

# SPECIÁLIS ERŐDÍTÉSI LÉTESÍTMÉNYEK A KRITIKUS INFRASTRUKTÚRA SZOLGÁLATÁBAN

*Szalai János mk. alezredes*  
*HM Ingatlankezelési Hivatal*  
*Létesítményi Osztály*  
*osztályvezető*

## **Bevezető**

Az 1990-es éveket megelőzően más típusú fenyegetettséggel kellett számolni, mint ezt követően. A nyugati országok nem foglalkoztak a kritikus infrastruktúrák (továbbiakban KI) megzavarásának, megsemmisülésének kérdésével, sőt nem vették tudomásul, hogy a technológiai fejlődés által a fenyegetettségek megváltoztak. Óriási informatikai forradalom zajlott le az elmúlt évtizedben, mely behálózza az egész világot, átszövi életünk minden területét. Az infrastruktúrák biztonságának fő területei az egyének, közösségek védelmének, és a kritikus infrastruktúrák biztonságának magasabb szintre emelése. Ezeken a területeken a fenyegetettségek fizikai és informatikai eredetűek lehetnek.

A kritikus infrastruktúrák egyes elemeinek védelmére egy lehetséges megoldást javaslok. A rendszerből kivont speciális erősítési létesítmények (továbbiakban SEL) rendelkeznek olyan képességekkel, melyek alkalmassá teszik azokat a több KI egyes elemeinek védelmére, az egyes ágazatokon belül.

Előadásomban SEL–ek hasznosítására teszek néhány javaslatot a KI védelme oldaláról, az alábbi szempontok alapján:

- 1) A kritikus infrastruktúra nemzetközileg elfogadott definíciója.
- 2) A kritikus infrastruktúra fenyegetettsége és osztályozása.
- 3) KI védelmének helyzete Magyarországon:
  - a) Jogszabályok megalkotása,
  - b) Speciális erődítési (védett) létesítmények helyzete,
  - c) Speciális erődítési létesítmények alkalmazása, hasznosítása a KI védelme céljából.
- 4) A KI ágazatai Magyarországon.

### **1) A kritikus infrastruktúra nemzetközileg elfogadott definíciója**

*„Kritikus infrastruktúrának nevezzük a nemzeti és szövetségi vagy uniós infrastruktúra azon létfontosságú elemeit, melyek jelentős károsodása, üzemzavara vagy megsemmisülése súlyos következményekkel járna a nemzet vagy a nemzetek biztonságára, a gazdaságra, a környezetre és közegészségre, illetve az egyes kormányok, az állam hatékony működésére.”<sup>1</sup>*

A kritikus infrastruktúra védelem definíciója:

*„Azok a programok, tevékenységek és kölcsönhatások, amelyeket az állam, a tulajdonosok, az üzemeltetők használnak a kritikus infrastruktúrájuk védelmére.”<sup>2</sup>*

---

<sup>1</sup> Dr. Kovács Ferenc: Az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére vonatkozó intézkedési javaslatok kidolgozása. Tanulmány. Budapest, 2005.

<sup>2</sup> Ua. mint az 1.

## 2) A kritikus infrastruktúra fenyegetettsége és osztályozása

Mint a definícióból látható, a kritikus infrastruktúra (továbbiakban KI) az állam működését és a lakosság biztonságát tekintve létfontosságú elemek halmazából épül fel. Ezeket az elemeket vizsgálva, fenyegetettségük eltérő. Az 1. számú táblázat néhány ország kritikus infrastruktúrához sorolható ágazatait és szektorait mutatja.

Fsz.	KI ágazatok és szektorok	Országok									
		Ausztri	Egy.	Finno.	Francia	Holland	Németo	Olaszo.	Svédó.	Magya	USA <sup>3</sup>
1.	Info- kommunikáció, távközlési szektor	*	*	*	*	*	*	*	*	*	*
2.	Bank és pénzügyi szektor	*	*	*	*	*	*	*	*	*	*
3.	Műsorszórás	*		*							
4.	Katasztrófavédelem	*	*	*			*			*	
5.	Energiatermelés és elosztás	*	*	*	*	*	*	*	*	*	*
6.	Információs, tájékoztató szolgáltatások	*		*							
7.	Honvédelem, fegyveres erő	*	*			*	*			*	
8.	Rendészeti szektor	*	*		*	*	*			*	
9.	Postai szolgáltatás	*		*							*
10.	Közigazgatás, közszolgáltatás	*	*	*		*	*	*			
11.	Közegészségügy	*	*	*	*	*	*	*		*	*
12.	Közjólét	*		*	*						
13.	Szállítás és közlekedés	*	*	*	*	*		*		*	*
14.	Közművek	*		*						*	
15.	Vízellátás	*	*	*	*	*	*	*		*	*

<sup>3</sup> A KI ágazatait és szektorait nem teljesen fedik az európai rendszert.

16.	Terror és szuperterror (ABV) elleni védelem		*								
17.	Élelmiszer ellátás		*	*		*	*			*	*
18.	Védelmi ipar			*							*
19.	Vegyí- és biotechnológiai ipar				*						*
20.	Nukleáris erőművek				*						
21.	Jogrend					*					
22.	Vízminőség biztosítás					*					
23.	Polgári védelem							*			
24.	Földgáz							*			
25.	Elektronikus kormányzás							*			
26.	Országos vezetési /parancsnoki rendszerek								*		
27.	Légtér ellenőrző rendszerek								*		
28.	Távközlés									*	
29.	Mezőgazdaság										*
30.	Tűzoltó, mentő, rendőri szolgálatok (veszélyhelyzeti szolgáltatások)										*
31.	Kormányzati működés										*

#### 1. számú táblázat<sup>4</sup>

A kritikus infrastruktúrához sorolható ágazatok és szektorok  
azonosítása az egyes országokban

A KI ágazatainak és szektorainak fenyegetettsége vizsgálatának szempontjából az alábbi „kihívások” vehetők számításba<sup>5</sup>:

a) háborúk, fegyveres konfliktusok (Öböl háború, délszláv háború, stb.),

<sup>4</sup> Forrás: ua. mint az 1.

<sup>5</sup> A kritikus infrastruktúrák védelmének hazai és nemzetközi szabályozása, a lehetséges veszélyforrások azonosítása és hatásainak elemzése, az infrastruktúra kritikus elemeinek meghatározására alkalmas vizsgálati módszerek. Szakmai vitaanyag. Budapest, 2006.

- b) terrorizmus (2001. szeptember 11-i terrortámadás, stb.),
- c) természeti- és ipari katasztrófák (Cunami, Katrina.. hurrikánok, angliai olajtároló robbanása),
- d) infrastruktúrák teljesítőképességének kimerülése (áramkimaradások a világ több részén, stb.).

A természeti- és ipari (civilizációs) katasztrófák csoportosítását tovább bonthatjuk megjelenési formája<sup>6</sup> szerint:

I. Természeti katasztrófák (elemi csapások):

- A) fizikai jellegű
- B) kémiai jellegű
- C) biológiai jellegű

II. Civilizációs (ipari) katasztrófák:

- A) fizikai jellegű katasztrófa
  - a) tűz-és robbanás veszély előidézői
  - b) mérgezés veszélyek
  - c) vizek által okozott veszélyforrások
  - d) környezetszennyezés
- C) biológiai jellegű katasztrófák
  - a) fertőzés-és járványveszély
  - b) kártevők elszaporodása

III. Közlekedés, szállítás katasztrófák:

- A) a szállítás veszélyforrásai
- B) szárazföldi közlekedésben keletkezett károk
- C) vízi közlekedésben keletkezett károk

---

<sup>6</sup> Elemi csapások, természeti és ipari katasztrófák következményeinek felszámolása. Építéstudományi Tájékoztatói Központ. Budapest, 1984.

D) légi katasztrófák

IV. Társadalmi katasztrófák:

- A) eszmei veszély
- B) társadalmi, gazdasági tervezési hibák,
- C) háborúk

V. Pszichológiai katasztrófák:

- A) stressz hatások,
- B) pszichózis

A veszélyeztető tényezők egymás hatását erősítve is előfordulhatnak (pl. a vizek által okozott károk esetében előfordulhat fertőzés- és járványveszély, tűz- és robbanás veszély esetén előfordulhat stressz hatás). A tényezők kiváltója, lehet maga az ember és lehet a természet egyaránt.

Magyarországon a települések polgári védelmi besorolásához hasonlóan (134/1996. Kormányrendelet) a KI elemei fenyegetettségének besorolását<sup>7</sup> az alábbiak szerint végezhetjük:

- I. kategória: Kiemelten veszélyeztetett infrastruktúra elemek
- II. kategória: Fokozottan veszélyeztetett infrastruktúra elemek
- III. kategória: Veszélyeztetett infrastruktúra elemek
- IV. kategória: Kismértékben veszélyeztetett infrastruktúra elemek

A fent felsorolt osztályozás a KI elemek védelme fontosságának mutatója is egyben. Az osztályozás végrehajtására, a besorolás elkészítésére a jogszabályi háttér ez idáig még nem született meg.

### **3) KI védelmének jogszabályi háttere Magyarországon**

---

<sup>7</sup> Ua. mint az 1.

A KI védelmével kapcsolatban nemzetközi (USA, EU) szinten komoly erőfeszítések folynak. Az EU 2005. novemberében „Zöld Könyv”-ben fogalmazta meg a KI és annak védelmével kapcsolatos programját, és javaslatokat kért a témával szoros összefüggésben megfogalmazott kérdésekre. Magyarország csatlakozott a programhoz. A jogszabályok körének megalkotását már korábban elkezdték, néhány korábbi Kormányhatározat tárgyalja a KI védelmével összefüggő feladatokat, de konkrétan a KI védelmével és hazai szabályozásával kapcsolatban még nem történt meg a jogalkotás.

### **A KI védelmével kapcsolatban korábban megalkotott jogszabályok**

#### **2073/2004. (IV. 15.) Kormányhatározat a Magyar Köztársaság nemzeti biztonsági stratégiájáról**

Az országban a rendszerváltozás óta olyan folyamatok mentek végbe, melyek alapján kimondhatjuk, hogy Magyarország biztonsága szilárd alapokon nyugszik. Alapvető garanciát nyújt a NATO-hoz és az Európai Unióhoz (továbbiakban EU) történt csatlakozás.

A kétpólusú világrend megszűnt ugyan, de megjelentek új típusú biztonsági kockázatok, melyek nem ismernek országhatárokat. Ezek befolyásolhatják az ország biztonságát és nemzetközi környezetét.

A teljesség igénye nélkül csak néhányat ismertetek:

- Globális kihívások: információs technológia, közlekedés, pénzügyek, közegészségügy

- Terrorizmus: destabilizáló hatást gyakorol a nemzetközi viszonyokra (a támogatásukat szolgáló tevékenységek aláássák a nemzetközi rendszer működését)
- Tömegpusztító fegyverek elterjedése: terrorista csoportok kezébe kerülhetnek
- Információs társadalom kihívásai: az informatika világában a számítógépek, az internet használata teljes függőséget okoz mindennapjainkban. A információs és telekommunikációs felzárkózást tovább kell folytatni a fejlett világ szintjére. Az informatikai infrastruktúra feltételeinek biztosítása mellett biztosítani kell e rendszerek védelmét és tartalék képzését. Az informatikai rendszerek sebezhetősége kockázati tényezőt jelent az ország számára.

A Kormányhatározat a kockázati tényezők csökkentése céljából feladatokat fogalmaz meg, melyekből csak a legfontosabbakat —a témához kapcsolódókat— ismertetem:

- Globális fenyegetések és kihívások elleni fellépés: Magyarország számára a nemzetközi szervezetekben való részvétel nyújtja a legjobb védelmet a globális kihívások kezeléséhez.
- Terrorizmus: a terrorizmus anyagi feltételei kialakulásának akadályoztatása, ellehetetlenítése, biztosítva ezzel a KI védelmét.
- Információs rendszerek védelme: biztonságos informatikai infrastruktúra kialakítása, kormányzati információs rendszerek védelme. Kormányzati információs rendszerek felkészítése a kibernetikai támadások kivédésére.
- A természeti és civilizációs környezet védelme: Nemzetközi összefogással a környezeti és közegészségügyi problémák kezelése, melyben aktívan kell részt venni Magyarországnak is.



## **2112/2004. (V. 7.) Kormányhatározat a terrorizmus elleni küzdelem aktuális feladatairól**

A Kormány, a terrorizmus elleni küzdelem aktuális feladataira, egyetértését fejezte ki a jelen kormányhatározat 1. számú mellékletében foglalt II. Terrorizmus Elleni Akciótervvel. A belügyminiszter irányításával tárcaközi munkacsoportot hozott létre.

Az uniós Akcióterv alapján, a KI védelme céljából, feladatul tűzte ki az információs rendszerek elleni támadásokról szóló kerethatározat elfogadását, melyet 2005. február 24-én elfogadtak. Többéves folyamat eredményeként valósítják meg a teljes védett kommunikációs rendszer kialakítását.

Az uniós Akcióterv további lényeges feladata, a polgárok, az alapszolgáltatások védelmének erősítése, valamint felügyeleti, korai figyelmeztető és reagáló mechanizmusok kiépítése a terrortámadások következményeinek kezelése érdekében, valamint a KI fenyegetettségének és ezek védelmi politikájának elemzése. Döntés született a Kritikus Infrastruktúra Védelem Európai Programjának támogatására.

Autonóm magyar intézkedés történt a Nemzeti Válságreakálási Rendszer szabályairól szóló kormányrendelet kidolgozására és elfogadására. A nemzeti rendszer úgy kerül kialakításra, hogy az összhangban áll a NATO válságkezelési rendszerével és a EU válságkezelési mechanizmusával.

## **2151/2005. (VII. 27.) Kormányhatározat a Terrorizmus Elleni Akcióterv felülvizsgálatáról**

A Kormány egyetért a II. Akciótervvel, és elrendeli a benne foglalt intézkedések végrehajtását.

Végre kell hajtani a KI fenyegetettségnek és ezek védelmi politikáinak elemzését. Az elemzés alapján meg kell tenni a szükséges intézkedéseket. Fel kell készülni a KI Védelem Európai programjának támogatására.

Szakértőt kell kijelölni a Kritikus Infrastruktúra Figyelmeztető Információs Hálózatba.

#### **4) Speciális erősítési létesítmények alkalmazása, hasznosítása a KI védelme céljából**

##### **a) Speciális erősítési létesítmények helyzete**

###### **Védelmi felülvizsgálat hatása**

A Magyar Honvédség védelmi felülvizsgálatát 2003-ban hajtották végre abból a célból, hogy egy kisebb létszámú és költségvetésű, képességalapú hadsereg létrehozására tegyenek javaslatot.

Az ország gazdasági teherbíró képessége olyan ponton van, hogy a jelenlegi haderő szerkezettel a Magyar Honvédség finanszírozhatatlanná válhat.

1999. óta tagja vagyunk a NATO-nak, 2004. óta pedig az EU-nak. Érdekeink érvényesítésének színtere e két szervezet. Sőt, a NATO és tagországai ellen hagyományos jellegű támadással nem kell számolni, továbbá az Észak-atlanti szervezet tagjaként, Magyarországra is vonatkozik a Szervezet V. cikkelye.

Egy fontos tényről viszont nem szabad megfeledkezni. A hidegháború befejezésével valóban csökkent a fix, nem telepíthető vezetési elemek (bunkerek, vezetékes híradás) jelentősége –mivel ezek a szervezeti elemek korábban háborús idősakra voltak tervezve-, azonban a már említett új típusú kihívások néhány tényezője azt mondatja, hogy ezt célszerű volna újra

átgondolni, és mint védelmi elemeket bevonni a KI védelme céljából megvalósítandó magyarországi programba.

A védelmi felülvizsgálat alapján elkészült az a kormányhatározat, melynek következménye lett ezen szervezeti elemek megszüntetése.

### **2236/2003. (X. 1.) Kormányhatározat a Magyar Honvédség 2004-2013 közötti időszakra vonatkozó átalakításának és új szervezeti struktúrájának kialakításáról**

A nevezett Kormányhatározatban írták elő azokat a feladatokat, melyeket az új képességalapú haderő létrehozása céljából kell végrehajtani.

Az ország biztonságát a szövetség rendszerében kell értelmezni. Ebből következően —az új típusú biztonsági kihívások ellenére— a Magyar Köztársaságot várhatóan az elkövetkező 10 évben nem fenyegeti hagyományos támadás veszélye.

Konkrét feladatként került megfogalmazásra a védett vezetési rendszer fenntartása szükségességének a vizsgálata, valamint annak egyes elemei más, különösen válságkezelési célra történő alkalmazásának a lehetősége.

Ennek következményeként további Kormányhatározat rendelkezett az egyes speciális erődítési létesítmények sorsáról. Mivel az állam ezek fenntartását költségesnek tartja és nemzeti értékeket is jelentenek, feladatként jelentkezett a létesítmények hasznosítása, békeidőszaki alkalmazási lehetőségeinek keresése, mely jelenleg is tart.

#### **b) Speciális erődítési létesítmények hasznosítása**

A speciális erődítési létesítményeket a hidegháború idején hozták létre. Kezdetben csak óvóhelyeket építettek, majd egyre nagyobb igény mutatkozott arra, hogy ipari üzemek (hadiüzemek), pályaudvarok területén is épüljenek

bomba- gáz- szilánk (ún. BGS típusú óvóhelyek) ellen védő óvóhelyek. Később már több országos hatáskörű szerv építetett hasonló védelmet saját szervezete részére. Épültek olyan óvóhelyek, melyekbe kialakításra került a kor színvonalának megfelelő teljes kommunikációs és távközlési rendszer, védettsége pedig az atombomba hatásai ellen is védelmet biztosított. Ebben az időben került sor az állami és a honvédelmi vezetés részére történő ún. vezetési pontok építésére is.

A rendszerváltás után megváltozott a politikai helyzet. A kétpólusú világrendszer megszűnt, elmúlt egy totális atomháború veszélye, viszont kialakultak más, új típusú biztonsági kihívások, fenyegetések, melyeket már korábban említettem.

Mivel a speciális erősítési létesítmények háborús időszakra voltak tervezve, jelentőségük a rendszerváltás után csökkent. Az új típusú kihívások viszont más feladatokat fogalmaztak meg a szakemberek számára. Az utóbbi néhány évben előtérbe kerültek a kritikus (létfontosságú) infrastruktúrák védelmének vizsgálata, melyre nyomós ok volt a 2001. szeptember 11. terrortámadás.

A speciális erősítési létesítmények, a kritikus infrastruktúrák egyes elemei részére képesek teljes körű védelmet biztosítani, továbbá képesek más békeidőszaki feladatok ellátására is.

### **1) Információs rendszerek védelme**

Ezt a témát a 3. fejezetben már érintettem. Jelenleg a számítógépek és az informatika világában élünk, melyek meghatározzák mindennapjaink életét. Szinte már számítógép „függőségben élünk”. De nem csak a hétköznapi ember számára fontos az információhoz való hozzáférés, hanem talán még fontosabb a gazdasági-és az üzleti élet, valamint a kormányzati működés számára. Éppen

ezért, az ország működése szempontjából fontossá vált az adatok biztonságos tárolása és az adattárolók biztonságos helyen történő elhelyezése.

A gazdaságfelkészítési tervezés és a gazdaságmozgósítási tevékenység<sup>8</sup> hatékony támogatása érdekében a gazdasági és közlekedési miniszter a nemzetgazdaság folyamatait leíró aktuális információk fogadására kész, megfelelő jogosultsággal közvetlen hozzáférést biztosító adatbázisokat, valamint állandó telepítésű és hordozható számítógépeket tartalmazó, központi állomásból és a tervező szerveknél kihelyezett munkaállomásokból álló informatikai rendszert működtet.

Egy-egy adatbázis illetéktelen kezekbe kerülése óriási méretű károkat okozhat. De említeni lehet pl. a társadalombiztosítás adatainak elvesztését. Sajnos az adatbázisok csak egy tárolóra vannak mentve. Nem történik meg a tartalék adattárolóra történő mentés. Így az egyetlen tároló sérülése adatvesztést von maga után. Ennek kiküszöbölésére, szerverfarmokat kell létrehozni, melyeket egymástól elkülönítetten, földrajzilag nagy távolságra kell elhelyezni, a nagyobb biztonság céljából (pl. Ausztria).

A nyugati országokban erre a célra már alkalmazzák a védett létesítményeket.

Az Interneten szolgáltatásként is hirdetik egyes szervezetek a védett létesítmények alkalmazását<sup>9</sup>:

*„Létesítményünk, mely a földkéreg monolit rétegében, egy folyamatos, több kilométer hosszú és mély geológiai képződményben van elhelyezve, a szikla kemény védelmet biztosít az Ön adatai részére. Ez direkt erre a célra épített létesítmény képes a Richter-skála szerinti 9,5—ös földrengés hatásainak elviselésére. 40 méteres mélységével úgy jellemzik, mint az északi Fort Knox-ot.”*

---

<sup>8</sup> 131/2003. (VIII.) Korm. rendelet a nemzetgazdaság védelmi felkészítése és mozgósítása feladatai végrehajtásának szabályozásáról. Hatályos Jogszabályok Gyűjteménye. 2004. dec. 16.

<sup>9</sup> <http://www.nfti.com/ccdrs.html>

*„Az év minden napján, 24 órában működő biztonsági rendszer biztosítja a bio érzékelést, és zárt láncú televíziós megfigyelést, kártyás beléptetést, valamint a számítógéppel vezérelt vibrációs és mozgásérzékelést.”*

Az USA-ban már 2002-ben komolyan foglalkoztak egy lehetséges kibertámadás esélyének következményeivel<sup>10</sup>. USA-t jelképező cégoriasoknak (GE, GM, IBM, stb.) célszerű volna egy biztonságos csatornát kiépíteni az óriás cég és a helyi FBI igazgatósága között, javasolta egy hírszerző.

Egy fizikai támadást követő kibertérből érkező támadás alapjaiban rengetheti meg az országot, és ezermilliárd dollár nagyságrendű károkat is képes okozni a nemzetgazdaságnak.

## **2) Stratégiailag fontos anyagi készletek (gyógyszerek, eszközök, élelmiszerek, stb.) tárolása**

Az anyagi javak védelme a történelem folyamán mindig lényeges kérdés volt. A nagy háborúk alkalmával úgy a hadsereget, mint a lakosságot el kellett látni élelemmel, fegyverekkel, ruházattal, stb., és nem csak a személyek védelmére alakítottak ki óvóhelyeket, hanem az előbb felsorolt anyagok védelme céljából is.

A speciális erődítési létesítmények kitűnően alkalmazhatók tárolási, raktározási feladatok végrehajtására is, az anyagok frissítő cseréjét is meg lehet oldani.

Ide tartoznak a nemzetgazdaság inósített időszakai működését biztosító anyagok, eszközök.

A Kormány a gazdaságmozgósítási igények biztonságos kielégítése érdekében védelmi célú állami tartalékokat tart fenn

---

<sup>10</sup> [http://www.szt.hu/hirek\\_hir.php?id=29093](http://www.szt.hu/hirek_hir.php?id=29093)

Ezek<sup>11</sup>:

- ipari termékek, eszközök, különösen haditechnikai, hadfelszerelési és közlekedési eszközök,
- hírközlési és informatikai eszközök,
- egészségügyi és gyógyszeripari termékek, gyógyászati eszközök,
- vízügyi és árvízvédelmi termékek,
- pénzeszközök.

A védelmi célú állami tartalékon csoportjába az alábbiak tartoznak:

- *Gazdaságbiztonsági tartalék* (a nemzetgazdaság működését, lakossági alapellátást és védelmét szolgáló, valamint a fegyveres erők és rendvédelmi szervek feladatai végrehajtását szolgáló ipari és félkész termékek, alapanyagok, termékek),
- *Állami egészségügyi tartalék*, fegyveres erők és rendvédelmi szervek minősített időszakos és katasztrófa sérültjeinek ellátásához (gyógyszerek, orvostechnikai eszközök, gyógyászati segédeszközök, szükséggyógyintézetek felszereléseinek készletezése),
- *Állami Céltartalékok*, egyes minisztériumok minősített időszakos ágazati feladatai ellátásához szükséges anyagok (termelési, szolgáltatási, helyreállítási tevékenységhez szükséges, anyagok, alkatrészek, félkész és késztermékeket tartalmazó készletek),
- *Deviza és pénztartalékkészlet*, az ország pénzforgalmának mindenkor zavartalan biztosításához szükséges bankjegytartalék.

---

<sup>11</sup> Ugyan az mint a 8.

Finnországban több olyan gyár létezik, melyet hasonló létesítményekben alakítottak ki, és a védelmi szféra részére gyárt különleges mérőeszközöket.

A nagy terekből átépítéssel kialakíthatók akár több szintű tároló helyek is. Némi korlátozást jelenthet a bejáratok mérete, éppen ezért a kiválasztott termék dimenzióit pontosan ismerni kell.

### **3) Nemzeti kincsek védelme, irat-és levéltárak kialakítása**

Legtöbb múzeum azzal a problémával küzd, hogy drága, történelmi ereklyéket, festményeket és műkincseket poros, nedves pincékben, közművezetékek által behálózott folyosókon kell tárolni. Az irat-és levéltárak esetében hasonló a helyzet. Egyes levéltári anyagokról mikrofilmet készítenek a könnyebb tárolás céljából. Megfelelő tároló szerkezetek kialakításával ezek az értékek biztonságos elhelyezést kaphatnak a védett létesítményekben.

### **4) Műsorszóró és távközlési rendszerek védelme**

A nevezett rendszerek esetében léteznek olyan berendezések, melyek fizikai sérülése esetén megbéníthatják az ország tömegtájékoztatási rendszerét. Nyilván egy antennarendszert nem lehet elhelyezni létesítményben, de a teljes informatikai és elektronikai háttérét igen. Így egy fix telepítésű antenna megsemmisülése esetén a kiváltására alkalmazható egy járműre szerelt antenna is. Ebben az esetben csak megfelelő csatlakozási pontot kell kialakítani és akár műholdas összeköttetés is biztosítható.

### **5) Békétől eltérő (minősített) időszak feladatok végrehajtása**

Alapvető követelmény, hogy a kormányzat részére a vezetés, az irányítás és a biztonságos működés feltételeit biztosítani kell. A gazdaságossági szempontok és a biztonsági feltételek, valamint a folyamatos üzem fenntartása



érdekében az informatikai és távközlési rendszerek békében is működnek. Minősített időszakban a biztonságot szervezési (adminisztratív) intézkedésekkel és technikai eszközökkel hozzák az időszak követelményeinek szintjére.

### **Összességében**

Valamennyi létesítményről elmondható, hogy szigorúan előírt klímaparaméterek segítségével biztosíthatók a belső levegő állapotjelzői, melyek az elhelyezett anyagok fajtájának függvényében tovább szabályozhatók. Különleges értékek esetében további lokális klímaberendezés telepíthető a helyiségekbe.

#### **4) A KI ágazatai Magyarországon**

A „Zöld Könyv”, a KI szolgáltatásainak és szektorainak azonosítására a 2. számú táblázatban bemutatott javaslatot teszi, melytől el lehet térni az adott ország sajátosságait figyelembe véve, de mindenképpen fontos feladat végrehajtani felmérni, az egyes ágazatokon belüli KI szektorokat és azok elemeit. Mivel a KI-t tartalmazó ágazatok eltérőek, nehéz volna előírni, milyen szempontok szerint kell megvédeni azokat. Ezért ágazatonként célszerű kidolgozni védelmüket. Az is biztos, hogy minden elemet (terméket) nem lehet elhelyezni védett létesítményben, sőt az egyes elemek védelmét is csak a legkülönbözőbb módon lehet kialakítani.

Szektor	Termék vagy szolgáltatás
I. Energia	1. Kőolaj és földgáztermelés, finomítás, kezelés és tárolás, csővezetékekkel együtt 2. Villamosenergia termelés 3. Villamosenergia, gáz és kőolaj szállítás 4. Villamosenergia, gáz és kőolaj elosztás
II. Információs és kommunikációs technológiák (ICT)	5. Információs rendszerek és hálózatok védelme 6. Műszeres, automatizálási és vezérlőrendszerek (pl. SCADA) 7. Internet 8. Fix távközlési szolgáltatás 9. Mobil távközlési szolgáltatás 10. Rádióhírközlés és navigáció 11. Műholdas hírközlés 12. Műsorszórás
III. Víz	13. Ivóvíz szolgáltatás 14. vízminőség szabályozás 15. Vízmenyiség biztosítása és szabályozása
IV. Élelmiszerügy	16. Élelmiszer biztosítás és élelmiszerbiztonság őrzése
V. Egészségügy	17. Orvosi és kórházi ellátás 18. Gyógyhatású készítmények, szérumok, oltóanyagok és gyógyszerek 19. Biolaboratóriumok és biológiai hatóanyagok
VI. Pénzügy	20. Pénzügyi szolgáltatások és rendszerek (privát) 21. Kormányzati pénzügyi rendszer
VII. Jogi és közrend biztonság	22. Jogi és közrend, közbiztonság fenntartása 23. Igazságszolgáltatás és büntetés-végrehajtás irányítása
VIII. Polgári közigazgatás	24. Állami funkciók 25. Fegyveres erők 26. Polgári közigazgatási szolgáltatások 27. Veszélyhelyzeti szolgáltatások 28. Postai és futárszolgáltatások
IX. Közlekedés	29. Közúti közlekedés 30. Vasúti közlekedés 31. Légi közlekedés 32. Belvízi közlekedés 33. Tengeri hajózás
X. Vegyi és nukleáris ipar	34. Vegyi és nukleáris anyagok előállítása és tárolása/feldolgozása 36. Veszélyes áruk (vegyi anyagok) csővezetékei
XI. Világűr és világűr kutatás	36. Világűr 37. Világűr kutatás

**2. számú táblázat<sup>12</sup>**  
**Zöld Könyv által javasolt kritikus szektorok**

<sup>12</sup> Forrás: Európai Közösségek Bizottsága: Zöld Könyv a kritikus infrastruktúra védelem európai programjáról. COM(2005) 576 final. Brüsszel, 2005.

## **Magyarországon a KI ágazatai és szektorai az alábbiak<sup>13</sup>:**

- 1) Informatikai és kommunikációs rendszerek,**
- 2) Távközlés,**
- 3) Energiatermelés és elosztás,**
- 4) Vízellátás-közművek,**
- 5) Szállítás és közlekedés,**
- 6) Közegészségügy,**
- 7) Élelmiszer ellátás,**
- 8) Bank-és pénzügyi szektor,**
- 9) Katasztrófavédelem,**
- 10) Honvédelem-védelmi ipar,**
- 11) Rendészeti szektor.**

Mindegyik ágazat és szektor működése az informatikán alapul, ezért a védelem kialakítását megítélésem szerint innen kell kezdeni.

Az informatikai rendszerek terjedésével a hálózatok bővülésével egyre nehezebbé válik az informatikai eszközök biztonságának fenntartása. Minél többen kerülnek kapcsolatba az informatikával, annál nagyobb az esély a nemkívánatos jelenségek kialakulására.

Egy informatikai rendszer számtalan pontján és sokféle módon támadható, ezért a védekezés helye és módja nehéz. A támadás<sup>14</sup> és a védelem célpontja az adat, mint az információt hordozó elem. A támadások azonban közvetve érik az adatokat, az őket körülvevő rendszerelemeken (hardver, szoftver, környezeti infrastruktúra) keresztül.

---

<sup>13</sup> Ua. mint az 1.

<sup>14</sup> Támadás alatt kell érteni minden olyan fenyegetést, mely a rendszer megbízható működését, az adatok rendelkezésre állását és az eszközök követelmények szerinti működést veszélyezteti.

Az adatot az alábbi rendszerelemek veszik körül:

- szoftver,
- hardver,
- hálózati elemek,
- adathordozók,
- dokumentációk,
- a rendszer fizikai környezete és infrastruktúrája,
- külső és belső személyi környezet.

A rendszerelemekre hatnak azok az alapfenyegetések, amelyek miatt az adatok által hordozott információk védelmét kell biztosítani.

Ezért a védelmi intézkedéseket a rendszerelemekhez kell kapcsolni.

## **Befejezés**

A védett földalatti létesítmények, a védelem egy lehetőségét kínálják a KI egyes elemeinek részére. A földalatti létesítmények esetenként vonzóak lehetnek, amikor az észlelt fenyegetettségi szint, vagy a veszteségek következményei súlyosak, és a sebezhetőség nem szüntethető meg a rendszer redundanciájával, vagy más nem építészeti intézkedésekkel. Bár az épületek megerősíthetők a földrengésekből, robbanásokból, vagy balesetektől adódó szerkezeti sérülések ellen, egy fenyegetettségi szint, vagy szerkezeti terhelés fölött a megerősített földfeletti szerkezetben lévő kritikus elemek védelme többbe kerülhet, mint egy földalatti létesítmény építése.

## Felhasznált irodalom

1. Use of Undergrond Facilities to Protect Critical Infrastucture. Summary of a Workshop. 1998. Rome.
2. Pásztor Péter: A speciális erődítési (védett) létesítmények béke időszaki alkalmazásának lehetőségei. Kard és toll. Válogatás a hadtudomány doktoranduszainak tanulmányaiból. Honvédelmi Minisztérium Oktatási és Tudományszervező Főosztály. Budapest, 2004/1.
3. Dr. Kovács Ferenc: Az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére vonatkozó intézkedési javaslatok kidolgozása. Tanulmány. Budapest, 2005.
4. 2073/2004. (IV. 15.) Kormányhatározat a Magyar Köztársaság nemzeti biztonsági stratégiájáról. Hivatalos CD Jogtár. 2005/5.
5. 2112/2004. (V. 7.) Kormányhatározat a terrorizmus elleni küzdelem aktuális feladatairól. Hivatalos CD Jogtár. 2005/5.
6. 2151/2005. (VII. 27.) Kormányhatározat a Terrorizmus Elleni Akcióterv felülvizsgálatáról. Hivatalos CD Jogtár. 2005/5.
7. 2236/2003. (X. 1.) Kormányhatározat a Magyar Honvédség 2004-2013 közötti időszakra vonatkozó átalakításának és új szervezeti struktúrájának kialakításáról. Hivatalos CD Jogtár. 2005/5.
8. [http://www.szt.hu/hirek\\_hir.php?id=29093](http://www.szt.hu/hirek_hir.php?id=29093)
9. Forrás: Európai Közösségek Bizottsága: Zöld Könyv a kritikus infrastruktúra védelem európai programjáról. COM(2005) 576 final. Brüsszel, 2005.
10. 131/2003. (VIII.) Kormányrendelet a nemzetgazdaság védelmi felkészítése és mozgósítása feladatai végrehajtásának szabályozásáról. Hatályos Jogszabályok Gyűjteménye. 2004. dec. 16.

11. Elemi csapások, természeti és ipari katasztrófák következményeinek felszámolása. Építéstudományi Tájékoztatási Központ. Budapest, 1984.
12. Szakértők egy lehetséges kibertámadás esélyének következményeiről. COMPUTERWORLD. [http://www.szt.hu/hirek\\_hir.php?id=29093](http://www.szt.hu/hirek_hir.php?id=29093)
13. Bodlaki Ákos. Az informatikai biztonság tervezési kérdései. Informatika a Felsőoktatásban '96 – Networkshop '96 Debrecen, 1996. augusztus 27-30.
14. Gazdasági és Közlekedési Minisztérium Védelem-koordinációs Főosztály: A kritikus infrastruktúrák védelmének hazai és nemzetközi szabályozás, a lehetséges veszélyforrások azonosítása és hatásainak elemzés, az infrastruktúra kritikus elemeinek meghatározására alkalmas vizsgálati módszerek. Szakmai vitaanyag. Budapest, 2006.
15. <http://www.nfti.com/ccdrs.html>