintézetek, iskolák)." [2]

Egy másik szakirodalom szerint az infrastruktúra nem más, mint „egy adott rendszer (termelő vagy elosztó, szolgáltató rendszer, tudományos, állami, magán, nemzeti vagy nemzetközi szervezet, ország, város, vagy régió stb.) rendeltetésszerű működéséhez feltétlenül szükséges intézetek, intézmények, felszerelések és berendezések és a működtetést ellátó személyzet szabályszerűen működő összessége. Az infrastruktúra tehát a fizikai építményekből és berendezésekből és azokat szakszerűen működtetni tudó szakszemélyzetből áll." [3]

1997-ben az amerikai kormány egyik bizottsága a következőképpen fogalmazta meg az infrastruktúra fogalmát: „Az infrastruktúrák olyan egymástól függő hálózatok és rendszerek összessége, amelyek meghatározott ipari létesítményeket, intézményeket (beleértve a szakembereket és eljárásokat), illetve elosztó képességeket tartalmaznak. Mindezek biztosítják a termékek megbízható áramlását az Egyesült Államok védelmi és gazdasági biztonságának fenntartása, valamint a minden szinten zavartalan kormányzati munka és a társadalom egésze érdekében."[4]

Véleményem szerint a Magyar Larousse Enciklopédia meghatározása az infrastruktúráról teljes mértékben kimerítő, és lefedi a hazai infrastruktúrákat. Sorra veszi azokat, amelyek hiánya kihatással lenne életünkre.

## KRITIKUS INFRASTRUKTÚRA FOGALMA

Míg az infrastruktúra fogalma kellő körültekintés árán kielégítő pontossággal meghatározható, a kritikusság ismérvei sokrétűek, szerteágazóak, tudomány- és iparáganként változnak. Egy infrastruktúra tehát nagyon sok szempontból lehet kritikus, kritikussá minősítéséhez viszont az is elég, ha csak egyetlen egy kritérium szerint az.[5]

A kritériumok lehetnek a következők:

- Hatókör: földrajzi kiterjedésben mutatja a kritikus infrastruktúra megsemmisülése, működésképtelenné válásának hatását. Ez lehet nemzetközi, nemzeti, regionális, territoriális vagy helyi.[6]
- Nagyságrend: a veszteség vagy a hatás nagyságrendje (például: nincs hatás, minimális, mérsékelt vagy jelentős a hatás). A nagyságrend megállapításához a következő szempontokat is érdemes figyelembe venni:
  - népességre gyakorolt hatás (az érintett lakosság száma, áldozatok, betegségek, súlyos sérülések, kitelepítések);
  - gazdasági hatás (GDP-re gyakorolt hatása, jelentős gazdasági veszteség és/vagy termelés, szolgáltatás fokozatos romlása);
  - környezetvédelmi (a lakosságra és lakókörnyezetére gyakorolt hatás);
  - interdependencia (a kritikus infrastruktúrák elemei közötti függőség);
  - politikai (az államba vetett bizalom).[6]
- Időbeli hatás: mely megmutatja, hogy az adott infrastruktúra vagy elemének vesztesége mennyi idővel később fejti ki komoly hatását (pl.: azonnali, 24-48 óra, egy hét, egyéb).[6]

Ezek után célszerű megvizsgálni, hogy a biztonság terén élenjáró Amerikai Egyesült Államok és az Európai Unió milyen fogalmi meghatározásokat alkottak a témában.

Az Amerikai Egyesült Államok meghatározása szerint: "a kritikus infrastruktúrák azok a valós és virtuális rendszerek, eszközök, amelyek alapvető fontosságúak az Egyesül Államok számára, és e rendszerek illetve eszközök működésképtelensége vagy megsemmisülése csökkentené a biztonságot, a nemzetgazdaság biztonságát, a nemzeti közegészséget és annak biztonságát vagy mindezek kombinációját." [7]

Az Európai Unió dokumentuma szerint: "a kritikus infrastruktúrákhoz azok a fizikai erőforrások, szolgáltatások és információtechnológiai létesítmények, hálózatok, és infrastrukturális berendezések tartoznak, melyek összeomlása vagy megsemmisülése komoly következményekkel járna a polgárok egészségére, biztonságára, védelmére vagy gazdasági jólétére, illetve a kormányok hatékony működésére." [8]

A fogalmi meghatározás alapján az Európai Unió illetékes bizottsága a kritikus infrastruktúrák közé az alábbiakat sorolja:

- energiatermelés és hálózat (áramszolgáltatás, olaj és gáztermelés, energiatárolók és finomítók, energiaátadó és elosztó rendszerek);
- kommunikációs és információs technológia (távközlés, műsorszórórendszerek, szoftver, hardver és hálózatok, beleértve az Internetet);
- pénzügy (bankügyletek, kötvények és befektetések);
- egészségügy (kórházak, egészségügyi és vérellátó intézmények, laboratóriumok és gyógyszertárak, kutató és mentőszolgálatok, mentők);
- élelmiszerellátás (élelmiszerbiztonság, termelés, nagykereskedelem és élelmiszeripar);
- vízellátás (gátak, víztározók, víztisztítás és vízhálózat);
- közlekedés (pl.: repterek, kikötők, vasúti és tömegközlekedési hálózatok, közlekedésirányító rendszerek);
- veszélyes áruk termelése, tárolása és szállítása (kémiai, biológiai, radiológiai és nukleáris anyagok);
- kormányzat (kritikus szolgáltatások, létesítmények, információs hálózatok, eszközök és jelentős nemzeti emlékhelyek műemlékek). [9]

Magyarországon a 2112/2004. (V.7.) kormány határozat a következő területeket sorolja a kritikus infrastruktúrák közé:

- az energiaellátás;
- a közművesítés;
- a közlekedés és szállítás;
- a távközlés, elektronikus adatforgalom és informatikai hálózat;
- a bankrendszer; a szolgáltatások;
- a média;
- az ivóvíz és élelmiszer alapellátás;
- az egészségügyi biztosítás. [10]

Látható, hogy az Európai Uniós állásfoglalás szerteágazóbb, és több infrastruktúrát sorol kritikus státuszba mint a hazai.

Véleményem szerint az Európai Uniós állásfoglalás a kritikus infrastruktúrákról, és ezen infrastruktúrák besorolása tükrözi az Uniós normákat. Hazánkban a jogalkotók nem sorolták a

kritikus infrastruktúrák közé például a veszélyes áruk tárolását és szállítását. A veszélyes anyagok egyre nagyobb mennyiségben keletkeznek valamilyen más termék melléktermékeként. Tárolásuk, szállításuk és megsemmisítésük egyre nagyobb kihívást jelent a hazánknak.

## KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA FOGALMA

Az, hogy mit tekintünk kritikus információs infrastruktúrának, a kritikus infrastruktúrák védelmére vonatkozó európai programról szóló zöld könyv a következőképpen fogalmazza meg: "Kritikus információs infrastruktúrák közé azok sorolandók, melyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, Internet, műholdak stb.)". [8]

Szinte minden fajta kritikus infrastruktúrát különböző szintű és rendeltetésű infokommunikációs rendszerek vezérelnek, irányítanak és ellenőriznek. Így tehát egy ország információtechnológiára alapozott infrastruktúrája joggal nevezhető a társadalom idegrendszerének, és ennek következtében az információs infrastruktúrák, illetve azok részei is a kritikus infrastruktúrák közé sorolandók. E megállapítás szerint, pl. egy ország nyilvános mobil távközlő hálózatai, mint önmagukban is kritikus infrastruktúrák, egyben kritikus információs infrastruktúráknak is minősülnek, illetve pl. az energiaellátó rendszert irányító, vezérlő számítógép-hálózat is ez utóbbiak közé sorolandó. [6]

Rendeltetés szerint az információs infrastruktúrákat két csoportba sorolhatjuk:

- funkcionális információs infrastruktúra;
- támogató információs infrastruktúra.

A funkcionális infrastruktúrák fizikailag lehetővé teszik a társadalom valamilyen információs funkciójának zavartalan működését, vagyis infrastrukturális alapon információs alapszolgáltatásokat végeznek.

A támogató információs infrastruktúrák létrehozzák, és folyamatosan biztosítják a funkcionális információs infrastruktúrák nagy halmazainak zavartalan működéséhez és fejlődéséhez szükséges anyagi és szellemi alapokat, valamint támogatási háttereket. [11]

A funkcionális információs infrastruktúrák egyféle megközelítésből a következőek lehetnek:

- légi forgalmat, repülésirányítást és légi navigációt biztosító rendszerek;
- távirányító és robotok vezérlését biztosító rendszerek;
- légvédelmi fegyverirányítást biztosító rendszerek;
- zárt távközlési különhálózatok;
- műsorszóró és tájékoztató hálózatok;
- vezetési rendszerek;
- informatikai hálózatok;
- távérzékelést, távellenőrzést biztosító rendszerek;
- nyílt előfizetői távközlési hálózatok.[13]

A funkcionális információs infrastruktúrák a különböző infokommunikációs rendszerek köré csoportosíthatók:

- Számítógép-hálózatok (LAN, MAN, WAN, WWW)

- Vezetékes távközlő rendszerek (analóg, ISDN)
- Vezeték nélküli távközlő rendszerek
  - Mobil cellás rádiótelefon rendszerek (GSM)
  - Diszpécser Földi Mobil Hálózatok (TETRA)
  - Személyhívó rendszerek
  - Műholdas távközlési rendszerek
- Műholdas navigációs rendszerek (GPS), stb.[13]

A támogató információs infrastruktúrák pedig a következők:

- elektronikai és informatikai vállalatok;
- raktárak, nagykereskedelmi ellátó vállalatok;
- elektronikai és informatikai képzéssel foglalkozó tanintézetek;
- villamos energetikai ellátó rendszerek;
- elektronikai és informatikai kutató és fejlesztő intézetek.[3]

A fent említett infrastruktúrák egymással valamilyen szinten kapcsolatban vannak, de egyéb szolgáltatásaikat csak különböző korlátozásokkal bocsátják a felhasználók rendelkezésére. Például egy tartalomszolgáltató vagy egy hálózat-rész lehet egy kisebb információs infrastruktúra része úgy, hogy ugyanakkor nem része egy kapcsolódó nagyobb infrastruktúrának.

Az összekapcsolt információs infrastruktúrákat kiterjedésük szerint a következőképpen csoportosíthatjuk:

- globális (világméretű);
- regionális (pl. európai);
- nemzeti (országos). [13]

A globális információs infrastruktúra fogalmát a következőképpen fogalmazták meg:
„A globális információs infrastruktúra összekapcsolt információs rendszerek és az őket összekapcsoló rendszerek világméretű összessége.”
„A globális információs infrastruktúra kommunikációs hálózatok, számítógépek, adatbázisok és felhasználói elektronika világméretű összekapcsolódása, amely óriási mennyiségű információt tesz hozzáférhetővé a felhasználók számára.”
„A globális információs infrastruktúra a következő hat elemet foglalja magában: kommunikációs infrastruktúra; számítógépek és berendezések; szoftverek és alkalmazások; az információtartalom; az infrastruktúra összetevőit fejlesztő, gyártó, forgalmazó és szervizelő személyek és szervezetek; valamint az infrastruktúrát használó személyek és szervezetek.” [11]

A fenti fogalmakból látszik, hogy megfogalmazóik inkább az alkotó elemeket tartották fontosnak és nem az infrastruktúrát magát.

Véleményem szerint a globális információs infrastruktúrák lehetővé teszik, hogy bárki bárhonnan kommunikálni tudjon vezetékes, mobil, vagy műholdas hálózatokon.

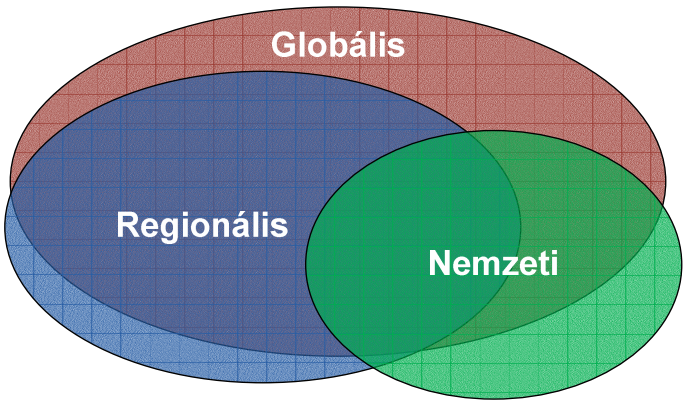
A regionális információs infrastruktúrák a globális információs infrastruktúrák szerves részei. A világot átszövő információs infrastruktúrák régiókra bonthatók, amelyek lehetnek például a kontinensek, vagy valamilyen szövetség által meghúzott határvonalak (pl. EU).

A nemzeti információs infrastruktúra fogalmát a következőképpen fogalmazták meg:
„A nemzeti információs infrastruktúra kommunikációs hálózatok, számítógépek, adatbázisok és felhasználói elektronika nemzeti szintű összekapcsolódása, amely óriási mennyiségű információt tesz hozzáférhetővé a felhasználók számára.”
„A nemzeti információs infrastruktúra szervezetek, eszközök és erőforrások széles körben hozzáférhető, egységes rendszere, amelynek rendeltetése elsősorban egy
adott nemzet kormányzati, gazdálkodó és más szervezetei, valamint állampolgárai alapvető információ- és információs szolgáltatás-igényeinek elsősorban az adott ország területén történő kielégítése. „ [11]

Ezek alapján a nemzeti információs infrastruktúrák tekinthetőek a világot átszövő hálózat legkisebb alkotóelemeinek, amelyek nélkül nem valósulhatna meg kommunikáció.

Ezen infrastruktúrák nagy hányadának nem az állam a tulajdonosa. Ez nem azt jelenti, hogy az állam nem fordít figyelmet ezen infrastruktúrák védelmére, hanem azt, hogy a védelmet közösen valósítják meg.

Az összekapcsolt infrastruktúrák kapcsolatát és egymástól való függőségét az 1. ábra mutatja be.




**1. ábra:** Összekapcsolt információs infrastruktúrák egymásra hatása kiterjedésük szerint

Az ábrából jól látszik, hogy egy nemzeti információs infrastruktúra lehet regionális és globális is, de vannak a csoportoknak olyan szereplői, amelyek csak az egyik csoportba tartoznak, de az is jól látszik, hogy az információs infrastruktúrák jól egymásra épülnek és csak kis szegmensei különülnek el egymástól. Például egy távközlési vállalat kommunikációs szolgáltatásainak fennakadása alapvetően nemzeti probléma, de ha ez kihatással van a környező országokra, akkor már regionális, amely továbbgyűrűzve globális méreteket is ölthet. A közelmúltban, Németországban egy építkezésen átvágtak egy fontos telekommunikációs vezetéket, amely lavinaszerűen először az országban, majd a kontinensen, később globálisan okozott fennakadást a telefon összekötetésekben.

A fent említett kommunikációs hálózatokat a következőképpen csoportosíthatjuk:

- magáncélú;
- zártcélú;
- különcélú;
- közcélú. [14]

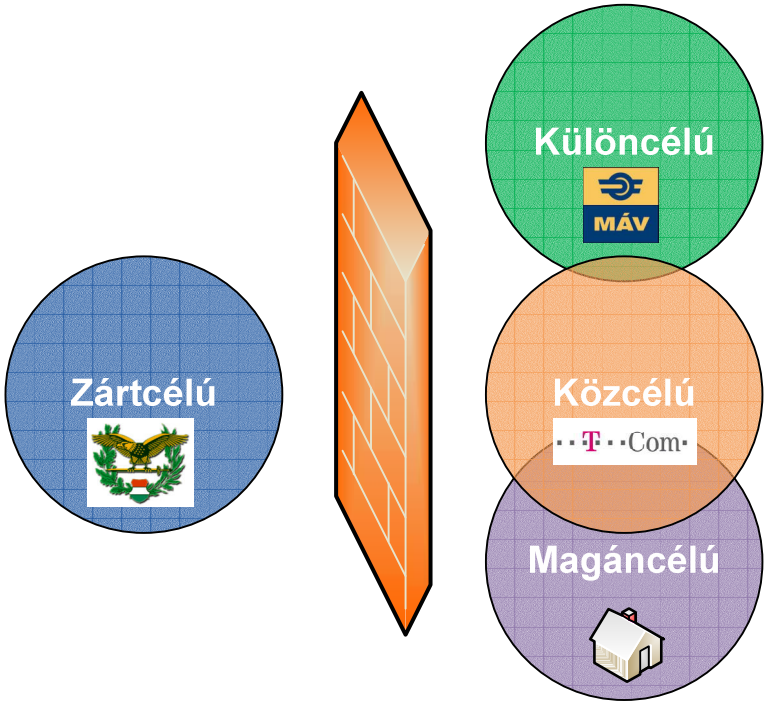
Magáncélú hálózat egyéni vagy valamilyen csoportos használatra készül. Szervesen kapcsolódik a közcélú hálózathoz.

Zártcélú kommunikációs hálózatokat államigazgatási szervezetek használják. Ide sorolhatóak a fegyveres testületek, kormányszervek, közigazgatási szervek.

A különcélú kommunikációs hálózatokat zárt érdekcsoportok használják meghatározott területen.

Közcélú kommunikációs hálózatok közhasználati célúak, nyilvános és nem nyilvános vezetékes és mobil rendszerek alkotják.

A hálózatok kapcsolatait a 2.ábra mutatja be.




**2. ábra:** Magáncélú, zártcélú, különcélú és közcélú kommunikációs hálózatok kapcsolata

Az ábrán jól látszik, hogy a zárt kommunikációs hálózatok minden esetben különálló hálózatok. Zártságuk megőrzése fontos szempont. A többi hálózattípusra is jellemző, hogy egymással való kapcsolataik szigorúan szabályozottak. Ezek a szabályok szavatolják az információs infrastruktúrák zavartalan működését.

## ÖSSZEGZÉS

Az Európai Unióban és ezen belül hazánkban nincs egységes dokumentum, amely megfogalmazná, hogy mi is az a kritikus infrastruktúra, s azon belül mi minősül európai kritikus infrastruktúrának. [5] A kritikus információs infrastruktúra helyzete sem egyértelmű.

Hazánkban ezen infrastruktúrák tulajdonjogát nem az állam gyakorolja, ezért az állami és a gazdasági élet vezetőinek konszenzusra kell törekedni a biztonság fokozása érdekében.

E rendszerek rendkívüli mértékben sebezhetők, és ezért ezek védelme, biztonságának szavatolása, nemzeti, kormányzati feladat mely adott esetekben nemzetközi koordinációt is feltételez.

## Felhasznált irodalom


[1] Magyar Értelmező Kéziszótár, Akadémiai Kiadó, Budapest, 1978./2003., 609 p.

[2] Magyar Larousse Enciklopédikus szótár, Akadémiai Kiadó, Budapest, 1992.

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

[4] Critical Foundations Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Washington, 1997. október

[5] Précsényi Zoltán - Solymosi József: *Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé*, Hadmérnök II. Évfolyam 1. szám - 2007. március,
elérhető: http://w3.zmne.hu/hadmernok/archivum/2007/1/2007_1_precsenyi.html
2007.08.27.

[6] Muha Lajos: *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme*, Doktori értekezés 21.oldal, Budapest 2007.

[7] Haig Zsolt: *Az információs társadalmat fenyegető információalapú veszélyforrások*, Hadtudomány, XVII. Évfolyam 3. szám, 2007. szeptember
elérhető: http://www.zmne.hu/kulso/mhtt/hadtudomany/2007_3_4.html
2008.01.10.

[8] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. 2001.09.26

[9] Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final

[10] Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the Fight Against Terrorism. Brussels, 20.10. 2004 COM(2004) 702 final

[11] Munk Sándor: *Információs színtér, információs környezet, információs infrastruktúra*, A Zrínyi Miklós Nemzetvédelmi Egyetem Tudományos Lapja ISSN 1417-7323
elérhető: http://www.zmne.hu/tanszekek/kvt/digitgy/20022/vszt/munk.html
2008.01.10

[12] 2112/2004. (V. 7.) Kormány határozat a terrorizmus elleni küzdelem aktuális feladatairól

[13] Haig Zsolt: *Kritikus információs infrastruktúrák védelme az információs terrorizmus tükrében I.,* ITTK-Szakmai Klub 2007. 02. 15.
elérhető: www.ittk.hu/web/docs/klub/HaigZs_ITTKKlub53.ppt
2008.01.10

[14] Budai Balázs Benjámin: *M-kormányzat Technológiai meghatározók*,
elérhető: www.m-government.hu/m-gov%20techno.ppt
2008.05.28.

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Horváth Zita**
Zrínyi Miklós Nemzetvédelmi Egyetem

# A MINŐSÍTETT IDŐSZAKOK SZABÁLYOZÁSÁNAK RENDSZERE, TARTALMA

## Bevezetés

Az Alkotmány meghatározza a minősített időszakokat, bevezetésük (kihirdetésük) feltételeit, és az egyes időszakok tartalmát.

Minősített időszakban megváltoznak a normál időszaki jogok és kötelezettségek, a békeidőszaki működéshez képest szigorításokat jelentő, úgynevezett rendkívüli intézkedések bevezetése alkotmányos garanciális szabályokhoz kötött.

A minősített időszakok alatt 2004. december 31-ig a Rendkívüli állapotot, a Szükségállapotot, a Veszélyhelyzetet és az Alkotmány 19/E. § szerinti helyzetet értettük. 2005. január 1-el változott a helyzet, az önkéntes haderőre történt áttérés, a hadkötelezettség békeidőszaki megszüntetése kapcsán, a 2004. évi CIV. törvénnyel módosításra került az Alkotmány, és egy új minősített időszak, a Megelőző védelmi helyzet került beemelésre a szabályozási rendszerbe.

## A Rendkívüli állapot

Az Alkotmány 19.§ (3) bekezdés h. pontja szerint az Országgyűlés "…hadiállapot, vagy idegen hatalom fegyveres támadásának közvetlen veszélye (háborús veszély) esetén kihirdeti a rendkívüli állapotot, és Honvédelmi Tanácsot hoz létre".

Rendkívüli állapot kihirdetésére az ország függetlenségét, vagy területi épségét közvetlenül veszélyeztető idegen (külső) hatalom erőszakos fellépése esetén kerülhet sor, annak nem feltétele a konkrét harctevékenység megindulása, elegendő jogalapot teremt a fegyveres államközi konfliktus veszélye vagy a hadiállapot deklarálása.

A rendkívüli állapot kihirdetésére, a hadiállapot kinyilvánítására és a Honvédelmi Tanács létrehozására az Országgyűlés, akadályoztatása esetén a köztársasági elnök jogosult. Az Országgyűlés akkor tekinthető akadályoztatottnak, ha nem ülésezik és összehívása az idő rövidsége, továbbá a hadiállapotot, a rendkívüli állapotot vagy a szükségállapotot kiváltó események miatt elháríthatatlan akadályba ütközik. Az akadályoztatás tényét, a kihirdetés indokoltságát az Országgyűlés elnöke, az Alkotmánybíróság elnöke és a miniszterelnök együttesen állapítják meg.

## A szükségállapot

Az Alkotmány 19. § (3) bekezdés i) pontja alapján az Országgyűlés (akadályoztatása esetén a köztársasági elnök) "az alkotmányos rend megdöntésére, vagy a hatalom kizárólagos megszerzésére irányuló fegyveres cselekmények, továbbá az élet- és vagyonbiztonságot tömeges méretekben veszélyeztető, fegyveresen vagy felfegyverkezve elkövetett súlyos erőszakos cselekmények, elemi csapás vagy ipari szerencsétlenség esetén (a továbbiakban együtt: szükséghelyzet) szükségállapotot hirdet ki."

A szükségállapot kihirdetésére három eltérő tartalmú és eltérő intézkedéseket követelő körülmény esetén, vagyis a legális hatalom megdöntésére irányuló belső fegyveres cselekmények (polgárháborús körülmények), vagy a belbiztonságot jelentősen veszélyeztető fegyveres vagy felfegyverkezve elkövetett erőszakos cselekmények, illetve egyéb súlyos, a veszélyhelyzetnél nagyobb kihatású, az állampolgárok élet- és vagyonbiztonságát tömeges méretekben veszélyeztető események, elemi csapás, katasztrófa bekövetkezése esetén kerülhet sor.

A szükségállapot kihirdetésére a rendkívüli állapotnál leírt szabályok vonatkoznak, azzal az eltéréssel, hogy egyrészt az Országgyűlés és a Kormány eredeti jog- és hatáskörében működik (az Országgyűlés - akadályoztatása estén a Honvédelmi Bizottság - folyamatosan ülésezik), másrészt a köztársasági elnök szükségállapotban nem alkothat előre meg nem határozott tartalmú rendkívüli intézkedéseket, hanem csak a külön törvényben meghatározott rendkívüli intézkedéseket vezetheti be, köztársasági elnöki rendelet formájában, melyről tájékoztatja az Országgyűlés elnökét.

Kihirdetett szükségállapot esetén a Honvédség alkalmazásának alkotmányos feltétele, hogy a bekövetkezett erőszakos cselekmények kezelésére a rendőrség alkalmazása ne legyen elegendő.

## A veszélyhelyzet

Az Alkotmány 35. § (1) bekezdés i) pontja alapján a Kormány „az élet- és vagyonbiztonságot veszélyeztető elemi csapás, illetőleg következményeinek az elhárítása (a továbbiakban: veszélyhelyzet), valamint a közrend és közbiztonság védelme érdekében megteszi a szükséges intézkedéseket; "

Veszélyhelyzet kihirdetésére akkor kerülhet sor, ha az élet- és vagyonbiztonságot veszélyeztető elemi csapás bekövetkezése, illetve az elemi csapás következményeinek elhárítása azt kívánja, hogy a Kormány különleges felhatalmazást kapjon a veszélyt előidéző okok megszüntetésére, következményeinek felszámolására.

A veszélyhelyzet tényállásának megállapítása, a szükséges intézkedések megtétele, az elrendelt rendszabályok bevezetésének és végrehajtásának irányítása egyaránt a Kormány kompetenciája. A veszélyhelyzetben tett intézkedéseiről a Kormány köteles tájékoztatni az Országgyűlést.

## Az Alkotmány 19/E. § szerinti időszak

Az Alkotmány 19/E. § (1) bekezdése alapján "Külső fegyveres csoportoknak Magyarország területére történő váratlan betörése esetén a támadás elhárítására, illetőleg az ország területének a honi és szövetséges légvédelmi és repülő készültségi erőkkel való oltalmazására, az alkotmányos rend, az élet- és vagyonbiztonság, a közrend és a közbiztonság védelme érdekében a Kormány a köztársasági elnök által jóváhagyott védelmi terv szerint - a

támadással arányos és erre felkészített erőkkel - a szükségállapot vagy a rendkívüli állapot kihirdetésére vonatkozó döntésig azonnal intézkedni köteles."

Ennek a máig nem nevesített minősített időszaknak a kihirdetésére külső, nem állami erő (idegen hatalom) fegyveres támadása esetében lehet szükség, amikor a Kormány hatáskörébe tartozó olyan „azonnali sürgősségű" intézkedések foganatosítására van szükség, amelyek segítségével megakadályozhatóak a nem kívánt események, illetve biztosítják a Kormány számára az időt és a cselekvési szabadságot.

A Kormány köteles a hatáskörében bevezetett intézkedésekről tájékoztatni az Országgyűlést, illetve a köztársasági elnököt, és előterjeszteni javaslatait a további intézkedések megtételére.

## A Megelőző védelmi helyzet

Az Alkotmány 19. § (3) n) pontja alapján (E jogkörében az Országgyűlés) „külső fegyveres támadás veszélye esetén vagy szövetségi kötelezettség teljesítése érdekében meghatározott időre kihirdeti (meghosszabbítja) a megelőző védelmi helyzetet, és felhatalmazza a Kormányt a szükséges intézkedések megtételére."

A hadkötelezettség békeidőszaki megszüntetése miatt elfogadott új minősített időszaknak, az Országgyűlés minősített többséggel történő kihirdetésére vagy korábbi elrendelés esetén annak fenntartására külső fegyveres támadás közvetlennek nem minősíthető veszélye esetén vagy szövetségi kötelezettség teljesítése érdekében kerülhet sor. Az Országgyűlés az erről szóló döntés meghozatalakor szabadon határozza meg a minősített időszak időtartamát, egyidejűleg a veszély elhárításához vagy a szövetségi kötelezettség teljesítéséhez szükséges intézkedések megtételére hatalmazza fel a Kormányt.

A megelőző védelmi helyzet a békeidőszaki rendhez képest magasabb fokú védelmi készültséget jelent, azonban nem ad módot az alapvető jogoknak az Alkotmány 8. § (4) bekezdése szerinti felfüggesztésére.

Fentiekhez kapcsolódóan az Alkotmány 35. § (1) bekezdése új m) ponttal egészült ki:

(A Kormány) „a megelőző védelmi helyzet kihirdetésének kezdeményezését követően a közigazgatás, a Magyar Honvédség és a rendvédelmi szervek működését érintő törvényektől eltérő intézkedéseket vezethet be; az így bevezetett intézkedések hatálya az Országgyűlés döntéséig, de legfeljebb 60 napig tart, azokról a Kormány a köztársasági elnököt és az Országgyűlés illetékes bizottságait folyamatosan tájékoztatja."

A megelőző védelmi helyzetre okot adó körülmény felmerülését követően a minősített időszak kihirdetésére irányuló kormányzati kezdeményezés és az arról szóló országgyűlési döntés közötti időszakban is biztosítani szükséges annak lehetőségét, hogy a Kormány megindítsa a felkészülést, amely a magasabb védelmi szint tényleges eléréséhez vezet a közigazgatás, a Magyar Honvédség és a rendvédelmi szervek működésében.

Ilyen előzetes intézkedések biztosíthatják, hogy a megelőző védelmi helyzetben a hadkötelezettség azonnali elrendeléséhez szükséges intézményi feltételek megfelelő időben megteremthetőek legyenek. Az Alkotmány ezért felhatalmazást ad a Kormány számára, hogy a megelőző védelmi helyzet feltételeinek fennállása esetén, a minősített időszak kihirdetésének kezdeményezését követően az Országgyűlés döntéséig megtegye azokat az intézkedéseket, amelyek biztosítják, hogy a közigazgatás, a Magyar Honvédség és a rendvédelmi szervek késedelem nélkül elláthassák az országot fenyegető veszély vagy a szövetségesi kötelezettség teljesítése által megkívánt feladataikat.

Ezen intézkedések nem érinthetik az alapvető jogokra és kötelezettségekre vonatkozó törvényi rendelkezéseket. Az intézkedésekről a Kormány a köztársasági elnököt és az Országgyűlés illetékes bizottságait folyamatosan tájékoztatja. Garanciális jelentősége van annak, hogy az Alkotmány az Országgyűlés döntésének időpontjától függetlenül legfeljebb hatvan napban határozza meg a Kormány ezen intézkedéseinek időbeli hatályát.

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Koronváry Péter**
Zrínyi Miklós Nemzetvédelmi Egyetem
koronvary.peter@zmne.hu

# GONDOLATOK A VEZETÉSTUDOMÁNY FELADATÁRÓL

A vezetéstudomány – társadalomtudomány, a szociológia, a szociálpszichológia, a pszichológia, a közgazdaságtan, a politológia, a történettudományok, a hadtudomány, stb. társtudománya. Módszereit, szemléletmódját, rendezőelveit részben ezektől lesi el, részben saját maga alakítja ki a társadalomkutatás normáinak, logikai, episztemológiai, filozófiai hátterének megfelelően.

A vezetés, mióta írás létezik, az írástudók egyik legfőbb témája. A kínai klasszikus filozófia (pl. **Konfuciusz**[1], **Lao-ce**), a görög filozófusok, történetírók munkái (pl. **Hérodotosz**[2], **Platón**[3], **Arisztotelész**[4], stb.), a római kor irodalma (pl. **Cicero**[5] munkássága) éppúgy tartalmaznak jelentős felismeréseket a vezető társadalmi szerepéről és a vezetés gyakorlatáról, mint az óegyiptomi intelmek (pl. **Dzsedefré**[6] fáraó vagy **Ptahhotep**[7] vezír intelmei), a sumer-akkád bölcseletirodalom (pl. a **Gilgames**-eposz[8]) vagy a **Bhaghavad-Gítá**[9], sőt a **Biblia** egyes részletei[10]. Az államvezetéstől a hadvezetésig (pl. **Szun-ce**[11]) az adott kor és társadalom igényeiről próbálják ezek a művek tájékoztatni a korszak, illetve felkészíteni feladatukra a jövő vezetőit.

[1] A klasszikus kínai filozófia remekeinek legjobb magyar fordítása: Tőkei Ferenc, *Kínai filozófia; Ókor I-III.* (Magiszter Társadalomtudományi Alapítvány, 2005).
[2] Hérodotosz, *A görög-perzsa háború* (Osiris, 2004)
[3] *Platón összes művei I-III*. (Európa Könyvkiadó, 1984)
[4] Ld. pl.: Arisztotelész, *Politika* (Gondolat Könyvkiadó, 1984).
[5] Ld. pl.: Cicero, *Az állam* (Akadémiai Kiadó, 1995)
[6] Az óegyiptomi bölcsességirodalomhoz ld.: Helmut Brunner, *Die Weisheitsbücher der Ägypter* (Artemis Verlag, 1991)
[7] Az előbbi mellett ld.: Wessetzky Vilmos, „Egyiptomi kultúra – egyiptomi bölcselet Ptahhotep tanításában" *Valóság*, XXXI. évf. 3. szám, 1988. március 22. 82-94. oldal.
[8] A sumer forrásokhoz ld. pl.: Komoróczy Géza, „Fénylő ölednek édes örömében …"; A sumer irodalom kistükre (Európa Könyvkiadó, 1970)
[9] Ld. pl.: Baktay Ervin (ford.), *Bhagavad Gítá; A Magasztos szózata* (Filosz Kiadó, 2008)
[10] Saul, Dávid és Salamon történetein keresztül pl. jól megvilágítható volt a pogány zsarnok, a keresztény király és a krisztusi birodalmat építő császár közötti különbség.
[11] Ld. pl. Szun-ce, *A hadviselés törvényei* (Balassi Kiadó, 1998)

Az ókori írások többnyire igen praktikusak – akár *etikai alapon* kritizálják koruk vezetőit, hogy helyes cselekedetekre sarkallják őket, mint a *konfuciánusok* (amiért nemegyszer saját könyveiken égették meg őket), akár szintén példamutatással, de a fölösleges beavatkozás elkerülésével próbálkozó *taoisták*, akár a pragmatikus szakkönyveket író *legisták*[12]. Akár a görög hadvezér és államférfi **Xenophón**[13], akár a római történetíró **Livius**[14], akár a machiavellista **III. Heti** fáraó írásait böngésszük, mindenhol a *gyakorlati célok elérését* próbálják meg ezek a művek segíteni – a *jobb*, *hatékonyabb*, *sikeresebb*, *eredményesebb* vezetői munkát. A céljuk jobb vezetés – nem csoda, hogy mind Konfuciusz, mind a görög filozófusok legnagyobbjai iskolaalapítóként és/vagy magántanári, illetve tanácsadói minőségben sokat tettek koruk vezetőinek segítéséért, illetve a következő vezetőnemzedék megfelelő kiképzéséért. *Az ő „vezetéstudományuk", filozófiájuk társadalmi feladata – és ezáltal lényege – a szervezet (állam, hadsereg, mezőgazdasági termelőegységek, stb.) vezetésének, a rendelkezésre álló vezetési tudásnak és képességeknek javítása generációról generációra.*

A középkorban a kereszténység terjesztői állam-és vezetéselméletet is terjesztettek *az ótestamentumi történetek példái*val a megkeresztelt germán királyok között. Vezetői mintákat adtak a *krónikák* és *geszták*, a nagy királyok, szent uralkodók életrajzai is (pl. **Nagy Károly** két vitaja[15], **Szt. István** legendái), gyakorlati tanácsokat az *intelmek* és *királytükrök* – pl. *István király intelmei Imre herceghez*[16], vagy a *18. századi tatár királytükör*[17], ahol **Dzsingisz** kán a jó, **Timur Lenk** pedig a rossz uralkodó archetípusaként jelenik meg.

A vallásos irodalom vezetőképének egyre kevesebb köze volt a gyakorlathoz, a valósághoz. A gótika lovagkirályaitól a barokk többet imádkozó, mint kormányzó „eszményéig" – mely azonban (szerencsére) többnyire csak egyes legendákban létezett – vezető út az uralkodói ideált kopott térdű, sápatag, a női nemre nem néző, a gyóntatóatyja által könnyen irányított trottlivá silányította (ld. Szt. Imre késői legendája). Ezek a minták inkább az egyház által irányítható, semmint az egyéni döntéseket hozni képes vezetőt állítják elénk.

A valóságérzéket egyre inkább mellőző katolikus vezetői és állameszmény-képek kritikáival léptek fel katolikus egyházi szerzők (**Thomas More**[18], **Tommaso Campanella**[19]), reneszánsz világiak (**Machiavelli**[20], **Francis Bacon**[21]), és reformátusok (**Erasmus**[22]), sőt vallásreformátorok is (pl. **Luther**[23]) az újkor hajnalán. Ekkor alakultak ki a vezetőképzés egyre modernebb formái is – az egyházi és világi vezetés alapjául szolgáló jogi képzés mellett megjelennek a

[12] A kínai filozófia klasszikus iskoláihoz remek bevezető Fung Yu-lan, *A kínai filozófia rövid története* (Osiris, 2003).
[13] Ld. *Xenophón történeti munkái* (Osiris, 2001) és *Xenophón filozófiai és egyéb írásai* (Osiris, 2003).
[14] Titus Livius, *A római nép története a város alapításától I-IV.* (Európa Könyvkiadó, 1982)
[15] Einhard and Notker the Stammerer, *Two Lives of Charlemagne* (Penguin, 1969)
[16] István legendái és intelmei egy kötetben: Tormay Cecilia (ford.), *Magyar Legendarium* (Móra Ferenc Könyvkiadó, 1993; reprint)
[17] Ivanics Mária, „Nomád királytükör *A Dzsingisz-legenda könyvé*ben" in: Felföldi Szabolcs, Sinkovics Balázs (szerkk.), *Nomád népvándorlások, magyar honfoglalás* (Balassi Kiadó, 2001), 161-172. o.
[18] Thomas More, *Utopia* (Penguin, 1965)
[19] Tommaso Campanella, *A Napváros* (Lazi Bt., 2002)
[20] Niccolo Machiavelli, *A fejedelem* (Kossuth Könyvkiadó, 1991)
[21] Francis Bacon, *Esszék* (Európa Könyvkiadó, 1968)
[22] Rotterdami Erasmus, *A balgaság dicsérete* (Európa Könyvkiadó, 1994)
[23] Martin Luther, *Asztali beszélgetések* (Helikon, 1983)

kor legveszélyesebb ágazata számára vezetőket képző intézményrendszerek (a portugál **Tengerész Henrik** próbálkozása után **VIII. Henrik** angol király hajóskapitány-és navigátorképző rendszere a *Trinity Hall* felügyelete alatt, illetve a francia, bajor, szász, porosz stb. *tisztképző akadémiák*). A jó vezető egyre inkább az, aki – akár törvény, hatalom, vallás, sőt isten ellenében – bizonyos tudás és képességek, valamint kapcsolatok (és szerencse) birtokában – döntéseket hoz, túléli azokat, sőt, emellett a kasszája is telik, vagyis: sikeres (ld. **Erzsébet** királynő angliai kultuszától kezdve az *Onedin család*ig[24] és a *Ságun*ig[25]).

A modern közgazdaságtani elmélet *Adam Smith* nevéhez fűződő kezdetei (*The Wealth of Nations*, 1776[26]) után Angliában egyenes út vezetett az ipari forradalom kora kulcsszervezeteinek, a gyáraknak a vizsgálatához (**Charles Babbage**, *On the Economy of Machinery and Manufactures*, 1932[27]; **Andrew Ure**, *The Philosophy of Manufactures*, 1835[28]). A 19. században kialakul a mérnökképzés modern főiskolai-egyetemi rendszere is, képzett irányítókat adva az egyre szaporodó gyáraknak. A mérnökök vezetési szemlélete – szakmai kultúrájuk szempontrendszeréből adódóan – elsősorban a munkafolyamatok, elsősorban a termelés megszervezését helyezte előtérbe. Az irányítási kérdéseket is tkp. az anyagi folyamatok szabályozásának mintájára próbálták megoldani. Ugyanez figyelhető meg a korabeli németországi üzemszervezési és -vezetési irodalomban, ahol az irodai adminisztráció formalizálásának kialakuló szabályai egyre „üzemszerűbbé" tették a hivatalnoki tevékenységeket is.

Ennek a voltaképpen az Adam Smith-féle *specializáció elv*ére visszavezethető, a mérnöki gondolkodást átható gondolatnak – a formalizáció és standardizálás általi költséghatékonysági szemléletnek – az összefoglalását és minőségileg is új szintre emelését hozza az első valódi menedzsment-teoretikus: **Frederick Winslow Taylor** munkássága[29].

Taylor számára a menedzser munkájának lényege a költséghatékony termelés biztosítása. Tanai, amelyek „tudományos vezetés" (*scientific management*) néven váltak ismertté, a „mérnöki hagyomány" talaján állva vallotta, hogy **a menedzser feladata a (termelési) folyamatok hatékonyságának biztosítása, amit ezek tudományos módszerekkel való elemzésével és optimalizálásával lehet elérni**. Ha az optimális munkafolyamatot az optimális adottságokkal és felkészültséggel rendelkező munkás az optimális szerszámokkal végzi – amihez persze biztosítani kell együttműködését (később ezt nevezték motivációnak), valamint hogy mindenki (menedzser és dolgozó egyaránt) tisztában legyen a maga felelősségével –, akkor a vezetés sikerrel teljesítette feladatát. A menedzser már nem példakép, mint a konfuciánus vagy taoista filozófia vezetője, nem is a személyiség fejlődésének egy bizonyos szakaszán álló ember, mint pl. Platónnál, hanem *felelős alkalmazott* – csak nem fizikai munkára, hanem *a munkafolyamatok tudományos tervezésére, a munkások szakszerű kiképzésére, a megfelelő munkaeszközök és körülmények kialakítására és biztosítására, valamint munkakapcsolatok és hatáskö-*

[24] Cyril Abraham, *The Onedin Line* (Tandem, 1972)
[25] James Clavell, *Ságun* (Európa, 1987)
[26] http://www.gutenberg.org/etext/3300
[27] http://www.gutenberg.org/etext/4238
[28] Kiadta: Lenox Hill Publishers, 1969 (3. kiadás)
[29] Ld. pl.: *The Principles of Scientific Management*: http://www.gutenberg.org/etext/6435 és *Shop Management*: http://www.gutenberg.org/etext/6464 Magyarul: Frederick Winslow Taylor, *Üzemvezetés; A tudományos vezetés alapjai* (KJK, 1983)

*rök kiépítésére és hatékony működtetésére* alkalmazott vezető. A vállalat számukra rendszer – hasonlatos azokhoz a gépi rendszerekhez, amelyek körében egy mérnök olyan otthonosan mozog.

Európában a francia **Henri Fayol**[30] más úton indult el. Rá – mint ahogy a francia középburzsoáziára általában – hatott a korabeli francia *gloire* és a tisztikar vezetőideálja is. A menedzser az ő gondolkodásában nem egyszerűen a termelési folyamat, de minden szervezeti folyamat szakszerű irányításáért felel. A folyamatok irányítása (fr. *administration*) ugyanúgy zajlik minden vállalati tevékenységkör („*funkció*") esetében – a gyártásban éppúgy, mint a kereskedelemben, a biztonsági vagy a könyvelési részlegnél, vagy akár a pénzügyinél egyaránt *tervezni* és *előre jelezni*, *szervezni*, *irányítani* (*commander*), *összehangolni* és *ellenőrizni* kell a folyamatokat. Ezért szerinte a szervezet szakmai funkciói mellé fel kell venni egy „általános" vezetési funkciót is, amely azonban nem mellettük elkülönülve, hanem azokat áthatva, bennük folyamatosan működik. Ezért nevezik őt és későbbi követőit „általános vezetési iskolának" (*general management school*). A funkciók összehangolásáért a szervezetkormányzás (*gouvernement*) a felelős.

Fayol vezetési elvei jól mutatják, hogy a vezető – legyen szó az egész vállalatot, vagy annak egy részét igazgató menedzserről – a szervezet hatékonyságát az emberein keresztül, azok segítségével tudja elérni. Ahogy azt egy felszólalásában kifejtette: „… *a vezetés az emberekkel való bánás művészete* …". Vezetési elvei a *centralizációt* és *hatékony működés*t éppúgy szolgálják, mint a *dolgozók érdekeit*. A vezetőt teszi például felelőssé azért, hogy beosztottjai tisztességes munkáért *tisztességes bér*t kapjanak éppúgy, mint hogy a szervezetben a központosítás ne nyomhassa el az emberek *kezdeményező- és újítókészség*ét, hogy a szervezetben *méltányosan* bánjanak egymással az emberek, hogy megfelelő *testületi szellem* uralkodjék, illetve hogy *a dolgozót csak közvetlen főnöke utasíthassa*. A fayoli elvek ma is igen modernnek hatnak, még ha a centralizáció a modern, gyorsan változó világban nem is egyértelmű erény vagy előny.

Összefoglalva: Fayol szerint a vezetés az emberek és folyamatok harmonikus működtetése – egyrészt, ami az emberi oldalt illeti, „művészet", vagyis valami emberi (a latin kultúra hatására az *ars*, *artes* (f) szó és leszármazottai egyszerre jelentik a művészetet, valamint az emberekkel foglalkozó, „puha" tudományokat, mint pl. a történelem, a szociológia vagy a pszichológia), másrészt egy olyan tudományág (*discipline*), amely kutatható, törvényekkel leírható, és iskolai keretek között tanítható. Fayol volt a vezetéstudomány főiskolai-egyetemi oktatásának első apostola – fáradhatatlanul hirdette, hogy a mérnöki tudományok mellett vezetéstudományt is kellene tanulnia a mérnök-hallgatóknak. Sőt, még ennél is tovább ment – mivel, érvelése szerint, gyakorlatilag mindenki vezető vagy vezetett, hasznára lenne a fiataloknak, sőt az egész francia nemzetnek, ha már a középiskolában találkozhatnának a tanulók a vezetés tudományának egy – a korosztály számára érthetővé tett – változatával. Ezen javaslatai azonban akkor még süket fülekre találtak.

[30] Henri Fayol, *Ipari és általános vezetés* (KJK, 1984)

Fayol nyomán megfogalmazhatjuk – a vezetéstudomány, a vezetőképzés és a vezetők folyamatos fejlesztése nem csak egy-egy szervezet hatékonyságának és sikerének egyik legfontosabb kulcsa, hanem *az egész társadalom hatékony, demokratikus, sikeres működéséé*.

A taylori gondolatokat a folyamatok optimalizációjára, a kiválasztásra, valamint az ergonómiára (a munkaeszközök és munkakörülmények hatékonyságsegítő kialakítására) visszaszorító amerikai mérnöki gyakorlat korlátait mutatták ki a *Hawthorne-i kísérletek*, ahol, a Harvard Egyetem üzleti karának kutatói, jórészt professzoruk, **Elton Mayo** vezetésével, az *ipari pszichológia* akkor új tudományának segítségével igazolták, hogy a folyamatszervezés „kemény", „tudományos" eszközrendszere milyen keveset ér az „emberi oldal" szakszerű kezelése nélkül. Az „emberi kapcsolatok" iskolája jelentős eredményeket hozott – a vezetésnek a folyamatszervezés mellett ismét el kellett kezdenie foglalkoznia a folyamatokat működtető emberek egyéni, pszichés és csoportos, szociálpszichológiai igényeivel és indíttatásaival. A kísérlet-sorozat igazolta a „*feladatorientált*" vezetés gyengébb eredményességét a „*támogató*", „*emberorientált*" vezetésével szemben. Az amerikai vezetéstudományba, úgy látszott, visszakerül az „emberi oldal": elindultak az első „vezetési stílus" kísérletek (**Kurt Lewin**), az első rendszertani megközelítések (**Chester Barnard**[31]), stb. A *hatékonyságközpontú* gondolkodás megmaradt, a hatékonysághoz vezető útról azonban már nem „lökdösték le" az embereket. Sőt, nyilvánvalóvá vált: a vállalati eredményekhez az embereken, a beosztottakon keresztül vezet az út – csak velük együttműködve, nem őket legázolva lehet hatékony szervezetet építeni.

A 2. világháború folyamán *az amerikai katonai kutatások* egyrészt új statisztikai-analitikus módszerekkel gazdagították a tudományos vezetés eszköztárát, modernizálva a hadigazdaságban megújuló taylorista szemléletet, másrészt felvetett motivációs kérdéseket („hogyan lehet rávenni egy katonát arra hogy öljön?" „hogyan lehet rávenni egy tisztet arra, hogy szükség esetén a halálba küldje embereit?"), harmadrészt kialakította a hosszú távú vezetői gondolkodás keretrendszerét, a stratégiai tervezés, a stratégiai menedzsment első, a gazdasági szervezetekre később adaptálható változatát, negyedrészt szembesítette az amerikai hadvezetést azzal a kellemetlen ténnyel, hogy az elit katonai akadémiákon kiképzett, közép-és felsőosztálybeli, fehér, kék-vagy acélszürke szemű, szőkésbarna, protestáns tisztek, bármennyire remekül végezték az alaki gyakorlatokat, a fronton, tisztelet a kivételnek, nemegyszer alkalmatlanok. Ráadásul az alsóbb néposztályok fekete, olasz, spanyol, stb. származású, sokszor kétes iskolázottságú tagjai, esetenként kiemelkedően teljesítettek (ld. az első fekete vadászrepülő század történetét[32]). A gyakorlat megbuktatta a születés, az öröklött tulajdonságok, a „tenyésztett" vezető nimbuszát, és fel kellett tenni a kérdést: ha nem a gének, akkor mi teszi vezetővé az embert? Ez a valami modellezhető-e az oktatásban? Ha igen – ezek szerint bárkiből lehet vezető, ha megfelelő kiképzésben részesül. A 2. világháború, a tömeges női munkavállalás mellett, meghozta az egyenjogúság és demokrácia első fecskéit: elkezdődik a vezetés és a vezetőképzés demokratizálódása.

[31] Chester I. Barnard, *The Functions of the Executive* (Harvard College, 1938)
[32] Ld. pl.: http://www.nasm.si.edu/interact/blackwings/history/story03a.html és http://memory.loc.gov/ammem/aaohtml/exhibit/aopart8.html

A motivációs kutatások a háború után is folytatódtak – az „emberi kapcsolatok új iskolája” (*neo-human relations school*) motiváció-kutatói (pl. **Abraham Maslow**[33]) a vezetőben az emberi motivációs folyamatok alakítóját látták, a *szervezetpszichológiá*val foglalkozó társaik (pl. **Chris Argyris**) pedig olyan még ma is modern kérdéseket elemeztek, mint a szervezeti tanulás problematikája. Kutatásaik eredménye volt az a felismerés, hogy az egyéni motivációs folyamatok annyira sokfélék, sokrétűek, sokoldalúak, hogy lehetetlen a vezetőnek egyesével motiválnia a beosztottjait. A megoldás a sokféle modell együttes felhasználása egy olyan szervezet felépítésére, amely maga tömegméretekben motiválja az ott dolgozókat. A vezető fő feladata tehát a motiváló szervezetek (szervezeti egységek) kialakítása. Ez a felismerés volt az „emberi erőforrás-menedzsment” kiindulópontja, az emberközpontú szervezetépítés (**Douglas McGregor**) alapja.

Az ötvenes években immár a civil szféra igényeire szabva megindultak a vezetői stíluskutatások is. Az első kutatók (**Likert**, **Halpin** és **Winer**) és követőik lépésről lépésre tisztázták a vezetési stílus szerepét és hatását a szervezetben. A kibontakozó kép egyre megdöbbentőbb volt. Kiderült, hogy bár az emberorientált vezetés nagy általánosságban sokkal hatékonyabb, mint a feladatorientáltság, nincs „királyi út”, nincs egyedül üdvözítő módszer. A vezetőnek igazítania kell a magatartását a feladathoz éppúgy, mint az emberei képességeihez kiképzettségéhez és motiváltságához, a csoport milyenségéhez, a szervezeti kultúrához, a döntési helyzet jellemzőihez, stb. Ha ezt nem teszi, baj van – a szervezeti problémák mögött ugyanis egyre erőteljesebben rajzolódtak ki a vezetés hibái. A Pareto-arányt többen megpróbálták – többé-kevésbé sikeresen – alkalmazni a szervezeti kudarcok és a vezetési elégtelenségek viszonyára: a szervezet hibái 80%-ban visszavezethetők a vezetés hibáira. Ehhez hozzátehetjük, mintegy az érem másik oldalaként: a szervezet sikereiért 80%-ban viszont a dolgozó, az „első vonal” a felelős.

*A vezetési és szervezeti kiválóság* kutatása már egy olyan szervezetképpel dolgozik, amelyben a vezető a központi tengely – ha az elgörbül, a szervezet nem működik. A vezetői személyiség és a vezető személyiségfejlődése, majd a vezetőképzés és vezetőfejlesztés kérdései innentől kezdve alapvető fontosságúak lettek. A vezető egyre inkább felelőssé vált nem csak beosztottai fejlődéséért, hanem saját maga folyamatos, céltudatos, és hatékony fejlesztéséért is. Nem elég már a háttérben maradva menedzselnie – ki kell jönnie a falak mögül, hogy megfelelő példát mutatva ezen keresztül „állítsa be” szervezete kultúráját. Amilyen a kutya, olyan a gazdája – *amilyen a vezető, olyanok lesznek a beosztottai is*.

A vezető tevékenységének 20. századi elméleteit szociológusok (**Henry Mintzberg**[34], **Charles Handy**[35]) foglalták összefüggő rendszerbe. Ők jöttek rá arra is, hogy a főiskolák és egyetemek nem képesek megfelelő minőségű és mennyiségű vezetőt adni a modern demokratikus társadalmaknak. Az eredmény vagy a vezetőképzés átalakítása, vagy a demokrácia szűkülése lehet – amennyiben nem áll rendelkezésre elég hatékony és jól képzett vezető, a társadalmak vissza fognak térni a kevesebb vezetőt igénylő, centralizáltabb és hierarchikusabb formációkhoz. Ahhoz, hogy ezt elkerülhessük, a vezető-utánpótlás feladatát össztársadalmi

[33] Maslow, A. H. *Motivation and Personality* (Harper, 1954)
[34] Ld. pl. Henry Mintzberg et al., *The Strategy Process: Concepts, Context, Cases* (Prentice Hall, 2002)
[35] Ld. Charles Handy, *Understanding Organizations* (Penguin, 1993)

feladatnak kell tekinteni. Ebben az oktatási intézmények támogató feladatokat elláthatnak ugyan, a felelősség nagy része azonban a társadalmak más szervezeteire hárul – konkrétabban a vállalatokra, nonprofit szervezetekre, a munkahelyekre, s ezek között is a legnagyobbakra: a nemzetközi vállalatokra, a hadseregekre, és az összes nagyszervezetre, ezek ugyanis hatékonyabban képesek nagy mennyiségű vezető folyamatos, jelentős részben feladatain keresztüli fejlesztésére.

A vezetéstudomány feladatai tehát az egyes iskolák elvei szerint így összegezhetők:

1. *Klasszikus kínai filozófia* (konfucianizmus, taoizmus, legizmus):
    a. „mikro"-szint (= az egyén: „Harmónia önmagamban" – a személyiség kiteljesítésének egyik fázisa a vezetői lét, amelynek sikerei átvezetnek a teljes személyiség, a „bölcsesség" szakaszába.): **A vezetéstudomány a vezetői személyiségfejlesztést és a vezetői tudás gyarapítását szolgálja.**
    b. „mezo"-szint (= a csoport, team, csapat: „Harmónia a családomban" – a példamutatás szabályozza a vezető közvetlen környezetét.): **A vezetéstudomány elősegíti a hatékony csapatépítést.**
    c. „makro"-szint (= a szervezet: „Harmónia a fejedelemségemben"[36] – a jó példával elöljáró uralkodó országában béke, virágzás, becsületesség és a hagyományok tisztelete lesz a jellemző.): **A vezetéstudomány az ország virágzásának kulcsa.**
2. *„Tudományos" vezetés*: A vezető felelőssége tudományos eszközökkel kialakítani az optimális munkafolyamatot, kiválasztani és betanítani rá a munkást, biztosítani neki a megfelelő szerszámot és környezetet („mikro"-szint), együttműködésre késztetni, és elfogadni hogy a munkás csak a végrehajtásért felelős – minden másért a vezető. **A vezetéstudomány a vezetői felelősség beteljesítésének eszköztára** („mezo"-szint). **A cél a ráfordítások csökkentése, s ezzel a szervezeti szintű profitmaximalizálás** („makro"-szint).
3. *„Általános" vezetés*: A vezető felelőssége *saját maga megfelelő felépítése* („mikro"-szint), az *egységének igazgatása* az általános vezetési funkciók (tervezés, szervezés, irányítás, ellenőrzés) segítségével („mezo"-szint), a *szervezet működéseinek összehangolás*a az ott dolgozók megelégedésére és hatékonyságuk javára, a szervezeti centralizáció megőrzése és működtetése mellett („makro"-szint).
4. *„Emberi kapcsolatok"*: A vezető felelőssége az **emberekkel való bánás** („mikro"-szint). A vezető felelőssége az *informális csoportok* felhasználása a szervezeti célok érdekében („mezo"-szint). A vezető felelőssége a dolgozókat emberszámba vevő, „*támogató*" (*szupportív*, itt: emberközpontú) *vezetői stílus* elterjesztése a szervezetben („makro"-szint).

[36] A harmóniák koncentrikus körei a konfuciánus vezetésfilozófia alapja: „A régiek, amikor világossá akarták tenni a fényes erényt az egész égalattiban, először rendet teremtettek a fejedelemségükben. Amikor rendet akartak teremteni a fejedelemségükben, először rendbe tették családjuk ügyeit. Rendbe akarván tenni a családjuk ügyeit, először tökéletesítették saját magukat. …" *A nagy tanítás*, in: Tőkei Ferenc, *Kínai filozófia; Ókor I.*, (Magiszter Társadalomtudományi Alapítvány, 2005), 185. o. Az akkori társadalmi viszonyok között az uralkodó „családja" megfelel a fejedelemség vezető tisztségviselő körének.

5. *„Új emberi kapcsolatok”*: A vezető felelőssége *önmaga motivációinak* megismerése és felhasználása a fejlődéshez („mikro”-szint), *mások egyéni és csoportos motivációinak* feltárása és felhasználása a fejlődéshez („mezo”-szint). A vezető feladata a saját és mások hibáiból **tanulni képes, a személyiségfejlődést segítő szervezet építése** („makro”-szint).
6. *„Emberi erőforrások”*: A vezető feladata az *egyéni motivációk felderítésének és felhasználásának szabványos rendszerét kiépíteni* („mikro”-szint), csoportos tevékenységek fejlesztő hatásait kihasználni *az egyén személyiségi és szakmai fejlődésének elősegítésére*, a *szinergia* fejlesztésére („mezo”-szint), illetve **az autonóm munkavégzésre alkalmas és kész, érett, megfelelő kihívásokkal motivált személyiségekből álló szervezet** építése („makro”-szint).
7. *„Vezetőcentrikus” elméletek*: A vezető feladata *saját személyiségének, vezetési és szakmai ismereteinek* megfelelő fejlesztése („mikro”-szint), a vezetési hibák kiküszöbölése *a vezetői teamek kreatív működtetésével és a döntéskialakítás megfelelő megosztásával* („mezo”-szint) és a ***tudásalapú hálózati* működésekre épülő, *sikerorientált*, *„kiváló” szervezet* építése** („makro”-szint).

A vezetéstudomány, a vezetőképzés és -fejlesztés célja tehát (1) egyéni szinten a vezető munkájának segítése, (2) csoportszinten a szinergikus működések hatékonyság- és kreativitásnövelő, a vezetővé válást elősegítő folyamatainak megismer(tet)ése és támogatása, illetve a vezetői csoportkultúra terjesztése, (3) szervezeti szinten a versenyelőny növelése a vezéregyéniségek kifejlesztése, (4) társadalmi szinten pedig a demokrácia fennmaradási esélyeinek növelése minél több, minél jobban képzett vezető előállításával.

## További irodalom:


Bakacsi Gyula, *Szervezeti magatartás és vezetés* (KJK, 1997)

Belbin, M., *A team* (SHL Hungary 1998)

Blanchard, K., Carlos, J. P., Randolph, A., *Empowerment* (SHL Hungary Kft., 1998)

Champy, J., *A vezetés újjáalakítása* (SHL Hungary Kft, 2000)

Covey, S. R., *Principle-Centered Leadership* (Simon & Schuster, 1992)

Csepeli György, *A szervezkedő ember* (Osiris, 2001)

Huczynski, A., Buchanan, D., *Organizational and Behaviour; An Introductory Text* (2nd ed., Prentice Hall, 1991)

Kieser, A., *Szervezetelméletek* (Aula, 1995)

Klein Balázs, Klein Sándor, *A szervezet lelke* (EDGE 2000 Kiadó, 2006)

Klein Sándor et al., *Vezetés és szervezetpszichológia* (SHL Hungary Kft., 2001)

Perrow, Charles, *Szervezetszociológia* (Osiris-Századvég, Panem-McGraw-Hill, 1994)

Shein, E. H., *Organizational Culture and Leadership* (2nd ed. Jossey-Bass Publishers, 1997)

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Majer Milán hallgató**
Zrínyi Miklós Nemzetvédelmi Egyetem
mahac@freemail.hu

# A GYŐR-MOSON-SOPRON MEGYEI VÉDELMI BIZOTTSÁG TEVÉKENYSÉGE AZ ÁRVÍZ ELLENI VÉDEKEZÉSBEN

***Absztrakt***

*Alábbi cikkemben a Győr-Moson-Sopron Megyei Védelmi Bizottság tevékenységéről, illetve árvíz elleni munkájáról írok, kiemelten az elmúlt években elvégzett tevékenységéről, mely fontos és aktuális, hiszen Győrben a minden évben előforduló árvíz jelentős károkat okoz. A városvezetés azonban felismerte a védekezés fontosságát, mivel hosszú távon az árvízre történő felkészülés, és az annak elkerülésére irányuló törekvés kifizetődő. Ezáltal a kárenyhítés is egyszerűbb, és a lakosság szempontjából sem elhanyagolható dolog az, hogy a mindennapok során egyel kevesebb gond adódik, mellyel szembe kell nézniük.*

*In the following article, I show the work of the Defence Committee of Győr-Moson-Sopron County, especially its activities against floods, the work it has performed in the last few years in that area, as it is important and current since the annual floods occurring in Győr make significant damages. However, the city management has realized the importance of prevention as, in the long run, the preparations for floods and the effort to escape floods are profitable. By doing so, the damage alleviation is also easier, and it is not negligible from the point of view of local residents that they have to face fewer problems in their everyday lives.*

***Kulcsszavak:*** *árvíz, árvízvédelem, gát, gyakorlatok, kárenyhítés, újjáépítés, költségcsökkentés, városvezetés, szisztematikus tevékenység ~ flood, flood prevention, dyke, practices, damage alleviation, rebuilding, cost reduction, city management, systematic activity*

2005. Szeptember 22-én, csütörtökön a Győr-likócsi laktanya adott otthont a Győr-Moson-Sopron Megyei Védelmi Bizottság (MVB) által szervezett – „A Befogadó Nemzeti Támogatás [1] keretén belül segítségnyújtás megyei feladatait gyakorló foglalkozás”-nak.

A védelmi-igazgatási rendezvény részleteiről, a nap részletes programjáról dr. Szakács Imre, a megyei védelmi bizottság elnöke sajtótájékoztató keretében adott előzetes tájékoztatást Győrött, a Megyeházán.

A Győr-Moson-Sopron Megyei Védelmi Bizottság 2004 decemberében döntött arról, hogy – az előző, 2001-ben megtartott gyakorlás után – megyei szintű gyakorlás keretében ismét végrehajt egy gyakorlatot.

A választás a NATO tagság kötelezettségéből fakadó, a Befogadó Nemzeti Támogatás (BNT) keretén belüli segítségnyújtás témájára, illetve az ehhez kapcsolódó feladatrendszer kimunkálására esett.

A „témaválasztás" indoklása: ez a terület a Győr-Moson-Sopron Megyei Védelmi Bizottságnak is új. A gyakorlás során egy új típusú feladat, egy olyan esemény, lehetséges probléma dolgozandó fel, amellyel eddig – bár az előírt szükséges okmányokkal, tervekkel már 2004 közepe óta rendelkezett a megye – a védelmi bizottság testülete a gyakorlatban, összefüggő végrehajtási folyamat során még nem találkozott.

Az MVB 2004 évben – a tervek kidolgozása, szervezetek kialakítása, kimutatások összeállítása kapcsán – több esetben foglalkozott a Befogadó Nemzeti Támogatással, annak hátterével, megjelenésének okaival, illetve mint a bizottság előtt álló új feladattal, melynek lényege:

A Magyar Köztársaság 1999. március 12-i csatlakozását követően vált az Észak-atlanti Szerződés teljes jogú tagjává. A teljes jogú tagság egy sor olyan követelményt, kötelezettséget ró a magyar társadalom egészére, amelyek gyors, rugalmas és maradéktalan végrehajtása új kihívásként jelentkezett és jelentkezik ma is, a közigazgatás, a védelmi-igazgatás, illetve a védelem bármelyik aspektusával foglalkozó polgári köztisztviselőkre, szervezetekre.

Ahhoz, hogy a szövetségesi kötelezettségekből fakadó feladatokat Magyarország, a Magyar Honvédség, a polgári társadalom – esetünkben a Megyei Védelmi Bizottság, [2] amely a lakosság ellátásának, életének, egészségének és anyagi javainak megóvására alakult – megoldja, szükségessé vált egy új, a felsorolt feladatok mellet kialakításra kerülő feladat,- és tervrendszer kimunkálása.

Ez az új feladatrendszer a Befogadó Nemzeti Támogatás (BMT) elnevezés alatt működik. Az ezzel kapcsolatban jelentkező feladat a NATO csapatok átvonulását, ellátását, illetve az ezek során felmerülő igények kielégítésének biztosítását, tervezését jelenti megyei szinten. Hogy a bizottság a kapott feladatokat eredményesen megoldja, szükségessé vált:

1. a megyei szintű okmányok, kimutatások és munkacsoportok kialakítása, létrehozása

2. a különböző helyzetekben alkalmazható Intézkedési Terv elkészítése

3. a megyei, valamint a Honvédelmi Körzetek Képesség Listáinak összeállítása

4. és a Megyei Koordinációs Munkacsoportot létrehozása

Röviden és összefoglalva ezek tartalmáról, témájukról:

Az Intézkedési Terv a 2004. évi CV. törvényben [3] rögzített védelmi-igazgatási szervek részére összegyűjtve biztosítja mindazon ismereteket, szabályzókat, adatbázisokat, amelyek bevezetésével, alkalmazásával végzi a bizottság a szövetségesi kötelezettségből a megyére háruló tevékenységet.

A Képesség Lista olyan tervezési eszköz, amely átfogó képet ad a megye, a városok, Honvédelmi Körzetek képességeiről. Összefoglalja és rendszerezi azokat a polgári képességeket, amelyek a felmerülő igények kielégítését szolgálják. Például: javító, karbantartó szolgáltatások, tárolási, egészségügyi szolgáltatások, polgári létesítmények igénybevételi lehetőségei, stb.

A Koordinációs Munkacsoport, olyan tervező, koordináló, feladat végrehajtó közösség, amely az Intézkedési Tervben meghatározott feladatokra történő felkészülést, maradéktalan végrehajtást végzi. A csoport összetétele széles szakmai bázison alapul, ezáltal alkalmas bármely probléma gyors, operatív megoldására.

A 2005. év szeptember 22-i gyakorláson mindhárom tervezési, illetve végrehajtási modul szerepelése megtörtént. A gyakorláson, a Befogadó Nemzeti Támogatás keretén belüli segítségnyújtás lehetőségeinek, formáinak megismerését, a meglévő megyei – városi képességlisták alapján, a gyakorlati segítségnyújtás kivitelezésének megszervezését gyakorolták.

A végrehajtás folyamatába bevonták Mosonmagyaróvár, Győr megyei jogú város és Tét Helyi Védelmi Bizottságait.

Azt kívánták elérni, hogy a Megyei Védelmi Bizottság, a bizottság Koordinációs Munkacsoportjának tagjai, illetve a gyakorlásba bevont Helyi Védelmi Bizottságok elnökei ismereteket szerezzenek az ilyen típusú feladatok kezeléséről.

A gyakorlás során nem törekedett senki arra, hogy egy – egy részfeladatot teljes mélységében kielemezzen, kidolgozzon. Nem ez a cél. A gyakorlás azt szolgálja, hogy magát a folyamatot ismerjük meg: amely magában foglalja az események bekövetkezése kapcsán kialakuló helyzetekre adandó válaszok egymást követő láncolatát, a megoldásban érintett szervezetek lehetőségeinek olyan aspektusú felmérését, amelyek az előkészítést, a döntést, a végrehajtásra történő felkészülést, és az azt követő gyakorlati segítségnyújtást szolgálják.

Egy, a valós helyzetet jól megközelítő körülmények beállításával azt gyakorolták, hogy a megyei és a helyi védelmi bizottságoknak hogyan kell reagálniuk hasonló helyzetben.

Melyek azok az együttműködési formák, segítségnyújtási lehetőségek, amelyek a szövetségesi kötelezettségből adódó feladatok ellátása mellett, a lakosság biztonságát, az élet- és anyagi javak védelmét, az esetleges károk gyors felszámolását is elősegítik.

Mik és milyen tartalmúak azok az intézkedések, amelyek a döntés eredményeként a probléma megoldásához, a kialakult veszélyhelyzet elhárításához, illetve a segítségnyújtás legcélszerűbb formáihoz vezetnek. A gyakorlást hat mozzanatban tervezték végrehajtani, sikerrel.

Ezt követően, a gyakorlást követően technikai bemutatót tekinthettek meg a MH 12. Légvédelmi Rakétadandár, [4] a Katasztrófavédelmi Igazgatóság, a Győri Határőr

Igazgatóság, Győr megyei jogú város Hivatásos Önkormányzati Tűzoltóság, a Megyei Rendőr-főkapitányság, illetve a Közlekedési Felügyelet eszközeiből.

A Győr-Moson-Sopron Megyei Védelmi Bizottság (MVB) 2004. év februári testületi ülésen határozatot hozott, mely alapján – figyelembe véve a 244/2003.(XII.18.) számú Kormányrendeletben foglaltakat – két új Honvédelmi Körzetközpont kialakítására került sor a megyében, Tét és Pannonhalma városok irányításával

A 2004. év március hónapban megkezdett szervező, kidolgozó munka befejezését követően mindkét városban 2004. június 24-én került sor a körzetközpontot irányító Helyi Védelmi Bizottságok összeülésére.

Az üléseken az új Helyi Védelmi Bizottságok elnökei – Szabó Ferenc és Pánczél Benedek, polgármesterek - áttekintést adtak az év első félévében a védelmi igazgatás területén végzett munkáról, a felkészülés helyzetéről, illetve a bizottság további munkájával kapcsolatos elképzeléseikről.

A védelmi bizottságok elfogadták Szervezeti és Működési Rendjüket, valamint a 2004. második félévére szóló Munka- és Ellenőrzési Tervüket.

Az alakuló testületi üléseken részt vett dr. Szakács Imre, a Megyei Védelmi Bizottság elnöke, aki elmondta, hogy a Dunántúlon elsőként Győr-Moson-Sopron megye hajtotta végre azt az átalakító, átszervező munkát, amelynek eredményeként valamennyi kistérségi székhely egyben Honvédelmi Körzetközponttá is vált.

Megemlítendő külön a Téten és Pannonhalmán megalapított Kistérségi Vegyes Feladatú Társulás is, [5] melyek e két városban 2006. év nyara óta működnek, és az fentebb említett feladataik mellett magas szintű gazdasági tevékenységet is ellátnak. Így a gazdasági gyarapodás célja mellett, sikereik esetén generálják a veszélyhelyzetekben megvalósított védekezés és tevékenység egyre magasabb szinten lehetővé válását.

Tekintettel arra, hogy a felkészülés, reagálás és védekezés minősége nagyban függ a képzések, illetőleg a rendelkezésre álló személyi állomány számától (személyi feltételek), illetve a berendezések számától és minőségétől (tárgyi feltételek), fontos erre a két feltételre gondot fordítani.

A kistérségi társulások nagyban hozzá tudnak járulni anyagi támogatásukkal a tárgyi feltételek javulásához, illetve legújabb törekvésükként a személyi feltételek javításához. A fentebb említett két társulás illetékességi területén csak a polgármesterek részesültek oktatásban, ellenben fél éve egy olyan tendencia látszik kibontakozni, melyben a társulások kedvező telek, illetve házvásárlási lehetőségekkel támogatják az arra a vidékre letelepedni szándékozó hivatalos szervek dolgozóit, ezáltal is a bővíteni igyekeznek a lehetséges hozzá értő személyek létszámát.

A tűzoltóság, rendőrség, katonaság dolgozói ezeken a vidékeken jobb eséllyel szállhatnak harcba ingatlan szerző tevékenységük során, mint „civil” társaik. Jól mutatja e törekvést a szolgálati lakások számának bővülése, illetve Téten a Kistérségi Rendőrállomás létre hozása,

valamint a Pannonhalmi Rendőrőrs munkába állítása, természetesen mindkét épület új építésű, friss átadással, természetesen komoly technikai (számítógépek, szolgálati autók) felszereltséggel.

Dr. Szakács Imre felhívta az új testületek figyelmét arra, hogy a katasztrófahelyzetekre történő időbeni felkészülés minden város, illetve körzetközpont vezetésének elengedhetetlen feladata.

A győri polgármester helyettes hangsúlyozta, hogy az erre irányuló feladatok eredményes végrehatásában a védelmi bizottságoknak kiemelkedő szerepe, feladata, és körültekintést igénylő tevékenysége van, hiszen Győr-Moson-Sopron megye nagy vízfelületekkel rendelkezik, Győr város a „vizek városa", [6] rengeteg folyó és holtág található a megyében.

Ezek évi rendszerességgel kis is öntenek medrükből, tehát a védelmi bizottságok legfontosabb, és legaktuálisabb feladata az árvíz elleni védekezés. Így a gyakorlatokkal el lehet érni, hogy minél kisebb anyagi kárt okozzon az árvíz, illetőleg kisebb forrásokból, gyorsabban, egyre magasabb szinten lehessen elvégezni a munkákat.

2006-ban harmadfokú készültség volt Győrben: több csónakházat, szórakozóhelyet és a városi uszodát is elöntött a víz.

Az Észak-dunántúli Vízügyi Igazgatóság védelmi osztagát is készültségbe helyezték, és harmadfokú árvízvédelmi készültséget rendeltek el a Nagy-Duna Dunaremete és Vének közötti szakaszán is. Janák Emil igazgató szerint nem számítottak vészhelyzetre, de árvízi jelenségekre – például buzgárokra – igen. Továbbá megállapította, hogy megközelítőleg 600-700 centiméteren tetőzik a folyó. Csak összehasonlításként: az emlékezetes 2002. augusztusi áradásnál nyolc méternél magasabb vízállást mértek.

Az árvíz a Mosoni-Dunát és a Rábát is érintette, de ezeken a folyókon még csak elsőfokú szokott lenni a készültség. Győrben 540–560 centiméteres vízállás valószínű az árvíz első szakaszában, míg a tetőzés hat méter felett lesz, ami még így is 1 méterrel elmarad a 2002. évi kiemelkedően nagy árvíztől.

Mindez azonban azt jelenti, hogy több csónakház és uszoda is víz alá kerülhet. Molnár Péter városi sportigazgató arról tájékoztatta a közvéleményt, hogy az előrejelzések ismeretében ilyenkor bezárják az uszodát. „Minden pontos ütemterv szerint zajlik. Az alagsorból és a földszintről menekíteni kell a felszereléseket és az eszközöket, de még az ablakokat is, amelyek korábban többször betörtek árvízkor". A sportigazgatóság műszaki igazgatója, Csatári Jenő szerint a 22 tagú személyzetnek azonnal menteni kell a szivattyúkat, a motorokat, a szauna kályhát, az öltözőkben található személyes holmikat pedig szintén feljebb kell hozniuk egy szinttel.

Az az árhullám időtartamától függ, mennyi ideig nem használhatják az uszodát, hiszen a falaknak meg kell száradni festés és fertőtlenítés előtt. A 2002-es árvíz után két és fél hónapig szünetelt a nyitva tartás és 33 millió forintos kárt szenvedett az intézmény. A költségeket csökkenti, hogy az alagsort korábban kicsempézték; növeli, hogy annak idején a medence került az első emeletre és a gépészet a földszintre.

A Mosoni-Duna másik partján, a Révfaluban álló népszerű szórakozóhely föld alatti diszkó [7] helyiségében az árvizek során átlagban 1 méter 20 centiméter magasan áll a víz.

Főként ismerősök és rokonok segítenek abban, hogy a hangtechnikai berendezést és az árut felhozzák az emeletre. Szarvas Zoltán üzletvezető maga is búvárruhát szerzett a mentéshez, ebben gyakorlatot szerezhetett négy éve minden éven, amikor a fenti asztaloknál ülők fejmagasságáig ért a víz.

A helyiséget egyébként igyekeztek úgy kialakítani, hogy még a legnagyobb tömegű árhullám se tegyen benne kárt, a fapadlót például megfelelő lakkal vonták be, a fenti és a lenti helyiség áramellátását pedig szakaszolták. Mindez elemi érdeke a vállalkozónak, mivel ártéri épületekre biztosítást sem lehet kötni.

A tetőzés várható időpontját akkor tudják megmondani, ha Ausztriában már nem árad a Duna. Folyamatosan több, vagy az összes szivattyútelepet kell működtetni.

A győri Káptalan domb az árvíz előtt.


A győri Káptalan domb az árvíz alatt.

A 2003. évi védelmi igazgatási rendszergyakorlat:

A Kormány az éves védelmi felkészítési terve alapján 2003. szeptember 26. és október 20. között vezette le a VÉDELEM-2003. védelmi igazgatási rendszergyakorlatát.

A gyakorlat általános célja az országos irányítószervek és a megyei védelmi bizottságok válsághelyzeti védelmi igazgatási tevékenységének gyakorlása, továbbá az új típusú kihívásoknak megfelelő szervezetek és eljárási szabályok alkalmazása volt.

A dr. Szakács Imre, a Győr-Moson-Sopron Megyei Védelmi Bizottság elnöke által vezetett megyei gyakorlaton részt vettek a helyi védelmi bizottságok, a kijelölt megyei szervek, önkormányzati hivatalok, összesen 23 szervezet válságkezelő törzsei.

A gyakorlat során megtörtént a védelmi igazgatási szervek készenlétbe helyezése, ügyeleti rendszerük felállítása, működött a megyei védelmi bizottság adatgyűjtő, értékelő, elemző Monitoring-rendszere. [8]

Az ország biztonsági stratégiájának megfelelően a megyei gyakorlat középpontjában is a lakosság, a közigazgatás, a gazdasági élet komplex biztonságának szavatolása, garantálása és megőrzése állt.

Szerepeltek a gyakorlat levezetési tervében a megelőző válságkezelési feladatok, a megye településeinek potenciális veszélyeztetettsége alapján betervezett katasztrófa-elhárítási feladatok, a nemzetközi terrorizmus elleni védekezés feladatai, a migrációs,- menekült helyzet válságkezelése és a közigazgatás mozgósítási feladatainak gyakorlása is.

A megye adottságai alapján a védelmi igazgatás szervei fokozott figyelmet fordítottak, és fordítanak a mai napig is a közlekedési, ipari, vegyi katasztrófák megelőzésére, a

határforgalomból adódó válsághelyzeti feladatokra. A vízkár elhárítási veszélyhelyzetek kezelésére, a humán- és az állatjárvány megelőzésével, kezelésével kapcsolatos feladatokra.

Minden veszélyhelyzet esetén van egy szakmailag illetékes megyei irányítószerv, amelyet más együttműködő szervek segítenek a válságkezelésben. A válsághelyzetek kezelését az illetékes polgármester, helyi védelmi bizottság, vagy a megyei védelmi bizottság koordinálja, így történt ez a gyakorlat során beállított helyzetekben is.

A megyei védelmi bizottság a gyakorlat végén tartott ülésén értékelte a végrehajtást. Megállapította, hogy a gyakorlatba bevont szervek felkészülése, a gyakorlat végrehajtása szükséges és eredményes volt, a tapasztalatokat feldolgozza és a jövőben hasznosítja a védelmi felkészítés, válságkezelés során.

## Hivatkozások


1. http://web.b-m.hu/belugy/bmjog.nsf/cda8258f45faba0cc12569480042e930/b20d9a9644ae3060c1256dd4003850e9?OpenDocument
2. http://cyberpress.sopron.hu/article.php?id=11789
3. http://www.hm.gov.hu/files/9/3857/2004._evi_cv._torveny.pdf
4. http://www.raketadandar.hu/
5. http://www.b-m.hu/idea/tan1.doc
6. http://www.sze.hu/ep/arc/irod/SA1998_Gyor_vizpartjai/
7. http://www.gyori-bahnhof.hu/
8. http://www.kvvm.hu/szakmai/karmentes/kiadvanyok/karmutmutato2/karmutm2-1.htm

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Pántya Péter**

# A MAGYAR KÖZTÁRSASÁG FEGYVERES ÉS RENDVÉDELMI SZERVEI

***Absztrakt***

*A fegyveres és rendvédelmi szervek végzik az ország területén az igen speciális feladataikat az állampolgárok életének, testi épségének és vagyonának biztonságáért. Eltérő feladataikat, felépítésüket és létszámaikat ismertetem jelen cikkben. Célom egy általános információ adása ezen szervekről (Rendőrség, Polgári Védelem, Vám és Pénzügyőrség, Honvédség, Büntetés-végrehajtás, Hivatásos Tűzoltóság, Nemzetbiztonsági Hivatal). A szolgálati törvényből (Hszt.) vett idézetekkel „helyzetspecifikusan" teszem érthetőbbé a rendvédelem működését és a jogszabályi kereteket.*
*A megcélzott olvasói réteg elsősorban a nem kifejezetten ezen területek valamelyikén dolgozók, de remélem, hogy a rendvédelmi szervek állománya is talál valami új információt.*

*Armed forces and defence authorities deal with safety of the life, soundness, properties of citizens in the country of Hungary. My article talks about their several duties and numbers. My aim is to tell you some general information about these authorities (Police, Citizen Defence, Customs and Excise Guard, National Defence, Penalize Authority, Fire Brigade, National Security Agency). I make understand the work of defence authorities with citing from the duty laws, specified on situations.*
*Perhaps, people who read this article do not work at these fields of activity, but I hope that others, who work for the defence can also find some new information in this article.*

***Kulcsszavak:*** *fegyveres, rendvédelem, szervek, rendőrség, polgári védelem, vám és pénzügyőrség, honvédség, büntetés-végrehajtás, hivatásos tűzoltóság, nemzetbiztonság ~ armed forces, defence, authorities, police, citizen defence, customs and excise guard, national defence, penalize authority, fire brigade, national safety*

Sok témánál megjelennek a címben említett szervezetek, de talán nem mindig kerülnek meghatározásra mibenlétük, feladataik. A fogalmak tisztázása nélkül nehéz lenne érintett

témáról beszélni. Nézzük tehát, hogy melyek is az úgynevezett fegyveres és rendvédelmi szervek a hivatásosok szolgálati törvénye alapján, zárójelben az országos vezetést jelöltem:

- **Rendőrség** (Országos Rendőr-főkapitányság, immár a Határőrséggel integrálódva);
- **Polgári védelem** (Országos Katasztrófavédelmi Főigazgatóság);
- **Vám- és pénzügyőrség** (Vám és Pénzügyőrség Országos Parancsnoksága);
- **Büntetés-végrehajtási intézet** (Büntetés-végrehajtás Országos Parancsnoksága);
- **Állami és Hivatásos önkormányzati tűzoltóságok** (Országos Katasztrófavédelmi Főigazgatóság);
- **Polgári nemzetbiztonsági szolgálatok (**vezetője a főigazgató**).**

A felsorolt szerveknek – meghatározott feladataik ellátása mellett – békében fel kell készülniük a jelenlegi új típusú kockázatok kezelésére, melynek egyik biztosítéka a Hszt. előírásainak szakszerű, következetes betartása.

*„Az új típusú kockázatok lehetnek belső és külső típusúak. Belső típusú fenyegetés az országon belül jelentkezhet, feszültség, válság, akár polgárháború formájában,…."*[1]

A Magyar Köztársaság alkotmányos rendjét és biztonságát tehát ezek a szervek biztosítják saját területükön, a számukra meghatározott feladatok ellátásával. E szervek összlétszáma körülbelül ötvenötezer fő.
A fenti felsorolás és a létszámadatok nem tartalmazzák a Magyar Honvédséget. Létszámuk jelenleg körülbelül 25.000, szolgálati viszonyukat egy másik törvény szabályozza eltérően a fent említett szervektől, azonban kevés különbséggel.

A feladatok ellátásának módjáról az 1996. évi XLIII-as törvény világosan fogalmaz:
*„A Magyar Köztársaság függetlenségének, alkotmányos rendjének, valamint a lakosság és az ország anyagi javainak védelmét ellátó szervek hivatásos állományától az állam tántoríthatatlan hűséget, bátor helytállást követel."*


1. sz. kép:
Mozaik a fegyveres és rendvédelmi szervek jelképeiből. (Saját összeállítás, 2008.)

[1] Dr. Horváth László: Az országvédelem szervezeti rendszere egyetemi jegyzet, 13. oldal (Távoktatási tananyag), ZMNE, Budapest, 2005.

Az állomány hivatásos állományú tagját igazolja egyenruhája, némely szerveknél jelvénye valamint akár civil ruházatban is, szolgálati igazolványa.
A fegyveres és rendvédelmi szervek tagjait megkülönböztethetjük az állományra utaló jelzéssel, eltérő rendfokozatokkal és más-más beosztásokkal.
Például.: rendőr orvos alezredes, tűzoltó törzszászlós (hírközpont-kezelő), pénzügyőr őrmester (kutató), polgári védelmi százados (osztályvezető).

2. sz. kép:
Alezredesi rendfokozati jelzés. (Forrás: *www.nemzetorseg.hu*, 2007.)

A rendvédelemben részt vevő szervezetek tevékenységét és állományuk létszámát ismertetem röviden a következőkben, valamint kitérek a Magyar Honvédségre is. A szolgálati törvényből vett idézetekkel a szellemiséget próbálom visszaadni.

## A RENDŐRSÉG

Nagy változás következett be a Rendőrséget és a Határőrséget érintően, amikor 2008. elején a két rendvédelmi szervezetet összevonták, a Rendőrség állományába szervesen integrálva a határőröket. A többi rendvédelmi szerv is tapasztalhatta a változást, hiszen az a határőr, akinek valamilyen okból nem fogadta el a felkínált új beosztását, az (megfelelő körülmények esetén) vagy nyugállományba került vagy leszerelt, vagy pedig – és ez a gyakoribb – más rendvédelmi szervhez kérte át magát.

A Rendőrség eredeti létszámához képest jelentősen felduzzadt és megkapta a Határőrség infrastruktúráját és eszközeit is. Sokáig fogunk még látni zöld vállapos rendőrt kiszállni zöld színű gépjárműből, amin már Rendőrség felirat látható.
A szolgálati törvény, azaz a Hszt. rendelkezésének értelmében rendőri szolgálati viszony akkor létesíthető, tartható fenn, ha:

- a jelentkező életvitele kifogástalan és a szolgálat törvényes, befolyástól mentes ellátását veszélyeztető körülmény nem áll fenn, továbbá
- a jelentkező írásban hozzájárul a meghatározott személyes adatai és bűnügyi személyes adatai kezeléséhez, életvitele kifogástalanságának a felvételét megelőzően és a szolgálati viszony tartama alatti ellenőrzéséhez.

A Rendőrség teljes létszáma napjainkban mintegy 50 ezer fő. Ebből körülbelül 40.000 fő hivatásos állományú.
Feladatköre röviden és egyszerűen fogalmazva:
A közbiztonság és a belső rend védelme.

4. sz. kép:
Rendőri váll-lapok a rendszerváltás előtti rendfokozati jelzésekkel.
*(még ötágú csillagok, tisztesi jelzések) (Forrás: www.karjelveny.hu, 2007.)*

A Rendőrség létszáma a legmagasabb volt mostanság a hivatásos állománnyal bíró szervezetek között ideértve a Magyar Honvédséget! A Határőrség integrációjával egy még nagyobb állományú és szélesebb feladatkörű szerv jött létre. A 2006-os esztendőre vonatkozóan az egy napra jutó ismertté vált bűncselekmények száma több mint 1100.[2] A bűncselekmények közel egyharmada közterületen kerül elkövetésre, így nagy teher van az itt szolgálatot teljesítő rendőrökön.

5. sz. kép:
Tiszthelyettesi rendőr tányérsapka.
Viselete az új típusú (baseball) sapka mellett még megengedett.

A rendőr esküje:
*„Én ..... a Magyar Köztársaság ..... tagja esküszöm, hogy a Magyar Köztársaság alkotmányához, törvényeihez és más jogszabályaihoz híven, becsületesen teljesítem kötelességemet. Elöljáróim és feljebbvalóim parancsainak engedelmeskedem.*

*Esküszöm, hogy hazám alkotmányos és törvényes rendjét, nemzetünk biztonságát, ha kell, életem kockáztatásával is hűségesen megvédem. Mindenkor az állampolgári jogok érvényesítését tartom szem előtt, és a nép érdekeinek megfelelően járok el.*

*Esküszöm, hogy elöljáróimat, munkatársaimat megvédem, fegyveremet, felszerelésemet megóvom. A szolgálati ismereteket elsajátítom. A rendet és fegyelmet minden törvényes eszközzel fenntartom. Alárendeltjeimről a legjobb tudásom szerint gondoskodom,*

[2] Forrás: www.orfk.hu, az Országos Rendőr-főkapitányság honlapja

*őket öntudatos hazafiakká, a népek kölcsönös tiszteletére nevelem. Minden erőmmel, törekvésemmel, tudásommal a Magyar Köztársaság fejlődését szolgálom.*

*Az állam- és szolgálati titkot híven megtartom. Szolgálatban és szolgálaton kívül példamutatóan viselkedem."*[3]

## A POLGÁRI VÉDELEM

A létszámában a legkisebb rendvédelmi, hivatásos szervezet. Körülbelül 800-1000 fős állományú. Az 1935-ben létrejött szervezet akkor még a lakosság légitámadások elleni védelmét hivatott biztosítani. Feladatköre napjainkra teljesen átalakult és komplex lett, a fő cél azonban – a lakosság védelme – mindvégig megmaradt. A Honvédség szervezetéből kikerülve jelenleg az Országos Katasztrófavédelmi Főigazgatóság alá tartozik. A légoltalom helyett a katasztrófavédelmi tevékenységek és előkészületeik alkotják az elsőrendű célokat.

6. sz. kép:
Védekezési munkálatok. (Forrás: www.zalamedia.hu)

*„A hivatásos állomány tagjának munkateljesítményét az adott fegyveres szerv kiemelt céljának és az érintett munkakörének figyelembevételével meghatározott teljesítménykövetelmények alapján az állományilletékes parancsnok mérlegelési jogkörében eljárva, évente írásban értékeli."*[4]

## A VÁM ÉS PÉNZÜGYŐRSÉG

A mintegy 6.000 fős vám és pénzügyőr állomány végzi a Magyar Köztársaság által és annak érdekében meghatározott tevékenységeket. A feladatok meghatározása – amely meglehetősen szerteágazó - a Vám és Pénzügyőrség Alapító Okiratában is megtalálható:

*„- az államhatáron át lebonyolódó áru- és utasforgalom vámellenőrzése, a vámterhek és egyéb közterhek kiszabása és beszedése,*
*- külön törvényben meghatározott idegenrendészeti feladatok ellátása,*
*- közvetlenül vagy közvetve meghatározott körben termékek, termények, áruk azonosságának… …a vizsgálata, illetve a vizsgálat megtörténtének ellenőrzése,*
*- a vámokmányok adatainak vám- és statisztikai célú ellenőrzése, javíttatása, nyilvántartása,*

[3] 1996.évi XLIII-as törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról
[4] 1996.évi XLIII-as törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról

*összesítése, feldolgozása és átadása,*
*- külön jogszabályban szabályozott, nemzetközileg ellenőrzött termékek és technológiák forgalmának ellenőrzése,*
*- ...meghatározott ellenőrzési és utólagos ellenőrzési feladatok, valamint a különböző, feltételtől függő vámkedvezmények elbírálásához szükséges ellenőrzési feladatok ellátása,*
*- a jövedéki adóról és a jövedéki termékek forgalmazásának különös szabályairól szóló 1997. évi CIII. törvényben és a végrehajtására kiadott jogszabályokban meghatározott ellenőrzési, adóztatási-, hatósági feladatok ellátása,*
*- a büntetőeljárásról szóló törvény által hatáskörébe utalt pénzügyi bűncselekmények megelőzése, felderítése, valamint nyomozás a az erre vonatkozó külön jogszabályok rendelkezései szerint, valamint a törvényben meghatározott és nemzetközi együttműködési kötelezettségből adódó felderítési feladatai végzése során észlelt egyéb bűncselekmények esetében a halaszthatatlan nyomozati cselekmény végzése, a helyszín és a bizonyítékok biztosításával, valamint a hatáskörrel rendelkező nyomozó hatóság értesítésével,*
*- a külön jogszabályban meghatározott pénzügyi (vám-, deviza és adó) szabálysértések megelőzése, felderítése és elbírálása,*
*- a testület kezelésében lévő anyagi javak, értékek őrzése, kísérése,*
*- a nemesfémforgalommal és fémjelzéssel kapcsolatos ellenőrzési feladatok ellátása,*
*- a közúti határátkelőhelyek üzemeltetése, fenntartásukra és fejlesztésükre vonatkozó feladatok végrehajtása,*
*- a nemzetközi egyezményekben vagy a pénzügyminisztertől kapott felhatalmazás alapján külföldi vámigazgatásokkal és nemzetközi vámszervekkel a munkakapcsolat alapján felmerülő vám szakmai feladatok ellátása,*
*- továbbá az alaptevékenységgel összefüggő, azzal kapcsolatos kiegészítő tevékenység végzése a mindenkor hatályos jogszabályok figyelembevételével."*[5]

7. sz. kép:
Ellenőriz a vám és pénzügyőr. (Forrás: www.bp18.hu A XVIII. Kerület honlapja)

*„A vám- és pénzügyőrség hivatásos állományú tagja nem végezhet olyan gazdasági tevékenységet, amely a vám- és pénzügyőrség alaptevékenységéhez kapcsolódik."*[6]

[5] A Vám- és Pénzügyőrség egységes szerkezetbe foglalt alapító okirata (száma: 14303/21/2003)
[6] 1996.évi XLIII-as törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról

## A BÜNTETÉS VÉGREHAJTÁS


8-9. sz. kép:
A budapesti Kozma utcai börtön. (Forrás: Kis Guczi Péter 2001.)

Magyarországon napjainkban körülbelül 17-18.000 fő fogvatartott van. Az őrzésükkel, szállításukkal és az egyéb járulékos feladatokkal a mintegy 4.000 fős büntetés-végrehajtási állomány foglalkozik. Az igen nagy zsúfoltság miatt Tiszalökön és Szombathelyen is új börtönt alakítottak ki.

*„A büntetés-végrehajtási szervezetnél a hivatásos szolgálati viszony létesítésének feltétele, hogy az érintett hozzájárul a személyes adatai kezeléséhez, illetve beszerzi közeli hozzátartozói és a vele közös háztartásban élő nagykorú személyek írásos hozzájárulását személyes adataik kezeléséhez.*

*A büntetlen előélet ellenőrzéséhez a (3) bekezdésben felsoroltak írásbeli hozzájárulását csatolni kell. A büntetlen előéletnek való megfelelést a büntetés-végrehajtási szerv a szolgálati viszony létesítésekor ellenőrzi, annak fennállása alatt pedig ellenőrizheti."*[7]

## A TŰZOLTÓSÁG


11 - 12. sz. képek
(Forrás: Kis Guczi Péter, 2000., valamint Komáromi Tűzoltóság, 2007.)

A Magyar Köztársaság területén a tűzoltás, műszaki mentés és katasztrófák esetén az elsődleges beavatkozás megtétele elsősorban a Hivatásos Önkormányzati Tűzoltó-

[7] 1996.évi XLIII-as törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról

parancsnokságok feladata. Tevékenységüket kiegészítik a működési területtel rendelkező Önkéntes Tűzoltóságok (köztestületi). Jogállás szempontjából kissé eltérnek a többi rendvédelmi szervtől, mivel fenntartásukban önkormányzati hatáskörbe kerültek és központi költségvetési forrásból kerülnek finanszírozásra.
A Hivatásos szolgálati törvény hatálya alá csak a hivatásos tűzoltók tartoznak. Létszámuk napjainkban több mint 8000 fő a vonulós egységgel rendelkező Tűzoltóságokon. Ebből 7000 fő feletti a készenléti, vonulós, tehát a konkrét beavatkozó állomány. Az Európai Uniós jogharmonizációs munkaidő-csökkentési folyamatnak köszönhetően már idén is a tavalyihoz hasonlóan, újabb 500 fővel nőhet a létszámuk.

*„A szolgálati viszony az állam és a hivatásos állomány tagja között létrejött különleges közszolgálati jogviszony, amelyben mindkét felet a sajátos szolgálati körülményeknek megfelelő, e törvényben és más jogszabályokban meghatározott kötelezettségek terhelik és jogosultságok illetik meg.*

*A hivatásos állomány tagja a szolgálati viszonyból fakadó kötelmeit - a fegyveres szerv rendeltetés szerinti feladatainak megvalósítása érdekében - önkéntes vállalás alapján, élethivatásként, szigorú függelmi rendben, életének és testi épségének kockáztatásával, egyes alapjogai korlátozásának elfogadásával teljesíti.”*[8]

A hivatásos Tűzoltóságok elsődleges és segítségnyújtási működési körzetükben végzik tűzoltási és műszaki mentési tevékenységüket, valamint a Riasztási és Segítségnyújtási Terveknek megfelelően meghatározott rendben segítséget nyújtanak más Tűzoltóságoknak. Az illetékességi területükön végzik a tűzvizsgálati és szakhatósági tevékenységüket.

*„A műszaki mentés természeti csapás, baleset, káreset, rendellenes technológiai folyamat, műszaki meghibásodás, veszélyes anyag szabadba jutása vagy egyéb cselekmény által előidézett veszélyhelyzet során az emberélet, a testi épség és az anyagi javak védelme érdekében a tűzoltóság részéről – a rendelkezésre álló, illetőleg az általa igénybe vett eszközökkel – végzett elsődleges beavatkozói tevékenység.”*[9]

A műszaki mentési beavatkozások elő vannak írva különösen:
- az épületkároknál, építménybaleseteknél,
- a közlekedési baleseteknél,
- a természetes vizekben (folyó és álló vizekben) bekövetkezett baleseteknél,
- a csatornákban, kutakban és egyéb víztározókban bekövetkezett baleseteknél,
- a közüzemi berendezések, közművek meghibásodásával összefüggő veszélyhelyzeteknél, baleseteknél (gépi és villamosbaleseteknél),
- a magasban, mélyben, föld alatti üregekben (barlangokban, szakadékokban) bekövetkezett baleseteknél,
- a veszélyes anyagok szabadba jutásánál, nukleáris baleset során,
- a természeti csapásoknál, valamint minden hasonló esetben az élet- és a vagyonmentés, valamint az alapvető élet- és vagyonbiztonság érdekében.

[8] 1996.évi XLIII-as törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról
[9] 1/2003 BM rendelet, a Tűzoltóság tűzoltási és műszaki mentési szabályairól

13. sz. kép:
Műszaki mentés balesetnél
(Forrás: www.langlovagok.hu A tűzoltóportál, 2007)

Amint látható a hivatásos és az önkéntes (köztestületi) Tűzoltóságok tevékenysége talán a legszerteágazóbb a rendvédelmi szervezetek között.

## A NEMZETBIZTONSÁGI HIVATAL

14. sz. kép:
Az NBH előtere. (Forrás: www.nbh.hu A Hivatal honlapja)

*„A polgári nemzetbiztonsági szolgálatok hivatásos állományú tagja fontos és bizalmas munkakört betöltő személynek minősül……A polgári nemzetbiztonsági szolgálatok hivatásos állományú tagja külföldre utazásának tervezett napját, útvonalát, célját, hazatérésének várható időpontját az állományilletékes parancsnoknak köteles bejelenteni. Az állományilletékes parancsnok a külföldre utazást szolgálati és biztonsági érdekből megtilthatja, illetőleg korlátozhatja.”*[10]

Feladatköréből adódóan a polgári nemzetbiztonsági szolgálatok működésével kapcsolatosan nem sok információ lelhető fel és ez így szolgálja országunk érdekeit.

[10] 1996.évi XLIII-as törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról

Több szakszolgálat működtetésével látja el feladatát, létszáma szintén titkos, körülbelül 1.500 – 3.000 fős állománya van. Közvetlen országgyűlési felügyelete biztosítja törvényes működését a Nemzetbiztonsági Bizottságon keresztül. Irányítását a szakminiszter látja el, ellenőrzését az Állami Számvevőszék végzi.
Tevékenységét alapvetően az 1995. évi CXXV. Törvény (a nemzetbiztonsági szolgálatokról) alapján végzi.

## A MAGYAR HONVÉDSÉG

Magyarországot mintegy 80.000 fős hivatásos állomány szolgálja. Ebből a létszámból körülbelül 25.000 fős a Magyar Honvédség hivatásos és szerződéses állománya. Tagjainak szolgálati viszonyát 1996-tól a Hszt. szabályozta, azonban a 2001. évi XCV törvény (a honvédelemről és a Magyar Honvédségről, [Hjt.]) új kereteket teremtett számukra.

15. sz. kép:
A Magyar Honvédség címere

Fő feladata a Magyar Köztársaság területének és függetlenségének védelme. A NATO csatlakozás hazánk számára is meghatároz feladatokat és kötelességeket. Ennek teljesítése elsősorban a Magyar Honvédség feladata.
További feladatai: hozzájárul más, közösen vállalt szövetséges küldetésekhez, részt vesz a nemzetközi szervezetek által zajló béketámogató és humanitárius akciókban, segítséget nyújt a súlyos ipari és természeti katasztrófák elhárításánál.

16. sz. kép: Szolgálatban a honvédek,
(Forrás: www.honvedelem.hu, a Honvédelmi Minisztérium honlapja)

## ÖSSZEGZÉS

A hivatásos állományúak szolgálati törvénye a jogalkotó szándéka szerint részletesen szabályozza a hatálya alá tartozók jogviszonyát, munkakörülményeit, a különös részekkel az eltérő feladatú rendvédelmi szervezetek közötti különbségek szabályzását teszi lehetővé.
Tartalmában megjelenik a szabadságszámítás, az érdekképviseleti szerv jogai és a rendfokozatok várakozási idejének meghatározása mellett a fegyelmi szabályok valamint a nyugdíjjal kapcsolatos előírások is.
A körülbelül 55.000 fős rendvédelmi szervezet és tagjainak helyzete nem elhanyagolható az ország érdekében sem bár a közszolgálatban dolgozóknak csak egy kis részét alkotják. Gyakorlatilag a veszélyes feladatvégzéssel járó végrehajtói területen való feladatokra jöttek létre a fent felsorolt fegyveres és rendvédelmi szervek.

## FELHASZNÁLT IRODALOM:


- A Civilisztikai és Igazságügyi Szakállamtitkár előterjesztése a foglalkoztatási jogviszonyok felülvizsgálatának Hszt-re vonatkozó irányairól, Igazságügyi és Rendészeti Minisztérium, 2006.
- Dr. habil. Horváth László: Az országvédelem szervezeti rendszere egyetemi jegyzet (Távoktatási tananyag), ZMNE, Budapest, 2005.
- - Koltay Jenő és Neumann László szerkesztésében: Közelkép, Munkaügyi kapcsolatok Magyarországon. 2005.
- Dr. Szakács Gábor: Előtanulmány a hivatásos állomány rendfokozati, illetve bér és besorolási rendszere között meghúzódó ellentmondás feloldására, egy új differenciált bér és besorolási rendszer kialakítására, BM Oktatási Főigazgatóság, 2005.

**Törvények:**

- 1949. évi XX. törvény, A Magyar Köztársaság Alkotmánya.
- 1996. évi XLIII. törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról.
- 2001. évi XCV törvény, a Magyar Honvédég hivatásos és szerződéses állományú katonáinak jogállásáról.
- Dr. Horváth László: Az országvédelem szervezeti rendszere egyetemi jegyzet (Távoktatási tananyag), ZMNE, Budapest, 2005.

HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

**Kucsera Péter**
Budapesti Műszaki Főiskola
kucsera.peter@kvk.bmf.hu

# ELSÖPRŐ SIKERT ARATOTT A KANDÓ CSAPATA A DESIGN CHALLANGE 2008 NEMZETKÖZI ROBOTÉPÍTŐ VERSENYEN

Idén második alkalommal vettek részt a BMF Kandó Kálmán Villamosmérnöki Karának diákjai a Wilhelmshaven-ben 2008. május 7-én megrendezésre került nemzetközi robotépítő versenyén. A verseny lényege, hogy a minden csapatnak ugyan azon alkatrészekből kell felépíteni egy olyan mobil robotot, az idei évben egy hajót, mely egy előre megadott tesztpályán képes feladatokat végrehajtani. A robot felépítésére a szabályok alapján mindössze két hét állt rendelkezésre, így nem csak az alkatrészekkel, de az idővel is takarékoskodni kellett. A verseny során díjazásra került a legjobb konstrukció, valamint a robotok a valóságban, időmérő versenyek keretében is megmérkőztek. A Budapesti Műszaki Főiskola Kandó Kálmán Villamosmérnöki Karának csapata az időmérő futamokon elsöprő fölénnyel győzött, valamint elhozta a legjobb elektronikáért járó zsűri különdíjat is. A csapatban részt vett Maróti Zsolt, Winkler Péter (2. éves), Fáth Bálint és Ruff Norbert (3.éves). A csapatvezető Kucsera Péter tanársegéd volt, aki a Zrínyi Miklós Nemzetvédelmi Egyetem doktorandusz hallgatója.

1. kép:
A BMF csapata

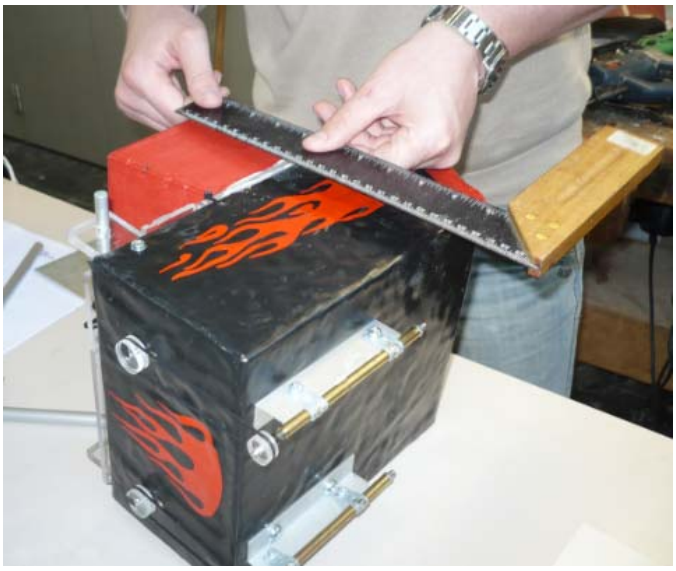
Az építéshez rendelkezésre álló anyagok közt villanymotorok, csapágyak csavarok plexilemez, alumíniumlemez, alumínium profilok és egyszerű szerelési anyagok, valamint a vezérlő elektronika elkészítéséhez szükséges mikrokontroller és elektronikai alkatrészek találhatók.

A feladat egy olyan hajó építése volt, amely egy start pozícióból indulva, megfelelő helyre beállva, infra-kódsorozat kiadásával vizet vételez, majd abból egy adott mennyiséget egy, a pálya másik pontján található tölcsérbe betölt. A haladást nehezíti a pályán található zsiliprendszer, melyet szintén infra kóddal lehet nyitni, zárni. A átfuvarozott víz feltölt egy szárazdokkot, melyből egy hajót kivontatva a start pozícióba visszatérve a feladat lezárul. Mivel a versenyt a Mayer Werft hajógyár támogatta, a pálya és a kivontatandó hajó egy lekicsinyített mása a valóságos hajógyár egy dokkjának és hajótípusának. A tesztpálya a 2. képen látható.

2. kép: A tesztpálya

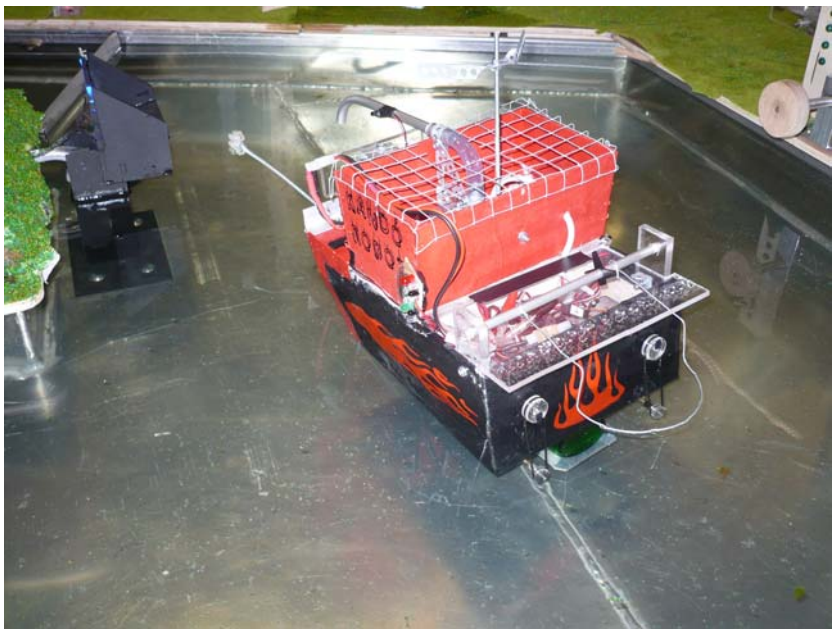
Mivel a csapatok csak a verseny előtt két héttel kapják meg az alkatrészeket és a feladatot, az idő és a pontos tervezés nagy jelentőséggel bír. A verseny szabályainak megfelelően csak azok az alkatrészek használhatók, amelyek a megküldött csomagban találhatók, így sok esetben a legalapvetőbb kötőelemekkel, csavarokkal is takarékoskodni kell. A verseny érdekessége, hogy ugyanazon alkatrészekből a legkülönbözőbb megoldások születnek és csak a verseny napján derül ki, hogy mely megoldás állja meg a helyét a való életben. Érdekességként kell megemlíteni, hogy a szervezők a csapatok biztatására hat üveg sört is elhelyeztek az alkatrészek között, melyeket a csapatok többsége a friss gondolatok serkentésére el is fogyasztottak, ám a BMF csapata feláldozott egy üveg sört a jó ügy érdekében, így a hajó tőkesúlyaként használt sör stabilabb jobban irányítható hajót eredményezett. Egy hajó építése mérnöki szempontból rendkívül érdekes feladat. Fontos szempont a jó manőverező képesség, valamint meg kell oldani az elektronika víztől való védelmét. A Kandó - Robot robosztus, stabil kivitelével és néhány apró ötlettel magasan kiemelkedett a mezőnyből. A két hajócsavar a hajó alján két oldalt került elhelyezésre, így

ellenkező irányban hajtva őket a hajó saját középpontja körül el tudott fordulni. A kapott motorok fordulatszámát egy ékszíj áttétel háromszorosára növelte, így annak ellenére, hogy a hajó lényegesen nehezebb lett a versenytársakénál, lényegesen erősebb és gyorsabb lett (3. kép). A mechanikai ötleteken kívül fontos szerepet játszott a győzelemben a fedélzeti elektronika, mely elegáns és megbízható módon vezérelte a motorokat.



3. kép: A készülő hajó

A Wilhelmshaveni szervezőgárda megadta a módját az időmérő futamok lebonyolításának is. A teremben zene, villódzó fények, szórakoztató élő közvetítés tette rendkívül szórakoztatóvá a csapatok tesztjeit. A közönség pedig zászlókkal, biztató szavak skandálásával próbálta a neki legszimpatikusabb csapatnak segíteni. A szervezők láthatóan nem számoltak a Magyar győzelemmel, mivel az eredmény kihirdetésénél, sajnálkozva közölték, hogy nem áll rendelkezésükre a magyar himnusz. A versenyen, hazánkon kívül több német csapat, Lettország és Románia is képviseltette magát.



2. kép: A Kandó-Robot működés közben

Az ilyen és ehhez hasonló versenyek jó alkalmat teremtenek arra, hogy a résztvevők játékos formában, gondolataik szabadon eresztésével oldjanak meg bonyolult feladatokat, szerezzenek új, hasznos ismereteket.

A versenyről további információk a http://dc2008.design-challenge.de/ internetes oldalon találhatók.