

Doktori (PhD) értekezés

Pataki János

2017

NEMZETI KÖZSZOLGÁLATI EGYETEM

Hadtudományi Doktori Iskola

Pataki János

Terrorizmus, mint biztonsági probléma, a kritikus infrastruktúra
védelmi szabályainak tükrében

Doktori (PhD) értekezés

Témavezető:

Dr. Resperger István ezredes

.....

Budapest, 2017

TARTALOMJEGYZÉK

BEVEZETÉS	6
1. FEJEZET:	14
TERROZMUS, MINT GLOBÁLIS BIZTONSÁGI PROBLÉMA ÉS A FENYEGETÉSEK EGYIK LEGFŐBB ELEME	
1.1. GLOBÁLIS BIZTONSÁGI KIHÍVÁSOK	14
1.2. TERRORIZMUS TERMÉSZETE	30
1.3. ÖSSZEGZÉS, KÖVETKEZTETÉSEK	41
2. FEJEZET:	43
TERRORIZMUS PROBLÉMÁI	
2.1. TERRORIZMUS HATÁSA A VILÁG GAZDASÁGÁRA	43
2.1.2. TERRORIZMUS HATÁSA A KRITIKUS INFRASTRUKTÚRÁK MŰKÖDÉSÉRE	50
2.2. TERRORIZMUS ELLENI KÜZDELEM RÉSZTVEVŐI	51
2.2.1. Kormányzati (titkosszolgálati és rendészeti) feladatok	51
2.2.2. Civil biztonsági és más vállalatok feladatai	59
2.2.3. Védelmi képességfejlesztés és beruházás költségeinek viszonya	60
2.3. ÖSSZEGZÉS, KÖVETKEZTETÉSEK	67
3. FEJEZET:	68
NEMZETKÖZI VÁLLALATOK VÉDELMI RENDSZERE	
3.1. A KRITIKUS INFRASTRUKTÚRA ÁLTALÁNOS VÉDELMI SZABÁLYAI	69
3.1.1. Kritikus infrastruktúrák védelmének nemzetközi és nemzeti szabályozása	69
3.2. BIZTONSÁGI HELYZET ÉS BIZTONSÁGPOLITIKA	81
3.2.1. Biztonsági stratégia	81
3.2.2. Biztonságpolitika	83

3.2.3. Biztonsági szervezetek szakpolitikái	87
3.3. ÁLTALÁNOS BIZTONSÁGI KÖVETELMÉNYRENDSZER KIALAKÍTÁSA	103
3.3.1. Biztonsági szervezetek	103
3.3.2. Általános biztonsági intézkedések	104
3.3.3. Biztonság- és védelempolitika	123
3.4. BIZTONSÁGI SZERVEZETEK OPERATÍV FELADATAI	125
3.4.1. Tűzvédelem	125
3.4.2. Katasztrófavédelem	130
3.4.3. Iparbiztonság	131
3.4.4. Vagyonvédelem	132
3.5. BIZTONSÁGI RENDSZEREK INTEGRÁLT ALKALMAZÁSA	137
3.5.1. Tűzvédelmi rendszerek	137
3.5.2. Vagyonvédelmi rendszerek	142
3.5.3. Telekommunikációs rendszerek	147
3.5.4. Biztonsági rendszerek integrálása	148
3.6. OBJEKTUMOK ÉS ÉPÜLETEK TERRORROBBANTÁS ELLENEI VÉDELMEK SZABÁLYAI	149
3.6.1. Anti-terrorista minimum szabályozás az épületek védelméhez	150
3.6.1. Anti-terrorista intézkedések integrált megvalósítása	151
3.7. OBJEKTUMOK TERRORTÁMADÁSOK ELLENEI VÉDELME	154
3.7.1. Terrorelhárítás elvei	158
3.7.2. Védelmi fokozatok	165
3.8. ÖSSZEGZÉS, KÖVETKEZTETÉSEK	167
 4. FEJEZET:	 167
EGY NEMZETKÖZI VÁLLALAT HELYZETELEMZŐ ÉS VÁLSÁGKEZELŐ KÖZPONTJÁNAK MŰKÖDTETÉSE	
4.1. HELYZETELEMZŐ ÉS VÁLSÁGKEZELŐ KÖZPONT	167

4.1.1. Vállalati válságkezelés elve	167
4.1.2. Helyzetelemző és válságkezelő központ szervezeti felépítése, feladatai ..	170
4.1.3. Válságkezelő szervezetek felépítése és feladatai	172
4.2. HELYZETELEMZŐ ÉS VÁLSÁGKEZELŐ KÖZPONT RENDSZEREI	181
4.2.1. Biztonsági rendszerek felügyelete	181
4.2.2. Térinformatikai és egyéb információs rendszerek alkalmazása	184
4.2.3. Riasztási feladatok	185
4.3. SITCEN VÉDELME	186
4.3.1. Szervezeti intézkedések	187
4.3.2. Mechanikai védelem	188
4.3.3. Elektronikus biztonsági rendszerek	189
4.3.4. Beléptetés rendje	189
4.3.5. Információvédelem	191
4.4. ÖSSZEGZÉS, KÖVETKEZTETÉSEK	193
BEFEJEZÉS	195
FELHASZNÁLT IRODALOM	203
RÖVIDÍTÉSEK JEGYZÉKE	216
DIAGRAMMOK, ÁBRÁK, TÁBLÁZATOK JEGYZÉKE	221
MELLÉKLETEK	223
PUBLIKÁCIÓS JEGYZÉK	269
SZAKMAI-TUDOMÁNYOS ÖNÉLETRJAZ	270

BEVEZETÉS

„Minden diverzió olyan vidékre viszi a háborút,
ahová az nem jutott volna el nélküle;”¹

Carl von Clausewitz

A tudományos probléma megfogalmazása

A terrorizmus célja a félelem- és pánikkeltés, a demokratikus társadalmi és politikai intézményrendszerekbe vetett hit és bizalom gyengítése, megkérdőjelezése. A terrorista mozgalmak nem fogadják el a demokratikus értékrendet, illetve destabilizáló hatást gyakorolnak a történelmileg kialakult nemzetközi rendszerre és viszonyokra.²

A témaválasztásomat a megváltozott világpolitikai és európai biztonsági helyzet indokolja. Az iszlám³ nevében fellépő fundamentalista⁴ és militáns csoportok veszélyforrást és biztonsági kockázatot jelentenek a demokratikus államok értékközösségére. Az európai államok fenyegetettsége folyamatosan változik. A terrorfenyegetettség kapcsán egy országgal kapcsolatban csak trendeket vázolhatunk fel. Természetesen a fenyegetettség mértéke országonként változik.⁵ Az iszlám nem fenyegeti a nyugati civilizáció létét, de a XXI. század elején minden államban, amely jelentős iszlám kisebbséggel rendelkezik

¹ Carl von CLAUSEWITZ: *A háborúról*, Zrínyi Kiadó, Budapest, 2013, pp. 622.

² Samuel P. HUNTINGTON: *A civilizációk összeecsapása és a világtrend átalakulása*, Európa Kiadó, 2006, pp. 58-61, [...] „A nyugati civilizáció kialakulásának idejét rendszerint i.sz. 700-ra vagy 800-ra teszik. A tudósok általában három fő alkotórészét különböztetik meg, az európai, az észak-amerikai és latin-amerikai. [...] Latin-Amerikának külön identitása van, mely megkülönbözteti a Nyugattól. Bár az európai civilizáció leszármazottja, Latin-Amerika Európától és Észak-Amerikától igen eltérő úton fejlődött tovább. [...] Latin-Amerikát tekinthetjük a nyugatihoz tartozó egyik alcivilizációnak, ugyanakkor olyan külön civilizációként is számolhatunk vele, amely szorosan kötődik a Nyugathoz tartozik-e vagy sem. [...] A Nyugat magába foglalja tehát Európát, Észak-Amerikát, továbbá más európai telepések által létrehozott országokat, így Ausztráliát és Új-Zélandot. [...] Amikor aztán az Egyesült Államok kilépett a világpolitika porondjára, kialakult egy tágabb azonosulás Európával. Míg a 19. századi Amerika Európától különbözőként és vele szembenállóként definiálta önmagát, addig a 20. századi Amerika egy tágabb identitás, az Európát is magába foglaló Nyugat részeként, sőt annak vezetőjeként szerepel.”

³ Ziauddin SARDAR – Zafar Abbas MALIK: *Introducing Islam*, Icon Books UK - Totem Books USA, © SZAKÁCS Gergely – Hungarian translation, Edge 2000 Kiadó, pp.4. ISBN 963 86450 7 5,

⁴ Karen AMSTRONG: *Az iszlám*, A Weidenfeld & Nicolson book, Hungarian translation © Péri Benedek, Európa Kiadó, Budapest, 2005, pp. 259 - 274

⁵ TÁLAS Péter: *A nemzetközi terrorizmus és a szervezett bűnözés hatása a nemzetközi biztonságra és Magyarország biztonságára*, MTA Társadalomtudományi Kutatóközpont Kisebbségkutató Intézet, 2007. január. pp.11 - 16,

Európában, érezhetően megnövekedett az iszlám lakosság körében a fundamentalista szellemi, kulturális és társadalmi mozgalmak befolyása.⁶

A terrororganizációk fokozottan veszélyeztetik az államok és a nemzetközi intézmények működését. Ez újabb és mélyebb politikai, gazdasági, kereskedelmi, migrációs és egészségügyi válságok kialakulásához vezethet. A terrorizmus és a szervezett bűnözés között az együttműködés egyre szorosabb⁷. A terrororganizációk a pénzügyi forrásaik⁸ beszűkülése miatt jól működő kapcsolatrendszert építettek ki a különböző kábítószerrel, fegyverkereskedelemmel, gépjármű- és embercsempészettel foglalkozó bűnszervezetekkel, azonban a terrorizmus és a szervezett bűnözés céljai jelentősen eltérnek egymástól.

Liddel Hart (2002) szerint „A gerillaháborút kevesen vívják, de sokak támogatásától függ. Bár önmagában ez a legindividuálisabb tevékenységfajta, csak akkor hatékony, és csak akkor éri el célját, ha a tömegek támogatása áll mögötte.”⁹ Liddel Hart e gondolatait erősíti meg Hans-Georg Maßen a Német Alkotmányvédelmi Hivatal elnökének kijelentése, mely szerint 2014-ben kb. 400 aktivista harcol az Iszlám Állam oldalán Közép-Kelten (IÁ)¹⁰. Németországban 6000 aktív szalafistáról és 40.000 aktív támogatóról tudott a szolgálat, valamint a németországi iszlám közösség közel 10%-a egyetért a szalafisták irányvonalával.¹¹ A terrorizmus elleni felderítő munkát nagyon megnehezíti, hogy a szervezetek zártak és laza hálózatot alkotnak. A szervezetek által létrehozott sejtek vagy csoportok sok esetben csak egy meghatározott feladatra jönnek létre.

⁶ NATIONAL INTELLIGENCE COUNCIL „ *Mapping the Global Future - Projekt 2020*”, , Pittsburgh, 2004, pp. 83 –92, ISBN 0-16-073-218-2, Az „Új Kalifátus” fejezet bemutatja, miként értékelendek el a nyugati értékek, amennyiben megerősödnek egyes radikális, fundamentalista vallási csoportok. A kultúrák közötti ideológiai viták felerősödnek, a nyugati világ információs társadalma és a muzulmán világ közötti ellentétek elmélyülnek.

⁷ EURÓPAI BIZOTTSÁG: *Európai biztonsági stratégia: Biztonságos európa egy jobb világban*, Európai Unió Kiadóhivatala, Luxemburg, 2009, pp. 12, ISBN 978-92-824-2427-8

⁸ Prof. Dr. PADÁNYI József: *Az aszimmetrikus hadviselés során alkalmazandó eljárások, eszközök és módszerek*, HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 25: (1-2) pp. 82.

⁹ B.H. Liddel HART: *Stratégia*, Európa Könyvkiadó, Budapest, 2002, p. 559.

¹⁰ 2004-ben Irakban alakította meg Abu Muszab al-Zarkavi, Iraki al-Kaida néven (Al-Qaeda in Iraq, „AQI”). 2006-tól vezetését Abu Bakra l-Bagddadi vette át, de már új névvel Iraki Iszlám Állam (Islamic State of Iraq „ISI”). 2013-14 között a nevet a megszerzett befolyási övezetek és az elfoglalt területek miatt, Iraki és Levantei Iszlám Államra (Islamic State of Iraq and the Levant, „ISIL”), majd átnevezték Iraki és Szíriai Iszlám Államra, (Islamic State Iraq and Syria, „ISIS”) változtatták, majd 2014 nyarán bejelentették az Iszlám Állam/Kalifátus (Islamic State, „IS”) megalakítását.

¹¹Verfassungsschutzbericht 2013, p. 191-205., www.verfassungsschutz.de/download/vsbericht-2013.pdf (Letöltve: 2014.08.25.)

A terrrorszervezetek finanszírozása fedő intézményeken keresztül valósul meg, működésük alkalmazkodik az adott térség biztonsági környezetéhez.¹²

A gazdasági globalizáció az egyik legjelentősebb nemzetközi trend. A világgazdaság 2050-re 300%-kal lesz magasabb, mint 2005-ben volt, az egy főre jutó átlagos jövedelem pedig 240%-kal emelkedik¹³. Ezekből az adatokból arra lehet következtetni, hogy a gazdaság biztonságos működése nagyban befolyásolja az emberiség jólétét az egész világon, ezért fontos most és a jövőben a világgazdaság biztonsága. Gazdaságbiztonsági szempontból a kritikus infrastruktúrák védelmének megvalósításában az állam partneri együttműködést törekszik kialakítani az infrastruktúra-működtető tulajdonosokkal. Egy megfelelő kockázatelemzés alapján kell a tulajdonosok védelmi ráfordításainak és felelősségvállalásának mértékét meghatározni.

A magyarországi állapotokra jellemző, hogy az igazgatási, jogszabály előkészítési és végrehajtási, valamint a vállalatok alkalmazói szintjén eltérő a szakmai felfogás és nincs teljes körű egyetértés¹⁴. Ez értelemszerűen adódik abból, hogy minden résztvevő a saját szempontjai szerint kívánja optimalizálni a végrehajtás folyamatát. Erre a legszemléletesebb példa, hogy Magyarországon jelenleg nem fogalmazznak meg általános előírásokat, hogyan lehet/kell kialakítani a különböző objektumok és épületek védelmét. A terrorrobbantások, valamint a terrortámadások elleni védelem az integrált védelmi rendszer szerves részét képezi. Megfelelő válságkezelés hiányában, a fundamentalista vallási irányzatok terrortámadásai teszik leginkább sebezhetővé politikai és gazdasági szempontból a fejlett infrastruktúrával rendelkező nemzetállamokat.¹⁵

¹² Dr. RESPERGER István: *Az iszlám világ és hatása a biztonságra*, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003., pp. 54 – 55.

¹³ David GREGOSZ: *Wirtschaftspolitische Megatrends bis 2020*, Konrad-Adenauer-Stiftung, Bellin, 2012, ISBN 978-3-944015-02-6, pp. 7.

¹⁴ A vállalatok saját munkavállalói, akik a biztonsági és védelmi feladatokat szervezik és irányítják, optimális esetben külön szervezeti egységként a felsővezetésnek van közvetlenül alárendelve, valamint a különböző magán biztonsági vállalkozások, amelyeknek főprofilja a különböző biztonsági tevékenységek.

¹⁵ Dr. RESPERGER István mk. ezredes: *Biztonsági Kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig*, KNBSZ, Felderítő Szemle, 2013/3, pp. 34

Kutatómunka célkitűzései

Értekezésemben bemutatom azokat a törekvéseket, melyek mentén vizsgálhatjuk a terrortámadások hatását a gazdaságra, valamint a kritikus infrastruktúrák¹⁶ védelmi rendszerére.

Munkámban szeretném bemutatni azokat a kormányzati, rendvédelmi és más civil biztonsági társaságok feladatait, amelyek a kritikus infrastruktúra védelem feladatainak maradéktalan végrehajtásához szükségesek, valamint a hazai kritikus infrastruktúra „civil”¹⁷ védelmének aspektusait.

A kritikus infrastruktúra védelmének előkészítéséhez szükséges az állami szervezetek, intézmények és hatóságok szoros együttműködése, illetve a tulajdonos és a biztonsággal foglalkozó civil vállalkozások bevonása. Az értekezés elkészítésének célja, hogy a különböző „biztonsági szervezetek és hatóságok” egyformán értelmezzék a részükre meghatározott biztosítási és védelmi feladatokat, azok kapcsolódási pontjait és a kritikus infrastruktúra védelmének biztosításához szükséges új technikák, taktikai elemek alkalmazását.

Értekezésem első részében kívánom bemutatni és elemezni a biztonsági kihívásokat, a *terrorizmus természetét*, illetve a biztonsági szervezetek és az országos hatáskörű hatóságok *terrorizmus elleni harc (védelem) feladatait*, valamint a terrorizmus hatását a *világ- és nemzetgazdaság működésére*.

Munkám második részében ismertetem a nemzetközi és nemzeti jogszabályokban lefektetett elveket és szabályokat. A megszerzett tapasztalatokra és törvényszerűségekre alapozva olyan megoldási lehetőségeket kívánok felvázolni, amelyek *integrált*¹⁸ módon alkalmazott elemei révén hatékonyan végrehajtható a kritikus infrastruktúra *biztosítása és védelme*. Bizonyítani szeretném, hogy a jövőbeni biztosítási műveletekben történő szerepvállalás elérte a magyar rendvédelmi szervek lehetőségének határát. Ezért szükséges bevonni a civil tulajdonban lévő kritikus infrastuktúrák tulajdonosait és a civil biztonsági társaságokat.

¹⁶ A szolgáltatói szektor része, azonban direkt módon nem vesznek részt a termelésben, viszont indirekt módon befolyásolják a termelés biztonságát.

¹⁷ Vállalkozás keretében végzett biztonsági/védelmi szolgáltatást végző cégek.

¹⁸ Irányítási rendszer, egymással kapcsolatban vagy kölcsönhatásban álló részegységek összekapcsolása a kívánt cél elérése érdekében.

A kutatómunkám során két hipotézist állítottam fel:

- 1) A XXI. század biztonsági kihívásainak – különös tekintettel a megújult terrorizmus – hatása a világ gazdaságára működésére, mely szektorok leginkább érintettek és okoz-e valamilyen többletköltséget?
- 2) Melyek azok a szervezeti, építészeti-, biztonságtechnikai megoldások, taktikai elemek és menedzsment folyamatok, melyekkel a kritikus infrastruktúrák veszélyeztetése csökkenthető?

A konkrét célkitűzések:

- A) A terrorszervezetek kialakulása, bemutatása és működésének elemzése történeti összehasonlító elemzések alkalmazásával,
- B) Elemzem a terrorizmus milyen hatásással van a gazdaság különböző szereplőire,
- C) Áttekintést adok a kritikus infrastruktúrák védelmének nemzetközi és nemzeti szabályozásáról, bemutatom azokat az integrált szervezeti, építészeti, biztonságtechnikai, taktikai megoldásokat és menedzsment folyamatokat, melyekkel a kritikus infrastruktúrák veszélyeztetése csökkenthető,
- D) Elemzem a válságkezelés lehetőségeit egy nagy vállalat szintjén, illetve bemutatom a két szintű válságkezelés feladatrendszerét.

A kitűzött célok megvalósítása érdekében:

Tanulmányoztam a nemzetközi és nemzeti terrorizmus elleni védelem civil biztonsági szervezetek biztosítási feladatokkal kapcsolatos hazai és nemzetközi szakirodalmát és megismertem a napjainkban ismert kutatási eredményeket.

Elsajátítottam a Budapesti Műegyetem Mérnöktovábbképző Intézet „Hírszerzés” kurzusának tananyagát.

Elvégeztem a Zrínyi Miklós Nemzetvédelmi Egyetem „Biztonság- és védelempolitikai szakértő, illetve Biztonságtechnikai szervező mérnök (MSc)” szakát. A két szak elvégzése

során átfogó elméleti ismeretekre és gyakorlati¹⁹ tapasztalatokra tettem szert a biztosítási és védelmi műveletek megtervezésének és végrehajtásának témakörében.

Több alkalommal szakmai gyakorlatot teljesítettem²⁰ és több nemzetközi látogatás biztosításában vettem részt²¹ a Köztársasági Őrezrednél²².

A munkakörömből adódóan folyamatosan konzultáltam a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, a Katonai Nemzetbiztonsági Szolgálat, a Terrorelhárítási Központ, az Országgyűlési Őrség, a Készenléti Rendőrség, a Magyar Honvédség és a Katasztrófavédelem biztosítási műveletekkel foglalkozó munkatársaival.

A biztonsági kihívások témakör kidolgozása során a Nemzeti Közszolgálati Egyetem, a Nemzetbiztonsági Intézet és a Katonai Nemzetbiztonsági Szolgálat szakértőinek puclikációit, illetve a nemzetközi szervezetek (EU²³, NATO²⁴) stratégiai dokumentumait vizsgáltam.

A biztonsági és védelmi feladatok áttekintésében elsődlegesen a német biztonsági szakirodalomra, az elismert kutatási eredményekre és megközelítésekre építtem. A terrorrobbantások és terrortámadások elleni védekezések kutatásánál az Egyesült Államok Védelmi Minisztériumának és a NATO idevonatkozó minimum előírásai szolgáltak alapul.

A Zrínyi Miklós Nemzetvédelmi Egyetem Magasabb Parancsnoki Tanfolyamának szervezésében több ebben a témakörben megtartott előadásán vettem részt.

Konzultációt folytattam különböző biztonság- és védelempolitikai szakemberekkel itthon és külföldön, valamint az Audi Hungaria biztonsággal foglalkozó szakterületeinek vezetőivel.

¹⁹ Nemzetközi és hazai védett személyek és kijelölt létesítmények őrzése, védelme. 2012. július 01-én megszűnt önálló szervezatként működni, feladatait több szervezet vette át (Készenléti Rendőrség, Terrorelhárítási Központ, Országgyűlési Őrség).

²⁰ Kiemelt biztosítási feladat volt a „Védelmi minisztereinek informális értekezlete” 2008, Budapest

²¹ 2003: Hr. Stoiber bajor miniszterelnök, 2004: Fülöp herceg, spanyol trónörökös; Hr. Schröder kancellár, †Hr. Rau német államelnök, Haladó Kormányzás konferencia (Mr. Tony Blair ...);

2005: Német egység napja; 2006: Mr. Tony Blair hivatalos látogatása, Mr. Putin elnök látogatása, Mr. Kazimierz Marcinkiewicz látogatása, 1956-os forradalom 50. évfordulója ünnepségén 51 védett személy (uralkodók, állam- és kormányfők, egyházi méltóságok). 2007-től a hazai védett személyek biztosításában vettem részt a kormánnyal közös rendezvényeken.

²² Országos Rendőr-főkapitányság, Köztársasági Őrezred önálló szervezatként működött 2012. július 1-i feloszlásáig

²³ EU – Európai Unió

²⁴ NATO (*angolul North Atlantic Treaty Organisation, franciául Organisation du Traité de l'Atlantique Nord, OTA*), Észak-atlanti Szerződés Szervezete

Részt vettem a Magyar Tartalékosok Szövetségének és a Német Szövetségi Haderő Tartalékos Szövetségének²⁵ tagjaként több biztonsági és védelmi témában tartott magyar és nemzetközi konferencián.

Az Audi Hungaria Biztonságpolitika és adatvédelem szervezeti egység vezetőjeként szerzett tapasztalataimat összehasonlítottam a hazai és nemzetközi elméleti ismeretekkel és ezen eredményeket felhasználtam értekezésem elkészítésében.

Folyamatosan kapcsolatot tartottam a VW-konzern²⁶ biztonsági szervezeteivel, vezetőivel és több közös rendezvénybiztosítási feladatot szerveztem és irányítottam itthon és külföldön²⁷.

Részkövetkeztetéseimet és részeredményeimet előadásokban, konferenciákon és írásos publikációkban jelentettem meg.

Értekezésemnek a téma összetettsége és terjedelme miatt **nem volt célja**:

- > Az aszimmetrikus kihívások²⁸ fajtáinak részletes elemzése, bemutatása,
- > A terrorizmus részletes elemzése, valamint a terrorszervezetek és radikális csoportok bemutatása és tevékenységének vizsgálata,
- > A terrorizmus hatásának vizsgálata a gazdaságot jellemző komplex folyamatok összeségére,
- > A kritikus infrastruktúrák minden biztosítási és védelmi elemének ismertetése,
- > A válságkezelési feladatok teljes elemzése, átfogó, részletes vizsgálata és az e témában született tudományos ismeretanyag elemzése, illetve bemutatása,
- > Az Európát súlytó migrációs válság és az ehhez kapcsolódó biztonsági kihívások és veszélyek.

Szakirodalmi kitekintés – témában készült korábbi értekezések –:

²⁵ Verband der Reservisten der Deutschen Bundeswehr

²⁶ Volkswagen, AUDI, Bentley, Bugatti, Lamborgini, Porsche, Skoda, Seat, Ducati, SCANIA, MAN ...

²⁷ Felügyelő Bizottsági ülések, TOP menedzsment találkozók, 100 éves az AUDI rendezvénysorozat

²⁸ FORGÁCS Balázs - KALÓ József - NÉMETH József Lajos: *Aszimmetrikus kihívások a haderő, az állam, valamint a társadalom viszonyában*, Magyar Hadtudományi Társaság, Konferenciája – Aszimmetrikus hadviselés, 2015/1-2, pp. 106 - 110

- > Béres János mk. ezredes: Napjaink muszlim terrorizmusának gyökerei és visszaszorításának lehetőségei – doktori (Ph D) értekezés –
- > Dr. univ. Károlyi László ny. t. ezredes: A kritikus infrastruktúrák védelme és az operatív erők tevékenységirányítása a honi katasztrófavédelemben, különös tekintettel az EU konformitásra – doktori (Ph D) értekezés –
- > Somkuti Bálint: A negyedik generációs hadviselés – az érdekérvényesítés új lehetőségei – doktori (Ph D) értekezés –
- > Balogh Zsuzsanna: Objektumok robbantásos cselekmények elleni védelmének lehetőségei – doktori (Ph D) értekezés –

A kidolgozás munkamódszere

Elemzések alkalmazásával, illetve konkrét eseteken keresztül mutatom be azokat a megfontolásokat és érdekváltozásokat, amelyek segítségével meg lehet határozni azokat a trendeket, melyek szükségesek a kritikus infrastruktúrák védelméhez.

A lábjegyzetben szereplő információk szerves részei a tanulmánynak mint az értekezés főanyaga, mely többnyire háttérismeret és magyarázat.

A tanulmány alapjául szolgáló ismeretanyag gyűjtését 2016. február 28-án zártam le.

1. FEJEZET: TERROZMUS, MINT GLOBÁLIS BIZTONSÁGI PROBLÉMA ÉS A FENYEGETÉSEK EGYIK LEGFŐBB ELEME

1.1. GLOBÁLIS BIZTONSÁGI FENYEGETÉSEK

A globális gazdaság korában a nemzetállamok és nemzetbiztonság kérdéseit politikai, katonai, gazdasági, környezeti, humán és jogi szempontok alapján kell elemezni és kiértékelni. Prioritásokat meghatározhatunk, de a világ változásait, a bekövetkező eseményeket, a globális kihívásokat és a regionális veszélyeket *csak komplexen* lehet értelmezni.

A nemzetállamok és a nemzetbiztonság kérdését az adott államhatalmi státusza határozza meg, úgymint politikai és társadalmi berendezkedése, geopolitikai és geostratégiai helyzete.

A hidegháborút követően a határok mindinkább megnyíltak, így a biztonság belső és külső vonatkozásai szétválaszthatatlanul összefonódnak. A kereskedelem és a beruházások áramlása, a technológiai fejlődés, a demokrácia terjedése sok embernek hozta el a szabadságot, valamint a prosperitást. Mások szemszögéből a globalizáció a frusztráció és az igazságtalanság forrása. Ezek az események is növelték a nem állami szereplőkből álló csoportok mozgásterét a nemzetközi ügyekben, Európa függőségét. Ezzel sebezhetősége is fokozódott a szállítás, az energia, az információ és más területek kölcsönkapcsolatban álló infrastruktúrájában.

A NATO új stratégiai koncepciójának²⁹ kidolgozói hasonló következtetésre jutottak³⁰, mint az Oroszországi Föderáció nemzeti biztonsági stratégiáját³¹ kidolgozók, amikor 2020-ig felvázolták a lehetséges globális kihívásokat és regionális veszélyeket.

²⁹ NATO 2020: Assured security; dynamic engagement: [...] „A Lisszabonban rendezett 24. NATO-csúcstalálkozó egyik fő célkitűzése az volt, hogy elfogadja a szervezet új stratégiai koncepcióját. [...] Az 1999-ben elfogadott második „új stratégiai koncepció” alapján a NATO célja „a szabadságnak és a biztonságának a – politikai és katonai értelemben vett – biztosítása lett Európában és Észak-Amerikában, más szóval a nyugati érdekek és a piacgazdaság fegyveres szárnyává változott. [...] A szakértői csoport megalkotta a NATO 2020: Megerősített biztonság, dinamikus beavatkozás névre keresztelt jelentést, amely a szervezet stratégiai irányultságát határozza meg a következő tíz évre.”, <http://www.nato.int/strategic-concept/expertsreport.pdf>, (Letöltve: 2010.07.01)

Mindenek előtt figyelembe vették a világban és az európai kontinensen bekövetkezett geopolitikai és geostratégiai változásokat, amelyek hatással vannak és lehetnek a NATO jövőjére. A jövőben a hagyományos fenyegetéseket nem lehet figyelmen kívül hagyni, mert a világ számos térsége és állama halmoz fel olyan jelentős modern katonai képességeket, amelyek hatással lehetnek a nemzetközi stabilitásra és az euro-atlanti térség biztonságára.³² Ezeket a hatásokat nehéz kiszámítani. Ehhez szorosan kapcsolódik a ballisztikus rakéták ellenőrizetlen elterjedése.

Elméleti alapok³³

A nem kormányzati szervezeteknél, különösen a multinacionális vállalatok biztonsági helyzetének elemzése során – gyakorlati tapasztalatok alapján³⁴ – a kormányzati besorolás eltérő. Egy nagyvállalat esetén, amelynek több kontinensen több leányvállalata és telephelye van, más-más biztonsági problémák vannak jelen.³⁵

A kihívások: olyan általános, globális³⁶ biztonsági kérdések, amelyek bekövetkezése esetén hátrányosan³⁷ befolyásolják a nagyvállalat működését és hatásaival hosszú távon kell számolni.

A fenyegetések: olyan általános, regionális³⁸ biztonsági kérdések, amelyek bekövetkezése esetén indirekt hatást³⁹ gyakorol a nagyvállalat működésére, de csak közép- és/vagy rövidtávon befolyásolja a működést.

A kockázatok: olyan általános, lokális⁴⁰ biztonsági kérdések, amelyek közvetlenül és azonnal jelentkeznek, továbbá azonnali biztonsági intézkedések alkalmazását követeli meg.

³⁰ Report on the NATO's, New Strategic Concept Workshop, Centre for Defence and Security Studies, University of Manitoba, 2010, ISSN 1922-7027

³¹ DEÁK János: *Oroszország katonai stratégiája a második világháború befejezésétől napjainkig*, Egyetemi jegyzet, Budapest, 2010, pp. 204–231

³² Prof. dr. SZTERNÁK György ny. ezredes: *A fegyveres erő feladatai valamint fejlesztése közötti kapcsolat*, Ludovika Digitális Tudástár és Archívum, Hadtudomány, 2011, pp. 3 - 4

³³ civil szemmel és a szerző megjegyzéseivel

³⁴ Feladatkörömből adódóan 2003-tól készítik elemzéseket, tanulmányokat a vállalat felső vezetése részére a biztonságot érintő kérdésekről.

³⁵ Hans FRANK: *Sicherheitspolitik in neuen Dimension*, Bundesakademie für Sicherheitspolitik, 2001, ISBN 3-8132-0776-5, pp. 15 - 28

³⁶ Teljes, az egész világra vonatkozó ...

³⁷ A lehetséges veszélyek szintje ebben az esetben a legalacsonyabb.

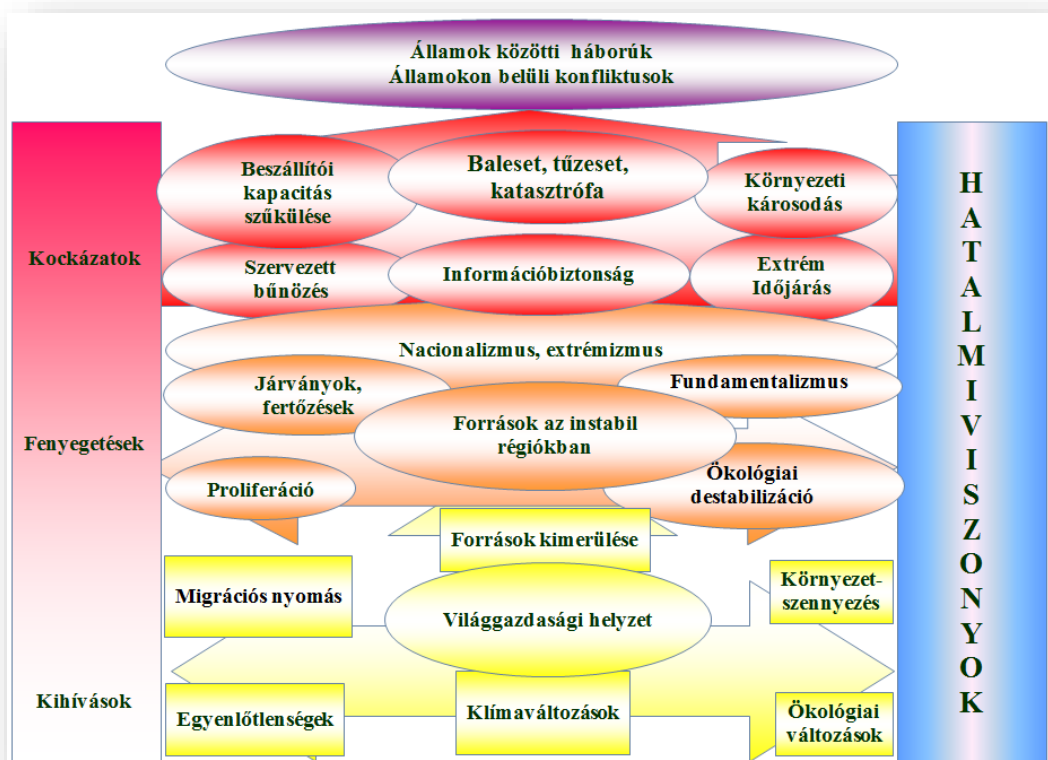
³⁸ Egy adott térségre, kontinensre, több országra vagy egy adott országra érvényes ...

³⁹ A lehetséges veszélyforrások magasabb szinten fejtenek ki hatást a szervezet működésére.

⁴⁰ Helyi, csak egy telephelyet érint.

Ebben az esetben a vállalat működési feltételei nem biztosíthatók és veszteségek keletkeznek.

Ezekből a meghatározásokból eredően a globális kihívások, a regionális fenyegetések és a lokális kockázatok/risikók különböző mértékben befolyásolják egy nagyvállalat működését, amely a kormányzati válságkezeléstől eltérő módszereket követel meg. A vállalati válságkezelés egymásra épülő feladatok összessége, amelyek alkalmazása során a vállalat üzleti folyamatai a biztonsági helyzet függvényében dinamikusan változhatnak.



1. ábra. Kihívások, fenyegetések és kockázatok⁴¹
(szerző által módosítva)

A XXI. század biztonságát befolyásoló kihívásai

A multinacionális vállalatokat a konfliktusok és válságok csak indirekt módon érintik. Ezen biztonsági veszélyforrások felismerése, kezelése és megoldása alapvetően a nemzetközi szervezetek és a nemzetállamok hatáskörébe tartoznak.

⁴¹ Dr. RESPERGER István mk. Ezredes: *Biztonsági Kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig.*, KNBSZ, Felderítő szemle, 2013/3, pp. 6.

Globalizáció

A globalizáció kifejezés⁴² kevesebb, mint 30 éves múltat tekint vissza. Viszont nem a XX. században alakultak ki ezek a folyamatok, amelyeket ma „globalizáció”-nak nevezünk. Már az ókorban megjelent első birodalmak a meghódított területeken megszilárdították gazdasági és kulturális befolyásukat, ezzel próbálva a leigázott nemzeteket integrálni több-kevesebb sikerrel.⁴³ Az I. világháború befejeztével a gyarmattartó birodalmak lassú, majd a II. világháború utáni „gyors” szétesése volt jellemző. A korábbi gyarmatok függetlenségük kivívása után a volt gyarmattartók hatalomgyakorlási módszereiben egyre inkább háttérbe szorult a politikai és a katonai nyomásgyakorlás eszköze. Gazdasági és technikai eszközök alkalmazásával helyettesítették a korábbi módszereket.⁴⁴

Gazdasági (közgazdasági) kihívások

A felgyorsult világgazdasági folyamatok megkövetelték, hogy globális szinten szabályozzák a legfontosabb elveket, amelyek segítségével megelőzhetőek és elkerülhetőek a kereskedelmi (gazdasági) háborúk.

Genfben 1995-ben az Általános Kereskedelmi és Vámtarifa Egyezmény tagállamai (GATT)⁴⁵ megalakították a Kereskedelmi Világszervezetet (WTO)⁴⁶. A szervezetet megalapító 153 ország célja az volt, hogy az emberiség életszínvonalát növeljék világszerte. Így a teljes foglalkoztatottság megvalósításával nő a fizetőképes kereslet, ami hatással lesz a termelés és a kereskedelem bővülésére. Az erőforrások optimális felhasználásával biztosítható a környezet védelme, összehangolva a fenntartható fejlődéssel⁴⁷.

⁴² "globalizáció", a XXI. században már egyre inkább egy hálózatba kapcsolt világot jelent, amely megvalósul az egyén (privát), szakmai, katonai, gazdasági és politikai szinteken. (Szerző megjegyzése)

⁴³ Görög városállamok, a Római Birodalom, Tatárjárás, Hanza-város sok, Oszmán Birodalom, Spanyol és portugál hódítások, Orosz Birodalom térhódítása, Brit világbirodalom kiépítése, Amerikai Egyesült Államok megerősödése.

⁴⁴ ARTNER Annamária: Globalizáció alulnézetben, Elnyomott csoportok – lázadó mozgalmak, Napvilág Kiadó, @ Artner Annamária, 2006, pp.27, HU ISSN 1587-6128

⁴⁵ a Marrakesh-i Egyezményben egy kereskedelmi világszervezete, Általános Vám- és Kereskedelmi Egyezmény (GATT: *General Agreement on Tariff and Trade*), amely 1995. január 1-jén lépett hatályba

⁴⁶ WTO: *World Trade Organization*, Kereskedelmi Világszervezet, multinacionális vállalatok és a transznacionális vállalatok térnyerése

⁴⁷ UNESCO Magyar Nemzeti Bizottság: *A fenntartható fejlődés fogalma, célkitűzése*

<http://www.unesco.hu/termeszetudomany/fenntarthato-fejlodesre/fenntarthato-fejlodes-091214> (Letöltve: 2014.11.10.)

A világgazdasági folyamatok megváltozása kiélezte az államok közötti ellentéteket, amelyek mögött elsősorban a gazdasági érdekek érvényesítésének lehetőségei húzódtak meg. A világ különböző térségeiben eltérő fejlődési modellek találhatók, amelyek szinte azonos lehetőségeket kínálnak az államok számára az energetikai- és a gazdasági erőforrások tükrében.⁴⁸

A kommunikációs és a közlekedési technológiák gyors fejlődése tette lehetővé az emberek mobilitását és az áruk forgalmának globális növekedését. A jelenlegi helyzetet a nemzetközi pénzügyi piacokon történő soha nem látott mobilitás jellemzi.

A globalizáció hatással van a központi⁴⁹ és a marginális⁵⁰ régiók eltérő növekedési ütemére. Jól példázza ezt a migrációs tendenciák megváltozása és felgyorsulása a marginális régiókból a központi régiók irányába. Ezáltal nagymértékben megváltozott a központi régiók országainak biztonsága, mert a nehezen vagy ellenőrizhetetlen háttérrel rendelkező beáramló tömegek kockázatot és fenyegetést jelentenek egy ország/régió társadalmi és gazdasági biztonságára. A különböző régiókban jelentkező veszélyek⁵¹, amik jelentős hatással vannak az ott élő emberek biztonságérzetére és olyan folyamatokat indíthatnak el, amelyek hatásai közvetlen és/vagy közvetett módon jelentkezhetnek világszerte.

Pénzügyi biztonság

2008-ban a világ pénzügyi rendszere instabillá vált, több ország került fizetőképessége határára. Az adósságválság a nyugati világban, mint pénzügyi probléma jelentkezett és az Amerikai Egyesült Államok egyes bankjaiból⁵² indultak ki, majd áterjedt Európára és a világ más térségeire is. Maga a válság történelmi megrázkódtatásokat okozott a világpolitikában, amely új biztonságpolitikai kérdéseket vetett fel, hogy milyen kockázatokat jelenthet a pénzügyi bizonytalanság a világ egyes régióiban és országaiban, illetve milyen konfliktusok keletkezhetnek regionálisan.

⁴⁸ Prof. Dr. Anja-Désirée SENZ – Th. HEBERER: *Deutschland und China, Zusammenarbeit und Wettbewerb*, in: Bundesakademie für Sicherheitspolitik: *Sicherheitspolitik in neuen Dimensionen, Ergänzungsband II*, Verlag E.S. Mittler & Sohn GmbH, Hamburg, 2004, pp.183-202, ISBN 3-8132-0823-0

⁴⁹ Nyugati civilizáció régiói (Európa, Észak-Amerika)

⁵⁰ Harmadik világ országai (Latin-Amerika, Szub-szaharai térség, Közel-Kelet...)

⁵¹ az erőszakos konfliktusok, polgárháborúk, terrorszervezetek térhódítása, a pénzügyi válságok (a fizetéseképtelen államok), munkanélküliség hatalmas növekedése, környezeti károk (esőerdők kiirtása)

⁵² SZEPESI György: *A pénzügyi világválság néhány eddigi tanulsága II*. Köz-gazdaság, 4 (3), 2009, pp. 73 - 75. ISSN 1788-0696

Erre legjobb példa az Egyesült Államok államadósság növekedése, ami már nemzetbiztonsági kockázatot jelent a maga ugrásszerű növekedésével. Ez 2013-ban elérte 17,2 billió dollárt⁵³. Csak 2008-ban 637 milliárd dollárral növekedett az Egyesült Államok külső államadóssága⁵⁴. Az államadósság növekedése azzal fenyeget, hogy megbontja a világgazdasági egyensúlyt, amely az Amerikai Egyesült Államok (továbbiakban USA)⁵⁵ meggyengüléséhez vezethet és ez által a kialakult világregendet is megváltoztathatja. Csak a nagyon optimisták gondolják azt, hogy ez a folyamat korlátlan ideig fenntartható. Az elmúlt néhány évben több ország súlyosan eladósodott⁵⁶, mint bármikor az emberiség történelme során.

A legnagyobb közvetlen veszélyt a lejáró tartozások feltorlódása jelenti. Ez a kockázat jelenleg meredeken emelkedik, ez egybeesik a nyugati központi bankok kontrollálatlan pénzkibocsátásával. A monetáris rendszer működése egyre jobban eltér a korábban megszokott mértéktől. Ez igen kockázatos magatartás, mert a jelenleg növekvő „pénznyomtatás” a nyugati társadalmaknak rendszerszintű problémákat okozhat. Ennek ellenére a nemzetközi pénzügyi intézmények és intézetek továbbra is bíznak a pénzkibocsátás gazdaság élénkítő hatásában.⁵⁷ Nem szabad figyelmen kívül hagyni direkt és indirekt veszélyeket sem, amelyek évről évre növekvő kockázatot jelentenek az államadósságok kezelésére. A hatalmasra nőtt államadósságok hatására az érintett államok sorra jelenthetnek államcsődöket és elindíthat egy „dominó hatás”-t, amely csak növeli az érintett térségek instabilitását. A Lehman adósságválság⁵⁸ figyelmeztetés volt az euró zónát érintő veszélyre, ami főként a nyugati civilizáció gazdasági stabilitását fenyegeti. Az esetleges pánikszerűen összeomló pénzügyi rendszer további biztonságpolitikai veszélyek sorozatát indíthatja el. Az államok adósságválsága a XXI. században aggasztó mértékben növekedésnek indult és jelenleg nincs megoldási javaslat vagy stratégia a láthatáron.

⁵³ HEGEDÜS Zsuzsanna: *Az Amerikai Egyesült Államok adósságválsága és okai*, MTA Közgazdaság- és Regionális Tudományi Kutatóközpont Világgazdasági Intézet. 206. sz., 2013. december pp. 2

⁵⁴ TrendsDerZukunft.de, Heidorn GmbH: Staatsverschuldung der USA – Wer sind die Gläubiger? <http://www.trendsderzukunft.de/staatsverschuldung-der-usa-wer-sind-die-glaebiger/2009/03/30/>, (Letöltve: 2014.12.02.)

⁵⁵ United States of America (USA)

⁵⁶ Görögország adósságválsága

⁵⁷ Kiszámoló.hu: Hiperinfláció a küszöbön?, <http://kiszamolo.hu/hiperinflacio-a-kuszobon/> (Letöltve: 2013.11.18.)

⁵⁸ A Lehman Brothers volt a világ vezető brókercege és a negyedik legnagyobb amerikai befektetési bank. A 1858-tól New York-i cég korábban már számos krízist, például az 1800-as évek vasúti csődjeit, majd az 1929-33-as nagy gazdasági világválságot is átvészelte. 2008-ban azonban a nem fizető adósságok és hitelekkel fedezett értékpapírok árfolyamának összeomlása végül bedöntötte.

Nyersanyagok

A feldolgozatlan (kitermelt) nyersanyagokhoz hozzáférés (tulajdonlás) és azok világszerte ára befolyásolja az országok geopolitikai és geostratégiai helyzetét.⁵⁹ A világméretű trendekben egyre inkább teret nyernek azon szempontok is, amelyek szerint a környezet hatásai jelentősen befolyásolják a bányászati tevékenységet és a nyersanyag felhasználást, valamint e folyamatok társadalmi-gazdasági hatását. A trendek hatással vannak a befolyási övezetek megváltozására, amely magában hordozza a politikai és gazdasági viszonyok újragondolását, továbbá a biztonsági szervezetek és intézmények feladatrendszerének újragondolását.

A nyersanyagokért folyó hatalmi harcok – főként a vízért (BLUE GOLD⁶⁰) –, amelyet a következő évtizedekben bekövetkező klímaváltozások⁶¹ tovább fokoznak. Ez újabb konfliktusokhoz és migrációs hullámhoz vezethetnek a vízhiányos régiókban.

Számos szakértő szerint az egyik legnagyobb globális kihívás lesz az elegendő tiszta és megfizethető ivóvíz biztosítása.

Energiabiztonság

A megfelelő mennyiségben rendelkezésre álló energia döntő fontosságú létünk és az emberiség jövője szempontjából.

Mindennapi életünket meghatározzák és jelentősen befolyásolják azon alapszolgáltatások, mint a termelés, a mobilitás, az információ és a kommunikációs szolgáltatások. Az energia jelentős mértékben hozzájárul a biztonságérzetünkhöz, közérzetünkhöz, meghatározzák az ipari és a tudásalapú társadalmak gazdasági jólétét. Az energia technológia fejlesztésének elsődleges feladata, hogy növelje a gazdaság rentábilis működtetését, biztosítsa az emberek jólétét a környezeti kockázatok csökkentésével egyidejűleg.⁶² Ha ezek az elképzelések nem valósulnak meg, akkor a klímaváltozás terhei a jövő generációját fogják terhelni.

Tehát a felelős energiapolitikának kell meghatározni a hosszú távú megbízható kereteket,

⁵⁹ SZTERNÁK György: *A geopolitikai, geostratégiai elemzés következtetései*, pp. 3 - 4.

http://www.kodolanyi.hu/oroszcivilizacio/doc/hasznos/szternak_geopolitikai.pdf (Letöltve: 2014.09.15.)

⁶⁰ Gordon G. CHANG: *Blue Gold: The Coming Water Wars*, World Affairs Journal, Washington, © 2013 World Affairs Institute

⁶¹ Például a globális felmelegedés miatti elsivatagosodás (szerző megjegyzése)

⁶² Prof.Dr. Raimund BLEISCHWITZ: *Internationale Rohstoffmärkte: steigende Preise und wachsendes Konfliktpotenzial*, Global Trends 2007, ©Stiftung Entwicklung und Frieden, Bonn,2006, pp. 318 – 320, ISBN 3-89-331-739-2

annak érdekében, hogy megvalósuljon a biztonságos, gazdaságos és környezetbarát energiaellátás az emberiség és a gazdaság számára.⁶³

A rendelkezésére álló exportálható energiaforrások hatással vannak a jelenlegi hatalmi viszonyokra és továbbra is meghatározzák az új világpolitikai és világgazdasági trendeket.

Európa és különösen Magyarország az energiafüggőség miatt különleges helyzetben van. 2030-ra Európa energia import bővülése elérheti az 50%-ot. A legnagyobb energia import a Perzsa-öbölből, Oroszországból és Észak-Afrikából származik.⁶⁴

Klímaváltozás - környezettechnológia

Mind ökológiai, mind gazdasági szempontból a világ éghajlatváltozása a XXI. század egyik legnagyobb kihívása. Az ENSZ⁶⁵ 1972-ben rendezett konferenciáján kezdték el vizsgálni az üvegházhatású gázok hatását az éghajlatra. Az IPCC⁶⁶ 1990-ben adta ki első prognózisát a globális éghajlati rendszer állapotáról, működéséről és a várható hatásokról. 2007 elején korrigálták a korábbi előrejelzéseket a globális felmelegedés mértékéről. Tendenciát fogalmaztak meg a környezeti változások alakulásáról neves tudósok széleskörű bevonásával. Az új hosszú távú éghajlatváltozásokat kutató tanulmányok szerint a klímaváltozás komoly következményei szintentarhatóak, ha a globális és nemzetközi közösségek hajlandóak azonnali pozitív politikai jelzéseket adni, drámai intézkedéseket bevezetni és azokat betartatni. Ezért fontos lenne a politika részéről a kötelező célok kitűzése nemzetközi szinten. Az Európában alkalmazott környezetbarát termékek és szolgáltatások jelentősen még nem befolyásolják az éghajlati változásokat, azonban mindenképpen példamutató és követendő trend a világ többi régiója számára. Közzétételét követően az ún. Stern-jelentés⁶⁷ és egyéb más vizsgálatok is nagy jelentőséggel rendelkeztek, mert felhívták a közvélemény figyelmét arra, hogy a klímaváltozás több problémát generálhat az élet más területein is.

⁶³ EURÓPAI BIZOTTSÁG: *Energiapolitika*, Az Európai Unió Kiadóhivatala, Luxembourg, 2013, pp.4, ISBN 978-92-79-34123-9

⁶⁴ Biztonságpolitikai Szemle, Corvinák – *Energiabiztonság 2*.

http://biztpol.corvinuembassy.com/?module=corvinak&module_id=4&cid=27 (Letöltve: 2014.10.21.)

⁶⁵ ENSZ: Egyesült Nemzetek Szervezete, (angolul: *United Nations*, rövidítése: *UN*)

⁶⁶ IPCC – Intergovernmental Panel on Climate Change – Éghajlat-változási Kormányközi Testület

⁶⁷ Sir Nicholas Stern: az alacsony üvegházhatású gázok kibocsátása milyen hatással lesz a gazdaság működésére, valamint a gazdasági feladatok, módszerek, időbeni hatásának vizsgálata és összegzése, a várható klímaváltozás hatásaihoz való alkalmazkodás potenciális lehetőségeinek vizsgálata. (Szerző megjegyzése)

Így került az éghajlatváltozás kérdése a figyelem középpontjába a WEF⁶⁸ 2007. évi davosi konferenciáján.

Az elmúlt évek katasztrófái rávilágítottak arra, hogy a természeti okokra visszavezethető (a hőségriasztások számának növekedése, a vulkán kitörések direkt és indirekt hatásai, földrengések pusztítása) vagy az emberi tevékenység hatására bekövetkező események, különösen az üvegházhatású gázok egyre növekvő kibocsátása miatti hőmérséklet növekedés, a tengerszint emelkedése, a hótakaró jelentős csökkenése vezettek a világszerte jelentkező extrém időjárás kialakulásához.⁶⁹

Demográfia

Európa lakossága csökken. Az „öslakosság” körében a legkisebb a világon a születési ráta. Európa marginalizálta magát.⁷⁰ Míg 1900-ban minden harmadik állampolgár európai volt, ma már csupán ennek nyolcada. 2050-ben már csak minden tizennegyedik ember lesz európai.⁷¹ Az európai országok a XXI. század közepére erős hátrányba kerülnek és a politikai egyensúly a világban jelentősen megváltozik. Európa elveszíti a mai súlyát a világpolitikában. Ezek a komor demográfiai számok nem a biológiai önfeláldozást jelentik, hanem feltűnő szimbóluma a civilizációs visszaesésnek Európában. Ha a gyermekvállalás elvesztette értelmét, a civilizáció léte is elveszítheti értelmét.

A demográfiai adatok javulását a jobb élelmiszer- és egészségügyi ellátás eredményezte, drasztikusan csökkent a halálozási ráta a XX. században. Ennek következménye a "népességrobbanás". Ez a demográfiai tendencia várhatóan tovább folytatódik a XXI. században is. A világ népessége több mint 7 milliárd ember, ami várhatóan 2050-ben meghaladja a 9,3 milliárdot⁷². Ugyanakkor várható, hogy a társadalom jelenlegi szerkezete megváltozik. A fejlődő országokban a születések száma dinamikusan nő. Az iparilag fejlett

⁶⁸ WEF – World Economic Forum – Világgazdasági Fórum

⁶⁹ Országos Meteorológiai Szolgálat (OMSZ): *Meteorológiai világ és kontinens rekordok*, http://owww.met.hu/omsz.php?almenu_id=misc&pid=met_rekordok&pri=1&mpx=3&stt=vilagrekordok (Letöltve: 2016.11.20.)

⁷⁰ Dr. Helge SCHRÖDER: *Wie viele werden wir werden? Demographische Entwicklungen*, Globale Herausforderungen, ©Bundeszentrale für politische Bildung, pp. 13 -30, ISBN 978-3-8389-7056-1

⁷¹ Reiner KLINGHOLZ: *Demographische Entwicklung*, Die Zeit, Zeitverlag Gerd Bucerius GmbH & Co. KG, Hamburg, 2014/7.

⁷² http://www.ksh.hu/szamlap/eletunk_nep.html (Letöltve: 2014.12.01.)

országokban az alacsony születésszám és a várható magas élettartam a társadalmak elöregedéséhez vezetnek.

Az előrejelzések szerint a világ népességének alakulásában nagyarányú regionális különbségek lesznek. A népesség növekedésével szinte kizárólag a fejlődő országokban számolnak, a fejlett országokban a lakosság száma stagnálni fog. A világ fejlődő országaiban a lakosság lélekszáma megháromszorozódik (0,8-1,7 milliárd ember), amely több mint kétszeresére a jelenlegi lélekszámnak. A lakosság növekedésének oka például - Afganisztánban, Ugandában, Nigerben, Kongóban – a nagyon magas termékenységi ráta, amely mellett jelentősen visszaesett a gyermekhalandóság, valamint javult az orvosi ellátás. Azt már feltételezik, hogy az átlagos születési ráta (ma 2,05-2,75) a fejlődő országokban, 2050-ben csökkenni fog, egy nőre egy gyermek fog jutni.⁷³

Különösen drámai változást prognosztizálnak a 60-as korosztálynál világszerte. A jelenlegi 60-as korosztály létszáma 673.000.000 fő. 2050-ig számuk megháromszorozódik, ez két milliárd embert fog jelenteni⁷⁴. 1950 és 2000 között a fejlett ipari országok és a fejlődő országok népességeloszlása között bizonyos mértékig párhuzam volt a 60-as korosztálynál. 2020-ra a fejlett országokban ezen emberek száma 750 millióra emelkedik. A fejlődő országokban ez a szám mintegy 400 millió volt 2000-ben és 2020-ra eléri az 1 milliárdot.

Egészségügy

„A fejlődő világ nagy részén a szegénység és a betegség hallatlan szenvedést okoz és a biztonsággal kapcsolatos egyre sürgetőbb aggodalmakra ad okot. A Föld népességének fele, csaknem 3 milliárd ember él napi 2 eurónál kevesebből. Minden évben 45 millióan halnak meg éhezés vagy alultápláltság következtében.”⁷⁵ A pusztító járványok⁷⁶ direkt módon befolyásolják az érintett régiók államainak működőképességét és a nem működő államok miatt egyre nagyobb mértékűt ölt a világ fejlett országaira nehezedő migrációs nyomás. Az új betegségek gyorsan terjedhetnek a világban a megnövekedett mobilitás miatt, így már globális fenyegetéssé váltak.

⁷³ <http://www.nyf.hu/others/html/kornyezettud/global/002.htm> (Letöltve: 2014.12.01.)

⁷⁴ <http://www.uni-miskolc.hu/~ecomojud/4neptermnepmozg.pdf> (Letöltve: 2014.12.01.)

⁷⁵ EURÓPAI BIZOTTSÁG: *Európai Biztonsági Stratégia: Biztonságos európa egy jobb világban*, Európai Unió Kiadóhivatala, Luxemburg, 2009, pp. 2, ISBN 978-92-824-2427-8

⁷⁶ AIDS (Acquired Immune Deficiency Syndrome - szerzett immunhiányos tünetegyüttes), EBOLA – vérzéses láz

A szegénység a világon

A globális társadalmat az egyre növekvő egyenlőtlenség jellemzi, amely a jövedelem eloszlásban mutatkozik. Ez a nemzetközi rendszer politikai ellensúlyozása nélkül társadalmi robbanáshoz vezethet.

A globalizáció és a szegénység kapcsolatáról szóló vitákat három érv határozza meg, amely jelentősen befolyásolja a globalizáció megítélését világszerte. Első ok a multinacionális vállalatok telephely választásánál az alacsony bérek, amelyek jelentősen befolyásolják a döntéseket és mozgatórugója a globális kereskedelemnek.

Másodszor a rossz munkakörülmények a harmadik világba telepített multinacionális vállalatok gyáraiban. Kirívó esetekben a gyermekmunka alkalmazásától sem riadnak vissza⁷⁷. A Nemzetközi Munkaügyi Szervezet⁷⁸ legújabb vizsgálatai alapján egyre inkább az a tendencia mutatkozik, hogy a fejlődő országokban a munkafeltételek és bérek a külföldi tulajdonú cégeknél általában jobbak, mint az adott ország „hazai tulajdonú” vállalkozásainál.

Harmadszor, problémát jelent az export orientált iparosítás, vagyis a nemzeti gazdaságok integrációja a világgazdaságba, amely az adott ország lakosságának rovására történik és a társadalomban torzulásokat okoz. Megfigyelhető azonban, hogy 1960 óta az oktatási és az egészségügyi rendszer, valamint a szociális mutatók (például a gyermekhalandóság, a táplálkozás és a várható élettartam) különösen azokban az országokban javultak, akik aktív részesei a világpiacnak⁷⁹.

A globális gazdaságba történő integráció alapfeltétele a globális folyamatokban való részvétel, amely nem valósul meg eredményesen a harmadik világ országaiban. Ez feltételezi a stabil politikai intézményrendszert, a mindenki számára elérhető alapfokú oktatást, valamint a szociális biztonsági rendszer fokozatos kiépítését és fejlesztését.

Nagy kihívás a szegény nemzetek számára, hogy nemzeti struktúrák hiányában a globális gazdaság rendszeréhez kapcsolódjanak. Ugyanakkor a globális keretek között ki kell terjeszteni a fejlődő országok mozgásterét, hogy minél előbb részesei lehessenek világgazdasági folyamatoknak. A WTO, az IMF és a Világbank által indított projektek segítségével, valamint a nyitott piacok megvalósításával, a fejlett országokba irányuló

⁷⁷ <https://btk.ppke.hu/uploads/articles/6414/file/reinischreka.pdf> (Letöltve: 2014.12.02.)

⁷⁸ ILO - International Labour Organization - Nemzetközi Munkaügyi Szervezet

⁷⁹ Erre legjobb példa a dél-koreai, egy olyan ország, amely a legszegényebb volt a világon az 1950-es években.

exporttámogatásokkal (különös tekintettel a mezőgazdasági termékekre vonatkozólag), hozzanak létre egy stabil nemzetközi gazdasági keretfeltételt és jelentősen növeljék a beruházásokat a fejlődő országokban.

Migráció⁸⁰

A nyilvános viták hatására félelmek fogalmazódtak meg a többségi társadalomban a migrációban érintett országokban, a terrorista fenyegetések és a kulturális különbségek miatt. A migránsok száma 2013-ban meghaladta az 50 millió embert, majdnem egy százaléka a világ népességének az ENSZ Menekültügyi Főbizottsága⁸¹ adatai szerint⁸². A statisztika pontatlanságát befolyásolhatja az illegális migráció⁸³. A nemzetközi médiában a migráció a figyelem középpontjában van a hozzá kapcsolható biztonsági kérdések miatt. A nemzetközi migráció és a nemzetközi terrorizmus gyakran összekapcsolódik. A félelem a terrorista fenyegetésektől, valamint a migránsok által elkövetett bűncselekményektől⁸⁴, illetve a párhuzamosan létre jövő társadalmak⁸⁵ radikalizálhatják a többségi társadalmat.

Regionális konfliktusok

A hidegháború utáni közép- keleti-európai és a közel-keleti térségekben kialakult helyzet közvetlen vagy közvetett módon hatással van Európa biztonságára. A regionális stabilitást fenyegetik az erőszakos vagy lappangó konfliktusok, amelyek közvetlen környezetünkben az egykori Jugoszláv háború befejeztével is fennmaradtak.⁸⁶ Emberi életet veszélyeztetnek, rombolják a szociális és anyagi infrastruktúrákat. Fenyegetést jelentenek a kisebbségeknek, az alapvető szabadságjogok és az emberi jogok számára. Ezek a konfliktusok szélsőségekhez, terrorizmushoz és az állam működésképtelenségéhez vezethetnek, ezáltal nagyobb mozgásteret biztosítva a szervezett bűnözés számára. A

⁸⁰ Lakhely változtatás, költözés, vándorlás (szerző megjegyzése)

⁸¹ UNHCR - United Nations High Commissioner for Refugees, Egyesült Nemzetek Menekültügyi Főbiztosa

⁸² The UN Refugee Agency : *Global Trend 2013*, <http://www.unhcr.org/5399a14f9.html> (Letöltve: 2015.01.12.)

⁸³ Az illegális migráns az, aki(k) illegálisan beutaznak/belépnek egy idegen országba, vagy illegálisan ott tartózkodnak. (A szerző...)

⁸⁴ RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: *Gerillaharc a betonzsungelban*, Hadtudomány, A Magyar Hadtudományi Társaság folyóirata, 2013

⁸⁵ KISS Álmos Péter: Generációk a hadviselésben – *A negyedik generáció*, Hadtudományi Szemle, 2009/2.

⁸⁶ BUNDESAKADEMIE FÜR SICHEHEITSPOLITIK: *Sicherheitspolitik in neuen Dimensionen, Ergänzungsband 2*, Verlag E.S. Mittler & Sohn GmbH, Hamburg, 2004, pp. 137 – 159, ISBN 3-8132-0823-0

regionális bizonytalanság okozza a megnövekedett igényt a tömegpusztító fegyverek iránt.⁸⁷ A gyakran nehezen megfogható új fenyegetések kezelésének legpraktikusabb módja a regionális konfliktusokból fakadó régi, történelmi⁸⁸ problémák helybeni kezelése.

Az állam működésképtelensége⁸⁹

A nemzetközi rendszerben az államok játsszák továbbra is a meghatározó szerepet, de az instabil vagy működésképtelen államok száma egyre növekedett a Magreb térségben, a szub-szaharai államokban és a közel-keleti régióban és jelentősen nőtt a többi földrészen is. Ugyanakkor a határokon átnyúló konfliktusok miatt, jelentősen megnövekedett a nemzetközi szervezetek és intézmények szerepe, valamint a nem állami szereplők nagyobb szerepvállalása.

A vesztegetés, a hatalommal való visszaélés, a rossz kormányzás, a gyenge intézményi háttér és az elszámoltathatóság hiánya, valamint a konfliktusok belülről erodálják az államot. Bizonyos esetekben ez az állami intézmények összeomlásához vezetett, mint

⁸⁷BUNDESAKADEMIE FÜR SICHEHEITSPOLITIK: *Sicherheitspolitik in neuen Dimensionen, Ergänzungsband 2*, Verlag E.S. Mittler & Sohn GmbH, Hamburg, 2004, pp. 175 -242, ISBN 3-8132-0823-0

⁸⁸ Európa legnagyobb kihívása az orosz-ukrán konfliktus esetleges eszkalációja, amely hosszú történelmi folyamat következménye. Az orosz-ukrán konfliktus már a X. században elkezdődött. Kievi Rusz volt az első nagy szláv államalakulat, amely létrejött. Ezt az államalakulatot 1240-ben a tatárok lerombolták és ezzel szétesett, majd a Moszkvai Nagyfejedelemség felemelkedése. Moszkvát 1147-ben említik először. Moszkvának önálló egyház központtá kellett válnia. 1439-ben alakul meg az önálló orosz egyház, melynek központja Moszkva. Lassanként Moszkva válik a keleti kereszténység központjává. 1453-ban Moszkvát II. Rómaként emlegették. Első terjeszkedése Moszkvának a XV. században kezdődött, ekkorra már megszabadulnak a tatároktól, elindul a terjeszkedés déli irányba, illetőleg keletre, Szibéria felé. Tehát folyamatosan próbál területeket szerezni, ez elmondható egészen 1945-ig. A sztálini vezetés célja egy szovjetbarát nyugati „előtér”, megteremtése volt. A háború befejezése után a Szovjetunió volt a legfőbb területi nyertes. Az orosz stratégiában két nagy vonulat figyelhető meg. Az első az, hogy mindig felülről jövő reformokkal próbálnak megoldani dolgokat. Aki nem azt csinálta, amit rendszer elvárt, azt száműzték (internálták) vagy kivégezték. Az oroszok – az idők folyamán - ebbe már beletörődtek. Oroszországban mindig kell egy ember, aki a legerősebb ember és akinek a döntése meghatároz mindent. A másik az orosz stratégia, mely szerint területeket szerez, majd veszít. Az orosz birodalom egyfajta pulzálásban van. Volt egy hatalmas terjeszkedési szakasz, amikor megalakult és folyamatosan szerzett területeket, egészen az I. világháborúig. Elfoglalták Kamcsatkát, Kelet-Európát és Közép-Európát, majd az I. világháborút követően visszaszorult. Levált róluk Finnország, Lengyelország, a balti államok és más határ menti területeit is elveszítette. A II. világháború idején megint vett egy nagy lendületet, ismét nagy területeket szerzett Kelet- és Közép-Európában. Akkor lett a legnagyobb, amikor Kuba, Afrika bizonyos országai, Vietnám mind-mind a fennhatósága alá tartoztak. Aztán jött a hidegháború vége és megint területeket veszített. A Szovjetunió fokozódó gazdasági lemaradása az új csúcstechnikától egyre nőtt, világgazdasági súlya csökkent, miközben például veszélyessé vált, a nyolcvanas évek elejétől már estek az olajárak is. Afganisztán megszállásának magas költségei miatt, a háború a Szovjetunió „Vietnamjává” vált. A Szovjetunió stratégiailag túlterjeszkedett, világpolitikai ambíciói, szerepvállalása és a világejlődéstől elmaradó gazdaságának teljesítőképessége között óriási szakadék volt. A jecini eladósodottság után a putyini erős kezű kormányzás, a nyersanyagok vilápiaci árának erősödése magával vonta Oroszország gazdasági és katonai megerősödését. Újra a világpolitika egyik meghatározó hatalmává vált. (Szerző megjegyzése)

⁸⁹BUNDESAKADEMIE FÜR SICHEHEITSPOLITIK: *Sicherheitspolitik in neuen Dimensionen, Ergänzungsband 2*, Verlag E.S. Mittler & Sohn GmbH, Hamburg, 2009, pp. 363 – 402, ISBN 3-8132-0823-0

Szomáliában, Libériában, Líbiában, Afganisztánban, majd Szíriában és Irakban. Az IS⁹⁰ megjelenése, térnyerése és megerősödése a közelmúlt legismertebb példája. Az állam összeomlása nagyban hozzájárul például a szervezett bűnözés vagy a terrorizmus megerősödéséhez. Az állam működésképtelensége riasztó jelenség az adott régióban, amely ellehetetleníti a globális kormányzást, fokozza a regionális bizonytalanságot és bizonyos esetekben „dominóhatást” is elindíthat.

Szervezett bűnözés

A szervezett bűnözést több olyan egymással szoros kapcsolatot fenntartó bűnözői körök, csoportok hajtják végre, amelyek törvénytelen módszereiket lehetőleg törvényesnek tüntetik fel. Ezek a bűnözői körök is profitorientáltak.

Szervezeti felépítésüknél előszeretettel alkalmazzák a „hálózatos” kapcsolattartást. Ez biztosítja a „független” irányítást, de bizonyos esetekben a központi (direkt) irányítási rendszert is alkalmazhatják. A csoportokon belül nagyon fontos a „hierarchikus” szervezet kialakítása, fenntartása és működtetése.⁹¹

A szervezett bűnözéssel a XXI. században már globális szereplőként kell számolni. Azokban az országokban, amelyek stabilitása megkérdőjelezhető. Beépülnek a politikai pártokba, az államigazgatásba és a gazdasági élet különböző szektoraiba. A szervezett bűnözés kiemelt működési területei a kábítószer-kereskedelem, emberkereskedelem, pénzmosás, fegyverkereskedelem.⁹²

A terrorizmussal való együttműködésük addig lehetséges, amíg a céljaik megegyeznek, vagy egy külön feladat végrehajtására kötnek megállapodást.

Terrorizmus

Az elmúlt évtizedekben a terrorizmus jelentős változásokon ment át. A terrorizmus nemzetközivé vált. Ez egyrészt köszönhető az emberek mobilitásának nagymértékű növekedésének, másrészt a civilizációs ellentétek erősödésének, amelyet a kulturális és vallási különbségek felerősödése okoz. Az 1970-es években az ideológia volt a domináns, de ez mára már háttérbe szorult. Az iszlám terrorizmusnak alap ideológiájává a vallási és a

⁹⁰ IS - Islamic State – Iszlám Állam

⁹¹ KENEDLI Tamás r.őrnagy: *Ellemzéseközpontú információfeldolgozás a szervezett bűnözés és a terrorizmus elleni harcban*, Doktori (PhD) értekezés, pp. 51-56

⁹² WESSEL, Jan: *Organisierte Kriminalität und soziale Kontrolle*, Springer Fachmedien Wiesbaden GmbH, 2001, ISBN 978-3-8244-441-0, pp. 54 -55, 96

kulturális különbségeken alapuló filozófia vált. A terrorizmus egyre inkább egy kommunikációs stratégia, amely a médián keresztül fenyegeti, és különböző tettekkel sokkolja a közvéleményt. A terroristák kihasználják a nemzetközi média által biztosított egyre növekvő érdeklődést. A médiában a terrorcselekményekről szóló híradások mindig a címlapokon szerepelnek. A terrorista támadások többségét a 70-es és 80-as években hagyományos eszközökkel (bombák és tűzfegyverek) hajtották végre. A 90-es évek közepétől a terroristák tömegpusztító fegyverek alkalmazásával terveztek és hajtottak végre terrortámadásokat. Támadásokat hajtottak végre kémiai⁹³ és biológiai⁹⁴ fegyverekkel, kísérleteket folytattak radiológiai fegyverekkel. A nukleáris fegyverek használata a terroristák által azonban valószínűtlen a belátható jövőben.

A terroristák fenyegetéssel már nem egyes személyekre vagy kisebb csoportokra akarnak nyomást gyakorolni, hanem a közvéleményre. A célpontok kiválasztásánál inkább szimbolikus helyeket, épületeket és az általuk képviselt értékeket részesítik előnyben, mert ezzel érhetőek el a terrorizmus alapvető célkitűzései.

Célpontok kiválasztásának szempontjai:

- > A támadásoktól való félelem,
- > Az események nagy média visszhangja,
- > Azon helyek, ahol több ember tartózkodik egyszerre.

Ezen elvek alapján kiválasztott „puha” célpontok, kevésbé védettek, mint egy politikai, más államigazgatási vagy fontosabb gazdasági szereplő, akik folyamatos védelemmel rendelkeznek.

Szemben a hagyományos terrorista csoportokkal a mai terrorista csoportok „franchise”⁹⁵ vagy „outsourcing”⁹⁶ rendszerben dolgoznak és hálózat alapú kapcsolatot tartanak.

⁹³ 1995-ben a Tokiói metróban a Aum Sinrikjo (Legfőbb Igazság) nevű szekta követett el ideg-gáztámadást szaringázzal, 16 halott és több mint 6000 sérült. (A szerző megjegyzése)

⁹⁴ 2001-ben Floridában történt az első Antrax (lépfene) fertőzés, majd a szenátus egy tagja kapott lépfenebaktériumot tartalmazó borítékot és további fertőzések során öten veszítették életüket és 17-en betegedtek meg. (A szerző megjegyzése)

⁹⁵ A különböző csoportok közötti „szerződéses” kapcsolat, amely megállapodás szerint az egyik fél - a rendszergazda – eszközöket, módszereket, kiképzést biztosít a másik félnek, így az átvevő a rendszernek megfelelően működteti terrorszervezetét. (A szerző megjegyzése)

⁹⁶ Outsourcing tevékenységen azt a különleges folyamatot értjük, amelyben egy terrorista szervezet saját erőforrásaival, módszereivel, tevékenységeit és „szolgáltatásait” „térítés ellenében” a megbízást adó

Törvénytelen és illegális gazdasági tevékenységet folytatnak és kapcsolatot tartanak szervezett bűnözői körökkel, hogy kihasználják egyrészt a finanszírozási lehetőségeket, másrészt a már működő logisztikai láncot.

A XXI. században megjelent egy új elkövetési módszer, az öngyilkos merénylők által elkövetett támadások. Az öngyilkos merényleteket általában a vallási-kulturális alapokon működő terrorszervezetek alkalmazzák különböző csoportok vagy az adott régió többségi társadalmi ellen. Ezt a terrorszervezetek azon fanatikus tagjai követik el, akik fundamentalista nézeteket követnek. A többségi társadalom megfélemlítésének „legeredményesebb“ formája. A „klasszikus“ terrortámadásoktól abban tér el jelentősen, hogy menekülési tervet, útvonalat nem terveznek. Viszont az esemény dokumentálását pontosan megtervezik és röviddel a támadás után már megjelentetik a médiában. A merényleteket hagyományos módszerekkel⁹⁷, ritkábban tömegpusztító fegyverekkel⁹⁸, valamint repülőgépekkel⁹⁹ és különböző „szükség“ eszközökkel¹⁰⁰ hajtják végre.¹⁰¹

A fejlődésnek előfeltétele a biztonság. A konfliktusok a kritikus infrastruktúrákat rombolják - beleértve a társadalmi infrastruktúrát is –, amely ösztönzést adhat a szervezett bűnözésnek és távol tarthatja a befektetőket, így akadályozhatja a gazdaság normális működését. A terrorfenyegetések és támadások miatt több ország és régió került a konfliktusok, bizonytalanság és szegénység csapdájába.

Cyber¹⁰²-terrorizmus, mint egy új és más formában jelentkező terrorizmus. Az IT¹⁰³ szektorban történt “robbanásszerű” fejlődés, a mindennapi életünkben is jelentős változásokat okozott. Egyre jobban függenek társadalmaink az infokommunikációs hálózatok meglététől és működőképességétől. Ezt a különböző terrorszervezetek felismerték és ezt saját céljaik elérése érdekében lehetőségeik szerint ki is használják.

rendelkezésére bocsájtja. Ezt a tevékenységet a terrorszervezet saját maga is el tudná végezni, de egyéb más megfontolások miatt a támadás végrehajtásával a másik szervezetet bízza meg. (A szervező megjegyzése)

⁹⁷ Lőfegyverek, robbanóanyagok, kések...

⁹⁸ Biológia (Antrax), Vegyi (szarin) harcanyagok

⁹⁹ 2001. szeptember 11-i terrortámadások az USA-ban, (9/11)

¹⁰⁰ Gépjárművekkel hajtanak be nagyobb tömegekbe, késelések...

¹⁰¹ TOMOLYA János – Prof.Dr. PADÁNYI József: A terrorizmus és a gerilla-hadviselés azonosságai és különbségei, HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 24: (1), pp. 127

¹⁰² A cyber (virtuális) téren alapvetően a internetet(világháló), hálózatokat és azokban működtetett hardverek-et és software-eket értjük.

¹⁰³ **IT**: Information technology, információs technológia

A terroristák az internetet használják mint műveleti területet, legyen szó akár a klasszikus felhasználásról, mint például a kapcsolattartás e-mail-en keresztül vagy a propaganda videók terjesztése. Az internet alkalmas az informatikai rendszerek elleni támadások végrehajtására és a hagyományos terrortámadások híradó támogatására. Az IT rendszerek biztonsága szempontjából szükséges, hogy a titkosszolgálatok folyamatosan figyelemmel kísérik és elemezzék a terroristák kommunikációját, számítástechnikai ismereteinek fejlődését és módszereit. Terrorista csoportok egyre magasabb szakértelemmel rendelkeznek és valószínű, hogy felveszik a kapcsolatot egyéb más radikális hacker¹⁰⁴ csoportokkal. Az együttműködésüknek két célja van, a potenciális cyber-támadások elvégzéséhez szükséges technikai és szervezési intézkedések biztosítása, valamint a saját informatikai eszközeik és rendszereik védelme a titkosszolgálatok felderítése ellen.

A jogállamiság fenntartásának egyik alapját képezi a cyber térben működő terrorista csoportok ellenőrzése és tevékenységük folyamatos figyelése. Ez azt feltételezi, hogy a terroristák szakértői-bűnözői csoportokat alkalmaznak egy adott terrortámadás megszervezéséhez és kivitelezéséhez, valamint saját tagjait látják el ma már olcsón és egyszerűen beszerezhető eszközökkel. Ezek segítségével olcsó, gyors és figyelemfelkeltő támadásokat tudnak végrehajtani a cyber térben.

1.2. TERRORIZMUS TERMÉSZETE

A terrorizmust mint jelenséget már több tudományág feldolgozta és több tudományos értekezésben elemezték. Én a terrorizmusról egy általános képet szeretnék adni és nem csak hadtudományi problémaként ismertetni, vizsgálni.

A jelenkor egyik fontos kihívása Európának – így Magyarországnak is – a muszlim terrorizmus, viszont a kritikus infrastruktúrák védelménél nem csak a muszlim terrorizmussal kell számolni, hanem általános értelemben vett terrortámadásokkal, amely független az elkövető(k) vallásától és származásától.¹⁰⁵

¹⁰⁴ Számítástechnikai szakember, akik hálózatokat építenek fel és működtetik, azonban ezen személyek képesek a rendszerekbe „behatolni”, adatkat megváltoztatni vagy eltulajdonítani, stb. ...

¹⁰⁵ Dr. SZTERNÁK György: *A terrorizmus, mint hadtudományi probléma I. rész*, NEMZETVÉDELMI EGYETEMI KÖZLEMÉNYEK, 2005/1

A terrorizmus definíciójának nehézségei

A terrorizmus olyan gyűjtőfogalom, amely nem ismer nemzeti határokat és mélyen gyökerezik az emberiség történetében.¹⁰⁶

A terrorizmus olyan politikai vagy nem politikai motiváltságú erőszak, amely nem állami szereplők szisztematikusan és tervezett formában, a lakosság és az adott közösség, egy/több személy pszichikai befolyásolása céljából hajtanak végre. A fennálló rend/személy elleni műveleteket/támadásokat úgy tervezik, hogy a lehetséges erőszakmentes opciókat elutasítják az arányossággal egyetemben, továbbá figyelmen kívül hagyják az alkalmazott eszközöket és annak várható következményeit. Ez utóbbi megfogalmazásnak igazából akkor van szerepe, amikor az a kérdés merül fel, hogy valaki magányos elkövető, szabadságharcos vagy terrorista. Ezzel kapcsolatban meg kell különböztetni a nem politikai célzatú támadásokat¹⁰⁷, amelyek személyes célok¹⁰⁸ elérése érdekében történnek és nem egy diktatórikus rezsim vagy demokratikus állam ellen. Ismerünk politikai alapfelfogásra vagy egyéni indíttatás hatására elkövetett támadásokat, de az elkövetők esetenként nem fogalmazzák meg politikai célokat.¹⁰⁹

A nem állami szereplők megfogalmazás annyiban különbözik a nem állami csoportoktól, hogy felöleli a magányos elkövetőt is, akinek nincsen kötődése politikai törekvésekhez. Ez az a „magányos harcos”, aki az interneten szerzett ismeretei révén önmagát radikalizálja.¹¹⁰ Az ilyen elkövetők cselekményei azonban ugyanúgy terrorisztikus jellegűek lehetnek, mint a társadalom más részei ellen irányuló támadások. A szélsőjobboldali terroristák általában

¹⁰⁶ „szikáriusok (a lat. *sica*, 'kis tör' szóból: 'törviselők'): fanatikus zsidó szekta, melynek tagjai ruhájuk alatt kis tör hordtak magukkal. Miután a rómaiak kiirtották a zelótákat, a szikáriusok folytatták az ellenállást. Attól sem riadtak vissza, hogy személyes zsidó ellenségeiket orgyilkosság elkövetésével eltegyék láb alól., <http://lexikon.katolikus.hu/S/szik%C3%A1riusok.html> (Letöltve: 2014.10.11.)

¹⁰⁷ családon belüli erőszak, munkahelyi zaklatás, szerelemföltés miatti támadások és túszejtések, szabotázs...

¹⁰⁸ Egy 23 éves férfi (Németország, Ingolstadt) volt barátnőjét folyamatosan zaklatta és naponta több mint 100 SMS-t küldött. A férfi 2013. augusztus 19-én a reggeli órákban az ingolstadt-i városházán három túszt ejtett, a volt barátnőjét, az alpolgármestert és még egy közalkalmazottat. A rendőrség azt feltételezte, hogy a túszejtő fegyverrel rendelkezik. Az alpolgármester elfedése után a másik két túszt még a késő délutáni rendőri beavatkozásig fogva tartotta. Rendőrség különleges erőinek beavatkozásával véget ért késő délután a túszejtés, a két túszt sértetlenül kiszabadult, a túszejtő férfi viszont megsebesült és kórházba szállították. Az egyik túszt a volt barátnője volt, aki az Ingolstadt-i városházán dolgozott. A túszejtő férfi korábban pszichiátriai kezelés alatt és botrányos viselkedése miatt a polgármesteri hivatalból már 2012-ben kitiltották.

¹⁰⁹ GROSS, Emanuel: *The struggle of democracy against terrorism, lessons from the United States the United Kingdom, and Israel*, 2006 by the Rector and Visitors of University of Virginia, pp.11, ISBN: 0-8139-2531-2

¹¹⁰ POLITIETS EFERRETNINGSTJENESTE, DANISH SECURITY AND INTELLIGENCE SERVICE, [Center for Terror Analysis \(CTA\) The role of the Internet in relation to radicalization and terrorism](#), 15. September 2008, p.4. (Letöltve: 2014.10.10.)

kisebbségekhez tartozó személyek ellen követnek el merényleteket és nem alkalmaznak erőszakot az állam képviselőivel vagy intézményeivel szemben. Az ilyenfajta erőszakos cselekmények ennek ellenére az állam megtámadását jelenti, hiszen az állam az a szereplő, aki még azon személyek esetében is garantálni köteles a testi épséget, akik nem saját polgárai.

A terrorizmus fogalma kapcsán felmerülő másik kérdés, hogy az erőszakra kész csoportok milyen mértékben számítanak egy nagyobb mozgalom, szervezet vagy párt részének. Előfordul például, hogy a politikai szereplők rendelkeznek fegyveres szárnyal, az ő esetükben a terrorcsoportra vonatkozó fenti jellemzők nagyon is alkalmazhatóak. Nem volna azonban tartalmilag helyes, ha a gyűjtőszervezeteiket kizárólag a terrorista dimenzióra redukálnánk. Sok esetben ezek mellett ugyanis párt vagy társadalompolitikai szárny is létezik, amely a társadalmi fellépés szempontjából sokkal erőteljesebb jelentőséggel bír.¹¹¹

A terrorizmus szakirodalmából hamar kitűnik, hogy milyen komplex jelenségről van szó. Hiszen a fogalmat egészen eltérő irányultságú, kiterjedésű, valamint erőszakos politikai törekvésekre is használják. Ide számítják a politikai szervezetekhez különösebben nem kapcsolódó magányos tetteket, a sejt-jellegű három-ötös csoportokat, a kb. 20 aktivistából álló és informális hierarchiával rendelkező csoportosulásokat, a több mint 20 főből álló katonai jellegű struktúrával rendelkező csoportosulásokat, amelyek erőszakos elemekkel bírnak és nagyobb politikai mozgalmak vagy pártok részei. Eltérő dimenziók figyelhetők meg az erőszak alkalmazásának konstituáló¹¹² ismérve alapján is. A különböző létesítmények és épületek ellen elkövetett támadásoktól, a nem tervezett személyi sérüléssel és halálessel járó támadásokon át, az egészen konkrét, egyes személyek vagy véletlenül kiválasztott áldozatok ellen elkövetett gyilkosságokig terjed a skála.¹¹³

¹¹¹ Anders Breivik 77 embert ölt meg egy kettős terrortámadás során Norvégiában 2011 júliusában. Breivik Oslo belvárosában a kormány negyedében egy autóba rejtett 950 kg robbanóanyaggal követett el merényletet, majd az egyik norvég szigeten Utoya-n a szociáldemokrata ifjúsági szervezet egy ifjúsági táborában lőtt le 69 résztvevőt. Breivik magát az interneten szélsőjobboldali fórumokon az európai multikulturalizmus és az iszlám elleni háborút kirobbantó „keresztes lovagnak” nevezte. Anders Breivik nem egy neonáci, hanem egy anti-muszlim mozgalom tagja volt tíz éven keresztül. Breivik elmondása szerint, az emberek fel kellene ismerni, hogy a multikulturalizmus elleni harc mennyire fontos és ezért támadta meg a fiatal szociáldemokratákat, mert szerinte ők jelképezték a multikulturalizmust.

¹¹² megállapító, előállító (latin),

¹¹³ PHILPOTT, Don: *Terrorism and Weapons of Mass Destruction: „The Future of Terrorism Task Force”*, Homeland Defense Journal, 04/2007, pp. 16 – 20, ... [...] „Mi [ellenségünk] proaktívak, innovatívak, jó hálózati kapcsolatokkal rendelkeznek, rugalmasak, türelmesek, fiatalok, technológiai hozzáértése és

Újra és újra felmerül tehát a kérdés, hogy a terrorizmus mennyire megfelelő megnevezés e törekvések jellemzésére. Az erőszak intenzitásának és a szervezetek méreteinek eltérései világossá teszik, hogy a tipologizálás értelmében erőteljesebb differenciálás szükséges, hiszen az egyes csoportok különböző ismérvei elmosódnak. Ezért fontos a terrorisztikus törekvések felismerése, besorolása és elemzéshez szükséges séma kidolgozása. Tartalmilag általános szempontokról van szó, amelyek különös szempontok alapján alpontokba sorolhatók. Mielőtt belemennék az alpontokba, ismételten felhívnom a figyelmet a terrorizmus fogalmának meghatározási nehézségeire¹¹⁴. a nyolc ismérvet külön-külön tekintetem át, amely során megmutatkozott, hogy ezek összefüggenek egymással.

A terrorista törekvések

A tényleges terrorista törekvések esetében nem szabad megállni az általános szempontok elemzésénél, hanem mindig vizsgálni kell a környezeti összefüggéseket:

- > a szereplők és az erőszak erősségét,
- > az ideológiát és a kommunikációt,
- > a stratégiát és a szervezetet,
- > a társadalmi viszonyokat és az esetleges támadások hatásainak összefüggéseit.

Előfordulhatnak olyan fejlemények is, amelyek más tényezőktől függetlenül alakulnak ki, ilyenek például a sejtstruktúra felé történő fordulás a különböző ideológiájú terrorizmus esetében. Ezek a szervezeti átalakulások - a tapasztalatok szerint - a bűnüldöző szervek elhárító tevékenységének fokozása miatt változik.

Az alábbiakban felsorolt tényezők segítségével lehet az adott terrorcsoport törekvéseit meghatározni. A kellően gondosan lebontott részszempontok megállapításával pedig pontos profilt lehet alkotni a vizsgált csoportról, annak ideológiai, szervezeti és stratégiai sajátosságai tekintetében. Következő lépés az adott szempontok kontextusának és összefüggéseinek vizsgálata. Ezek után van lehetőség elemezni, hogy milyen potenciális veszélyforrást jelent egy terrorcsoport egy konkrét erőszakos cselekmény vonatkozásában

alkalmazkodó képessége folyamatos, az egész világon ez adja az alapját a sikeres és a sikertelen műveleteiknek ...[...].”

¹¹⁴ Csupán egy munka definíciót kívánok kidolgozni értekezésem számára.

és annak társadalmi hatásait. Lehetővé válik továbbá olyan cselekmények tettesekhez való hipotetikus hozzárendelése, amelyekért nem vállaltak felelősséget.¹¹⁵

Ez egyben a módszer határait is jelenti. Hiszen ez által nem elemezhető a terrortevékenység kialakulásának magyarázata és nem választható ki az anti-terror stratégia sem.¹¹⁶

Ideológia

E kritérium szempontjából a terrorcselekmények tartalmának célkitűzését és politikai okát lehet hozzárendelni az elkövetőkhöz.¹¹⁷

- A) Autonómiára törekvő, illetve szeparatista csoportok, akik egy nemzetállamon belüli etnikai vagy vallási kisebbségként lépnek fel és a csoport nevében egy adott területnek a fennálló államról történő leválását vagy önálló állam alapítását szorgalmazzák.
- B) Fundamentalista, illetve vallási alapú terrorizmus, amely számára elítélendő a szekularizált¹¹⁸ társadalmi rend, amelyet teokratikus¹¹⁹ államberendezkedéssel kíván felváltani.
- C) Nacionalista vagy szélsőjobb csoportok, melyek gyakran etnikai kisebbségek tagjai ellen fordulnak és etnikailag homogén társadalmon alapuló, diktatórikus rendszer felépítésére törekszenek.
- D) Szélsőbal, illetve társadalmi forradalomra törekvő terrorizmus, melynek esetében egy elnyomónak számító reakciós államrend és igazságtalannak tartott tőkés gazdasági rend elleni küzdelemről van szó.

Az ideológia tartalmi jelentősége mellett nagy figyelmet érdemel a politikai irányultsággal összefüggésben a célpontok és az áldozatok csoportjainak elemzése. Például a szélsőbal csoportok általában a politikai és gazdasági elit képviselőit, a szélsőjobb elkövetők pedig az etnikai és vallási kisebbségek tagjait támadják. Előfordulhat azonban, hogy az iszlám

¹¹⁵ RESPERGER István ezredes – KISS Álmos Péter – SOMKUTI Bálint: *Negyedik generációs hadviselés: Néhány alapfogalom*, Zrínyi Kiadó, pp. 8-9, ISBN 9789633275924

¹¹⁶ FUCSKU Sándor: *A válságkezelő műveletekben résztvevő magyar kontingensek terrorfenyegetettsége, a felderítő csapatok különleges felderítő képességei*, Felderítő Szemle, 2006, január, V. évfolyam, pp. 54 – 55.

¹¹⁷ Dr. HANKISS Ágnes előadása: *Kihívások és ellentmondások a terrorizmus elleni harcban*, „A terrorizmus Rubik-kockája” avagy a fenyegetések komplex megközelítése” Nemzetközi tudományos-szakmai konferencia, Budapest, 2013. szeptember 30. – október 1., pp. 3 - 4.

¹¹⁸ az egyház befolyásának visszaszorítására törekvő állami tevékenység, világivá tétel (latin)

¹¹⁹ elméleti (görög)

szélsőjobb és szélsőbal csoportok amerikai és izraeli létesítményeket támadnak, mivel különböző motiváció alapján azonos ellenségképeket követnek.

Stratégia

A terroristák számára a klasszikus terrorcselekmények a győzelemhez vezető közvetett utat jelentik. Számukra az erőszak a terrorcsoport céljai érdekében kiváltott reakciók miatt fontosak. Maga a terrorszervezet politikailag általában nem erős. Ez az oka annak, amiért erőszakhoz folyamodnak, hiszen máskülönben rendelkezésükre állnának nagyobb támogatottságú lehetőségek is, mint például polgárháború, államcsíny, vagy akár jelöltek állítása választások alkalmával.

A stratégia meghatározása szempontjából a terrorszervezetnek át kell tekintenie:

- > az egyes elkövetőket,
- > magát a csoportot és annak közvetlen környezetét,
- > a többségi társadalmat és az államot,
- > a valószínű áldozatok csoportját és más szimpatizáns célcsoportokat.

Ez utóbbi a társadalomnak azon része, melyet az erőszakos cselekménnyel mobilizálni és megszólítani kívánnak. Amennyiben sikertelen a terrorcselekmény vagy az állam reakciója miatt mobilizálhatóak a szimpatizánsok, hiszen a hatóságok az elnyomás fokozása révén kiváltják a felháborodást a terrorcsoporttal rokonszenvező emberekben.¹²⁰

Szervezet

A szervezet elemzése szempontjából a terrorista törekvések esetében különösen érdekes a nagyságrend és a struktúra hierarchizáltságának mértéke. Amennyiben a magányos elkövetőt a terroristákhoz soroljuk, úgy ő jelenti a legkisebb szervezeti formát. Ők általában a médián keresztül, de nem személyes kapcsolatok révén kötődnek különböző terrorcsoportokhoz.

A következő szervezeti forma a 3 – 7 személyes kis sejt, amely külső útmutatás nélkül, önállóan cselekszik. Egy ilyen csoport létezhet önmagában, de lehet egy több sejtből álló konglomerátum¹²¹ tagja is.

¹²⁰ David FROMKIN: *The Strategy of Terrorism*, Foreign Affairs, Tampa, 1975, ISSN 0362-4331

¹²¹ különböző anyagokból (esetleg személyekből) álló halmaz

A terrrorszervezetek harmadik csoportja az informális, kb. 20 fős – egy vezető réteggel irányított – vagy ennél nagyobb számú csoportból álló szervezet, amelyet aktivisták és támogatók egészítenek ki. Szeptember 11-től az Al-Kaida is egy sejtekből álló struktúrára váltott.¹²²

A negyedik csoport egy magasabb szervezettségű és hierarchizáltabb szervezet, akik egyfajta ellenhadseregnek tekintik magukat, amelyet formális rendfokozatok és egyértelmű illetékességek meghatározásával hangsúlyoznak. Erre jó példa az Ír Köztársasági Hadsereg, ami már nevében is hordozza a szervezet jellegét.

A szervezetek ötödik és legmagasabb szintje pedig az a terrorcsoport, ami egy nagyobb mozgalom, csoport vagy párt részeként tevékenykedik. Ezek különleges formájaként említhető az állami terrorizmus, amikor valamely állam kormányának támogatásával tevékenykednek. Ezek már-már állami vagy legalábbis regionális szintet öltő csoportok.¹²³

Vezetők, tagok és aktivisták

Ebben az esetben konkrét egyénekről van szó a terroristaszervezet tagjaiként. Elsődleges fontosságú a szociális összetétel, hogy meg lehet-e figyelni feltűnő közös vonásokat olyan szempontok esetében, mint életkor, szakmai tevékenység, képzettség, nem, származás vagy különböző szervezetekben való tagság.¹²⁴

A szervezetekhez való tartozás sok mindent elmond arról, hogy milyen politikai, társadalmi vagy vallási összefüggéseket kell kiindulási alapként tekinteni. A szakmai tevékenységre és a képzettségre vonatkozó adatok lehetővé teszik azt, hogy megbecsüljük az intellektuális potenciált, ami nagyon fontos különböző cselekmények ideológiai, kommunikációs és gyakorlati/technikai dimenziójának esetében. Az elsődleges kérdés tehát az, hogy milyen társadalmi profil alakítható az adott terrorcsoport tagjairól, ha megfelelő adatokkal rendelkezünk a csoport aktivistáinak számáról, képzettségéről, életrajzáról. Ezek által könnyebben elemezhető az összetételük, valamint jobban rekonstruálható az egyének fejlődése és az a kérdés is, hogyan kezdtek kötődni a terrorcsoportokhoz. Így kiértékelhető közös és eltérő vonásaik. Ebből meghatározható

¹²² GÁL István László: *Új biztonságpolitikai kihívás a XXI. században: A terrorizmus finanszírozása*, KNBSZ Szakmai Szemle, 2012/1., pp. 5 -7.

¹²³ LAKATOS Zsolt: *A terrorista szervezetek felépítése és csoportosítása*, Felderítő Szemle (KFH), 2007/1. pp. 88.

¹²⁴ Prof.Dr. HÁRDI István: *A terrorizmusról*, A Magyar Tudományos Akadémia folyóirata. Alapítás éve: 1840, 170. évfolyam – 2009/8. szám, pp. 934 – 935

milyen mértékben készek a politikával szembeni erőszakra. El kell azonban kerülni a téves következtetéseket, például közös vonások esetében nem feltétlenül szükségszerű, hogy egyetlen ok miatt minden érintett a „terrorkarrier” irányába terelődik, lásd problémás családi viszonyok. Fennáll továbbá a pszichologizálás veszélye, ami az osztálytársadalmi keretfeltételeket hagyja figyelmen kívül. Az egyéni fejlődési utak elemzése során fontos a társadalmi normák és büntetőjogi elvek elfogadásának mértéke. Az erőszak alkalmazása egyfelől az állam erőszak monopóliumának elutasítását, másfelől politikai radikalizációt jelent az egyén erőszakos magatartása egy terrorcsoport ideológiája mellett. Differenciált elemzéshez mindkét szempontot külön-külön, majd kölcsönhatásukat kell elemezni. Ennek során fokozott figyelmet érdemel, hogy mi volt előbb az eltérő magatartás esetén, az erőszakra való hajlandóság vagy az ideológiai fanatizmus. Az utóbbi esetben nagy jelentőséggel bír a politikai felfogás az elemzéstől egészen a prevencióig. Ha azonban már a kezdetektől fogva hajlamos volt az erőszakra, akkor számára ez a fontosabb tényező.

Az erőszak intenzitása

A szereplők felismerése és hozzárendelése szempontjából éppen az erőszak intenzitása az egyik legfontosabb aspektus. A terrorizmus szempontjából az erőszak ugyan konstitutív¹²⁵ jegy, azonban mértéke eltérő. A XX. században elkövetett terrorcselekményekre még jellemző volt az, hogy a támadások célja elsődlegesen egyes személyek tervezett és célzott meggyilkolása. Az ilyen irányú akciók a XIX. századi „modern” terrorizmus korai időszakában ugyan még meghatározóak voltak, később azonban az erőszak intenzitása megnövekedett.¹²⁶

Egy lehetséges besorolás az erkölcsi és büntetőjogi súly szempontjából történhet, ami egzakt mérce a fentiek értelemben. Másképp kell megítélni egy létesítmény ellen elkövetett olyan támadást, amely csak csekély anyagi kárral jár és megint másként egy sok halálos áldozatot követelő merényletet. A terrorcselekmények szempontjából alapvetően meg kell különböztetni a személyek és a tárgyak (objektumok) elleni erőszakot. Az utóbbinál az első és legalacsonyabb intenzitású erőszak a járművek vagy épületek ellen elkövetett

¹²⁵ lényegét meghatározó (latin)

¹²⁶ VARGHA Ferenc: *A terror pszichológiája*, Magyar Jogi Szemle Könyvtára, Pallas Részvénytársaság Nyomdája, 1921, pp. 5, [...] „a terror pszichikai elemei közt nagy szelepet visz a rémület. Ha azonban az egész összetett lelki komplexumot elemezzük, a keletkezési és fejlődési sorrendet szem előtt tartva, a terror szintézisében következő elemeket találjuk: a) a terroristák célkitűzését; b) a érintést; c) a félelmet minden fokozatban; d) engedelmességet és behódolást a megrémültek részéről.” [...]

támadás. Léteznek olyan konkrét helykiválasztások vagy időpont meghatározások, amelyek arról tanúskodhatnak, hogy a tettesek tudatosan megpróbálják kizárni azt, hogy emberek sérüljenek vagy haljanak meg. Amennyiben viszont sebesültekre vagy halálos áldozatokra törekszenek, úgy az elkövető áldozatától való távolsága is növekszik.

A hidegvérűségének mértéke szempontjából az első fokozat, amikor a támadó „távolsága” a mérvadó egy adott akció megítélésében, mert ha saját életét nem kockáztatja, akkor az elkövető elszánt. Támadásával „csak” károkat akar okozni, NEM személyi sérülést. Utóbbi esetben a besorolás lényeges szempont, mert szándékában az is befolyásolja, hogyan fogja megítélni a közvélemény a támadó cselekedetét.

Az erőszak intenzitásának következő – második – fokozata egy ritkán felmerülő eset, amikor a támadó csak kisebb mértékű testi sértésre törekszik, azonban gyakoribb a nem halált okozó súlyosabb testi sértés szándéka.

Az erőszak intenzitásának harmadik fokozata a politikai vagy a gazdasági élet különböző személyiségei esetében végrehajtott életellenes támadás.

Az erőszak intenzitásának negyedik fokozata, amikor tudatosan elfogadják kívülálló személyek halálát is. További megkülönböztetési, illetve besorolási jegy lehet az is, milyen mértékben tervezik, illetve tolerálják a támadók kívülálló személyek megsebesítését vagy meggyilkolását.

Az erőszak intenzitásának ötödik és egyben legmagasabb fokozata a tömeges halálos áldozatokkal járó merénylet.¹²⁷

Kommunikáció¹²⁸

A terrorista törekvések elemzésekor fontos a kommunikáció módja, vagyis az a törekvés, hogyan kívánnak hatást gyakorolni a társadalom egészére vagy egy adott csoportra. Az idevonatkozó erőszakos cselekedetek stratégiai célkitűzése, mint a politikai üzenetek terjesztése, az erőszak elkövetői számára kimagasló fontossággal bírnak. A terrorizmusnak továbbra is az erőszak az egyik legfontosabb eleme és nem a kommunikáció. A média a stratégia fontos része, hiszen a támadások és a merényletek különösen kiemelt célja, hogy

¹²⁷ KAISER Ferenc – TÁLAS Péter: *Politikai erőszakformák*, Nemzet és Biztonság 2012/5-6. szám, pp. 139

¹²⁸ <http://www.spiegel.de/kultur/gesellschaft/medien-und-terrorismus-tausendundein-missverstaendnis-a-472517.html> (Letöltve: 2014.10.11.)

minél szélesebb körben ismertté tegyék az adott csoport politikai felfogását és ehhez a média szerepe nagy jelentőséget kap.

Ennek során meg kell különböztetni a közvetlen és a közvetett felelősségvállalást:

- > a közvetlen felelősségvállalás esetében a tettesek támadásaik és merényleteik után a médiában vagy a tetthelyen helyeznek el felelősségvállaló nyilatkozatokat¹²⁹.
- > A közvetett felelősségvállalás esetén magának a célnak, a helyszínek vagy a célszemélyeknek a kiválasztása hordozza az üzenetet. Ilyenek voltak például az anarchisták támadásai koronás fők ellen a XIX. század második felében.

A kommunikáció esetében fontos tényező még az is, hogy a társadalmat az erőszakos cselekmények révén mozgósítani vagy megfélemlíteni kívánják, az államból pedig azonnali reakciót akarnak kiprovokálni. Ugyanilyen lényeges az áldozatok csoportja is, hiszen az ideológiai irányultságnak megfelelően másképp gondolkodókat, más hitet követőket, katonákat, politikusokat, vállalkozókat vagy bevándorlókat kívánnak nyomás alá helyezni. Fontos célcsoport a környezethez tartozó személyek köre is, hiszen az erőszakos cselekménnyel a szimpatizánsok és támogatók számára sikerélményt akarnak közvetíteni. Nem utolsó szempont a nemzetközi figyelem felkeltése.

Társadalmi háttér¹³⁰

A társadalmi háttér szerepe azért kiemelkedően fontos a terrorcsoportok szempontjából, mivel azok általában elszigetelten tevékenykednek és a társadalmon belül éppen környezetük definiálja a társadalomban elfoglalt helyüket.

A társadalmi háttéren a különböző támogatásokat és azok megjelenési formáit értjük. A legelső szint az adott terrorcsoport illegális és közvetlen támogatása. Ez jelentheti többek között a cselekményeik elkövetéséhez szükséges illegális beszerzések kivitelezését vagy legalábbis támogatását, ami tulajdonképpen egyfajta logisztikai támogatás.

¹²⁹ Ilyen volt például az RAF vagy a későbbi Al-Kaida.

¹³⁰ BOLGÁR Judit – SZTERNÁK György: *A terrorizmus társadalmi és személyiség-lélektani háttere*, ZMNE Hadtudományi Doktori Iskola, Publikációk, 2005, pp. 56 – 57,

A második szintű támogatások, amelyek a közvetett és legális segítséget jelentik. Ebbe a kategóriába tartozik különösen a politikai agitáció az adott csoport céljai mellett, ami kiterjedhet azok teljes cselekedeteire és részeire:

- > az ideológia elfogadására és propaganda révén történő politikai támogatására,
- > sok esetben ezek különböző árnyaltságú és bonyolultságú kombinációjára.

A környezet harmadik szintje a politikai mozgalmak potenciálisan azonos beállítottsága és a terrorcsoport által propagált ellenségkép osztása. Végül pedig elképzelhető a lakosság támogatása, amely a terroristák tevékenységét társadalmilag és erkölcsileg elfogadhatja saját politikai aktivitása nélkül. Minél magasabb a tettesek vélt vagy valós elfogadottsága, annál inkább úgy érzik, hogy társadalmi támogatócsoportjuk nevében cselekszenek.

Hatás

A terror definíciójában nem véletlenül szerepel a rémület/pánik kiváltása. Ezáltal éppen az erőszakos cselekmény lélektani dimenziójára történik utalás. Általában a brutalitás mértéke vagy a célpontok kiválasztása határozza meg azt, hogy milyen mértékben kívánják a terroristák politikai üzeneteiket ilyen módon a nyilvánosság felé kommunikálni. A terroristák ennek megfelelően elemzik cselekményeik hatását abból a szempontból, hogy az elkövetett támadás vagy merénylet milyen mértékű figyelmet kaphat a lakosság, a média, a politikusok és az állam részéről.¹³¹ Az erőszakos cselekményekre való reakció a társadalomban kelthet lelkesedést vagy felháborodást, aminek mértéke általában a kívülálló áldozatok számával függ össze. Az állami reakció szempontjából döntő, hogy belesétál-e az adott kormányzati politika a terroristák számításában rejlő stratégiai csapdába. A rossz reakció egy adott célcsoport vonatkozásában akár még egyfajta utólagos legitimációhoz is juttathatja az erőszakos cselekményt. Ez akár azt is eredményezheti, hogy megnő a tett iránti társadalmi támogatás vagy a cselekmény félelmetes mivoltának kommunikációja révén a lakosság egy része akár félelemből is a terroristák támogatójává válhat.

A különböző erőszakos cselekmények hatása szempontjából célszerű még differenciálni a cselekmények helyét és hatását a környezetre. Ebből a szempontból három típust különböztetünk meg:

¹³¹ BOLZ, Frank Jr. – DUDONIS, Kenneth J. – Schulz, David P., *The Counter-Terrorism Handbook. Tactics, Procedures, and Techniques*. New York, Elsevier, 1990, pp. 4

- > A belső, azaz nemzeti terrorizmust, ahol az áldozatok és az elkövetők ugyanahhoz a nemzetállamhoz tartoznak és az erőszak nem terjed túl annak határain.
- > A külső, illetve nemzetközi terrorizmus, amelynek különlegessége abban rejlik, hogy külföldön is végrehajtanak célzott támadásokat, helyi csoportokkal együttműködve.
- > A transznacionális terrorizmus, amely noha hasonlít az előbbi típusra, de komoly különbségek is fennállnak, hiszen nem csupán regionális, hanem világpolitikai dimenziójú változásra törekszik és nemcsak különböző országokban tevékenykedik, hanem – hatósugarát megnövelve – más nemzetiségű elkövetőkből álló csoportokban is.

1.3. ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A progresszív globalizáció hatásait nem csak világszerte jelentenek biztonsági problémákat, hanem regionális vagy helyi szinten is megjelennek direkt vagy indirekt módon. A szegénység, polgárháborúk és egyéb konfliktusok, katasztrófák menekülthullámot eredményezhetnek a szomszédos országokba és régiókba. Ezeken a területeken biztonságpolitikai veszélyhelyzetek alakulhatnak ki, amelyet az érintett országok, régiók nem megfelelően kezelnek, akkor ez eszkalálódhat a közeli régiókba is. Ezért szükséges a világ válságrégióiban a nemzetközi szervezetek és intézmények szoros együttműködése. Ez azt jelenti, hogy akár egy helyi konfliktushatással lehet a közeli és/vagy távoli régiókra vagy akár az egész világra.

Európa földrajzilag nem egy sziget. Gazdaságilag és politikailag sem tudja magát a világ eseményeitől függetleníteni. Ez azt jelenti, hogy országokban és a kontinensen bekövetkező események közvetve vagy közvetlenül, de mindenképpen érintik Európa biztonságát vagy a lakosság jólétét. Ezen tények tekintetében fontos, hogy Európa ezekre a kihívásokra és fenyegetésekre megfelelő válaszokat tudjon adni.

Az éghajlatváltozás, konfliktusok, gazdasági válságok és államcsődök más országokban is jelentős hatást gyakorolhatnak az emberek migrációs viselkedésre, ahol a biztonságos élethez való jogot az állam vagy nemzetközi szervezetek nem tudják garantálni.

A világpolitikában a nagyhatalmak csak akkor tudnak együttműködni, ha minden egyes hatalomban meg van a szándék a megegyezésre és a szoros együttműködésre. Ezért fontos,

hogy erősítsék az egyes régiók a közös megjelenést és fellépést, így az Európai Unió tagállamai is. Ennek elengedhetetlen előfeltétele az uniós polgárok egyértelmű többségének támogatása.

Összességében az Európai Unió győztese a globalizációnak, de ez nem maradhat mindig így. Ezért fontos a világban végbemenő változások folyamatos követése és a különböző kihívásoknak megfelelő kész válaszok előkészítése.

Az energia és a nyersanyagok biztosításában harmadik országbeli beszállítókra vagyunk utalva. Ez a kitétség nagyban befolyásolja a már megszokott életmódunkat és jólétünket. Minél több biztos és demokratikus nemzet állam létezik a világon, annál nagyobb lesz a bizalom a világban. Az Európai Unió ezért szorgalmazza a harmadik világ országainak felzárkóztatását, gazdasági fejlesztését és a demokratizálódási folyamatok beindítását és kiteljesedését.

Az elmúlt időszakban jelentős változások történtek a terrorizmus ideológiájában és az alkalmazott módszerekben. A terrorizmus globálissá vált, amely kihasználja a globalizáció adta technikai vívmányokat és vissza is él ezekkel¹³². a civilizációs ellentétek csak tovább növekedtek, amit a kulturális és vallási különbségek felerősödése okozott. A XX. század végére az ideológiai különbségeken volt a hangsúly, de ez a XXI. században már teljesen megváltozott. Az iszlám terrorizmus alapját a vallási és a kulturális különbségeken alapuló filozófia váltotta fel. A terrorizmus egyre tudatosabban használja ki a média adta lehetőségeket, amely segítségével fenyegeti és terrortámadásaival sokkolja a világ közvéleményét.

A jövő biztonságpolitikája több dimenzióból épül fel, úgy, mint diplomáciai (politikai), gazdasági, katonai, társadalmi és ökológiai.

A nemzetállamok meghatározzák saját érdekeiket, amelyek alapját képezik a nemzeti biztonsági stratégiának. Ezt meghatározza az állam geopolitikai és geostratégiai helyzete, gazdasági lehetőségei. Az országok stratégiáját befolyásolják a nemzetközi szervezetekben való tagsága és egyéb más kötelezettségek.

Ez utóbbi felsorolás alapján kell a biztonsági erőfeszítéseket és új szabályzókat kialakítani,

¹³² Telekommunikációs eszközök elterjedése, az emberek és áruk mobilitásának ugrásszerű növekedése, stb.

amelyek multilaterális rendszerben valósulhatnak meg, azaz figyelembe véve összregionális (európai) elvárásokat.

A nemzeti biztonsági stratégiának tartalmaznia kell:

- > biztonságpolitikai környezetet,
- > az ország helyét és biztonságpolitikai érdekeit a világban,
- > az országot érintő biztonsági fenyegetéseket, kihívásokat és azok kezelését,
- > a Nemzeti Biztonsági Stratégia végrehajtásának eszközrendszerét.

Európa, így Magyarország biztonsági helyzetének nagymértékű változásának vagyunk szemtanúi. A válság övezetek megközelítették az Európai Unió külső határait, mint például az Észak-Afrikában, Ukrajnában és a Közel-Keleten keletkezett válságövezetek. Így megváltozott a biztonsági helyzet Európában és az elkövetkező időkben nem várható mérséklődés. Szükségesnek látom, hogy az Európai Unió és a NATO biztonság- és védelempolitika elveinek felülvizsgálatát, új stratégiai elgondolások kidolgozását és ezek megjelenését az operatív feladatok végrehajtása során. A jelenlegi konfliktusok már nem megoldhatók az egyes államok szintjén, ezért szükséges a nemzetközi együttműködés.

2. FEJEZET: TERRORIZMUS PROBLÉMÁI

2.1. TERRORIZMUS HATÁSA A VILÁG GAZDASÁGÁRA

A 2001. szeptember 11-i terrortámadások¹³³ után tudatosodott a nyugati civilizációkban, hogy egy új korszak kezdődött a globalizált világban, amelynek hatása csak történelmi dimenzióban lesz érzékelhető és értékelhető. A terrortámadásokról világszerte megjelent képeknek nagy hatása volt, de több évvel később a terrorellenes műveletek első

¹³³ GAZDAG Ferenc: *Biztonságpolitika*, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2011, pp. 177, ISBN 978-615-5057-23-6, [...] „A nemzetközi terrorizmus megítélésében az alapvető fordulatot az Egyesült Államok ellen 2001. Szeptember 11-én elkövetett öngyilkos merényletek hozták. [...] ...Előbb a New York-i World Trade Center két ikertornyát érte csapás, aminek következtében néhány órán belül mindkét épület összeomlott, majd a Pentagonra zuhant egy eltérített gép, míg a negyedik gép – a feltevések szerint az utasok ellenállása miatt- nem érte el Washington, hanem attól mintegy negyedórányi távolságra lezuhant. ...[...] a nemzetközi életben egyedüli szuperhatalomként maradt Egyesült Államokat meglepetésszerűen érte a saját területén ellene intézett támadás. Hatására Bush elnök meghirdette a terrorizmus elleni háborút, ... [..] ENSZ-felhatalmazásbirtokában az USA nemzetközi koalíciót szervezett (Operation Endurung Freedom) az Afganisztánban végrehajtott művelethez.”

tapasztalatainak elemzése során bizonyosodott be, hogy az afganisztáni és az iraki missziók „eredményei” nem győzték meg a nemzetközi szereplők egy részét.¹³⁴

A terrorizmus világgazdaságra gyakorolt hatását a 2001-es terrortámadások vizsgálatán keresztül szeretném bemutatni, mert ezen események elemzéséről áll rendelkezésre megfelelő mennyiségű szakirodalom.

A globalizáció miatti óriási gazdasági jólét nem csak előnyöket jelent, hanem magában foglal kockázatokat is. A 2001-es terrortámadások előtt már jelentősek voltak a szélsőségesek és a globalizáció kritikusainak támadásai annak nyerteseivel szemben. Ez felveti azokat a kérdéseket, hogy milyen jellemzői vannak (lesznek) az új globális terrorizmusnak és milyen gazdasági hatása van a terror elleni harcnak és a terrortámadásoknak.¹³⁵

A 2001-es támadások után kezdték a szakértők vizsgálni az események hatását a világgazdaságra és különböző ágazataira. Egyértelműen megállapítható, hogy a támadások közvetett kárai nagyobbak, mint a közvetlen károk mértéke. Ezek hatásai jelentkeztek a világ több régiójában, valamint hosszú távon befolyásolta a globális gazdaságot. Amerikában és Európában a támadások tovább gyengítették a már törékeny fogyasztói bizalmat, ami fokozódott a madridi és londoni támadások után. A bizalomvesztés és a kereslet esése, valamint a megnövekedett tranzakciós költségek világszerte tovább emelték a gazdasági veszteségeket, így ez már biztonságpolitikai kockázatot is jelentett.¹³⁶

Az USA-nak és az EU-nak közvetett károkat is okozott a terrorizmus és az ellene való küzdelem. A világgazdaság gyengülésének oka a fogyasztói bizalom csökkenése, amely kihatott az energiahordozók árának csökkenésre, viszont az iraki háború idején növekedés volt tapasztalható. Ezért a nyugat érdeke, hogy pozitív kompenzációs intézkedésekkel növekedési pályára állítsák a világgazdaságot, amelynek egyik eleme a fejlődő országokkal folytatott kereskedelem fellendítése volt, valamint a kereskedelmi akadályok csökkentése, amit a WTO¹³⁷-tárgyalások eredményeztek. Ezeken túlmenően a terrorizmus

¹³⁴ Dr. RESPERGER István: *Az iszlám világ és hatása a biztonságra*, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003, pp. 50 - 53

¹³⁵ STIFTUNG ENTWICKLUNG UND FRIEDEN: *Globale Trends 2007*, Bonn 2006, pp. 107 – 108, ISBN 3-89331-739-2

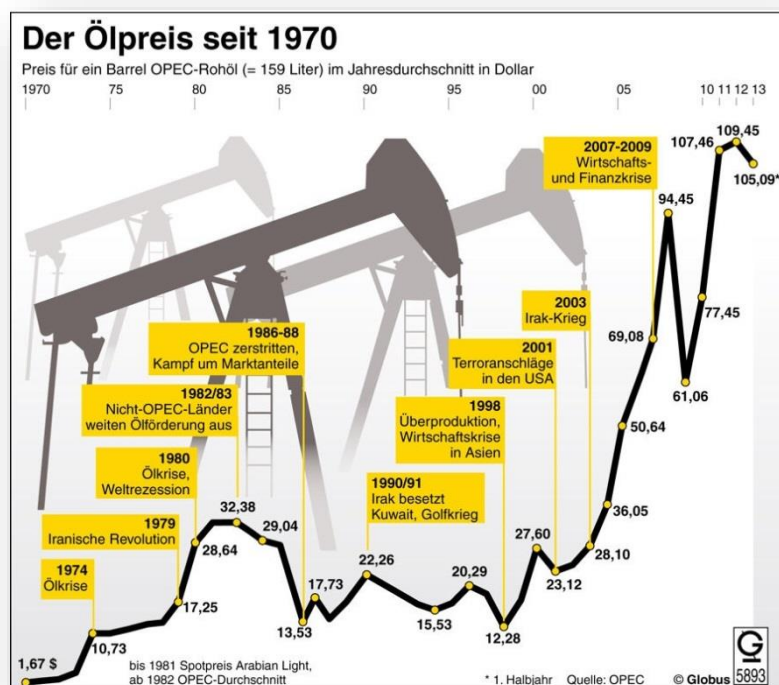
¹³⁶ STIFTUNG ENTWICKLUNG UND FRIEDEN: *Globale Trends 2007*, Bonn 2006, ISBN: 3-89331-739-2, p. 114 - 115

¹³⁷ Kereskedelmi Világszervezet: World Trade Organization, multilaterális kereskedelmi szervezet és a nemzetközi kereskedelem liberalizációját tűzte ki célul, Szerző megjegyzése

elleni harc a válságok katonai eszkalációjához vezetett, ami negatívan hatott a várt előnyökhöz képest. A madridi merényletekkel¹³⁸ összehasonlítva látható, hogy a szeptember 11-i támadások hatására a pénzügyi piacok jelentősen kisebb mértékű gyengülést mutattak, melynek oka a kormányzatok és hatóságok hatásos és gyors beavatkozása.¹³⁹

Az új globális terrortámadások gazdasági következményei

A nemzetközi szakértők szerint több évvel a támadások után a probléma összetettebb volt, mint eredetileg gondolták. Pozitív hatással volt a támadások utáni időszakban, hogy a dollár nem veszítette el stabil árfolyamát.¹⁴⁰



2. Számú ábra: Olajár 1970-től,

Forrás: Bundeszentrale für politische Bildung,
<http://www.bpb.de/politik/hintergrund-aktuell/172918/autofreier-sonntag-1973>
(Letöltve: 2014.12.29.)

¹³⁸ 2004. március 11-én végrehajtott terrortámadásokban 191 ember halt meg és 1800 sérültek meg, 10 robbanás történt négy vonaton. Szerző megjegyzése

¹³⁹ R. Barry JOHNSTON and Oana M. NEDELESCU: *The Impact of Terrorism on Financial Markets*, © International Monetary Fund, 2005

¹⁴⁰ Tilman BRÜCK: *The Economic Analysis of Terrorism*, Routledge, New York, 2007, ISBN1134216475, pp. 83 - 107

A folyamatos nemzetközi tőkeáramlás és az olajár „stagnálása” (4 dolláros csökkenése)¹⁴¹ ellensúlyozni tudta a befektetőket ért sokkot, valamint a FED¹⁴² és a nyugati államok programjai segítségével a légi szállítási ágazatban minimalizálni tudták a keletkezett károkat, így biztosították a cégek további működését. Összességében a devizaárfolyamokat nem érintette a támadások hatása. A globális tranzakciós költségek növekedése megállíthatatlannak tűnt, amit a különböző piacok és kormányok a fiskális terhek növelésével és a gazdasági kockázatok csökkentésével próbáltak enyhíteni.

A repülőgépekkel végrehajtott terrortámadások hatását fokozták a valós és vélt Antrax¹⁴³ fenyegetések, amelyek tovább növelték az amúgy is nagy bizonytalanságot. A világgazdaságban még mindig érzékelhetőek a szeptember 11-i események közvetett negatív hatásai.

A globális pénzügyi piacok stabilizálása

A politikai megrázkódtatás a világ pénzpiacait a szeptember 11-i támadások után tartósan befolyásolta. A korábbi politikai válságok, mint a kubai rakétaválság, vagy a kuvaiti háború „csak” bizonytalanságot okoztak a világ tőzsdéin, de komolyabb sokk nem érte a világgazdaság működését.

A XXI. században a kormányok, a nemzeti bankok és a piacok szakértői nem készültek fel megfelelően egy azonnal bekövetkező, a világgazdaság egészére kiható, előre nem látható válság kezelésére. A pénzpiacokra jellemző a mély integráció, a megnövekedett információ forgalom, a közvetlen függőség a pénzügyi szektoron belül, valamint közvetett módon egyéb más ágazatoktól. A terrortámadások bebizonyították, hogy a politikai válságok egyre nagyobb hatást gyakorolnak a pénzügyi szektorra és annak működésére. A befektetőknek új kockázati struktúrákat kellett kialakítaniuk. Bebizonyosodott, hogy a korábbi válságok nem befolyásolták nagymértékben a pénzpiacok működését, de a XXI. század információforradalma jelentős hatással bír a világgazdaság működésére. A terrortámadások jelentős hatással vannak a pénzpiacok működésére és így a nemzetállamok működésére,

¹⁴¹ Lásd: 2. számú ábra

¹⁴² Federal Reserve System: Szövetségi Tartalék Rendszer. Az USA központi banki rendszere, a Federal Reserve vegyes állami-privát rendszerben működik, Szerző megjegyzése

¹⁴³ vagy más néven lépfene, egy baktérium által okozott fertőző betegség, amely minden melegvérű állatot veszélyeztet természetes körülmények között, de az emberre is áttérjedhet, beteg állatokkal vagy fertőzött állati termékekkel való közvetlen érintkezés révén, Szerző megjegyzése

valamint adott esetben a válságok továbbgyűrűzhetnek más országokba is. A különböző országokban más és más kihívásokat jelenthetnek.¹⁴⁴

A kormányzatok és nemzeti bankok felelőssége a válságok rugalmas kezelése, ahol a megfelelő monetáris és fiskális politika, valamint a tőzsdék szabályozása biztosíthat nagyobb mozgásteret a kormányzatnak. Egy adott válságot időben és megfelelően kezelő kormányzat biztosít kellő likviditást és piaci stabilitást, amellyel megelőzhető az esteleges pánik.¹⁴⁵

A tranzakciós költségekre gyakorolt hatás

A kormányok, a vállalatok és az emberek mindennapi életének szintjén világszerte megerősítették a biztonsági rendszabályokat és újabb intézkedéseket vezettek be. Ezek az intézkedések új jogi környezet kialakítását követelték meg, amelyek első sorban a légi közlekedést érintették. Azonban a vállalatok és az emberek mindennapi életét megnehezítették. További biztonsági intézkedéseket vezettek be az információvédelem területén, ami az infó-kommunikációs csatornák ellenőrzését (lehallgatását) és biztonságát jelentette. Ezen intézkedések csökkenték az érintett cégek nyereségét, a kialakult biztonsági helyzet miatt a védelemre fordított költségek jelentősen megnövekedtek.¹⁴⁶

Természetesen ezen plusz költségek megjelentek a termékekben és szolgáltatásokban, ami a vásárlóerő és a kereslet csökkenését vonta maga után. Ezeket a biztonsági költségeket nem tekinthetjük adóemelésnek, de hatásukat tekintve hasonlóak voltak. Ezeket a negatív hatásokat további kormányzati kiadásokkal lehetett finanszírozni. A nyugati kormányzatok fontos célnak tartották a már kialakított társadalmi jólét fenntartását és a vállalatok működőképességének biztosítását. Az így kialakított feltételek hatására a nyugati társadalmakban hosszú távú pozitív visszajelzést diagnosztizáltak, mert az emberekben tudatosult, hogy a termékek és szolgáltatások biztonsága egyaránt fontos érdeke a közösségnek és az egyénnek.

¹⁴⁴ Roger M. KUBARYCH: *“Aftermath of the Terrorist Attack: Economic, Financial and Policy Consequences.”* Council on Foreign Relations. *council on foreign relations*, 2011, ISSN: 0015-7120

¹⁴⁵ R. Barry JOHNSTON and Oana M. NEDELESCU: *The Impact of Terrorism on Financial Markets*, © 2005 International Monetary Fund, p. 8 - 9.

¹⁴⁶ Jim SAXTON: Chairman Joint Economic Committee United States Congress: *The Economic Cost of Terrorism*, p. 11. <http://www.jec.senate.gov/public/cache/files/79137416-2853-440b-9bbe-e1e75d40a79d/the-economic-costs-of-terrorism---may-2002.pdf> (Letöltve:2015.01.05.)

Szakértők szerint az USA katonai költségvetése stagnált, viszont a kormányzat biztonsági kiadásai a további védelmi intézkedések miatt jelentősen megnövekedtek.

Az USA belbiztonsági kiadásai 2001 előtt 0,1 %-át tették ki a bruttó hazai terméknek, 2001 szeptembere után ez 0,35 %-ra emelkedett, ami több mint háromszoros növekedést jelentett.¹⁴⁷

A tranzakciós költségek a nemzetközi kereskedelem és a turizmus területén - például a közlekedésben - a támadások után közvetlenül jelentősen nőttek. Becslések szerint a termékek és szolgáltatások tranzakciós költségei az OECD országokban 3 százalékponttal növekedtek.

Az Egyesült Államokban a megnövekedett biztonsági kiadások miatt a munkaerő termelékenysége 1,12 %-kal, a teljes gazdaság termelékenysége 0,63 %-kal csökkent.¹⁴⁸

Terrortámadások miatti kereslet csökkenés

A szeptember 11-i támadás utáni kereslet csökkenés nem csak az Egyesült Államokban volt jelentős, hanem Németországban is érezhető volt. Ennek következtében a német kormány az állami kiadásokban új prioritásokat állított fel, így a mindennapi életre nem volt jelentős hatása. A költségvetés korrekációjával a kormány rövidtávon tud beavatkozni a gazdaság működésébe, de ez is csak korlátozott mértékben valósult meg. Közép és hosszú távon a kormányok a gazdaság szereplőit különböző intézkedésekkel tudják támogatni.

A kereslet csökkenés alapvetően csak bizonyos régiókban és ágazatokban jelentkezik közvetlen módon. A közvetlen hatás elsődlegesen a légitársaságoknál járt azonnali kereslet csökkenéssel, ami érintette az összes társaságot világszerte. Ezek árcsökkentéssel próbálták a károkat minimalizálni, valamint a tőzsdén csökkentették teljes portfóliójuk kockázatát. Szeptember 11. előtt is pénzügyi gondjai voltak a legtöbb légitársaságnak, ezért a részvények kockázati felárát a pénzpiac megduplázta. A csökkenő tendencia után a szektort ismét növekedés jellemezte, de a nagyobb kockázatnak megfelelően magasabb hozamokat generált, hogy a további kockázatokat tudják kompenzálni. A gazdaság

¹⁴⁷ Bart HOBIJN: *What Will Homeland Security Cost?*, FRBNY Economic Policy Review, November 2002, p. 22

¹⁴⁸ Bart HOBIJN: *What Will Homeland Security Cost?*, Federal Reserve Bank of New York, May 2002, p. 3

történelmében példa nélküli volt ez a nagymértékű kereslet csökkenés, amely közvetlenül csak egy ágazatot érintett.

A kereslet csökkenése a turizmusra és a hozzá kapcsolódó ágazatokra (szállás, közlekedés, vendéglátás ...) is jelentős hatással volt. Az Amerikai Egyesült Államokban a beutazások miatt 2000-hez képest több mint 22%-al csökkent 2003-ban, majd csak 2005-ben közelítette meg az öt évvel az előtti szintet.¹⁴⁹

A terrortámadásoknak a biztonsági szektor lett a győztese, mert a különböző nemzetközi szervezetek és nemzetállamok biztonsági intézkedéseinek hatására új technikai eszközöket szereztek be, illetve az alkalmazott személyi állomány létszámát is megnövelték.

Megnövekedett kockázati felár és a biztosítási feltételek átalakulása

A biztosítási ágazat nem volt felkészülve a szeptember 11-i eseményekre, mert nem számítottak arra, hogy több terrortámadást hajtanak végre egy időben, országban több objektum ellen, valamint a lehetséges károkat alulbecsülték. Amennyiben a hasonló méretű terrortámadások folytatódtak volna, akkor szükségessé vált volna a kormányzati szerepvállalás a biztosítási ágazatban is.¹⁵⁰

2001-től újragondolták a biztosítási szerződéseket és a maximális lehetséges károkkal számoltak. Vannak például olyan szerződések, amelyekben a terrorista támadások által okozott kár nagyságát maximalizálták vagy teljesen kizárták. A jelenleg érvényben lévő szerződéseket felülvizsgálták és a biztosítási díjakat a kockázatokhoz igazították. A biztosító társaságoknak gondot okozott, hogy az ő részvényeik is a pénzpiacon voltak és a már jelenlévő bizonytalanság kihatott az ő értékpapírjaikra is.¹⁵¹

¹⁴⁹ VARGA Henriett – BAGDI Róbert: *A terrorizmus hatása a nemzetközi idegenforgalomra*, Károly Róbert Főiskola Tudományos Tanácsa, Acta Carolus Robertus, 2011/2, pp. 175 - 186

¹⁵⁰ Jeffrey E. THOMAS: *Do the Costs Justify the Benefits?* Symposium: The Law and Economics of Providing Compensation for Harm Caused by Terrorism, Indiana University–Purdue University Indianapolis, 2003/2, pp. 402

¹⁵¹ Jeffrey E. THOMAS: *Do the Costs Justify the Benefits?* Symposium: The Law and Economics of Providing Compensation for Harm Caused by Terrorism, Indiana University–Purdue University Indianapolis, 2003/2, pp. 408

Terrortámadások hatása a nemzetközi kereskedelemre

A terrortámadások nemzetközi trendekre gyakorolt hatása attól fog függeni, hogy a támadás hol és mikor következik be. A hatása leginkább a külkereskedelemre lesz a legnagyobb, mert további tranzakciós költségeket okoznak.

Várható hatások:

- > Bizonytalanság a pénzpiacon és a befektetők körében,
- > Akadályozhatják a külkereskedelmet,
- > Növelik a költségeket az üzleti életben,
- > Befektetői hajlam csökkenése,
- > Fogyasztói bizalom, vásárlási hajlandóság csökkenése,
- > Külkereskedelmi szerződések magasabb kockázati szinten valósulnak meg,
- > A biztosítás költségeinek növekedése,
- > Biztonsági intézkedések lassíthatják a külkereskedelmi folyamatokat,
- > A biztonsági költségek az állami és nem állami szereplőknél növekednek,
- > Szállítási útvonalak megváltozása, szállítási határidők és költségek növekedése.

Kritikus infrastruktúrák támadása esetén az állam és a gazdaság (termelés, szolgáltatások) működésében és a lakosság ellátásában zavarok keletkezhetnek.

Fontos feladat a lehetséges terrortámadások előrejelzése, amely megköveteli a XXI. század technikáján alapuló titkosszolgálati módszerek, együttműködések kialakítását és eszközök alkalmazását, amelyek a nemzetállamok feladatai. A gazdaság és a pénzpiacok szereplőinek fel kell készülniük az esetleges támadások következményeinek kárenyhítésére. Ezért fontos feladat a fenyegetések időbeni megelőzése intézkedésekkel és forgatókönyvek kidolgozásával, valamint ezek alkalmazásával.¹⁵²

2.1.2. Terrorizmus hatása a kritikus infrastruktúrák működésére

Egy multinacionális nagyvállalatnál, amelynek exportvezérelt termelése az ország GDP¹⁵³-jének is meghatározó eleme, különösen fontos a termelési folyamatok biztonsága. Egy új termelőegység indítása során, már a tervezés első fázisától kezdve fontos szempont a

¹⁵² STAATSSSEKRETARIAT FÜR WIRTSCHAFT SECO: *Auswirkungen der Terroranschläge auf die Weltwirtschaft*, <http://www.seco.admin.ch/themen/00374/00375/00381/05253/index.html> (Letöltve:2015.01.05.)

¹⁵³ GDP - Gross Domestic Product (angol), mérőszám: egy adott idő alatti gazdasági termelés

biztonsági feltételrendszer kidolgozása. Ennek során összhangba kell hozni a külső szabályozókban általánosan megfogalmazott biztonsági követelményeket az adott beruházás költségkeretein belül megvalósítható „szükséges” biztonsággal. Ez egy optimum kereső folyamat, ahol a biztonság olyan közös érték, ami a külső és belső partnerek számára egyaránt fontos.

A nagyvállalatok kiemelt hangsúlyt fektetnek a biztonságon felül a termelési folyamatok folytonosságára is. Ezt az értekezésemben tárgyalandó számos alrendszer szolgálja ki, amelyek a külső és belső szabályozás szempontjából külön-külön kritikus infrastruktúrát képeznek. Egy új termelőegység indítása során, már a tervezés első fázisától kezdve fontos szempont a biztonsági koncepció megfogalmazása. Ennek során összhangba kell hozni a külső szabályozókban általánosan és elvontan megfogalmazott, ezáltal a maximumra törekvő biztonsági követelményeket az adott beruházás költségkeretein belül megvalósítható „szükséges” biztonsággal¹⁵⁴.

2.2. TERRORIZMUS ELLENI KÜZDELEM RÉSZTVEVŐI

2.2.1. Kormányzati (titkosszolgálati és rendészeti) feladatok

A rendvédelmi szolgálatok képességeinek áttekintése és átalakítása

A 2004-es a madridi terrortámadások után az állam- és kormányfők Európai Tanácsának március 25-26-i ülésén elfogadták a terrorizmus elleni Nyilatkozatot.

Magyarországon a belügyminisztert egy tárcaközi bizottság felállításával bízták meg a Nyilatkozatban foglalt feladatok teljesítésére. Feladata volt egy akcióterv kidolgozása a terrorizmus elleni harc nemzeti feladatairól, a felelőseikről és a határidőkről. A terv kormányhatározatban¹⁵⁵ jelent meg.

Az akcióterv több rövid, közép és hosszú távú feladatot határozott meg, amelyek végrehajtásához a Kormány közel 2 milliárd forintot biztosított.

A kormányhatározat - a belügyminiszter vezetésével - megalakította a Terrorizmus Elleni Tárcaközi Munkacsoportot. A munkacsoportot úgy alakították ki, hogy a vezetés és

¹⁵⁴ a biztonsági beruházás költségeinek meg kell térülni a piac által elismert termékárban

¹⁵⁵ 2112/2004. (V. 7.)

irányítás három szinten valósuljon meg. A politika szintjén hozzák a stratégiai döntéseket a Nemzetbiztonsági Kormánykabinetben¹⁵⁶.

A középszintű feladatok végrehajtása a Terrorizmus Elleni Tárcaközi Munkacsoport feladata. A NATO-val, EU-val és más nemzetközi szervezetekkel szoros együttműködésben vesz részt a terrorizmus ellen végrehajtott tevékenység folyamatos figyelemmel kísérésében, trendek kidolgozásában a kormányzati szervek részére. Ez előfeltétele annak, hogy a jogalkotási és szervezeti fejlesztési feladatokat, kiértékeléseket és változtatásokat időben határozzák meg az érintett kormányzati szervek részére, hogy legalább félévente vagy a kialakult helyzet miatt azonnal tudjanak reagálni az új veszélyforrásokra.

A harmadik az operatív¹⁵⁷ szint, a Terrorellenes Koordinációs Bizottság naponta hangolja össze, a rendvédelmi szervezetek és a különböző katonai és polgári titkosszolgálatok működését és feladatait.

Magyarország folyamatosan alkalmazkodik a változó globális kihívásokhoz és regionális fenyegetésekhez. A külföldön elkövetett terrortámadások miatt saját biztonsági és védelmi rendszerét is felülvizsgálta, valamint nemzeti szinten olyan terrorizmus elleni politika került kidolgozására, amely az ENSZ, NATO, EU és más egyéb nemzetközi politikára épít, és azokhoz igazodik.

2001-óta a Magyarország a következő feladatokat hajtotta végre:

- > 2001: Rendőrség terrorfelderítéssel és -elhárítással megbízott alegységének megalakítása,
- > 2003: Terrorellenes Koordinációs Bizottság felállítása,
- > 2004: Terrorizmus Elleni Tárcaközi Munkacsoport felállítása és a Nemzeti Akcióterv kidolgozása.

¹⁵⁶ „1. a) A Kormány a kormánypolitika elvi jelentőségű kérdéseinek megvitatására, ezek kezelésével és kidolgozásával kapcsolatos javaslatok meghatározására, valamint a halaszthatatlan kormányzati döntést igénylő eseményekkel összefüggésben szükséges sürgős intézkedések előkészítésére és koordinálására Kormánykabinetet létesít. A Kormánykabinet feladatköre más - döntés-előkészítő vagy döntéshozó - szerv feladat- és hatáskörét nem érinti.”

¹⁵⁷ Napi, végrehajtói szint

Az ORFK¹⁵⁸ átszervezésének részeként, 2004. július 1-én megalakították a Nemzeti Nyomozó Irodát¹⁵⁹. Az NNI keretein belül létrehozták a terrorizmushoz kapcsolódó bűnügyi felderítő és elhárító tevékenységet folytató rendőri szervezetet, a Terrorizmus és Extrémizmus Elleni Osztály-t¹⁶⁰. Az osztály országos hatáskörrel és teljes nyomozati jogkörrel, valamint közvetlen nemzetközi kapcsolattartási lehetőséggel rendelkezett. Kizárólagos hatáskörébe tartozott a Magyar Köztársaság területén elkövetett terrorcselekmények nyomozati munkája.

A bűnügyi felderítés csupán egyik eleme a megelőzés, a terrorizmus elleni küzdelemnek. Szükséges a megfelelő erő¹⁶¹ készenlétben tartása a terrorcselekményeket elkövető személyek elfogására, valamint a cselekmények felszámolására. A feladatok végrehajtása érdekében szükséges a Terrorelhárító Szolgálat¹⁶² alkalmazhatósági képességének folyamatos, magas szinten tartása. Kiemelt figyelmet kell fordítani a XXI. század kihívásainak megfelelő kiképzésre és a technikai eszközökkel való ellátottságukra.

A Rendőrség és a Határőrség integrációja után továbbra is fontos feladat, a többi biztonsági szervezettel egyeztetett, a terrorizmus elleni harc körébe tartozó feladatok végrehajtása. A mindennapi határrendészeti, idegenrendészeti (Schengeni határok kivételével)¹⁶³ tevékenységek során a rendőrség kijelölt személyi állománya végrehajtja azokat a fokozott ellenőrzéseket, illetve másodlagos intézkedéseket, amelyeket a vonatkozó jogszabályok részükre előírnak.

A rendvédelmi szolgálatok átalakítása és új képességek kialakítása

Terrorelhárítási Központ megalakítása¹⁶⁴

„1. § (1) A Terrorelhárítási Központ (a továbbiakban: Központ) az ország egész területére kiterjedő illetékességgel rendelkező, a rendészetért felelős miniszter (a továbbiakban: miniszter) irányítása alatt működő költségvetési szerv.

¹⁵⁸ Országos Rendőr-főkapitányság, a továbbiakban ORFK

¹⁵⁹ Továbbiakban: NNI

¹⁶⁰ Továbbiakban: TEEO

¹⁶¹ Beavatkozó(felszámoló) erő

¹⁶² továbbiakban: TESZ

¹⁶³ A Schengeni egyezmény az Európai Unió (EU) első és harmadik pillérének része, amely elsősorban a belső határőrizet megszüntetését és a külső határok közös ellenőrzését jelenti.

¹⁶⁴ 232/2010. (VIII. 19.) Korm. rendelete

(2) A Központ tevékenységének jellege alapján közhatalmi, a feladatellátáshoz gyakorolt funkciói szerint önállóan működő és gazdálkodó költségvetési szerv.”

A Terrorelhárítási Központ¹⁶⁵ feladatai közé tartozik Magyarország terrorfenyegetettségének elemzése-értékelése, terrorcselekmények, emberrablások felderítése és felszámolása, a köztársasági elnök, miniszterelnök és az Országgyűlés elnökének¹⁶⁶ személyvédelmi feladatainak végrehajtása, amelyet korábban az ORFK Köztársasági Őrezrede látta el.

A TEK főigazgató feladata a Terrorellenes Koordinációs Bizottság vezetése és irányítása¹⁶⁷ és a Nemzetbiztonsági Kabinet alárendeltségében hajtja végre feladatait.

A TEK a következő szervezetek átcsoportosított személyi állományából állították fel:

- > Alkotmányvédelmi Hivatal¹⁶⁸
- > Terrorizmus és Extrémizmus Elleni Osztály (NNI)
- > Köztársasági Őrezred
- > a Terrorelhárító Szolgálat (TESZ)
- > a megyei bevetési alosztályok.

Különleges jogrend fennállása esetén

A magyar alaptörvény¹⁶⁹ – KÜLÖNLEGES JOGREND 52. CIKK- ében – „ a különleges jogrendben fennállása esetén, hogy a rendkívüli állapot kihirdetésére vonatkozó döntésig a támadással arányos és arra felkészített erőkkel azonnal intézkedni köteleles. „

¹⁶⁵ továbbiakban: TEK

¹⁶⁶ Az Országgyűlésről szóló 2012. évi XXXVI. törvény szerint, 2013. január 01-én megalakul az Országgyűlési Őrség, amely főfeladata a házelnök személyvédelme, az Országház, az Országgyűlés Irodaháza, illetve az Országgyűlés Hivatala épületeinek védelme.

¹⁶⁷ A Kormány 1176/2010. (VIII. 19.) Korm. határozata a közbiztonság megerősítésével kapcsolatos egyes költségekkel összefüggésben a 2010. Évi központi költségvetés általános tartalékának előirányzatából történő felhasználásról, valamint a terrorfelderítés műveleti koordinációjáról és a Terrorellenes Koordinációs Bizottságlétrehozásáról szóló 2239/2005. (X. 28.) Korm. határozat módosításáról

¹⁶⁸ AH - Alkotmányvédelmi Hivatal

¹⁶⁹ Magyarország Alaptörvénye, 2011. április 25.

„Biztonságpolitikai elemzők véleménye szerint a kor új kihívásainak figyelembevételével a fegyveres erőnek már nem kizárólag az ország védelmére kell felkészülnie, hanem minél aktívabb részvételre a válságreagáló műveletekben, [...] a jövő Magyar Honvédsége a nemzeti és nemzetközi (szövetségi) követelményeknek és az információs társadalom kihívásainak egyaránt megfelelő, meghatározott elvek, eljárások és doktrínák alapján felépülő, képesség alapú haderő, amelynek feladatrendszere, szervezeti felépítése, felszerelése és fegyverzete, valamint személyi állománya és annak kiképzettsége egységes egészet képez, [...] A fegyveres erő képes lesz a válságreagáló műveletek feladatainak teljesítésére, más tagállamok fegyveres erőivel együttműködve.”¹⁷⁰

Ha Magyarország területén terrorcselekmény, fegyveres csoportok betörése történt, vagy ha olyan információkat kap a titkosszolgálat:

- > egy vagy több meghatározott helyen,
- > személy elleni terrorcselekmény,
- > fegyveres támadások bekövetkezése nagyon valószínű.

Ez azt jelenti, hogy a következő 24 órában valószínű egy támadás vagy már megtörtént a cselekmény.

Különleges jogrend fennállása esetén a Rendőrség egyedül nem tudja végrehajtani biztosítási és védelmi feladatait. Szükséges a fegyveres erő alkalmazása, a Magyar Honvédség¹⁷¹ bevonása. A Magyar Honvédség rendelkezik olyan speciális szakképzettségű katonákkal és képességekkel, akik a terrorcselekmény/fegyveres támadások bekövetkezése esetén megfelelő támogatást tudnak adni a rendvédelmi szervek részére¹⁷².

A MH válságkezelő tevékenységének több formája lehet, amelyek például katonai, gazdasági, politikai, emberi jogi, környezeti jellegűek¹⁷³.

¹⁷⁰ BENCE Balázs – Dr. DEÁK János – Dr. SZTERNÁK György: *Gondolatok a válságreagáló műveletekről II. RÉSZ, A fegyveres erő helye, feladatai a válságreagáló műveletekben*, Nemzetvédelmi egyetemi közlemények, 2005, 9. évf. 2. szám

¹⁷¹ Továbbiakban: MH

¹⁷² együttműködő erő

¹⁷³ PATAKI János: *Biztosítási feladatok Magyarország az Európai Unió soros elnöksége idején 2011-ben*, tanulmány, Zrínyi Miklós Nemzetvédelmi Egyetem, Magasabb Tanfolyami Parancsnokság, Budapest, 2009, (A szerző birtokában)

A globális biztonság katonai jellegű vetületei közül a legfontosabb feladat az ország szuverenitásának megőrzése, együttműködés a nemzetközi szervezetekkel és a nem kormányzati szervezetekkel. Regionális biztonsági kérdés Kelet-Közép-Európában a délszláv válság újbóli elmélyülése, a nem katonai jellegű feladatok, úgy, mint:

- > terrorizmus,
- > migráció,
- > proliferáció,
- > szervezett bűnözés elleni harc,
- > iszlám fundamentalizmus,
- > nukleáris balesetek,
- > természeti katasztrófák.

Az irányultság szerint lehetnek: országon belüli, befelé irányuló, több irányban ható, kifelé ható és egyszerre jelentkező. Ezen helyzetekben a fegyveres erők feladata a felderítés intenzitásának fokozása, az operatív vezetés biztosítása, a készenléti erők készenlétének fokozása, részleges vagy teljes mozgósítása, valamint a válságkezelésre kijelölt erők alkalmazása.

A MH készenléti és készségi szolgálatainak rendeltetése, az erők és eszközök készenlétének biztosítása, valamint a biztosítási és védelmi feladatok megkezdése a megadott normaidőn belül, előre nem látható támadás elhárítása. Feladata, az ország területére betört/itt tartózkodó fegyveres csoportok/terrorszervezetek felszámolása, illetve a fokozott védelmet igénylő létesítmények, objektumok őrzés-védelme, katasztrófavédelmi és más különleges feladatok végrehajtása.

Szárazföldi csapatok alkalmazási lehetőségei:

- > Különleges műveletek végrehajtása,
- > Felderítés (minden neme),
- > Területzárás,
- > EÁP¹⁷⁴ feladatok,
- > Mobilkórház telepítése,
- > ABV¹⁷⁵ mobil labor telepítése, ABV felderítés (HJMŰ¹⁷⁶ vagy helikopter),

¹⁷⁴ Ellenőrző Áteresztő Pont

- > Vízisztítás,,
- > EMÜ¹⁷⁷ katasztrófa felszámolásában,
- > Szállítási, raktározási feladatok,
- > Tűzszerész feladatok,
- > Laktanyák rendelkezésre bocsajtása (szállítás, étkezés, raktározás, technikai kiszolgálás, stb....),

Légi erő alkalmazási lehetőségei:

- > a légtér ellenőrzés,
- > (légi) terroristák elleni harc (RENEGADE)¹⁷⁸,
- > légi felderítés,
- > megakadályozza a különböző objektumokra a levegőből mérendő csapásokat,
- > támogatja a saját csapatok tevékenységét,
- > légi szállítási feladatok,
- > részt vesz katasztrófa- és polgári védelmi feladatok támogatásában.

A támogató és biztosító feladatok közül a különleges műveleteket szeretném kiemelni, mert ma Magyarországon nem ismert, hogy pontosan mit is jelent ez a fogalom. Ezért szeretném az MH ezen képességét hangsúlyozni és a különleges műveleti feladatokat röviden ismertetni.

Különleges műveleti feladatok

A XXI. század elejétől egyre több állam hadserege tart készülségben különleges műveleti erőket. Ezen erőkre azért van szükség, mert a különleges műveleti erő alkalmazási módszerei, illetve képességei lehetővé teszik a (had)műveleti szinten való bevetését. A különleges műveleti erők¹⁷⁹ kis létszámú (al)egységek, amelyek képesek a szembenálló fél

¹⁷⁵ Atom- biológiai-vegyi

¹⁷⁶ Harcjármű

¹⁷⁷ együttműködés

¹⁷⁸ 2011. évi CXIII. Törvény, a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről, 40. A légierőre vonatkozó különös fegyverhasználati szabályok, 40. A légierőre vonatkozó különös fegyverhasználati szabályok 62. §. , (6) A nemzeti alárendeltségű légvédelmi készenléti szolgálatot ellátó erők figyelmeztető vagy megsemmisítő tüze kiváltására vonatkozó parancsot a Honvédség légierő ügyeletes parancsnoka adhat." ("repülő eszköz fegyverkénti használata")

¹⁷⁹ A különleges műveleti erők (Special Operations Forces = SOF) nem alkalmazhatók a hagyományos katonai erők helyett. Leghatékonyabb a béke időszakában történő bevetése, a békeműveletek feladatainak, valamint terrorelhárítási feladatok végrehajtására. A különleges műveleti erők katonáit tervszerűen és

erőinek, eszközeinek többszörösét lekötni, illetve megsemmisíteni. Az aszimmetrikus hadviseléssel¹⁸⁰ szemben a különleges erők képesek a leghatékonyabban fellépni. A különleges erők műveletei és azok részletei nem nyilvánosak.

A terrorizmus elleni globális méretű küzdelem miatt szükséges a különleges műveleti katonák egyre fokozottabb szerepvállalása. A terrorizmus elleni harcban a katonai feladatokat a hagyományos kötelékek nem, vagy csak korlátozott mértékben képesek teljesíteni. A nemzetközi környezet folyamatos változása miatt a biztonság fogalmát újra kell értelmezni az aszimmetrikus fenyegetettség egyre nagyobb térnyerése miatt.

A különleges műveleti erők három fő feladata:

- > a közvetlen akciók végrehajtása,
- > a különleges felderítési feladatok végrehajtása ,
- > a katonai segítségnyújtás.

A közvetlen akciók feladatainak végrehajtása során a katonák kisebb csoportokban kerülnek alkalmazásra. Őket számos, speciálisan átalakított repülőeszköz is támogatja. A kommunikáció fejlődése napjainkra lehetővé tette, hogy a műveleti parancsnokok folyamatosan nyomon követhetik a különleges műveleti katonák helyzetét a felelősségi körzetekben, valamint a valós idejű kommunikációt is. Az általuk alkalmazott nyomkövető rendszereknek köszönhetően a műveleti parancsnok tisztában van az általuk végrehajtott manőverekkel és így képes a többi rendvédelmi erő mozgását velük összhangban koordinálni, miközben a különleges műveleti katonák stratégiaileg fontos létesítményeket, objektumokat foglalhatnak el és biztosíthatnak a rendvédelmi erők megérkezéséig. Ezen feladatok lehetnek:

- > Az ország fegyveres védelmében való részvétel során különleges műveleti feladatok végrehajthatják önállóan, vagy együttműködve más katonai szervezetekkel, rendvédelmi szervekkel, nemzeti, illetve nemzetközi parancsnokság alárendeltségében,
- > Katonai erő alkalmazását igénylő, váratlan (speciális) események megoldása,

alaposan felkészítik a meghatározott földrajzi térség éghajlati, domborzati és időjárási viszonyaira, a lakosság kulturális, vallási és ideológiai sajátosságaira, különös tekintettel a térség lakosságának nyelvi megosztottságára.

¹⁸⁰ 4G – negyedik generációs hadviselés

- > Alegységeivel a NATO doktrínákban meghatározott különleges műveleti feladatok és az ezekhez kapcsolódó tevékenységek végrehajtása nemzeti alárendeltségben, illetve különleges műveletekben való részvétel a szövetségben vállalt kötelezettségekből eredő feladatok teljesítése során,
- > A terrorizmus elleni harc katonai feladatainak végrehajtása,
- > A békeműveletekben vállalt feladatok teljesítésében való részvétel,
- > Béke és háborús kutató-mentő feladatokban való részvétel,
- > Külön tervekben meghatározottak szerinti válságkezelésben való részvétel.

A terrorizmus elleni harc magyar szereplői felkészültek egy esetleges terrortámadás/ fegyveres csoportok felderítésére és felszámolására. A különböző biztonsági szervezetek és intézmények, a terrorellenes küzdelem különböző aspektusaival foglalkozó szereplők közötti koordináció napi, közigazgatási és politikai szinten megfelel a törvényi elvárásoknak.

Különleges jogrend fennállása esetére tervezett biztosítási és védelmi feladatait a rendvédelmi szervek és a Magyar Honvédség speciális alakulatai, valamint szakemberei tudják eredményesen végrehajtani.

2.2.2. Civil biztonsági és más vállalatok lehetséges feladatai

A kritikus infrastruktúrák biztosításában növekvő szerep hárul a civil biztonsági vállalkozásokra. A kritikus infrastruktúrák biztosításába be kell vonni azon vagyonvédelmi és biztonságtechnikai cégeket, amelyek rendelkeznek „NATO beszállító”, illetve „Minősített NATO beszállító” certifikációval¹⁸¹. Alkalmazásuknál figyelembe kell venni a hazai és nemzetközi jogi előírásokat és belső utasításokat.

Természetesen a korábban kialakult rendszer szerint kell megszervezni a különböző kritikus infrastruktúrák védelmét. Ez azt jelenti, hogy a teljeskörű biztonsági szolgáltatás megrendelését pályáztatás útján kell kiválasztani.

Így kialakult egy integrált feladatrendszer, ami azonban nem jelentheti azt, hogy törvényekben rögzített állami feladatokat vesznek át civil biztonsági cégek. Ennek során a rendőrségi hatáskörökön kívül eső feladatokat, mint például vagyonvédelmi,

¹⁸¹ www.nbf.hu, Nemzeti Biztonsági Felügyelet (NBF)

biztonságtechnikai, tűzvédelmi, katasztrófavédelmi és iparbiztonsági teendőket hajtanak végre, a hatóságok megfelelő ellenőrzése mellett.

2.2.3. Védelmi képességfejlesztés és beruházás költségeinek viszonya vállalati szinten

Az objektumokat/kritikus infrastruktúrákat üzemeltető nem állami szereplőknél egységesen kell alkalmazni a biztonsági és védelmi intézkedéseket, amelyek alapján az adott szereplők egy egységes biztonsági politikát valósítanak meg, ehhez standardizált biztonsági szervezeteket építenek ki. Ez azért különösen fontos, mert itt már nem hierarchikus, hanem vertikális kapcsolatok vannak a stratégiai és operatív (napi) szintek között. Az operatív szintű biztonsági szervezetek között horizontális kapcsolatok a jellemzőek.

Nagyon fontos a megfelelő információs és riasztási rendszer kialakítása, mely elősegíti a megfelelő védekezési intézkedések alkalmazását és nemzetközi/nemzeti tapasztalatok és módszerek biztonságos megosztását, valamint továbbítja a közvetlen veszélyekre vonatkozó információkat. A rendszernek biztosítania kell, hogy az érintett személyek/szervezetek időben megkapják a szükséges információkat a döntéselőkészítéshez.

Vállalati biztonság fogalma és általános elvei

A vállalat biztonságát meghatározza, hogy milyen minimális veszélyeztetés mellett garantálható a vállalat üzleti/termelő tevékenysége. A minimálisan bevezetendő biztonsági intézkedéseknek figyelembe kell venni azokat a veszélyforrásokat¹⁸², amelyek szintje elérheti az átlagos vagy magasabb veszélyeztetettségi szintet. Ezen kijelentések vonatkoznak mind az aktív veszélyekre (security¹⁸³), mind a passzív veszélyekre (safety¹⁸⁴).

A vállalat biztonsági politikája határozza meg a középtávú védelmi célokat, iránymutatásokat és elvárásokat. A biztonsági politikának összhangban kell lenni a társaság általános stratégiájával és az ország Nemzeti Biztonsági Stratégiájában foglalt elvárásokkal és ajánlásokkal.

¹⁸² szabotázs, emberi mulasztások, technikai meghibásodások, vis major...

¹⁸³ terrortámadás, vagyon elleni bűncselekmények, tüzesetek, balesetek ...

¹⁸⁴ földrengés, extrém időjárás, ..

A lehetséges veszélyforrások folyamatos elemzésének és a bekövetkezett káresemények következményeinek vizsgálati eredménye együttesen határozzák meg, hogy szükséges-e a működő biztonsági rendszer megváltoztatása és/vagy kiegészítése, illetve új biztonságtechnikai elemek alkalmazása. A káresemény lehetséges vagy valóságos eszkalációja egy bizonyos szint meghaladásakor, megköveteli külső erők bevonását a kárelhárításba és felszámolásába.

A biztonsági politikában foglaltak megvalósulása nagyban függ a menedzsment és a munkatársak elkötelezettségén.

A biztonsági politikához szervesen kapcsolódnak a vállalat szakterületei¹⁸⁵ által kidolgozott szakpolitikák, melyek egy adott ágazat középtávú terveit fogalmazzák meg és ezen szabályozások is érvényesek minden munkatársra.

Biztonsági rendszerek tervezése

A biztonsági rendszereket és intézkedéseket mindig az aktuális védelmi célok alapján kell kialakítani. A megfogalmazott célok megvalósításához szükséges egy integrált biztonsági koncepció kidolgozása és az ehhez tartozó egyedi intézkedések bevezetése.

A biztonsági és védelmi feladatok legfontosabb területei:

Veszélyforrások azonosítása és folyamatos követése:

- > Információvédelem,
- > Objektumvédelem,
- > Üzemi katasztrófa-, tűz- és polgári védelem,
- > Iparbiztonság,
- > Munkabiztonság,
- > Egészségvédelem,
- > Környezetvédelem,
- > Termékszavatosság,
- > Folyamatbiztonság,
- > Rendezvénybiztosítás,
- > Személyvédelem,
- > Egyéb védelmi feladatok.

¹⁸⁵ Katasztrófa-, tűz-, munka-, környezetvédelem, egészségmenedzsment, IT-biztonság ...

Védelmi rendszer kiépítésének alapjai

A jelenlegi magyarországi civil biztonsági szakma megosztott, nincs egységes értelmezés a veszélyforrások egyértelmű azonosításában, az ezekre adott válaszok általában a biztonsági modell¹⁸⁶ egy adott eleme alá rendelik a többi feladatot. Ezért kijelenthetjük, hogy a különböző irányzatok nem vagy csak csekély mértékben alkalmazzák a biztonság összes elemét. A „biztonsági piramis” megmutatja a biztonsági rendszer felépítésnek sorrendjét. Minden elem egymásra épül és kiegészítik egymást.

Az élőerőre alapozott védelemre jellemző, hogy a „Monitoring” elem teljes egészében hiányzik, a többi viszont az élőerővel végrehajtott védelmi elemnek van teljesen alárendelve – ha alkalmazzák -, a különböző technikai rendszerek között nincs kapcsolat. Ma Magyarországon ezen irányzat a jellemző, mert 2013-ban kb. 97.000 vagyonvédelmmel foglalkozó személy kötelezett különböző szintű vizsgára, ekkor a lakosság létszáma kb. 10 millió fő volt.¹⁸⁷ Németországban¹⁸⁸ ez a szám kb. 185.000 főt jelentett 2013-ban, míg a lakosság lélekszáma 80 millió. Láthatjuk a hatalmas aránytalanságot, mely szerint ötször annyian foglalkoznak biztonsági feladatokkal hazánkban – Magyarországon a lakosság 0,01 %-a, Németországban 0,002 %-a –, amely az eltérő biztonsági filozófiából ered.

A technikára alapozott biztonságra jellemző, hogy a technikai elemek a dominánsak. Kapcsolat a technikai rendszerek között nem valósul meg. A „Monitoring” és „Válságkezelés” szegmensek ebből az irányzatból is hiányoznak. A mechanikai védelem alkalmazása nem teljeskörű, az élőerővel végrehajtott védelem szegmens csak mint beavatkozó erő jelenik meg.

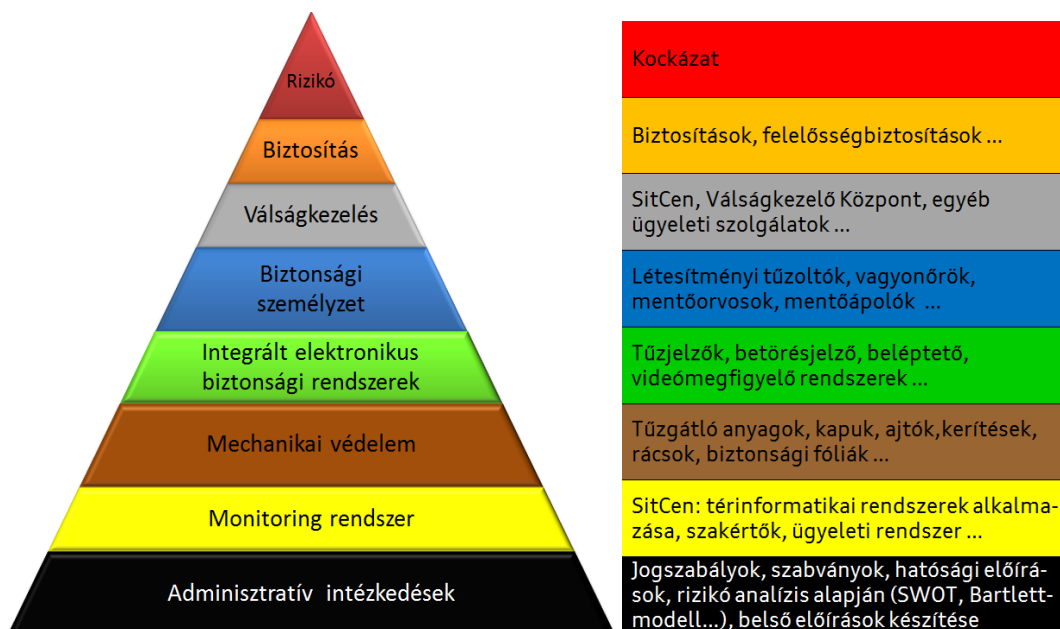
A komplex biztonsági rendszer tartalmazza a legtöbb elemet, de a „Monitoring rendszer” és „Válságkezelés” szegmensek ugyancsak hiányoznak vagy csak részlegesen alkalmazzák.

¹⁸⁶ „Biztonsági piramis”

¹⁸⁷ <http://biztonsagpiac.hu/mintegy-szazezren-vegzik-el-iden-a-kotelezo-tovabbkepzes> (Letöltve: 2014.09.21.)

¹⁸⁸ <http://de.statista.com/statistik/daten/studie/258775/umfrage/beschaefigten-bei-privaten-wach-und-sicherheitsdiensten-nach-bundeslaendern/> (Letöltve: 2014.09.21.)

Az *integrált biztonsági koncepció*¹⁸⁹ tartalmazza az összes elemet. Ebben határozzák meg a különböző szakterületek és üzleti egységek feladatát és kötelezettségeit, valamint az alkalmazott biztonsági rendszerek teljeskörű integrációját¹⁹⁰.



3. számú ábra: Biztonsági modell (Forrás: a szerző összeállítása)

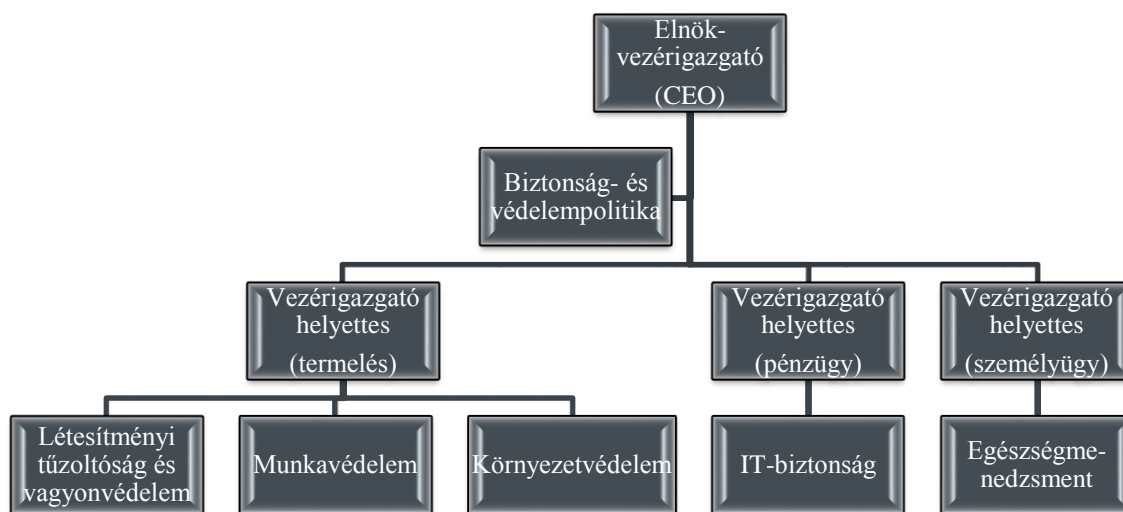
Biztonsági szervezetek

Ez a biztonsági szervezetek felelősségének és kötelezettségeinek szétválasztását jelenti, amely a vállalaton belül vertikális és horizontális kapcsolatokban és több szinten valósul meg. A biztonsági szervezetek irányítása és ellenőrzése, egy célorientált és integrált

¹⁸⁹ A tapasztalatok szerint, az integrált biztonsági koncepció egy első összefoglalása a biztonsági intézkedéseknek és terveknek, amelyek mindenre biztonsági területre kiterjed. Ennek megfelelően egy ismétlődő folyamatról beszélünk, amely bázisát adja a tervezési folyamatoknak. A koncepcióban meg kell határozni a védelmi célokat és a prioritásokat. A további fejlesztések, átépítések és átszervezéseknél is folyamatosan kell alkalmazni és így biztosítható a vállalat elvárt biztonsági szintje.

¹⁹⁰ PATAKI János – SULÁNYI Péter: *Lage- und Analysezentrum bei einem internationalen Unternehmen*, A ZMNE BOLYAI JÁNOS HADMÉRNÖKI KAR ÉS A HADMÉRNÖKI DOKTORI ISKOLA, ONLINE TUDOMÁNYOS KIADVÁNYA, VI. Évfolyam 3. szám 2011. szeptember

rendszer tervezését és kialakítását jelenti, amely a „hatalom-megosztás”¹⁹¹ elvén működik.



4. számú ábra: Biztonsági szervezetek (Forrás: a szerző összeállítása)

A vertikális kapcsolatok a Stratégia biztonsági vezetőhöz tartoznak (az állami/igazgatási szint), a horizontális kapcsolatok, jellemzően a helyi biztonsági hatóságokkal, szervezetekkel, az energia ellátást végző vállalatokkal az operatív (napi) biztonsági feladatokat végrehajtó szervezetek működnek együtt. Minden felső vezetőhöz rendelhetünk egy vagy több biztonsági területet (szervezetet), így nem egy vezető kezében van a vállalat biztonsági szervezeteinek irányítása és beszámoltatása. Természetesen ez nem befolyásolja az egyszemélyi felelősség megvalósulását.

2.2.3. Védelmi képességfejlesztés és beruházás költségeinek viszonya¹⁹²

A vállalatok fejlesztésénél már a tervezés időszakában figyelembe kell venni a várható biztonsági költségeket. A biztonsággal kapcsolatos irányítás tudatos folyamat, amely a kockázatok megállapítását, valamint a felismert kockázat meghatározott, elfogadható költségek mellett alacsony szintre való csökkentésére irányuló intézkedések meghozatalát

¹⁹¹ A különböző testületek egymást is ellenőrzik a menedzsment folyamatok alapján, amelyek szerves részét képezik egy vállalat minőségirányítási rendszerének

¹⁹² KIRÁLY László – PATAKI János: *Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz,*

A MAGYAR HADTUDOMÁNYI TÁRSASÁG ÉS A MAGYAR TUDOMÁNYOS AKADÉMIA HADTUDOMÁNYI BIZOTTSÁGA FOLYÓIRATA, XXIII. Évfolyam, 2013/1. elektronikus lapszám

és végrehajtását foglalja magában. E módszer jellemzője, hogy a kockázatokat egy meghatározott szint állapítja meg, méri és ellenőrzi.

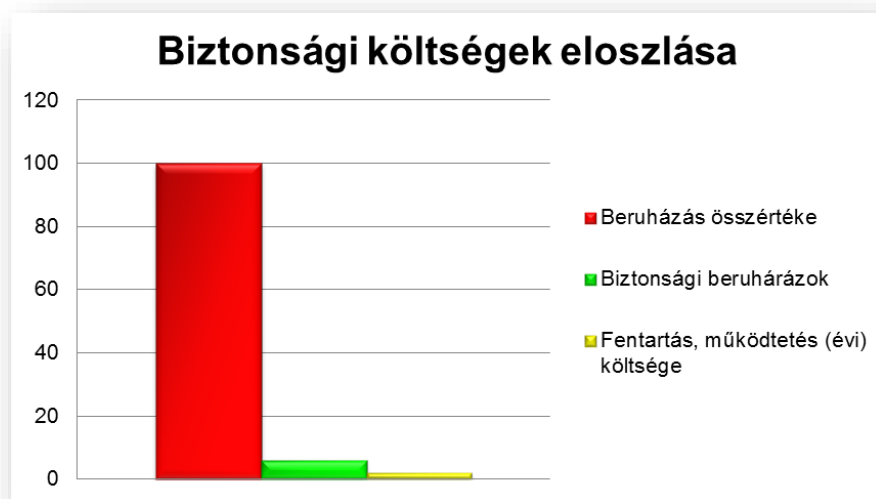
A biztonsági rendszerek finanszírozásának 1/20-a és 1/200-a szabálya, ahol:

K – a beruházás összköltsége,

V – a védelmi célú beruházásokra előirányzott fejlesztési forrás,

V – a működtetés során keletkező védekezési (megelőzési) kiadások

$$\mathbf{K : B : V = 100 : 20 : 200}$$



5. számú ábra: Biztonsági költségek megoszlása (Forrás: szerző összeállítása)

Egy beruházásnál a potenciális kár az időegység alatti termelés kiesés/elmaradt haszon lehetne, de a sok változó miatt, a nagyszámú tapasztalati adatot megkövetelő modellszámítás csak korlátozottan alkalmazható. Ezért a beruházók/tervezők a „kényelmesebb utat” az ún. „arany szabályok” alkalmazását választják.

A beruházások tervezésénél vannak „arany számok”¹⁹³, amelyeket a tervezés során figyelembe kell venni. A következő értékekkel szokás számolni egy általános projektnél (nem nukleáris): a beruházás összköltségének 5%-a a biztonsági rendszerek költsége, illetve a biztonsági

¹⁹³ „arany számoknak” nevezzük azokat az arányszámokat, amelyek tapasztalati értékeken alapulnak

rendszerek működtetési költsége 0,05%. A biztonsági költségek tartalmazzák a rendszerek tervezését, leszállítását, illetve beépítését/telepítését (installálását).

A működési költségek már nem a projektet terhelik, hanem az objektum/intézmény/vállalat (budget-jét¹⁹⁴) folyó költségvetését. A „budget” számításánál a „gördülő tervezést¹⁹⁵” ajánlott alkalmazni.

Egy gyakorlati példán keresztül mutatom be egy beruházás biztonsági költségeinek felosztását.

Ha egy beruházás összértéke 1000 Mrd. HUF¹⁹⁶, akkor a fent említett „arany szám” alapján a biztonsági rendszer költsége 50 Mrd. HUF. Természetesen ebbe az összegbe bele értendő az építés során felmerülő őrzés, tűzvédelmi és egyéb más (munka-, környezetvédelmi) költségek is.

Tervezés és megvalósítás fázisában

Biztonsági feladatok	Tételek	Mrd. HUF
Periféria védelem	Kerítés, porta, beléptető rendszer, videó megfigyelő rendszer...	8
Épületek védelme	Betöréssjelző-, beléptető-, videó megfigyelő rendszerek	3
Épületek védelme	Katasztrófa-, tűzvédelem, iparbiztonság	15
Létesítményi Tűzoltóság	TÜÖ ¹⁹⁷ , GJMŰ-vek, különböző eszközök, személyi állomány felszerelése	2
SitCen ¹⁹⁸	GIS ¹⁹⁹ , Biztonságtechnikai rendszerek központjai	4
Egyéb biztonsági rendszerek	Vészvilágítás, vészaramellátás ...	4
Munkavédelem	Berendezések, felülvizsgálatok, személyi védőfelszerelések ...	5
Környezetvédelem	Speciális GJMŰ-vek, berendezések, felülvizsgálatok ..	6
Egészségmenedzsment	Mentőszolgálat, üzemorvosi és egyéb egészségügyi szolgáltatások	3

6. számú ábra: Biztonsági területek költségeinek megoszlása

(Forrás: szerző összeállítása)

¹⁹⁴ költségvetés

¹⁹⁵ Középtávú tervezés – a vállalati stratégiai céljaira épít, figyelembe veszi a vállalati kultúrát a döntések és a felelősségek szintjén (ügyvezetés). Egy adott tervciklusban tervezésnél - tervezési horizont - a vállalat egy évet újonnan von be a középtávú tervezés folyamatába az elmúlt tervciklusokat figyelembe véve.

¹⁹⁶ Magyar forint

¹⁹⁷ TÜÖ - tűzoltó

¹⁹⁸ Situation Centre, Helyzetelemző és válságkezelő központ

¹⁹⁹ GIS - geographical information system = térbeli adatok gyűjtése, tárolása, adatbázis kialakítása

Természetesen ezen összegek csak tájékoztató jellegűek. Ezt több tényező határozza meg, mint például az alkalmazott technológiák, anyagok, tevékenység jelleg stb.

A beruházás működtetésénél számolni kell a biztonsági személyzet bér és egyéb más költségeivel, a karbantartási költségekkel, illetve a bevont külső szolgáltatók szerződésben foglalt vállalási díjaival is.

Ez a beruházás összköltségének 0,05%-a, azaz 5 Mrd. HUF. Ezen összeg megoszlásban jelentkezik a különböző biztonsági szervezeteknél.

2.3. ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Értekezésem második fejezetének első részében bemutattam, hogy a biztonságpolitika különböző tényezői kapcsolatban állnak egymással és kihatnak egymásra. Jelenleg a gazdasági dimenzió a legmeghatározóbb. A biztonságpolitikai irányelvek kialakítása a kormány politikájának fontos részét jelenti, amelyet a Nemzeti Biztonsági Stratégiában deklarálnak. Iránymutatást ad a létfontosságúnak ítélt nemzeti értékek és érdekek védelméhez, valamint a potenciális és/vagy valóságos támadással/ellenféllel szemben.

A kritikus infrastruktúrák védelmének tervezési fázisában figyelembe kell venni a „dominó hatást”, amely következtében a károk megtöbbszöröződhetnek és a bekövetkezett események hatására másodlagos, harmadlagos károk is keletkezhetnek.²⁰⁰

Véleményem szerint, a hazai terrorizmus elleni harc biztonsági szervezetei megfelelően működnek. A különböző biztonsági intézmények és szervezetek, a terrorellenes küzdelem különböző aspektusaival foglalkozó szereplők közötti koordináció napi, közigazgatási és politikai szinten megfelelő. Szeretnék rávilágítani, hogy a jövőbeni nemzeti biztosítási műveletekben (pl.: minősített időszakban a kritikus és létfontosságú infrastruktúrák védelme) történő szerepvállalás elérte a magyar rendvédelmi szervek lehetőségének határát. Az erő és eszköz, illetve képességek hiánya miatt javaslom a Magyar Honvédség bevonását a kritikus és létfontosságú infrastruktúrák védelmének biztosításába. A Magyar Honvédség állományában olyan speciális szakképzettséggel rendelkező katonák szolgálnak, akik hasonló feladatokat hajtanak végre különböző missziókban, így alkalmasak arra, hogy megfelelő támogatást nyújtsanak a rendvédelmi szervek részére.

²⁰⁰ ÜVEGES László: *A Magyar Köztársaság katasztrófa-veszélyeztetettsége és az arra adandó válaszok*, ZMNE, – Ph D értekezés –, Budapest, 2002, pp. 130

A védelmi feladatok végrehajtásába be kell vonni azokat a biztonsági profillal rendelkező vállalatokat, amelyek rendelkeznek a nemzeti hatóságok által kiadott biztonsági minősítéssel.

Megvizsgáltam a Magyarországon kialakult biztonsági irányzatokat és egyedül az *integrált biztonsági koncepció* alkalmazása garantálja az objektumok teljeskörű védelmét, amely tartalmazza a biztonság összes elemét. Az integrált biztonsági koncepcióban határozzák meg a különböző szakterületek és üzleti egységek feladatát és kötelezettségeit, valamint az alkalmazott biztonsági rendszerek teljeskörű együttműködését.

A vállalatok fejlesztésénél vagy új „zöld mezős” beruházásoknál már a tervezés időszakában figyelembe kell venni a biztonsági kihívásokat, amelyek nagymértékben befolyásolják a védelmi költségeket. A védelmi képességek kialakítása egy tudatos folyamat, amely során a definiált kockázatokhoz egy költséghatékony védelmi rendszer kiépítését irányozzák elő.

3. FEJEZET: NEMZETKÖZI VÁLLALATOK, MINT A KRITIKUS INFRASTRUKTÚRA VÉDELMI RENDSZERE

Egy létesítményen/vállalaton belül a legfontosabb feladat a működés és a termelési folyamatok biztonságának garantálása. Ebben a fejezetben bemutatom azokat a külső²⁰¹ és belső²⁰² szabályozásokat, szervezeti és létesítési feladatokat, valamint a minimálisan alkalmazandó biztonságtechnikai rendszereket, amellyel megvalósítható a zavartalan üzemmenet. Ezt azért tartom fontosnak, mert ma Magyarországon nem mindig érik el azt a cél a biztonság szereplői²⁰³, hogy egyformán értelmezzék a részükre előírt biztonsági és védelmi előírásokat és azok kapcsolódási pontjait.

A XXI. század globális biztonsági kihívásait csak az új biztonságtechnikai rendszerek és az új taktikai elemek alkalmazásával kezelhetjük, hogy elérjük az elvárt biztonsági szintet.

²⁰¹ jogszabályok, igazgatási előírások, hatósági eljárások, szabványok

²⁰² A konkrét létesítményre/vállalatra vonatkozó előírások

²⁰³ Hatóságok és a civil biztonsági szervezetek/társaságok

3.1. A KRITIKUS INFRASTRUKTÚRA ÁLTALÁNIS VÉDELMI SZABÁLYAI

3.1.1. Kritikus infrastruktúrák védelmének nemzetközi és nemzeti szabályozása

A kritikus infrastruktúra meghatározása

Minden kornak meg volt a maga kritikus infrastruktúrája²⁰⁴, amelyek megléte és működőképessége jelentősen befolyásolta egy civilizáció fejlődését és fennmaradását.

A XXI. századi társadalmak működése hálózatalapú rendszerekre épülnek, amelyekre jellemző, hogy komplex rendszereik egymástól is nagymértékben függenek. A kritikus infrastruktúrák zavarai és részeinek kiesése vagy megsemmisülése működési zavarokat idézhet elő a lakosság ellátásában, a gazdaság és az állam elvárt működésében.

Nemzetközi és nemzeti szinten ezért fontos feladat a rendszerek sérülékenységének kutatása és az ezen eredményeken alapuló fejlesztési irányok meghatározása. A különböző nemzetközi szervezetek alapfeladataik alapján más-más szemszögből vizsgálják a rendszerek fogalmát és a megvalósítandó célokat. Ma még nem jelenthetjük ki, hogy rendelkezünk a „Kritikus infrastruktúra”²⁰⁵ és a „Kritikus infrastruktúra védelme”²⁰⁶ nemzetközileg elfogadott definíciójával. A nemzetközi szervezetek között egyetértés tapasztalható az energia, a logisztika, az IT és a pénzügyi szektorokban, amelyek globális rendszert alkotnak és hálózati alapon működnek.²⁰⁷

Kritikus infrastruktúra védelem: „a kritikus infrastruktúra elem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység”²⁰⁸.

„A létfontosságú infrastruktúrákat kár érheti, működésükben zavar keletkezhet vagy azok meg is semmisülhetnek terrorcselekmény, természeti katasztrófa, hanyagság, baleset,

²⁰⁴ A Római birodalom vízvezeték rendszere és úthálózata, a középkori Magyarország decentralizált „vízügyi igazgatása”, az ipari forradalom alatti kiépített vasúthálózat, majd vezetékes telefonhálózat elterjedése a XIX. század végén ... 2000-ik évi dátumváltást miatt létrehozott Y2K szervezet nemzetközi és hazai feladatai ...

²⁰⁵ továbbiakban KI

²⁰⁶ továbbiakban KIV

²⁰⁷ KIRÁLY László – MEDVECZKY Mihály: *Védelemgazdasági ismeretek önkormányzati (védelmi igazgatási) válság menedzsereknek.*, Budapest, 2009. ZMNE. ISBN 978-963-7060-75-5

²⁰⁸ KIRÁLY László – PATAKI János: Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz, pp. 175.

hackertevékenység, bűncselekmény vagy rosszhiszemű magatartás következtében.”²⁰⁹ Az infrastruktúrák *biztonságának növelése* ezért elsőrendű kérdéssé vált a fejlett országok biztonságpolitikájában.

„*Gazdaságbiztonsági szempontból kritikus infrastruktúra elem*: a gazdaság folyamatos működéséhez elengedhetetlen ágazatok (energetika, közlekedés, informatika, pénzügy), valamelyikébe tartozó eszköz, létesítmény, rendszer vagy ezek része, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, a gazdasági és szociális jóléthez, valamint amelynek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.”²¹⁰ A válsághelyzeti speciális védelmi intézkedések kidolgozása a különleges jogrend rendkívüli intézkedéseinek tervezése keretében történik.

A gazdasági és szociális jólét szempontjából²¹¹ kiemelten fontos, hogy a nemzeti össztermék meghatározó hányadát előállító gazdasági társaságok működésének belső biztonsági szabályait külön ágazati törvények nem határozzák meg.

A védelmi célok irányítási modelljei:

- > CIIP²¹² modell a kritikus információs infrastruktúrák védelmének megszervezésével foglalkozik, amely egy központilag koordinált irányítás mellett a kormányzati (GO)²¹³ és nem kormányzati (nGO)²¹⁴ szervezetekre is kiterjed. (USA, UK, Németország, Hollandia, Kanada, ...).
- > Az „All Hazards²¹⁵” modellben a miniszteri szinten határozzák meg az elsődleges feladatokat az infrastruktúrák működtetéséhez (a stratégiai szintű szervezetek irányítják a fizikai védelem és az ICT²¹⁶ biztonság, a polgári védelem, katasztrófavédelem) együttes kezelése a meghatározó. Alapvetően kormányzati tevékenység, amelyben nincs lehetőség a magánszféra teljes bevonására, bár az infrastruktúrák jelentős része magánkézben van.

²⁰⁹ Király László – Pataki János: Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz, pp. 175.

²¹⁰ Király László – Pataki János: Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz, pp. 176.

²¹¹ olyan gazdasági társaságok, amelyek árbevételük nagysága miatt jelentősen befolyásolják az adott ország nemzeti jövedelmét

²¹² critical information infrastructure protection (CIIP), kritikus információs infrastruktúrák védelme

²¹³ Government Organisation – GO – (angol)

²¹⁴ non-Governmental Organizations – GO – (angol)

²¹⁵ összes veszély

²¹⁶ Information and Communication Technology, Információ és Kommunikáció Technológia, amely az adatfeldolgozással és adattovábbítással kapcsolatos feladatokat jelenti.

Az európai létfontosságú infrastruktúrák *komplexek*, több ponton *kapcsolódnak* és *függenek egymástól*.

A vállalatgyűjtések és új telephelyek közép-kelet-európai létesítése része az ipari racionalizációnak, a globális üzleti folyamatoknak - például az éppen időben történő gyártás²¹⁷ -, valamint a népesség városi és az új telephelyek térségekbe történő tömeges letelepedése mind hozzájárultak e helyzet kialakulásához. Európa létfontosságú infrastruktúrái esetében egyre nagyobb szükség van a redundáns²¹⁸, közös információs technológiák²¹⁹ alkalmazására. A problémák „dominó elv²²⁰” szerűen végigvonulhatnak az egymással összefüggő infrastruktúrákon, amelyek az alapvető szolgáltatások váratlan és egyre komolyabb zavarát vagy meghibásodását okozhatják. Az összekapcsolódás és az interdependencia²²¹ miatt ezek az infrastruktúrák sebezhetőbbek a zavaró tényezők vagy megsemmisítés szempontjából.

Egy adott infrastruktúrát vagy annak egy bizonyos elemét tanulmányozni kell ahhoz, hogy el lehessen dönteni, hogy létfontosságúnak minősíthető-e. A létfontosságú infrastruktúrák definiálásához a következő *három tényezőt kell* figyelembe venni:

Hatókör – a létfontosságú infrastruktúra egyik elemének zavara vagy kiesése a terület nagysága alapján határozható meg, amelyet a veszteség vagy a szolgáltatás megszűnése érinthet – globális, regionális, nemzeti vagy helyi.

Nagyságrend – értékelés szerint nincs, minimális, mérsékelt vagy jelentős hatás. Többek között a következő szempontok alkalmazhatók a nagyságrend megállapításához:

- > A lakosságra gyakorolt hatás (lélekszám, áldozatok, járványok, betegségek, komoly sérülés, kimenekítés),

²¹⁷ JIT, **Just-In-Time**, vezetélmélet, „éppen időben”: a raktárkészlet és raktárterülete csökkentése miatt, a beszállítótól az alkatrész rögtön a gyártásába kerül, közvetlenül a felhasználóhoz.

²¹⁸ párhuzamos, egymást helyettesítő

²¹⁹ Internet, műholdas telefonok, GPS-navigációs rendszerek ...

²²⁰ Duncan MCFARLAND, Paul KREHBIEL, Harry TARG: *Vietnam, From National Liberation to 21 st Century Socialism*, Committees of Correspondence Education Fund, Inc, New York, ISBN: 978-1-304-20457-8 „Eisenhower, 1953: *Tegyük fel, hogy elveszítjük Indokínát. Ha Indokínai elvész, azonnal több dolog is történik. [...] Egész India körbe lesz véve (kommunista államokkal). Burma is egészen biztosan, a mostani meggyengült állapotában, védtelen lenne. Szóval látják, valahol ennek gátat kell szabni. [...] Ez az, amit most a franciák csinálnak. Most, amikor az Egyesült Államok 400 millió dollárt támogatást szavaz meg, az nem ablakon kidobott pénz. Ezzel a lehető legolcsóbb megoldásra szavazunk, amellyel biztosíthatjuk az Egyesült Államok legfontosabb érdekét. A biztonságunkat!*”

²²¹ kölcsönös függőség

- > Gazdasági (nemzetgazdasági hatás, a gazdasági veszteség jelentősége, a termékek vagy szolgáltatások színvonalának fokozatos romlása),
- > Környezetvédelmi (a lakosságra és a környezetre gyakorolt hatás),
- > Interdependencia (a létfontosságú infrastruktúrák egyéb elemei között),
- > Politikai/társadalmi.

Időbeli hatás – meghatározásával előre jelezhető/tervezhető, hogy egy adott infrastrukturális elemmel kapcsolatos veszteség mennyi idő elteltével fejt ki hatását.

Jogszabályi háttér

Nemzetgazdasági szempontból a kritikus infrastruktúrák védelmének megvalósításában szükséges az állam együttműködése az infrastruktúrák tulajdonosaival, valamint arányos megosztása a védelmi feladatokból adódó felelőségeknek és kockázatoknak. A kormányzati és a magánszféra partneri együttműködésén alapuló hazai program az önköltségi alapú vállalati finanszírozást jelenti, kiegészítve a feladatok és felelőségek megosztásával.

Magyarországi kritikus infrastruktúrák védelmének jelenlegi helyzetére jellemző, hogy a jogszabályok előkészítés, igazgatás és végrehajtás szintjén, valamint az alkalmazói (vállalati) szinten eltérő a szakmai felfogás és nincs teljeskörű egyetértés. Ez abból adódik, hogy a résztvevők a saját szempontjaik szerint kívánják optimalizálni a végrehajtás folyamatát. Tágabb értelemben az igazgatási szint²²² a lakosság biztonságos ellátásának szempontjait érvényesíti, míg a vállalati végrehajtási szint egy szűkebb értelemben vett szempontra van figyelemmel, a termelés biztonságára, az üzletmenet folytonosságára és a gazdaságos működésre. Ezek többnyire hatással vannak a kritikus infrastruktúrák aktuális védelmi szintjére, esetenkénti hiányosságaikra.

Magyarországon a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (továbbiakban OKF) biztosítja nemzetközi szabályozások beemelését a nemzeti jogalkotási gyakorlatba, valamint a védelmi feladatok egységes értelmezéséhez állami és nem állami szinten.

²²² Járás, megye, régió, országos

Az ENSZ, EGB²²³ Ipari Balesetek Országhatáron Túli Hatásairól szóló Egyezményt, 1992. március 17-én, Helsinkiben fogadták el, amely alapján a tagállamoknak is ezzel összhangban lévő jogszabályt kellett kidolgozni és életbe léptetni²²⁴. Az egyezmény szerint különös fontossággal bír, a lakosság és a környezet védelme az ipari balesetek hatásaitól. Deklarálták a megelőzés fontosságát az ipari balesetek elleni védekezések során. A környezetbiztonság és a fenntartható fejlődés biztosításához szükséges az ésszerű és gazdaságilag fenntartható költségek figyelembevételével bevezetett intézkedések, amelyekkel megelőzhetőek és elháríthatóak a káresemények.

A globalizált világban fontos biztonsági kihívásként jelentkezik az ipari balesetek – az esetek többségében – káros hatásainak az országhatárokon túli áttérjedése. Ezért szükséges a nemzetállamok bi²²⁵- és multilaterális²²⁶ együttműködése.

A NATO Polgári Veszélyhelyzeti Tervezés (CEP)²²⁷ feladata, hogy segítse a tagállamok tervezési és felkészülési alapfeladatait, elősegítse a hatékony nemzetközi együttműködést, ha az érintett tagállam nem képes felszámolni a természeti vagy mesterséges katasztrófák okozta károkat, illetve az eredeti helyzet visszaállítani.

2002 novemberében a NATO Felsőszintű Polgári Veszélyhelyzeti Tervezési Bizottság meghatározta a Szövetség szempontjából fontos aspektusokat és ezek alapján a kritikus infrastruktúra definícióját. A SCEPC²²⁸ keretében nyolc tervező munkacsoport és bizottság működik, amelyek feladata a tagállamok kritikus infrastruktúra-védelmére irányuló intézkedéseinek elemzése és értelmezése.

2005-ben a NATO több tanácsa vizsgálta a kritikus infrastruktúrák szektorait és alszektorait. A vizsgálat első lépése az információ összegyűjtése a tagállamok helyzetének elemzéséhez és megítéléséhez. Az év őszén elfogadták a NATO Válságreagálási Rendszer²²⁹ alapján a Nemzeti Intézkedési Rendszer-t (továbbiakban NIR)²³⁰, amely a „278/2011. (XII.20.) kormányrendelet, a NATO Válságreagáló Rendszerével összhangban

²²³ Európai Gazdaság Bizottság

²²⁴ A 128/2001. (VII.13.) Kormányrendelet, az Egyesült Nemzetek Szervezetének Európai Gazdasági Bizottság keretében létrejött, az ipari balesetek országhatáron túli hatásairól szóló Helsinkiben, 1992. március 17-én kelt Egyezmény kihirdetéséről.

²²⁵ két oldalú

²²⁶ több oldalú

²²⁷ Civil Emergency Planning, Polgári Védelmi Tervezés

²²⁸ Senior Civil Emergency Planning Committee, Polgári Védelmi Tervező Főbizottság

²²⁹ Crisis Response System – NCRS

²³⁰ Nemzeti Intézkedési Rendszer, NATO Válságreagáló rendszer

álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről²³¹” lépett érvénybe. A rendelet alapját képezi a „Kormány a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény 81. § (1) bekezdés *b*) pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (3) bekezdésében meghatározott feladatkörében” elrendelt feladatai alapján a NIR alkalmazását. A NIR legfontosabb célkitűzései között kell megemlíteni:

- > a rendeltetés célját,
- > a bevezethető intézkedéseket, koordinációját,
- > az ágazati válságreagálás intézkedéseit,
- > az együttműködő szervezeteket,
- > az összeköttetés és riasztás rendszerét.

Az EU 2008/114/EK tanácsi irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről szóló intézkedésében határozza meg az egységes irányelveket a tagállamok részére.

A Kormányzati Koordinációs Bizottság szerveinél és a minisztériumoknál a KIV-vel kapcsolatos kormányzati felmérő, elemző tevékenység 2003-ban kezdődött meg Magyarországon, melynek eredményeképp 2007-ben elfogadták a „Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról”²³² című dokumentumot.

A biztonsághoz kapcsolódó irányítási feladatok, amelyek kapcsolatosak a tagállamok létfontosságú infrastruktúrái elemeivel, valamint azok egymástól való függőségével. A veszélyekre, előre nem látható eseményekre és a sebezhetőségre vonatkozó elemzések elvégzéséhez több forrásból származó információra van szükség. Minden szektornak és tagállamnak az EU harmonizált szabálya szerint saját hatáskörén belül és a biztonságért felelős szervezetek segítségével kell meghatározni a létfontosságú infrastruktúrákat.

²³¹ <http://net.jogtar.hu/jr/gen/getdoc.cgi?docid=a1100278.kor> (Letöltve: 2014.09.12.)

²³² A Kormány a KKB javaslatára a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) Korm. határozattal fogadta el a Zöld Könyvet.

Magyarországi intézkedések:

- > Európai Unió irányelvei alapján a kritikus infrastruktúrák azonosítása, architektúrák felülvizsgálatának évenkénti végrehajtása és dokumentálása, illetve elmélyítése a gyakorlatban,
- > 2011. évi CXXVIII. törvény, a katasztrófavédelemről és a hozzákapcsolódó egyes törvények módosításáról²³³,
- > 234/2011. (XI.10.) kormányrendelet, a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról,
- > 2080/2008. (VI.30.) kormányhatározat, amely a jogszabályi koncepcióalkotással, ágazati konzultációkkal, felmérésekkel foglalkozik,
- > 2012. évi CLXVI. törvény, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,
- > 65/2013. (III. 8.) kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról,
- > 1249/2010. (XI.19.) kormányhatározat, az európai kritikus infrastruktúrákról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról,
- > Ágazati intézkedések,
- > Projektek, együttműködési- és stratégiai megállapodások.

A definíciók és ágazati kritériumok alapján kritikusnak minősülő infrastruktúrák:

Az NKIV²³⁴ szektorok²³⁵:

- > Energia,
- > Infokommunikáció,
- > Közlekedés,

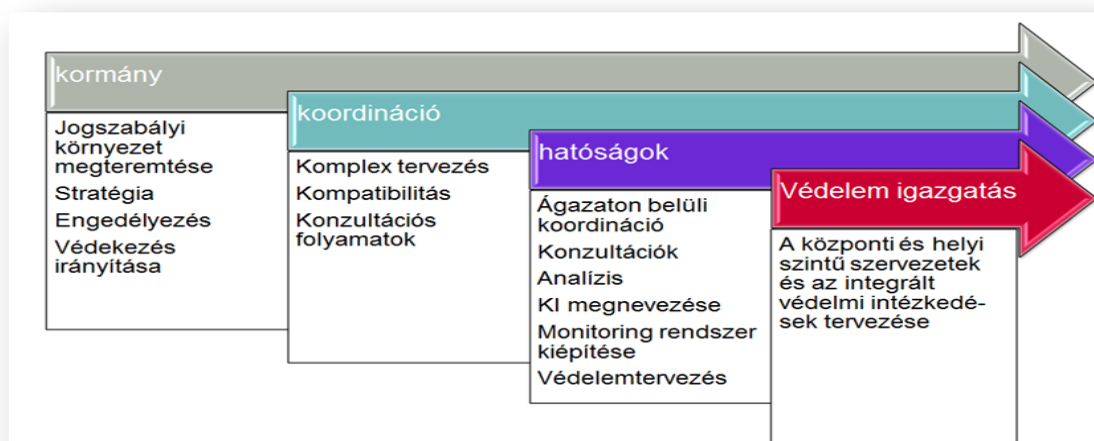
²³³ http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100128.TV#lbj1param (Letöltve:2014.10.10.)

²³⁴ NKIV – Nemzeti kritikus infrastruktúra védelem

²³⁵ 2080/2008. (VI.30.) Kormányrendelet, 2. számú melléklet

- > Víz,
- > Élelmiszer,
- > Egészségügy,
- > Pénzügy,
- > Ipar,
- > Jogrend – Kormányzat,
- > Közbiztonság – Védelem.

A KIV érdekében az állami/igazgatási szférában kifejtendő fő funkciókat az alábbi ábra foglalja össze:



7. számú ábra: KIV fő funkciói, Forrás: Dr. Király – Medveczky: Védelemgazdasági ismeretek önkormányzati (védelemi igazgatási) válság menedzsereknek. Budapest, 2009, ZMNE, ISBN 978-963-7060-75-5, 76. oldal (a szerző szerkesztésében)

Kritikus infrastruktúrák

Az ország - lakosság ellátásának, gazdaság és az állam - működése szempontjából létfontosságú elemek, objektumok, létesítmények, szolgáltatások, rendszerek és folyamatok hálózata, amelyek integrálódtak és egymástól kölcsönös függésben vannak. Fontos szerepük van a társadalom által elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot

kialakításában és működtetésében. Rizikóanalízis²³⁶ alapján definiálják, hogy mely szektorok és alszektorok minősülhetnek kritikusnak. Leegyszerűsítve: a kritikus infrastruktúrák közé tartoznak azok a rendszerek, berendezések és eszközök, melyek meghibásodása, megzavarása, kiesése, megsemmisülése esetén közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat a lakosság ellátására, a gazdaság és az állam működőképességére.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény²³⁷, valamint ennek végrehajtásáról szóló kormányrendelet nem határozza meg az üzembentartó részére, hogy milyen biztonsági rendszabályokat kell bevezetni, milyen biztonsági szervezeteket kell megalakítani és milyen rendszereket kell telepíteni.

A felsorolt szektorok és alszektorok listája módosulhat a kritikus szolgáltatások és termékek értékelésére irányuló elemzések során.

Előzetes elemzések alapján jogszabályok határozzák meg, hogy *mely szektorok és alrendszereik minősülhetnek kritikusnak az állampolgárok gazdasági és szociális jóléte, a közegészség, a közbiztonság, a nemzetbiztonság, a nemzetgazdaság és a kormányzat működése szempontjából.*

A magyar gazdaság szerkezetét a Vilfredo Pareto²³⁸ olasz közgazdász által kidolgozott elmélet szerint vizsgáltam. A Pareto-elmélet²³⁹, amelyet *80/20-as szabálynak is neveznek.* A tételek viszonylag kis hányada, 20 %-a meghatározó jelentőségű az összességében túlsúlyban levő és akár 80 %-ot is kitevő sok kis tétellel szemben. Az elv alkalmazásával *a jelentős kevés-től a szignifikáns²⁴⁰ tényező, jól elkülöníthető a jelentéktelen sok-tól.*

A Pareto-hatékonysági tényezőt széles körben alkalmazzák, mint:

- > A társadalom felépítése, interakciók, egyenlőtlenség vizsgálatánál,²⁴¹
- > Vállalati gazdálkodás (termékértékesítés, készletek, vevők, szállítók összetétele) vizsgálatához,

²³⁶ Kockázatelemzés: a lehetséges kockázatok beazonosítása, csoportosítása és értékelése/elemzése és követése

²³⁷ 2012. évi CLXVI. törvény

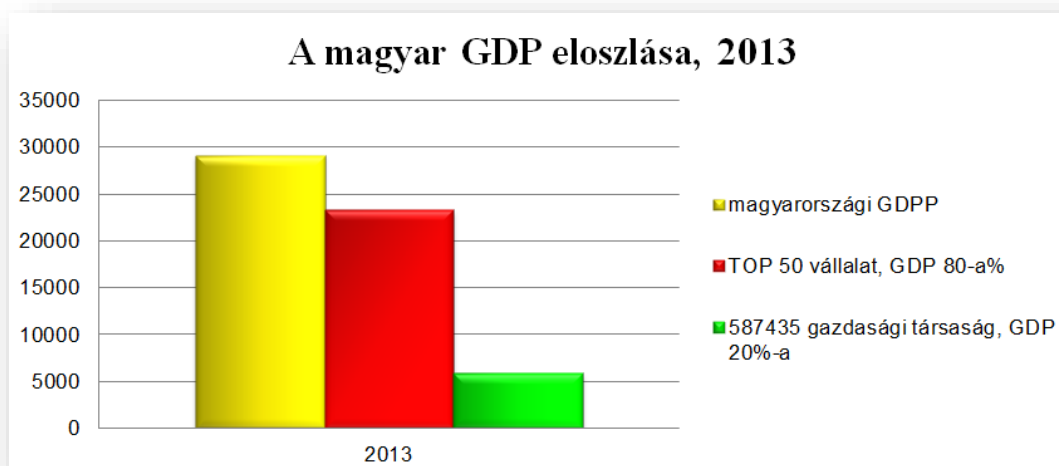
²³⁸ Az elvet több közgazdász is vizsgálta az 1950-es években és bebizonyították, hogy a Pareto-hatékonysági tényező csak bizonyos feltételek mellett teljesül a piacgazdaságban.

²³⁹ <http://www.absolventa.de/karriereguide/zeitmanagement/pareto-prinzip> (Letöltve:2014.10.10.)

²⁴⁰ Jelentős, meghatározó

²⁴¹ Tom BOTTORÉ: *Élites and Society*, Routledge N.Y., 1993, ISBN-13: 978-0415082716, pp. 1-7.

- > Minőségi problémák elemzéséhez (beszállítói hibák, hibás termékek aránya, ...)
- > Termelés kiesés elemzéséhez (gépkarbantartás, gyártósorok elavultsága miatt bekövetkező kiesés,...),
- > Logisztikai stratégiák és módszerek²⁴² (raktározási problémák, disztribúciós²⁴³ elemzések, készletgazdálkodás, ...),



8. számú ábra, A magyar GDP eloszlása, 2013, Forrás: GDP 2013²⁴⁴ eloszlása a szerző saját számítása szerint

A szektorok felülvizsgálatához a 2013-as magyar GDP szerkezetének elemzése szükséges, eszerint a megtermelt javak aránya alapján lehetséges a vállalatok besorolása. Ez azt jelenti, hogy a jelenleg érvényben lévő kormányhatározat²⁴⁵ 3. számú melléklete szerint szereplő szektorok és alszektorok kidolgozása során nem vették figyelembe „*az állampolgárok gazdasági és szociális jóléte*“-t biztosító vállalatok üzleti eredményeit, amelyek jelentős hatással bírnak a nemzetgazdaság működésére.

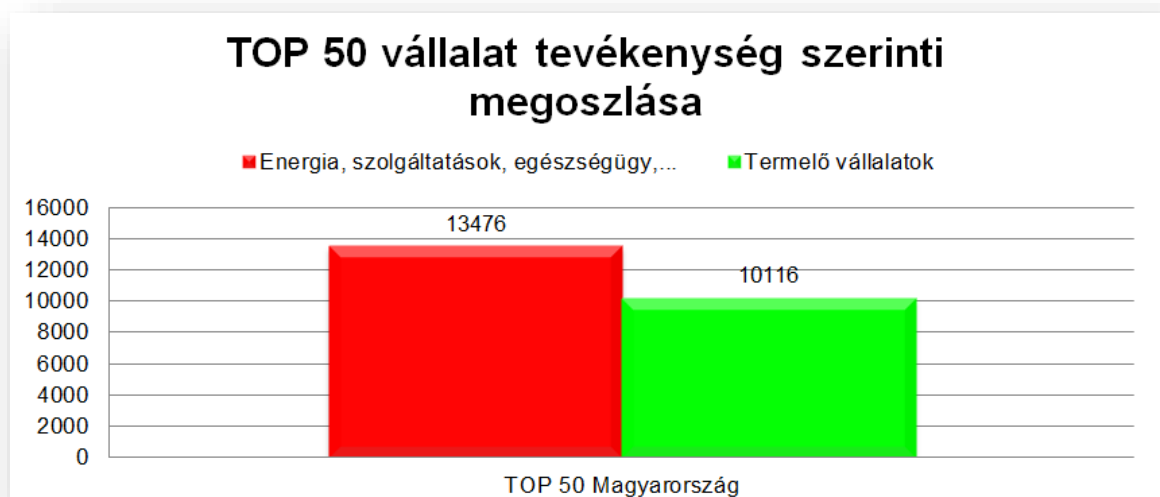
Magyarország GDP-je 29.114 milliárd forint volt 2013-ban. 80,09 %-át - 23.261 milliárd forint - a TOP 50 magyar vállalat állította elő. A TOP 50 vállalatból 26 vállalat a szolgáltatásban és 24 vállalat a termelési szférában működik.

²⁴² KÓTHAY János: *Általános logisztikai módszerek*, Katonai Logisztika, MH ATFCSE, 2. Évfolyam, 1994/1., pp. 2 - 16

²⁴³ felosztás, megoszlás

²⁴⁴ <http://statinfo.ksh.hu/Statinfo/haViewer.jsp?wcf9e2b1f9a=x> (Letöltve:2014.10.10.)

²⁴⁵ 2080/2008. Kormányhatározat, a Kritikus Infrastruktúra Védelem Nemzeti Programjáról



9. számú ábra, TOP 50 magyar vállalat tevékenység szerinti megoszlása,

Forrás: a szerző saját számítása szerint

A jelenlegi szabályozások szerint a TOP 50 vállalatból csak 26 tartozik a kritikus infrastruktúrák sorába a 2060/2008. kormányhatározat 3. számú melléklete szerint.

Ezen adatokból megállapítható, hogy a magyar gazdaság szerkezete aránytalan, a primer szektor²⁴⁶ aránya elenyésző a secunder szektor²⁴⁷, illetve a terciér szektor²⁴⁸ javára. Az ipar szerkezete jelentősen megváltozott a rendszerváltás óta. A meghatározó szerepet a járműipar és a hozzákapcsolódó beszállítói hálózatok töltik be, amelyet a vegyipar és az elektronikai ipar követ. Ezen termelő vállalatok alapvetően vidéki nagyvárosokba és azok környékére koncentrálnak. Így alakultak ki a fontosabb ipari centrumok (Győr, Kecskemét, Esztergom, Székesfehérvár...).

²⁴⁶ Mezőgazdaság: növénytermesztés, állattenyésztés, erdőgazdálkodás, ...

²⁴⁷ Ipar: járműipar, vegyipar, elektronika

²⁴⁸ Szolgáltatások, infrastruktúra, idegenforgalom, ...



10. számú ábra, Forrás: A termelő vállalatok értékelése telephelyek száma szerint, a szerző saját számítása alapján

Az ipari centrumok kialakulásánál biztonsági szempontból nagy hátrányt jelent a koncentráció. A termelő vállalatok telephelyeinek szerkezetét vizsgálva kockázatot jelent, hogy a 24 vállalatból a termelését 8 vállalat egy telephelyen valósítja meg, amely a GDP 14,2 %-át adja (4 158 milliárd forint).

11. számú ábra, Forrás: Németország GDP²⁴⁹ eloszlása a szerző saját számítása alapján

Ezt összehasonlítva Európa legnagyobb gazdasági szereplőjének szerkezetével, Németországban a GDP 79,1%-át a TOP 200 német vállalat állítja elő. A TOP 200 német nagyvállalatot vizsgálva megállapíthatjuk:

- > Struktúrát tekintve: konszernek, több leányvállalattal,
- > Földrajzi koncentráltság szerint: több tartományban, több telephellyel rendelkeznek,
- > Szerkezetét tekintve: elsődleges a secunder szektor, amelyben „minden iparág“ jelen van, másodlagos a szolgáltató szektor és harmadlagos a primer szektor.

A két ország gazdasági szerkezetét, struktúráját és földrajzi koncentrációját vizsgálva kijelenthetjük, hogy a magyar gazdaság secunder szektorát három iparág határozza meg.

²⁴⁹ <http://www.cio.de/top500> (Letöltve: 2014.10.12.)

Struktúráját tekintve külföldi tulajdonú leányvállalatok, illetve a földrajzi koncentrálttsága nagyon magas a német példához képest.

Véleményem szerint a magyar gazdaság kitettsége aránytalanul magas, amely magas kockázatot jelent gazdasági²⁵⁰ és biztonsági szempontból. A koncentrált szerkezet kialakulása miatt jelentős biztonsági kockázatot jelent egy nagyvállalat működésképtelensége a magyar gazdaságra, illetve „*az állampolgárok gazdasági és szociális jóléte*“-re.

Ezen tényezők figyelembevételével javaslom a 2080/2008. (VI.30.) Kormányrendelet, 2. számú melléklet módosítását, amely a NKIV szektorokat sorolja fel. Az „Ipar“ részt ki kell bővíteni azon vállalatokkal, akik az utolsó öt év adatai alapján legalább a GDP 2%-át megtermelték. Természetesen ezen nagyvállalatok listáját évente szükséges lenne felülvizsgálni és az aktuális adatok alapján módosítani.

3.2. BIZTONSÁGI HELYZET ÉS BIZTONSÁGPOLITIKA

3.2.1. Biztonsági stratégia

Az „általános stratégiában”²⁵¹ rögzítik a nagy vállalatok **hosszú távú célkitűzéseit**, meghatározzák a célok megvalósulásához szükséges erőforrásokat és a lényegesebb fejlesztési irányelveket.

A stratégia kialakítása és alkalmazása²⁵² elengedetlen feltétele egy nagyvállalat sikeres működtetéséhez. A stratégia irányt mutat a nagyvállalat menedzsmentje²⁵³ számára és ezzel meghatározza a tevékenységek határait, biztosítja egy folyamatosan változó környezetben, hogyan alkalmazkodjon a vállalat. Ezzel megvalósítható az üzleti kockázatok csökkentése, a veszélyek időbeni felismerése és elhárítása, a működés helyreállítása. A stratégia segíti a külső és belső környezet elemzését, bemutatja a nagyvállalat meglévő adottságait, az erőforrások elosztását, a fejlesztési lehetőségeit,

²⁵⁰ A gazdasági szerkezetet nem volt céлом mélységében vizsgálni. A szer. Megjegyzése ...

²⁵¹ A vállalati stratégiák hierarchiájában a legfelső szintű irányelv, amely alapján dolgozzák ki a központi szervezeti egységek a saját stratégiáikat (például: Biztonsági stratégia, Minőségbiztosítási stratégia ...), illetve az üzleti egységek ezekből származtatják a saját üzleti stratégiájukat

²⁵² „Seat at the Executive”, http://humanresources.about.com/strategichr/a/exec_success.htm (28.august 2011), (Letöltve: 2014.07.11)

²⁵³ menedzsment (management): az angol nyelv tágabb értelmezése szerint igazgatást jelent

valamint ezekkel összehangolja a környezeti lehetőségeket. A stratégia fontos szerepet tölt be a folyamatos versenyelőny elérésében és biztosításában.

Egy nemzetközi nagyvállalat biztonsági stratégiáját az adott nagyvállalat általános stratégiájából kell származtatni. A biztonsági stratégiában meghatározzák azokat a biztonsági irányelveket és elvárásokat, amellyel szavatolható a vállalattal kapcsolatba került emberek biztonsága és a vállalat működőképessége. A Biztonsági stratégia – az időhorizont szerint – hosszú távú koncepció.

Kidolgozása során két fontos szempontot kell figyelembe venni. A legfontosabb az adott ország nemzeti biztonsági stratégiája²⁵⁴ - ahol „leányvállalat” működik -, másodsorban az „anyavállalat” „worldwide”²⁵⁵ érvényes biztonsági intézkedései.

A gazdasági társaságok rendelkeznek biztonsági irányelvekkel, amelyekben meghatározzák az általános biztonsági előírásokat és a minimálisan teljesítendő szabályokat²⁵⁶.

A vállalat biztonsági stratégiája kimondja a cél eléréséhez szükséges biztonsági filozófiát, valamint a vállalati biztonságkultúra alapját és a felelősségi köröket. Definiálni kell a várható külső és belső fenyegetéseket, veszélyeket és a potenciális rizikóforrásokat. A kihívások azonosítása segítségével el kell készíteni a vállalatnál alkalmazott biztonsági modellt, amely alapján meghatározhatóak a megalakítandó biztonsági szervezetek és előírások rendszere.

A vállalat Biztonsági Stratégiájában²⁵⁷ megjelenő fenyegetések átfogó kezeléséhez a szakterületek²⁵⁸ szoros együttműködése szükséges. Ezzel összhangban erősíteni kell az információvédelmi²⁵⁹, tűzvédelmi, vagyonvédelmi, katasztrófavédelmi és polgári válságkezelési szervezetek szoros és hatékony kooperációját, koordinációját, illetve ezek átfogó, a biztonsági környezethez alkalmazkodni képes kereteit. Minden biztonsági szervezet feladata, hogy saját szakterületén folyamatosan értékeljék a nemzeti és

²⁵⁴ A Kormány 1035/2012. (II. 21.) Korm. határozata: Magyarország Nemzeti Biztonsági Stratégiájáról M A G Y A R K Ö Z L Ö N Y • 2012. évi 19. szám

²⁵⁵ világszerte

²⁵⁶ OTTEN, Wolfgang: *Eigensicherung*, ISBN-10: 3-452-26276-6 , Köln, 2006, pp. 333-335

²⁵⁷ GUNDEL, STEPHAN, MÜLLI, LARS: *Unternehmenssicherheit*, München: Oldenbourg, 2009, ISBN 978-3-486-58712-8, pp. 4.

²⁵⁸ olyan személyek és/vagy szervezeti egységek, amelyek egy adott biztonsági területért felelős(ek)

²⁵⁹ információbiztonság, üzleti hírszerzés elhárítás, adatvédelem, adatbiztonság, know-how védelem, titoktartás, prototípusvédelem ...

nemzetközi biztonsági helyzetet és a fenyegetettség mértékét, majd megtegyék a szükséges lépéseket azok kezelésére és elhárítására. Ez csak akkor lehet sikeres, ha a szervezeti erőforrások koordináltan és koncentráltan kerülnek alkalmazásra. **1. számú melléklet**

3.2.2. Biztonságpolitika

Csak egy adott országban működő vállalatra érvényes, amelyet az adott vállalat menedzsdmentje határoz meg középtávra. Évente vagy egy nagyobb jelentőségű esemény esetén kell felülvizsgálni.

A biztonságpolitika célja, hogy az értékek és érdekek számbavétele, valamint a biztonsági környezet elemzése alapján meghatározza azokat a vállalati célokat, feladatokat és eszközöket, amelyekkel a vállalat a globalizált világban szavatolja az emberek életét és egészségét, illetve a vállalat biztonságos működését.

Biztonsági környezet²⁶⁰

A biztonság fogalmát átfogóan kell értelmezni, mert a biztonsági környezet folyamatosan változik. A globális fenyegetések, regionális veszélyek és a lokális rizikók ma több szinten – az egyének, közösségek, államok és régiók szintjén, valamint globális szinten – jelentkeznek, amelyek érintik a nem kormányzati és transznacionális szervezeteket.

Ezért fontos a kihívások biztonságpolitikai, gazdasági és pénzügyi, társadalmi (humán²⁶¹) és környezeti dimenziójának integrált kezelése.

Biztonsági érdekek

A legfontosabb érték az emberi élet és egészség védelme. Másodsorban a vállalat működőképességének biztosítása, területének, berendezéseinek és vagyontárgyainak őrzés-védelme, belső rendjének és gazdasági stabilitásának megőrzése.

A vállalat vezetése elvárja, hogy a biztonsági szervezetek minél jobban alkalmazkodjanak az új típusú veszélyekhez és a lehetőségekhez mérten megfelelő válaszokat adjanak a megjelenő veszélyforrásokra.

²⁶⁰ Dr. SIMICSKÓ István: előadása a *A magyar védelempolitika aktuális kérdései és jövőbeni tervei* címmel 2015. november 13-án a Nemzeti Közsolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Felsőfokú Vezetőképző Tanfolyam hallgatóinak. <http://www.defence.hu/cikk/54098>, (Letöltve:2016.01.21.)

²⁶¹ Emberi, emberhez tartozó ...

Biztonság alapja

A biztonsági rendszabályok betartása minden személyre kiterjed, akik a vállalat illetékességi területén tartózkodnak.

A vállalat biztonsági stratégiájában megfogalmazottak alapján a legfontosabb tényező a *biztonságtudattal rendelkező munkatárs*, aki a biztonsági intézkedéseket elfogadja, végrehajtja és alkalmazza.

A biztonságpolitika alapvető keretét a munkatársak, a vezetők, a beavatkozó erők, a szakterületek és a vállalatvezetés együttműködése adja. Ez az együttműködés olyan érték közösséget képez, amely szavatolja a vállalat működőképességét és a vele kapcsolatba kerülő emberek biztonságát.

A megbízott szakterületek kidolgozzák a saját ágazati politikájukat a vállalat biztonsági stratégiája és biztonsági politikája alapján. A vezetőket tanácsadással támogatják a biztonsági intézkedések megvalósításában, valamint a vállalaton belüli biztonsági kérdések megválaszolásában.

Fenyegetések kezelése

A biztonsági intézkedéseket tudományos alapokon, az aktuális védelmi céloknak megfelelően kell kidolgozni.

A veszélyhelyzetekre való felkészülés magába foglalja az érintett szervezetek felkészítését és együttműködésének összehangolását, e mellett a munkatársak felkészítését és tájékoztatását, valamint a különböző védelmi képességek kialakítását.

A *pénzügyi stabilitás* kérdése a világgazdasági válság hatására jelentősen felértékelődött. A vállalat gazdasági és pénzügyi rendszerének stabilitása és ellenálló képessége fontos érdek és biztonságpolitikai szempont. A Biztonság- és védelempolitika szervezeti egység folyamatosan kiértékeli a kialakult helyzetet, tájékoztatja a vállalatvezetést és javaslatot tesz a válságkezelésre.²⁶²

²⁶² Dr. Helge SCHRÖDER: *Wie funktionieren Finanzmärkte? – Chancen und Gefahren globalisierter Geldströme*, Globale Herausforderungen, © Bundeszentrale für politische Bildung, Bonn, 2011, pp. 195 – 199, ISBN 978-3-8389-7042-4

Az *energiabiztonság* kulcsfontosságú kérdés a vállalat számára. Ezért szükséges az energiahordozók forrás- és útvonal-diverzifikáltsága²⁶³. Ennek hiánya számos kockázatot jelent. A vállalat működőképességének fenntartása miatt stratégiai jelentőségű a stabil, versenyképes áron hozzáférhető és tervezhető energiaellátás.²⁶⁴

A *globális éghajlat- és környezetváltozás*, az egyre szélsőségesebbé váló időjárás hatásai, a nyersanyag- és természeti erőforrások kimerülése komoly biztonsági kockázatot hordoznak magukban, konfliktusok forrásaivá válhatnak. A térség földrajzi adottságai miatt fokozottan hatnak a Kárpát-medence szomszédos országaiban keletkező környezeti és civilizációs ártalmak, az árvizek, a víz- és levegőszennyezés. A környezeti veszélyforrások közvetve hatással vannak a munkatársak egészségi állapotára és a vállalat működőképességére is. Ezért fontos a veszélyforrások időben történő beazonosítása és a vállalat biztonsági szervezeteinek és az állam érintett hatóságainak szoros együttműködése.²⁶⁵

A *természeti és ipari katasztrófák*, az egyes ipari, biológiai, vegyi és különösen nukleáris létesítményekben zajló folyamatok ellenőrizhetetlenné válása tömeges méretekben veszélyeztetheti vagy károsíthatja az emberi egészséget, a környezetet, az élet- és vagyonbiztonságot. További kockázatot jelent a veszélyes áruk közúti, vasúti, vízi, légi és csővezetékes szállítása.

A vállalat kiemelten kezeli a vállalat folyamatos működőképességének fenntartását, a gazdaság és az ehhez szükséges kritikus infrastruktúrák hatékony őrzés-védelmét.

Az élet- és vagyonvédelem érdekében különös figyelmet kell fordítani az ebben érintett biztonsági szervezetek megfelelő felkészülésére, a munkatársak katasztrófavédelmi felkészítésére.

²⁶³ a kockázat csökkentésére irányuló magatartás, amely a források és útvonalak bővítését jelenti

²⁶⁴ Dietmar DIRMOSER: *Energiesicherheit*, © Friedrich-Ebert-Stiftung, Bonn/Berlin 2007, pp. 2 – 5, ISBN: 978-3-89892-727-7

²⁶⁵ Hans-Joachim SCHNELLNHUBER – Meinhard SCHLUZ-BALDES – Benno PILADEAUX: *Umweltveränderungen und ihre Folgen*, Sicherheitspolitik in neuen Dimensionen, Bundesakademie für Sicherheitspolitik, 2001, pp. 567 - 584, ISBN 3-8132-0776-5

A *kiberbiztonság*²⁶⁶ révén egyre bonyolultabb kihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatokban, valamint a fizikai és virtuális térben, ahol a kapcsolódó kritikus infrastruktúrákat működtetik. Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszereket, illetve azok rendeltetésszerű működését.²⁶⁷

Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérése, priorizálása, a konszern²⁶⁸ koordináció erősítése, a munkatársak biztonságtudatosságának fokozása és az együttműködés javítása.

Az *illegális migráció*²⁶⁹ Magyarországot jelenleg elsősorban tranzit országgént érinti. A vállalat szállítási útvonalainak komplexitásából adódó feladatok és a külső határok fokozott védelmének eredményes megvalósítása a magyar rendvédelmi és migrációs, valamint a migrációval kapcsolatos feladatok végrehajtásában közreműködő szervek hatékonyabb együttműködését követelik meg. A konszern szintű támogatás biztosítása nélkül nem várható, hogy az érintett szervezetek hatékonyan lépjenek fel az illegális migráció megjelenési formái ellen.

A *terrorizmus* elleni védekezés fontos terület. A terroristák potenciális célpontjainak védelmét, biztonságuk erősítését jelenti, különös tekintettel a munkatársak biztonságára, illetve a vállalat kritikus infrastruktúrájára. A terrortámadások időbeni előrejelzése, megakadályozása és felszámolása az állam biztonsági szervezeteinek feladata.²⁷⁰

A biztonságpolitika végrehajtásának eszközzrendszere

A vállalat biztonságának szilárd gazdasági alapokon kell nyugodnia, mely biztosítja a hatékony biztonságpolitika erőforrásait. A vállalat ezért mindenkori feladatának és kötelességének tekinti, hogy a gazdasági helyzettel összhangban megfelelő forrásokat

²⁶⁶ Kiberbiztonság vizsgálata: sérülékenység vizsgálatát; ethical hacking lényege a biztonsági kontrollok kijátszása, behatolás...

²⁶⁷ Klaus-Rainer MÜLLER: *IT-Sicherheit mit System*, © Springer Fachmedien Wiesbaden, 2014, pp. 73, ISBN 978-3-658-04333-9

²⁶⁸ Vállalatok, vállalkozások csoportosulása, egyesülése meghatározott célok eléréséhez.

²⁶⁹ Dr. VIDA Csaba alezredes: *A jelenkori népvárdorlás hatásai*, KNBSZ Felderítő Szemle, XIV. évfolyam 3. Szám, 2015, pp. 7 – 14, ISSN 1588-242-X

²⁷⁰ Stefan PROCHOW: *Terrorism*, Globale Herausforderungen, © Bundeszentrale für politische Bildung, Bonn, 2013, pp. 81 -99, ISBN 978-3-8389-7086-8

biztosítson a vállalat és munkatársai védelmére. Alapvető biztonságpolitikai cél a gazdasági és pénzügyi stabilitás folyamatos erősítése és felügyelete, a külső kockázati kitétségeinek időbeni felderítése, a vállalat működőképességének megalapozása, biztonságos és hosszú távú erősítése.

Fontosnak tartom, hogy a stabilitás és biztonság fenntartásában meghatározó konszern biztonsági szervezetek között intenzívebbé váljon az együttműködés és ezek a szervezetek egymást erősítő és kiegészítő szerepet játsszanak.

3.3.2. Biztonsági szervezetek ágazati politikái

A különböző szakterületeknek a vállalat biztonságpolitikája és a hatályos magyar jogszabályok alapján kell elkészíteni a saját szakpolitikájukat.

A vállalati szinten összehangolt biztonságpolitika elősegíti, hogy szinergia²⁷¹ és koherencia²⁷² jöjjön létre a vállalat különböző szakpolitikái között.

Az egyes szakterületek biztonsággal összefüggő tevékenységének összhangban kell állnia a vállalat Biztonsági politikájával. A szakpolitikák és előírások időszakos felülvizsgálata során figyelembe kell venni a Biztonságpolitika ide vonatkozó rendelkezéseit.

Együttműködés a szakterületek között

A védelmi intézkedéseket egy integrált biztonsági koncepcióban kell meghatározni. Ennek kidolgozásáért és tartalmáért a biztonsági menedzsment biztonsági tervező csoportja a felelős. Ezeket az intézkedéseket a felelős üzleti egység vezetője köteles bevezetni és alkalmazni.

Az adott üzleti egységre vonatkozó biztonsági intézkedések kidolgozását egy *kockázatértékelésnek* kell megelőzni és ez alapján kell a megfelelő biztonsági intézkedéseket kidolgozni és alkalmazni. A biztonsági tervező csoportot és a szakterületeket - az ide vonatkozó tervek alapján - időben kell informálni és bevonni a biztonsági tervezés támogatásába.

A *szakterületek* (Egészségmenedzsment, Környezetvédelem, IT-biztonság, Biztonsági tervező csoport, Tűzvédelem, Katasztrófavédelem, Iparbiztonság, Fluid²⁷³ menedzsment)

²⁷¹ együttműködés

²⁷² összetartozás

szoros együttműködésben, közösen dolgozzák ki a biztonsági intézkedéseket és koncepciókat. Bizonyos elemeinek egyeztetése lehetséges a Személyüggyel, az Üzemi Tanáccsal²⁷⁴ és a munkavédelmi képviselőkkel.

Egészségpolitika²⁷⁵

A vállalat egészségpolitikájának célja, hogy biztosítsa az egészséget nem veszélyeztető biztonságos munkavégzést és a vállalat biztonságos működését.²⁷⁶ Folyamatosan figyelemmel követi az egyre növekvő, munkatársak (polgárok) egészségét érintő kihívásokat, a határokon átnyúló egészségügyi veszélyeket, valamint az egészségtelen életmódhoz és a munkavégzéshez kapcsolódó ún. foglalkozási megbetegedéseket.

A szakpolitika célja továbbá erősíteni az együttműködést azon szervezeti és üzleti egységek között, amelyek érintettek és felelősek a vállalat egészségügyi biztonságában²⁷⁷.

A vállalat egészségpolitikáját a hatályos magyarországi jogszabályok²⁷⁸, a vállalat biztonsági politikájából és a konszern (anya vállalat) idevonatkozó irányelvei alapján kell kidolgozni és a vállalat felső vezetésével elfogadtatni.

A betegjogokat, mint például a döntéshozatalban²⁷⁹ való részvétel és az egészségügyi tájékozottság jogát²⁸⁰ szintén figyelembe kell venni a vállalat egészségpolitikájának kidolgozása során.

Az egészségpolitika négy alapeladatot fogalmaz meg közép- és hosszútávra.

²⁷³ folyadék, cseppfolyós: gyártásban általában hűtő és sűrűlő csökkentő közeget jelent

²⁷⁴ 2012. évi I. törvény, XX. fejezet, Az Üzemi Tanács, 104. Általános szabályok, **235. §** (1) A munkáltató és a munkavállalók együttműködésére, a munkáltató döntéseiben való részvételle e fejezet rendelkezéseit kell alkalmazni. (2) A munkavállalókat az e fejezetben foglalt munkavállalói jogok tekintetében az üzemi megbízott, az üzemi tanács, a központi üzemi tanács, valamint a vállalatcsoport szintű üzemi tanács képviseli.

²⁷⁵ EURÓPAI BIZOTTSÁG: *Egészségpolitika, minden uniós polgár egészségének javításáért*, Luxembourg, Európai Unió Kiadóhivatala, 2014, ISBN 978-92-79-42343-7

²⁷⁶ A vállalat biztonsági politikája

²⁷⁷ Munkavédelem, környezetvédelem, iparbiztonság, katasztrófavédelem, polgári védelem

²⁷⁸ **A Munkavédelemről szóló 1993. évi XCIII. Törvény** határozza meg, hogy a munkáltatók foglalkozás-egészségügyi szolgáltatást kötelesek biztosítani valamennyi munkavállalójuk részére **A 89/1995 (VII. 14) sz. kormányrendelet** intézkedik a foglalkozás-egészségügyi szolgáltatás szervezéséről és működéséről, az alkalmazottak kategóriák szerinti besorolásáról.

²⁷⁹ Üzemi Tanács bevonása a munkatársakat érintő döntésekbe

²⁸⁰ **2011. Évi CXII. Törvény, az információs önrendelkezési jogról és az információszabadságról**, (Kihirdetve: 2011.VII.26)

Foglalkozás-egészségügy

Egy vállalat biztonságos működésének és prosperitásának kulcsa az egészséges munkavállaló. A munka-egészségügyi problémák kezeléséhez kapcsolódó kiadások komoly pénzügyi megterhelést jelentenek a vállalatok számára. A jogszabályokban előírt kötelező orvosi vizsgálatokat minden munkatársnál végre kell hajtani.

A foglalkozás-egészségügy körébe tartozó feladatok és felelőségek²⁸¹

- A foglalkozás-egészségügyi vizsgálatok rendjének meghatározása a hatályos jogszabályok és helyi igények alapján
- A külön jogszabályban meghatározott munkaköri alkalmassági vizsgálatok végrehajtása és az ehhez szükséges szakorvosi vizsgálatok kezdeményezése és elvégzése
- A foglalkozási megbetegedések, fokozott expozíciós esetek²⁸² kivizsgálása, jelentése
- A munkavégzés egészségkárosító hatásainak vizsgálata, az üzemi balesetek helyszíni kivizsgálása a munkabiztonsági szakfeladatot ellátó szakterülettel együttműködve
- Az egyéni védőeszközökkel kapcsolatos munkáltatói kötelezettségek teljesítése, valamint tanácsadás az üzleti egységek részére
- Felvilágosítás a munkavállalók munkakörülményeivel kapcsolatban

Általános és szakorvosi ellátás

Egy vállalat egészségügyi ellátórendszerének keretében nyújtott szolgáltatások alapvető célja, hogy hozzájáruljon a munkavállalók egészségi állapotának folyamatos felméréséhez és javításához, valamint a költségek hatékony felhasználásához, ellenőrzéséhez. Ez már a prevenció első eleme, mivel a különböző szűrések alkalmazásával lehet a különböző betegségeket megelőzni, továbbá biztosítani a kötelező orvosi vizsgálatok szakorvosi hátterét, hogy probléma esetén megfelelő szaksegítséget kapjon a munkatárs.

²⁸¹ 27/1995. (VII.25) NM rendelet, a foglalkozás-egészségügyi szolgáltatásról

²⁸² 27/1996. (VIII. 28.) NM rendelet, a foglalkozási betegségek és fokozott expozíciós esetek bejelentéséről és kivizsgálásáról

Javasolt elemek a fő foglalkozás-egészségügyi problémák kezelésének végrehajtásához:

- > A szakorvosi ellátás igénybevételének szabályozása (bőr-, belgyógyászat, szemészet, ortopédia, fül-orr-gégészet, fizioterápia stb.),
- > Vállalati Check-up rendszer²⁸³,
- > Egészségügyi szűrések vezetőknek,
- > Munkahelyi stressz megelőző programok
- > Munkahelyi mozgásszervi prevenciós program,
- > A vállalatnál kiküldetésben lévők (külföldi munkatársak) ellátása,
- > A helyi mentőszolgálat megalakítása, munkafolyamatainak szabályozása,
- > A munkatársak egészségügyi adatainak feldolgozása.

Egészségügyi promóció

Olyan programrendszer, amely a hatékony kommunikáció segítségével érdekelté teszi a munkavállalókat, hogy többet törődjenek egészségükkel és vegyenek részt a promóciós programokban. Ez jelenti a klasszikus értelemben vett prevenciót, amikor még nem betegségről beszélünk, hanem arról, hogyan védje-őrizzze meg az egészségét a munkatárs. Az egészségügyi kockázatok minősítésének rendszere (Health Risk Assessment - HRA²⁸⁴) alapján kell a kockázatokat elemezni és a betegség kialakulása előtt, fel kell hívni a figyelmet arra, hogy tenni is kell azért, hogy az egészség megmaradjon. Ez megvalósítható a felvilágosító-tájékoztató anyagok kiadásával és terjesztésével, valamint előadások szervezésével és megvalósításával:

- > Aktív élet,
- > Egészséges táplálkozás,
- > Az egészséges alvás és pihenés,
- > Munkahelyi stressz²⁸⁵ kezelése,
- > Fitten az irodában,
- > Mentális és érzelmi jóllét,
- > Dohányzás, alkohol és drog prevenció.

²⁸³ Ellenőrzés, időszakos orvosi felülvizsgálatok rendszere

²⁸⁴ egészségügyi kockázatok

²⁸⁵ Dr. TÚRI Viktória: *Az intrapszichés megküzdés típusai*, Gazdasági élet és társadalom, Wekerle Sándor Üzleti Főiskola Tudományos Folyóirata, 2013. I-II. szám, pp. 102 – 105, ISSN: 2060-7466

Az egészségügy szakpolitikai integrációja

Az egészségügyi szakpolitikához szervesen kapcsolódnak munkavédelemi szabályozások, környezetvédelmi és iparbiztonsági előírások. Ezért fontos a szakpolitikák és előírások közötti összhang megteremtése. A kooperáció adja meg a keretét a szakterületek közötti kapcsolatoknak, ahol az egészség megőrzése és a megelőzés jegyében együttműködnek a szakterületek és az érintett üzleti egységek. Mindenki a maga szaktudásával biztosítja, hogy a környezeti feltételek is megfelelőek legyenek, ezzel jó alapot biztosítva a prevenciós tevékenységnek.

- > A termelési terület támogatása:
 - projektek szakmai támogatása,
 - kockázatértékelés,
 - a munkavédelemi megbízottak szakmai támogatása,
 - a munkavédelemi képviselők szakmai támogatása.
- > Speciális témák:
 - veszélyes anyagok használatának engedélyeztetése, alkalmazása, foglalkozás-egészségügyi kritériumok meghatározása,,
 - a veszélyeztetettek besorolásának koncepciója,
 - az egyéni védőfelszerelésekkel kapcsolatos tanácsadás.
- > Munka higiénia²⁸⁶:
 - zaj- és rezgésmérés,
 - a megvilágítottság ellenőrzése,
 - sugárzásvédelem,
 - képernyő előtt történő munkavégzés.

²⁸⁶ A munkahigiénia feladata a munkahelyi egészségkárosító veszélyek előzetes kockázatelemzése, értékelése és megfelelő ellen intézkedések bevezetése.

Az egészségpolitikának megbízható tudományos alapokon kell nyugodnia. Ezért az Egészségmenedzsmentnek összehasonlítható adatokat kell gyűjtenie a népegészségi nyilvános adatokból, helyi egészségügyi mérőszámokból, a konzern más országokban működő telephelyeiről. Ezért szükséges egy egységes egészségügyi indikátorrendszer, amely lehetővé teszi a minden szinten begyűjtött adatok összehasonlító elemzését.

Fel kell készülni az új veszélyek közegészségre gyakorolt hatásaira, különösen az éghajlatváltozáshoz kapcsolódó világiárványokra, biológiai veszélyekre és bioterrorizmusra. Ezért nagyon fontos az egészségügyi veszélyek folyamatos megfigyelése, valamint az azokra adott válaszreakciók mechanizmusainak és folyamatainak kidolgozása, betartásának ellenőrzése.²⁸⁷

Környezetvédelmi politika

Az EU környezetvédelmi politikájának²⁸⁸ alapvető célja, hogy megőrizze természeti értékeinket, támogassa és erősítse az erőforrás-hatékony gazdaság kialakulását, valamint oltalmazza az emberek egészségét és a környezetet.

Uniós (nemzetközi) szinten kell összehangolni környezetvédelmi politikát, amely elősegíti a szinergia és koherencia létrejöttét a különböző uniós szakpolitikák között. A környezetvédelmi jogszabályoknak nagy jelentőséggel kell bírniuk a gazdasági szektorban. Így biztosíthatóak az egyenlő versenyfeltételek a vállalkozások számára.

A vállalat biztonsági politikájában a fenyegetések között szükséges definiálni a globális éghajlat- és környezetváltozás²⁸⁹ okozta környezeti veszélyforrások időbeni felismerését és azok kezelését.

²⁸⁷ Dr. KUTI Rajmund – GRÓSZ Zoltán: *Biológiai eredetű vészhelyzetek kezelése, előtérben a mentesítési feladatok*, Hadtudomány, XI. Évfolyam 1. szám, 2016, pp. 127 - 131, ISSN 1788-1919

²⁸⁸ Európai Unió környezetvédelmi politikája, http://europa.eu/pol/pdf/flipbook/hu/environment_hu.pdf (Letöltve: 2014.11.04.)

²⁸⁹ REPORT OF THE UNITED NATIONS CONFERENCE ON THE HUMAN ENVIRONMENT, Stockholm 1972: „A környezeti változások folyamatos megfigyelése és kiértékelése eredményeként megállapítható a globális éghajlati rendszer állapotának jelentős megváltozása. A kiváltó okok között meg kell említeni a természeti, társadalmi és gazdasági okokat, amelyek hatásait az 1970-es évektől emelték a nemzetközi politika napirendjére. A először az ENSZ-konferenciáján (UNCHE) 1972-ben vitatták meg a környezetvédelmi problémákat, ez követően Éghajlati Világkonferenciát tartottak 1979-ben, ahol megállapodtak arról, hogy támogatni kell a környezeti rendszer folyamatainak folyamatos megfigyelését és elemzését, amelyet tudományos alapokon kell definiálni a különböző mozgatóerőket, ok-okozati összefüggéseket, valamint a várható veszélyesforrásokat.”

<http://www.unep.org/Documents/Multilingual/Default.asp?DocumentID=97> (Letöltve: 2014.11.05.)

A környezetvédelmi politika célja

A szakpolitika legfontosabb célja a gazdasági folyamatok környezetvédelmi szempontok alapján fenntartható menedzselése, a vállalat környezetvédelmi feladatainak teljesítése és az energiahatékonyság javítása. Ezeket a célokat egy integráltan működő környezetmenedzsment – energiamenedzsment rendszer keretében valósítható meg.

Környezetvédelem irányelvei:

- > a környezetet legkevésbé terhelő termékek gyártása és szolgáltatások nyújtása,
- > a környezetvédelmi politikának megfelelő kutatási és fejlesztési folyamatok alkalmazása, amelyek ökológiailag hatékony eljárásokat alakít ki, így megtartható a nemzetközi versenyképesség,
- > a vállalat területén a környezetre gyakorolt hatások folyamatos megfigyelése, az esetleges káros hatások felmérése és megelőzése,
- > együttműködés az alvállalkozókkal a vállalat környezetbarát jellegének folyamatos javításában,
- > a vállalat felsővezetékének felelőssége a környezetvédelmi szakpolitika alapelveinek betartása és betartatása, valamint a környezetmenedzsment működőképességének garantálása,
- > a vállalatnak szoros együttműködést kell kiépíteni a hatóságokkal, ez magában foglalja a vészhelyzetek megelőzését és elhárítását,
- > fontos a munkatársak környezetvédelmi - beosztásuknak megfelelő - tájékoztatása, képzése és motiválása, elősegítve ezzel a környezettel szembeni felelősségtudatuk (a biztonságtudat) kialakulását,
- > környezetvédelmi politika kötelező érvényű a vállalat számára, konkretizálva a telephelyre jellemző fő környezetvédelmi irányvonalak megfogalmazásával.

A környezetvédelmi politika megvalósításának eszközrendszere

A nagyvállalatok környezetmenedzsment rendszert működtetnek a nemzetközi és nemzeti hatáskörben meghozott jogszabályoknak megfelelően. Ehhez megfelelő alapot biztosítanak a nemzetközi minősítési rendszerek (ISO 14001²⁹⁰, EMAS²⁹¹, EN 16001²⁹², ISO 50001²⁹³). A környezetmenedzsment rendszer képezi a vállalat környezetvédelmi intézkedéseinek alapját. Legfőbb célkitűzés a rendszer keretein belül a környezeti teljesítmény folyamatos javítása, mind a fizikai mennyiségek, mind a folyamatok hatékonysága szempontjából.

A környezetvédelmi és az energiahatékonysági célok megvalósításához szükséges egy integrált környezetvédelmi és energiapolitika alkalmazása. E céloknak tükrözniük kell a vállalat környezeti és energia tényezőinek és hatásainak elemzését. Részletes meghatározásukhoz szükséges egy Átfogó Környezetvédelmi Program²⁹⁴ és az egyes üzleti egységekre vonatkozó Területspecifikus Környezetvédelmi Program²⁹⁵ integrált rendszerének kidolgozása.

Munkavédelmi politika²⁹⁶

A vállalat biztonsági politikája a legfontosabbnak az emberi élet védelmét és a munkatársak egészségét tekinti, amely magába foglalja az egészséges és ergonómiai²⁹⁷ szempontok alapján kialakított munkakörnyezetet. A munkavédelmi szakpolitika szerves részét képezi a vállalat biztonsági kultúrájának, melyet a vállalat biztonsági politikájából kell származtatni. A munkavédelmi szakpolitika a vállalat középtávú összehangolt feladatrendszere, amelynek fontos eleme az együttműködés a szervezeti és az üzleti egységekkel, a munkavédelmi célok elérése érdekében.

²⁹⁰ Environmental management, környezeti menedzsment,

<http://www.iso.org/iso/home/standards/management-standards/iso14000.htm> (Letöltve: 2014.11.05.)

²⁹¹ Eco-management and Audit Scheme, Öko-menedzsment és audit rendszer, <http://www.emas.de/home/> (Letöltve:2014.11.05)

²⁹² Energiemanagementsystem, energia menedzsment rendszer,

http://www.dnv.de/Binaries/Whitepaper_Energie_final_tcm70-447552.pdf (Letöltve: 2014.11.05.)

²⁹³ Globale Standard zum Energiemanagement, nemzetközi szabvány az energia menedzsment minősítéséhez

²⁹⁴ A Program a stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendelet

²⁹⁵ A vállalati és az üzleti egységek célok megvalósítását biztosító felelőségeket, a célok megvalósításának határidejét és a szükséges eszközöket.

²⁹⁶ A szakpolitika alapját a munkahelyi egészségvédelem és biztonsági irányítási rendszerének (MEBIR:) kialakítása és tanúsítása az MSZ 28001:2008 (BS OHSAS 18001:2007) szerint

²⁹⁷ a munkafolyamatokkal, valamint a munkatársak számára pénzügyileg megtérülő és a lehető legkisebb erőfeszítést igénylő kidolgozásával foglalkozó tudomány

A munkavédelmi szakpolitika alapjai

A munkavédelmi célok teljesítéséhez elengedhetetlen az átlátható és gyakorlatias szabályok és előírások kidolgozása, valamint a tanácsadó és ellenőrző külső szervezetek bevonása, az ösztönző koncepciók kidolgozása az üzleti egységek számára. Biztosítani kell minden szinten a munkahelyi egészség és biztonság fenntarthatóságának személyügyi és pénzügyi feltételeit. A versenyszférában működő vállalatok számára fontos, hogy ne gátolja, hanem támogassa az innovációt.

A munkavédelmi szakpolitikában meghatározottak végrehajtásáért felelősek a munkatársak és a területileg illetékes vezetők. A megvalósítás során szükséges a vállalat menedzsmentjének teljes támogatása.

A vállalat munkavédelmi szakpolitikáját a hatályos nemzetközi ajánlások²⁹⁸, magyarországi jogszabályok²⁹⁹ és a konszern (anya vállalat) ide vonatkozó irányelvei alapján kell kidolgozni és a vállalat felsővezetékével elfogadtatni.

A munkavédelmi szakpolitika megvalósulása³⁰⁰

Az első lépés a munkavédelmi rendszer szereplőinek és a szereplők felelősségének, jogainak és feladatainak meghatározása. A megvalósítás alapelveit a vállalat felső vezetése határozza meg középtávra, amelyet felül kell vizsgálni évente vagy egy nagyobb jelentőségű esemény bekövetkezése esetén.

A második lépés a vállalat fő tevékenységének és az üzleti egységek feladatainak figyelembevételével a munkavédelem fő feladatainak definiálása, a kockázatértékelések alapján a megelőző intézkedések meghatározása.

A munkavédelem egy folyamatorientált rendszer, amely szervesen kapcsolódik a vállalat minőségbiztosítási rendszeréhez³⁰¹.

²⁹⁸ Nemzetközi Munkaügyi Szervezet (ILO), (<http://www.ilo.org/global/about-the-ilo/lang--en/index.htm>) A TANÁCS IRÁNYELVE (1989. június 12.) **a munkavállalók munkahelyi biztonságának és egészségvédelmének javítását ösztönző intézkedések bevezetéséről** (89/391/EGK) (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1989L0391:20081211:HU:PDF>)

²⁹⁹ A Munkavédelemről szóló 1993. évi XCIII. Törvény

³⁰⁰ ROZMAN Tamás: *Tananyag a TÁMOP-2.4.8-12/1-2012-0001, „ A munkahelyi egészség és biztonság fejlesztése, a munkaügyi ellenőrzés fejlesztése című projekt keretében a Nemzeti Munkaügyi Hivatal megbízásából került kidolgozásra*, BMGE, Budapest, 2014, ISBN 978-963-313-122-0, II. rész, p.47

³⁰¹ MSZ EN ISO 9000-es sorozatok

Munkavédelem mint folyamatorientált tevékenység

Munkavédelem elhelyezkedése a vállalati folyamatokban



12. számú ábra: Munkavédelem mint folyamatorientált tevékenység

(Forrás: Rozman Tamás, BMGE, Tananyag, II. rész, p. 48)

A munkavédelmi szakpolitika végrehajtásának eszközzrendszere

A foglalkozási kockázatok meghatározása és az ebből származtatott megelőzési intézkedések képezik az alapját a bevezetett munkavédelmi irányelveknek, szabályzatoknak és munkautasításoknak. Ezek garantálják a munkatársak biztonságát és egészségvédelmét, a kockázati és baleseti tényezők kiküszöbölését, valamint a munkavállalók és munkavédelmi megbízottaknak³⁰² a nemzeti jogszabályok illetve ezek gyakorlatának megfelelő tájékoztatását. A velük folytatott folyamatos konzultációk, permanens részvételük és oktatásuk az egyik legfontosabb pillér a munkatársak biztonságtudatának kialakulásában.

³⁰² Munkavédelmi megbízottak feladatai a biztonsági tudat előmozdítása az üzletei egységeknél és a kisebb szervezeti egységeknél, valamint támogatják a vezetőket a munkahely stabil egészségügyi és munkabiztonsági helyzetének kialakításában. Fontos szerepük van az előírt biztonsági berendezések megfelelő használatában, valamint abban, hogy meggyőzzék a munkatársakat a folyamatos használatról, amelyet folyamatos jelenlétükkel érnek el.

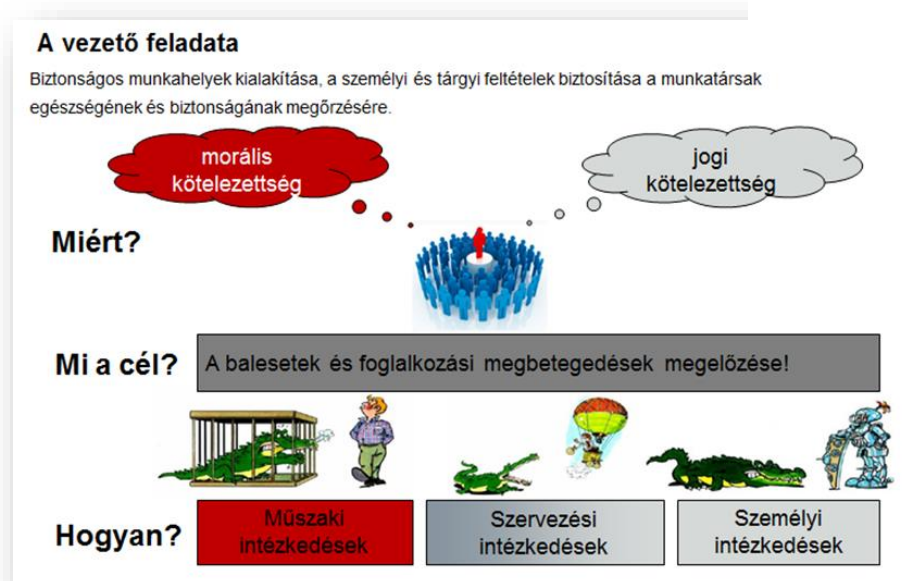
Munkabiztonság³⁰³

A munkavédelem területén kifejtett tevékenysége során a munkabiztonság szakterület támogatással és tanácsadással segíti az üzleti egységek munkáját. Ezen feladatok ellátásához a munkabiztonságot időben informálni kell a munkakörnyezet, munkahelyek, munkafolyamatok esetleges megváltoztatásáról a tervezés, kivitelezés és felújítás (építészeti) fázisokban.

A munkabiztonság feladata, hogy támogassa a vállalat vezetését a munkavédelemben és a baleset-megelőzésben, valamint az emberhez méltó munkavégzés kialakítását érintő minden munkavédelmi kérdésben. A biztonságtechnikai (safety)³⁰⁴ szakismereteik alkalmazása során a munkabiztonsági szakemberek utasítási jogkörrel rendelkeznek.

Vezetői felelősség

„A biztonsági felelősség része a vezetői felelősségnek, mely szerint a vezető feladata a biztonsági intézkedések érvényre juttatása a saját területén”³⁰⁵.



13. számú ábra: A vezető feladata

(Forrás: Rozman Tamás, BMGE, Tananyag, II. rész, p. 50)

³⁰³ 1993. évi XCIII. törvény a Munkavédelmről

³⁰⁴ biztonság

³⁰⁵ 1. számú ábra: Biztonsági stratégia, p. 8.

A munkavédelmi érdekképviselő³⁰⁶

A munkatársak jogosultak maguk közül képviselőket választani annak érdekében, hogy az egészséges és biztonságos munkavégzéssel összefüggő jogaikat és érdekeiket érvényesíteni tudják. A munkavédelmi képviselők megválasztásának, megbízatásuk megszűnésének, illetve visszahívásának rendjére, működési területére az Üzemi Tanács³⁰⁷ tagjaira, az üzemi megbízottra vonatkozó rendelkezéseket kell megfelelően alkalmazni, ideértve a központi munkavédelmi bizottság megalakításának lehetőségét is.

Munkavédelmi megbízottak

A munkavédelmi megbízott a saját üzleti- és szervezeti egységénél az illetékes vezetőket a munkavédelmi témákban támogatja, valamint folyamatosan meggyőződhet az előírt biztonsági berendezések és egyéni védőeszközök meglétéről és rendeltetésszerű használatáról. Ezt a folyamatos személyes jelenléte garantálja.

IT-biztonságpolitika³⁰⁸

Az IT-biztonságpolitika a vállalat biztonsági politikájának származtatott eleme. Ez a vállalat menedzsment-rendszerének szerves része, amely szükséges a vállalat üzleti folyamatainak megvalósításának és folyamatos fejlesztésének érdekében.

Az IT-biztonságpolitika definiálja az alapvető célokat, stratégiákat és felelőségeket, amelyek szükségesek a vállalat IT-biztonságának garantálásához.

Az IT-biztonságpolitika a nemzetközi szabályozások és szabványok³⁰⁹ végrehajtásán alapul.

Az üzleti folyamatok egyre növekvő mértékben függenek az információktól és információs rendszerek biztonságos működésétől és rendelkezésre állásától. Az információk és az információs rendszerek biztonsága többet jelent, mint a műszaki infrastruktúra biztosítása (fizikai biztonság³¹⁰), mert ez szavatolja az információáram ellenőrzését, vezérlését és

³⁰⁶ A Munka Törvénykönyvéről szóló 2012. évi I. törvénynek (Mt.)

³⁰⁷ Munka Törvénykönyvéről szóló 2012. évi I. törvénynek (Mt.) XX. Fejezet, 235 -269. §

³⁰⁸ 2001-től 2010-ig felelős voltam az IT-biztonságért, részt vettem a szabályok kidolgozásában egy projekt keretében egy multinacionális vállalatnál

³⁰⁹ ISO 27001:2013, ISO 9000:2000

³¹⁰ Lopás, rongálás, tűz, víz, rezgések, rengések, elektromos kisülések, elektromos hálózat zavarai, rágcsálók,

irányítását. Ehhez elengedhetetlen a biztonságtudat kialakítása a felhasználóknál, adminisztrátoroknál és a rendszergazdáknál egyaránt, ugyanakkor ez vonatkozik minden más munkatársra³¹¹ is. A vállalat IT-biztonságpolitika alapját képezi az IT-biztonság szabályoknak, melyek:

- > garantálják a vállalat információinak biztonságos kezelését,
- > segítséget nyújtanak az IT-biztonságon belül a felelőségek egyértelmű és világos meghatározásához.

Az IT-biztonsági architektúra szerves része az IT-infrastruktúra felépítésének és az információs rendszerek fejlesztésének, implementálásának³¹².

A vállalat felső vezetése hagyja jóvá az IT-biztonságpolitikát, amely alapján az IT-biztonsági szakterület és az IT-biztonsági team³¹³ elkészíti a szükséges szabályozásokat és folyamatokat, amelyek minden üzleti egységre, munkatársra és a menedzsment tagjaira nézve kötelező érvényűek.

Az IT-biztonságpolitika betartásával és betartatásával valósítható meg a piaci pozíció megtartása, amely biztos alapot jelent a további fejlesztések megvalósításában, valamint a munkahelyek megtartásában.

IT-biztonságpolitika célja

A vállalat információs értékeibe vetett bizalom megteremtése és megtartása, amelyeknek előfeltétele az információvédelmi szabályok elkészítése és megvalósítása, a vállalat „biztonsági kultúrájának”³¹⁴ figyelembevételével.

Ehhez olyan intézkedések szükségesek, melyek

- > növelik az információs technológia új kockázatainak³¹⁵ tudatosítását,
- > támogatják az információs értékek védelmének megértését,
- > az üzleti folyamatokba beépítik az IT biztonsági alapelveket.

³¹¹ Külső cégek dolgozói, karbantartók ...

³¹² gyakorlatba ültet, megvalósít

³¹³ Részleg, csapat

³¹⁴ Vállalat biztonsági stratégiája, p.3.

³¹⁵ Kiberháború, hackertámadás, ...

Alapkövetelmények

A modern információs technológia potenciáljának hasznosítása fontos feladat a vállalat versenyképességének és az elért biztonsági szintjének megtartásában. Ebből adódik az a szükségszerűség, hogy az IT-infrastruktúra és rendszerek tervezésénél, fejlesztésénél és beszerzésénél biztosítani kell az információk bizalmasságának, integritásának és rendelkezésre állásának védelmét. Ezen felül biztosítják az IT-n belüli feladatok, működés és folyamatok visszakövethetőségét.

A következő irányelvek szerint kell eljárni:

- > Bizalmasság,³¹⁶
- > Integritás,³¹⁷
- > Rendelkezésre állás,³¹⁸
- > Követhetőség / igazolhatóság.³¹⁹

Vállalati érdekek

A vállalat sikeres működőképességét és biztonságát tartósan veszélyeztetheti az információk, adatok és ismeretek ellenőrzés nélküli áramlása és manipulációja. A vállalat tulajdonát képezik az információk és adatok, valamint az információ feldolgozásához és kommunikációhoz átadott eszközök és berendezések. Ezért minden munkatárs személyesen köteles az információkat és a rendelkezésre bocsátott kommunikációs eszközöket elvesztés, meghamisítás, illetve bármilyen jellegű sérülés és visszaélés ellen védeni, a felhasznált munkaeszközöket gondossággal kezelni.

Felelőségek

Az IT-biztonságot meghatározza a menedzsment tagjainak, vezetőknél, munkatársaknak, valamint az informatikai rendszerek üzemeltetőinek és fejlesztőinek biztonság- és felelősségtudatos magatartása.

³¹⁶ olyan információkat, melyek nem a nyilvánosságnak szólnak, csak az arra jogosultak számára szabad elérhetővé tenni.

³¹⁷ biztosítani kell az információk hibátlan feldolgozását, valamint azok védelmét jogosulatlan módosításokkal szemben.

³¹⁸ az információkat egy megállapodás szerinti időtartamon belül rendelkezésre kell bocsátani

³¹⁹ a védelemre érdemes információkhoz való hozzáférés és a tranzakciók végrehajtása egyértelmű legyen

A menedzsment tagjai és a vezetők a saját illetékességi területükön felelősek azért, hogy az információk és információs rendszerek kezelése során mindig biztosítva legyen a megkövetelt IT-biztonsági szint.

Mindenki - aki információt kezel - köteles az információval és információs rendszerekkel gondosan bánni, valamint azokat kizárólag a munkaköri leírások és az azokban meghatározott feladatok értelmében és az érvényes szabályozások keretében használni.

IT-biztonság végrehajtási rendszere

Az IT-biztonság szakterület feladata az IT-biztonságpolitika megvalósítása, valamint az ezzel összefüggő IT-biztonsági szabványok, műszaki- és eljárási utasítások fejlesztése, folyamatok kidolgozása és azok terjesztése.

Integrált IT-biztonsági team

A szervezet egy mátrix-szervezet³²⁰, amely fellelős a biztonsági programok bevezetéséért az üzleti egységek igényeinek megfelelően, valamint a globális IT-biztonsági szolgáltatások biztosításáért a vállalat védelme érdekében.

Meghatározza a megfelelő intézkedéseket és az IT biztonsági szabályokat az IT-biztonságra vonatkozóan, ezeket folyamatosan illeszti az új követelményekhez és ellenőrzi betartásukat.

Feladatai:

- > Az IT-biztonság céljainak definiálása,
- > Az IT-biztonsági szabályok kidolgozása és folyamatos felülvizsgálata,
- > Folyamatok kidolgozása, melyek folyamatosan gondoskodnak az IT-biztonsági szabályok naprakészen tartásáról,
- > Az IT-biztonsághoz kapcsolódó projektek kezdeményezése és a végrehajtás ellenőrzése.

Az IT biztonsági team összetételét³²¹ és jelentési útját külön ügyrendben köteles szabályozni.

³²⁰ A mátrix-szervezés a szakmai és a tárgyi funkciókra bontja szét a vezetési és irányítási feladatokat. Ebben az esetben általában projektalapú, illetve új kihívások megjelenése esetén, válaszokat ad a probléma felszámolására.

3.3. ÁLTALÁNOS BIZTONSÁGI KÖVETELMÉNYRENDSZER KIALAKÍTÁSA

3.3.1. Biztonsági szervezetek

Egy nagyvállalat biztonsági rendszerét a „**hatalom-megosztás**” elvén kell kiépíteni és működtetni. Így szétválasztódik az üzleti egységek biztonsági felelőssége, a *szakterületek*³²², a *Létesítményi tűzoltóság és a vagyonvédelem (továbbiakban: Biztonsági menedzsment)*³²³ biztonsági felelősségétől.

A biztonsági intézkedések kidolgozása egy célorientált és integrált tervezést jelent, amely illeszkedik a vállalat biztonsági filozófiájába. A vállalati érdekek megfelelően kell a minimum előírásokat kidolgozni és terjeszteni. Ezek tartalmazzák a törvényi- és a vállalatra vonatkozó egyéb követelményeket, ezen belül az *integrált biztonsági koncepcióhoz* tartozó külön rendelkezések megvalósításának³²⁴ módját.

A biztonsági szervezetek célja

A szervezeti alapelvek szolgálják a vállalat biztonsági politikájában foglalt kijelentések megvalósítását, amely épít:

- > Az üzleti egységek biztonsági felelősségére,
- > A szakterületekre,
- > A beavatkozó erőkre.³²⁵

A biztonsági szervezetek elemei

- > Az üzleti egység vezetők kötelessége a minimum szabályokban foglaltak betartása és betartatása,
- > A szakterületek gondoskodnak az egész vállalat, illetve az egyes üzleti egységek részére:
 - a biztonsági intézkedések megvalósításáról,
 - a vállalaton belüli szaktechnikai ismeretekről,

³²¹ Biztonság- és védelempolitika, IT-biztonsági szervezet, Jogi osztály, Revízió ...

³²² Stratégiai szint

³²³ Operatív (napi) szint

³²⁴ GUNDEL, STEPHAN, MÜLLI, LARS: *Unternehmenssicherheit*, München, Oldenbourg, 2009, ISBN 978-3-486-58712-8, pp. 144-148

³²⁵ Létesítményi tűzoltóság, Beavatkozó csoport, javító és karbantartó szakemberek...

- a menedzsment tagjainak, a vezetőknek és a munkatársaknak biztonsági szemléletének támogatásáról és a minimum előírások betartásának ellenőrzéséről.

Stratégiai biztonsági szint

Corporate Security³²⁶ (továbbiakban Biztonság- és védelempolitika)

Az a szakterület, amely biztosítja a vállalatnál a szervezeti, technikai, építészeti, biztonsági és védelmi intézkedések szükséges integrációját tanácsadással, információval és koordinációval.

Feladatai:

- > A lehetséges kockázati tényezők helyzetének folyamatos értékelése
- > Tanácsadás és támogatás a szakterületek és az üzleti egységek részére
- > Szűrőpróbaszerű felülvizsgálata a szervezeti, technikai és építészeti biztonsági intézkedések működőképességének ellenőrzése.

Szakterületek

- > Biztonság- és védelempolitika
- > Egészségügyi szolgálat
- > Munkavédelem
- > Környezetvédelem
- > IT-biztonság

Operatív szint (Biztonsági menedzsment)

A védelem magába foglalja a vállalat és külső területeinek általános védelméhez szükséges építészeti, technikai és szervezeti intézkedéseket, valamint a különálló területeken lévő különleges biztonsági követelményeket igénylő létesítmények (üzembiztonsági vagy különösen értékes berendezések) minden károsodás elleni védelmét.

³²⁶ Corporate Security = Unternehmenssicherheit (német érdekeltségű vállalatoknál)

Beavatkozó erők:

- > SitCen (Situation Centre, Helyzetelemző Központ),³²⁷
- > Vagyonvédelem,
- > Létesítményi tűzoltóság,
- > Katasztrófavédelem, I
- > parbiztonság és a polgári védelem.

Fő feladatok:

- > Az Integrált Biztonsági Konceptió³²⁸ kidolgozása és működtetésének ellenőrzése különböző szinteken (telephely, üzleti egység ...),
 - Objektumvédelmi feladatok,
 - Beavatkozó erők készenlétben tartása, alkalmazása és irányítása,
 - Nyomozások és kiértékelések folytatása,
 - Gyakorlatok és ellenőrzések végrehajtása,
 - A munkatársak és vezetők biztonságtudatának kialakítása.

A kialakítandó minimum előírások:

A biztonság- és védelempolitika vezető funkciójából adódóan integrálja a minimum előírásokban foglaltakat, amelyek a korábban már kiemelt :

- > Információvédelem (Adatvédelem és adatbiztonság, titoktartás, fotózási szabályok, know-how³²⁹ védelem),
- > Tűzvédelem,
- > Objektumvédelem.

3.3.2. Általános biztonsági intézkedések

A vállalat sikeres működésének és a munkahelyek megtartásának előfeltétele a vállalat védelme, amelyet a természeti és mesterséges katasztrófák, szabotázsok, vagyon elleni bűncselekmények és kibertámadások veszélyeztetnek. A biztonság fenntartása a

³²⁷ Pataki János: Helyzetelemző Központ, Zrínyi Miklós Nemzetvédelmi Egyetem, LKBM-7242, Budapest, 2008.04.07., tanulmány, a szerző tulajdonában

³²⁸ Biztonsági tervezőcsoport feladata

³²⁹ vagyoni értékű gazdasági, műszaki, szervezési ismeret, folyamat, tapasztalat

munkatársak és a vezetés közös felelőssége, beleértve a biztonsági szabályok kidolgozását és betartását, valamint a biztonságtudat kialakítását a munkatársaknál.

A védelmi előírások biztosítják a vállalat veszélyeztetésének csökkentését és ezek egységes végrehajtását az üzleti egységek szintjén.

Információbiztonsági intézkedések

azon információk és adatok védelmét jelentik, amelyek a különböző fenyegetések hatására veszélyeztethetik a vállalat biztonságos üzletmenetét. Ezen körbe tartoznak például a tudás, a dokumentumok, adatok és fényképek, melyek részét képezik a vállalati és üzleti titkoknak.

Az információbiztonság *célja*, hogy megakadályozza a vállalatra vonatkozó információk felderítését³³⁰ és a gondatlan információ kezelést³³¹, a személyes adatokkal való visszaéléseket³³², a vállalat működéséhez szükséges adatok és tervek fizikai megsemmisülését³³³.

Alapelvek

Az információbiztonság célja, hogy megvédje a vállalat minősített információit a jogosulatlan hozzáféréstől. A bevezetett intézkedésekkel védeni kell az információkat:

- > az erőszakos behatolással szemben,³³⁴
- > a jogosultsággal rendelkező személyek ellen, akik nem tartják be az adatvédelmi és adatbiztonsági, a dokumentum kezelési, kommunikációs biztonsági, technikai és számítástechnikai biztonsági szabályokat.

Ezért fontos az „akire tartozik” elv alkalmazása, amely egy szigorított hozzáférést követel meg a minősített információkkal kapcsolatban.

³³⁰ üzleti hírszerzés

³³¹ titoktartás

³³² adatvédelem

³³³ adatbiztonság

³³⁴ fizikai biztonság

Biztonsági zónák fogalma

A biztonsági zónák kialakításának célja létrehozni egy olyan ellenőrzési módszert, amely megakadályozza a vállalat minősített információihoz való hozzáférést. Ez megvalósítható a szigorúbb minősítésű információk esetén személyi használatú biztonsági tárolókkal³³⁵.

Biztonsági zónák kialakítása

A fizikai biztonság alapját képezi a zónák megfelelő kialakítása, melyek az integrált biztonsági koncepció alkalmazásával létesíthető azért, hogy a vállalat BIZALMAS és/vagy TITKOS információit *csak* biztonsági zónákban lehessen tárolni és/vagy kezelni. A zónák kiépítésénél a következő elveknek kell megfelelni:

„Zárt területek”³³⁶

A „Zárt területek” biztonságilag kevésbé szigorú területek, mint az I-es vagy II-es besorolású biztonsági zónák. Az ilyen zónáknál szükséges egy egyértelműen definiált „fizikai”³³⁷ zónahatár, ahol lehetséges a személyek és a járművek ellenőrzése. Az itt kezelt és tárolt információk besorolási szintje „Belső használatra”.

Ilyen zónák kialakításánál nem kötelező minden biztonsági elem alkalmazása, de jelentősen javíthatja az üzleti egységek védelmi helyzetét és egyéb előnyöket is hordoz (pl. csökkenti az ellenintézkedések foganatosításának a követelményeit).³³⁸

Biztonsági zóna I: olyan terület, ahol a vállalat BIZALMAS vagy szigorúbb minősítésű, illetve bármely kategóriájú információit kezelik, tárolják oly módon, hogy akik beléphetnek a területre hozzáférhetnek minősített információkhoz (pl. ügyeleti központok és dokumentumtárolók). Az ilyen terület megköveteli:

- > Egyértelműen kijelölt és védett határt, amelyen keresztül minden be- és kilépés ellenőrizhető,
- > Beléptetési rendszert, amely csak a megfelelő engedéllyel és különleges felhatalmazással rendelkező személyek belépését teszi lehetővé.

³³⁵ Lemezszekrények, biztonsági szekrények, bútorszéf, pánccsaszekrény.

<http://www.mabisz.hu/hu/component/content/article/19-biztonsagtechnika/353-biztonsagtechnikai-fogalomtar.html> (Letöltve: 2014.10.01.)

³³⁶ Gesperren Area vagy Adminisztratív zóna

³³⁷ Fal, ajtó, kapu...

³³⁸ Beléptető rendszer csak meghatározott időben aktív, de nem lehet bevinni fotózásra/filmezésre alkalmas telefonokat, tabletteket....

Biztonsági zóna 2: olyan terület, ahol BIZALMAS és/vagy TITKOS minősítésű információkat kezelnek és tárolnak. A zónában kötelező kiegészítő biztonsági intézkedéseket alkalmazni:

- > Egyértelműen kijelölt és védett határt, amelyen keresztül minden be- és kilépés ellenőrizhető,
- > Szigorúan ellenőrzött beléptetési rendszert, amely – a szervezetszerűleg ott dolgozókon kívül – kíséret nélkül csak a különleges felhatalmazással rendelkező személyek belépését teszi lehetővé a zónába. Más személyek *csak* kísérettel léphetnek be az érintett területre, megakadályozva ezzel a vállalat minősített információihoz való illetéktelen hozzáférést.

Üzleti hírszerzés és elhárítás

Szun ce³³⁹ szerint „az előre tudást nem lehet a kísértetektől és szellemektől megszerezni, ... [] ... Belső kémek – alkalmazd azoknak az embereit, akik a kormányzatban pozícióval rendelkeznek. ... [] ... Fel kell kutatnunk az ellenség ügynökeit, akik nálunk kémkednek. Csábítsuk őket kedvezményekkel, lássuk el utasításokkal és tartsuk meg őket.”³⁴⁰

„A hírszerzés egy előre megtervezett program alapján összegyűjti és elemzi a versenytársak tevékenységét és az általános üzleti trendet, így támogatva a saját vállalat céljait.”³⁴¹

A nemzetközi nagyvállalatok biztonsági politikájában egyre nagyobb szerepet tölt be az üzleti hírszerzés, mert a globális gazdasági kihívások egyik fontos eleme az információ és az ehhez kapcsolódó információs feladatok. Így ez biztonsági problémaként jelentkezik, amelyre a nemzetközi nagyvállalatoknak megfelelő válaszokat kell adni az ezzel kapcsolatban felmerült kérdésekre.³⁴²

³³⁹ i.e. V. században élt, „A háború művészete” a hadtudományos irodalmának egyik legrégebbi és legismertebb műve. A könyv 13 fejezetében a szerző foglalkozik a hadviselés kérdéseivel, mint a diplomácia, a hadviselés és gazdasági feltételei, taktikai és hadműveleti problémák, ... [] ... terepviszonyok, valamint a hírszerzés ... []

³⁴⁰ SZUN CE: *A hadviselés tudománya*, Göncöl Kiadó, Budapest, 2012, ISBN: 9789639183742, p. 122 - 124

³⁴¹ Larry KAHANER: *Competitive Intelligence: How to Gather, Analyze, and Use Information to Move Your Business to the Top*, TOUCHSTONE ROCKEFELLER CENTER, New York, 1997, ISBN-13: 978-0-684-81074-4, p. 16

³⁴² Unternehmensschutz, Richard Boorberg Verlag, 2006, Stuttgart, 55-82. oldal

A vállalaton belüli folyamatok biztonságát alapvetően befolyásolják, hogy az adott vállalat ellen tud-e állni kívülről érkező támadásoknak³⁴³, illetve folyamatosan tudja-e üzemeltetni azokat a folyamatokat, amelyek belső biztonságát fokozzák.

Az üzleti hírszerzés egyik legfontosabb feladata a döntés-előkészítés és támogatás, valamint a vállalat gazdasági biztonságának garantálása.

HUMINT³⁴⁴: A titkos és bizalmas információk megszerzése érdekében a hírszerző szervezetek humán forrásokkal (személyekkel) létesítenek kapcsolatot. A humán források köre az „alkalmi adatszolgáltatóktól” a szervezetszerű (ügynöki) együttműködésig terjedhet. A titkos kapcsolati kört olyan személyek alkotják, akik az információk megszerzéséhez már meglévő vagy könnyen kialakítható lehetőségekkel rendelkeznek.

TECHINT³⁴⁵: A technikai hírszerzés egyik nemének átfogó megnevezése, amely a konvencionális titkosszolgálati eszközök (pl. lehallgatás) alkalmazásától az új elektronikus eszközökkel³⁴⁶ folytatott felderítésig, valamint tudományos módszerekkel kidolgozott eljárásokig³⁴⁷ terjed. A technikai információszerzés a távközlési csatornák és adatátviteli hálózatok³⁴⁸ lehallgatása, továbbá a rejtjelező és irodatechnikai berendezések műszaki eszközökkel és módszerekkel való támadásával megvalósuló információszerzést foglalja magában.

Lehallgatás

Azokban az irodákban vagy területeken, ahol szigorúan minősített információkról gyakran tárgyalnak, az aktív és passzív lehallgatások (audio és video) ellen védekezni kell, ha a kockázat megköveteli. A passzív lehallgatás elleni védelem - nem biztonságos kommunikációs csatornán történő kiszivárgás, direkt lehallgatás vagy direkt megfigyelés - magában foglalhatja a szaktanács kérését és az adott terület hangszigetelését. Az aktív

³⁴³ Üzleti hírszerzés, cyber-támadások, ...

³⁴⁴ Human Intelligence, humán forrásokkal (személyekkel) folytatott hírszerzés

³⁴⁵ Technical Intelligence, Technikai hírszerzés

³⁴⁶ Például: drónok (pilóta nélküli repülőgépek)

³⁴⁷ speciális elemző-értékelő szoftverek (programok)

³⁴⁸ Echelon: az egész világot behálózó lehallgató rendszer, National Security Agency (NSA)

lehallgatás elleni védelem - kiszivároztatás beépített eszközökön keresztül - megköveteli a terület, a berendezési tárgyak és az eszközök technikai és fizikai átvizsgálását.

OSINT³⁴⁹: a hírszerző szervezetek fontosnak tartják a nyílt információs forrásokat. Ezek lehetnek sajtókiadványok, tömegkommunikáció műsorai, nyílt adatbázisok, információs rendszerek és az Internet. Napjainkban az információk 70-80%-a megtalálható a világhálón³⁵⁰. A hírszerző szervezetek az így elérhető nagytömegű adathalmazból elemzik és értékelik a feladataik ellátásához szükséges információkat.

Általános információk az üzleti hírszerzésről

Az általános információvédelmi szabályok betartása mellett, különleges információvédelmi szabályok bevezetése szükséges az elhárítási feladatok sikeres végrehajtásához. A fejlesztési üzleti egységek és részlegek információvédelme alatt olyan szervezeti, technikai és műszaki intézkedéseket értünk, amelyek célja, hogy megakadályozzák az információ hitelességének, bizalmas vagy titkos jellegének, integritásának és rendelkezésre állásának veszélyeztetését, vagy megghiúsítását, megghiúsulását. Az információvédelem fenti elemeiből levezethetők azok a jellegzetes védelmi követelmények, amelyek teljesítését együttesen adatbiztonságnak nevezzük.

A veszélyeztetett dokumentumok:

- > Technológia,
- > Transzfer,
- > know-how,
- > nem műszaki know-how (szervezési, kereskedelmi, pénzügyi, üzemeltetési),
- > engineering,³⁵¹
- > találmányok és szabadalmak,
- > licencia adás.

³⁴⁹ Open Source Intelligence, nyílt információs források: Egy erre a célra kialakított és speciálisan felkészített szakember állománnyal feltöltött szervezet, amely a megfelelő technikai eszközökkel ellátva, a szükséges munkamódszereket alkalmazva, a rendelkezésre álló nyílt forrásokból első sorban olyan adatforrásokat kutat fel, amelyek (és az amelyeken található információk) minden tekintetben megfelelnek a hírszerző munka követelményeinek.

³⁵⁰ Facebook, Twitter, MySpace, Ning, Instagram, Pinterest, MyVIP...

³⁵¹ „mérnökség”, műszaki fejlesztés

Ha illetéktelenek használják fel az információkat, akkor a következők profitálhatnak a felhasználásukkal:

- > versenytársak,
- > szerződő partnerek,
- > egykori munkatársak,
- > rendszerházak.³⁵²

A versenytársak számára fontos adatok lehetnek:

- > know-how,
- > fejlesztési irányok,
- > ügyfelek/partnerek üzleti adatai,
- > fejlesztési/tervezési adatok,
- > üzleti adatok,
- > statisztikai adatok,
- > alkalmazott szoftverek,
- > vállalati/üzemi előírások, üzleti folyamatok, egyéb utasítások.

Az információvédelmi szabályok kialakításánál figyelembe kell venni, hogy a versenytársak bővebb információkkal rendelkeznek a vállalatról, mint gondolná a vállalat. A konkurencia folyamatosan figyelemmel kíséri az üzleti adatokat és a fejlesztési terveket, a nyilvános üzleti jelentéseket és az egyéb sajtóinformációkat.

Az üzleti hírszerzés szerepe:

- > elősegíti az állandó tudomásszerzést arról, hogy a versenytárs milyen eredményeket ért el, milyen elképzelései vannak a jövőre vonatkozóan,
- > a versenytárs adatainak és üzleti folyamatainak megszerzésével kompenzálni a hátrányt,
- > költségeket és időt lehet megtakarítani,
- > kiegészíteni a saját fejlesztéshez, tervekhez, üzleti tervekhez szükséges információkat,

³⁵² Jogi, pénzügyi és egyéb tanácsadással és egyéb tranzakciókkal foglalkozó vállalat

- > figyelemmel kísérni a piac helyzetét, felkészülni a változásokra.

Az üzleti hírszerzés hagyományos módszerei

Szabályosnak tekinthető módszerek:

- > A versenytárs által kiadott üzleti jelentések, sajtóközlemények és beszámolók értékelése,
- > A versenytárs volt alkalmazottainak a nyilvánosságra hozott információi elemzése,
- > Piackutatási és műszaki tanácsadók jelentéseinek tanulmányozása,
- > A versenytársak kiadványainak megismerése,
- > A versenytársak termékeinek vizsgálata,
- > Importőrök, képviselők és vevőszolgálatok nyilvános jelentéseinek nyomon követése.

Szabálytalan módszerek³⁵³

- > Versenytársak és munkatársainak fedett figyelése,
- > Színlelt tárgyalás a versenytárssal egy szabadalom licencének megvásárlására,
- > A versenytársak alkalmazásában álló szakemberek foglalkoztatására irányuló szándék,
- > A versenytársak szakembereinek kongresszusokon célirányos kikérdezése,
- > A versenytársak munkatársainak színlelt állásajánlatok, amelyek csak az információszerzést szolgálják,
- > „Hívatásos”³⁵⁴ üzleti hírszerzők/cégek bevonása egy adott információ megszerzéséhez,
- > A versenytárs munkatársainak elcsábítása az információk megszerzése miatt,
- > A versenytárs munkatársainak megvesztegetése,
- > „Fedett ügynökök” beépítése a versenytárshoz,
- > A versenytárs üzleti tárgyalásainak illegális lehallgatása,
- > Tervrajzok, prototípusok, dokumentumok stb. illegális megszerzése,

³⁵³ „sötét hírszerzés”:

³⁵⁴ Állami és privát.....

- > A versenytárs vállalat vagy munkatárs zsarolása és egyéb más módon való kényszerítése a szükséges információk átadására.

Defenzív (elhárítás) üzleti hírszerzés³⁵⁵

A személyekkel kapcsolatos tényezők:

- > Kulcspozíciók betöltésénél a Biztonság- és védelempolitika véleményét kikérni,
- > A pályázati anyagokat megvizsgálni,
- > Referenciákat kérni,
- > A pályázat okait megvizsgálni (túlképzettség),
- > A munkaszerződésekben rögzíteni kell a munkatárs biztonsági feladatait,
- > Jó munkahelyi légkör kialakítása,
- > Mindenkinek meg kell őrizni saját adatait, a jelszavait és a személyi kódjait,
- > „a papírkosár is beszélhet”,³⁵⁶
- > Munkatársakat fogékonnyá tenni a biztonsági kérdésekkel kapcsolatban.

Adminisztratív rendszabályok:

- > Biztonsági zónák kialakítása,
- > Idegenek belépésének minimalizálása a kiemelt biztonsági területekre,
- > Minden területre kiterjedő szigorú és folyamatos ellenőrzések végrehajtása,
- > Jogosultságok ésszerű kiadása,
- > Átmeneti lehallgatás-elhárítási intézkedések alkalmazása tárgyalások, konferenciák, stb. esetére (pl.: mobiltelefonokat a tárgyalásra TILOS bevinni).

Technikai intézkedések:

- > Biztonsági rendszerek telepítése,
- > Szigorított belépési eljárások alkalmazása,
- > Megfelelő technika eszközök alkalmazása a lehallgatások felderítésére.

Olyan személlyel, aki az üzleti hírszerzés érdeklődésének középpontjába kerülhet, ismertetni kell speciális helyzetét, pl.:

³⁵⁵ Unternehmensschutz, Richard Boorberg Verlag, 2006, Stuttgart, 108-182. oldal

³⁵⁶ A „szemétnek” gondolt dolgok egy hírszerző szakembernek fontos információkat tartalmazhatnak például: szokásainkról, mit eszünk, mit iszunk, számlák, ...

- > Mi az üzleti hírszerzés feladata és eszközei,
- > A biztonsági rendszabályokat az érintettekkel szóban kell tájékoztatni,
- > Ismertetni kell az információ-kiszivárgás nyomán a vállalatra és az elkövetőre, háruló esetleges súlyos következményeket.

Titoktartás hatálya / Know-how védelem³⁵⁷

A titoktartás³⁵⁸ vonatkozik az egész vállalat üzleti folyamataira és a kísérleti fázisban lévő termékekre, aktuális információkra, különös tekintettel az üzemi és üzleti titokra, amelyeket a vállalat vagy harmadik személy érdekében bizalmasan vagy titkosan kell kezelni. A titoktartási kötelezettség kiterjed a vállalat munkatársaira és a vállalati titokkal kapcsolatba került harmadik személyekre, amely a munkaszerződésben és/vagy harmadik szervezettel kötött szerződésekben is szerepel és meghatározott időre szól.

Minősítés³⁵⁹

Az információk minősítéséhez szükséges vizsgálni, hogy ha egy adott információ jogtalan személy vagy személyekhez kerül, mekkora kár érheti a vállalatot. A valószínűsíthető kár nagysága határozza meg az információ besorolását. Minősítések: nyilvános, belső használatra, bizalmas, titkos.

Titoktartási megállapodások / Titok hordozói

Ha a partner társaság és/vagy alvállalkozói stb. titkos, valamint bizalmas projektről ismereteket szerezhetnek, titoktartási szerződést és/vagy megállapodást kell kötni az érintettekkel.

Az üzleti egységtől ki kell jelölni egy kapcsolattartó személyt, aki informálja és ellenőrzi a szerződő külső céget vagy személyeket.

³⁵⁷ Olyan műszaki, szervezési, gazdasági vagy tudományos ismeret, amely különféle gyártmányok előállítását, ill. szolgáltatások végzését teszi lehetővé. Nemzetközi csere tárgya, s az eljárás átadása anyagi előnyökkel jár.

³⁵⁸ titoktartási megállapodások (gazdasági társaságokkal), titoktartási nyilatkozatok (saját és partner társaságok munkatársai részére)

³⁵⁹ Minősítések: Nyilvános, belső használatra, bizalmas, titkos.

Adatvédelem³⁶⁰ és adatbiztonság³⁶¹

A magyar Információs önrendelkezési jogról és az információszabadságról szóló törvény (a továbbiakban: **Itv.**)³⁶² és a vonatkozó jogi előírások mindenkor hatályos változatában foglalt jogszabályi rendelkezései érvényesek.

Valamennyi munkatárs és üzleti egység köteles az általa készített, rögzített vagy számára átadott, minősített személyes³⁶³ és vállalati adatokat³⁶⁴, üzleti titkokat³⁶⁵ óvni a legszélesebb értelemben vett rosszhiszemű és visszaélészerű felhasználástól.

Ennek során figyelembe kell venni a szükséges intézkedések és az elérni kívánt védelmi és biztonsági cél közötti arányosságot.

Az adatvédelmi felelősök tevékenységük gyakorlása során, az adatvédelem területén külső utasítások nélkül tevékenykednek. A felelős kiemelt feladata a személyes adatok kezelésére és feldolgozására szolgáló programok szabályszerű alkalmazásának felügyelete. Ezért szükséges az időbeni tájékoztatás a személyes adatok automatizált kezelésére és feldolgozására irányuló tervekről.

Adatvédelmi felelős köteles az adatvédelmet szolgáló megfelelő intézkedésekkel a személyes adatok kezeléséről és feldolgozásáról az ezekkel foglalkozó személyeket megismertetni a vonatkozó jogszabályok előírásairól, valamint más adatvédelmi előírásokról és az adatvédelem különleges követelményeiről.

³⁶⁰ Az adatvédelem a személyes és a vállalati adatok, üzleti titkok megóvása a vonatkozó törvényi előírásoknak megfelelően valamint a legszélesebb értelemben vett rosszhiszemű és visszaélészerű felhasználástól

³⁶¹ Az adatbiztonság az adatvédelem biztosítását szolgáló valamennyi műszaki és szervezési intézkedések összessége

³⁶² 2011. Évi CXII. Törvény, az információs önrendelkezési jogról és az információszabadságról http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV (Letöltve: 2014.10.10.)

³⁶³ bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

³⁶⁴ bármely meghatározott (azonosított vagy azonosítható) jogi vagy jogi személyiséggel rendelkező gazdasági társasággal (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés.

³⁶⁵ minden olyan fontos tény, információ, adat és megoldás, amelynek titokban maradásához a cégnek és partnereinek méltányolható érdeke fűződik, és amelyet üzleti titokká minősített, illetve amelynek titokban tartása érdekében a szükséges intézkedéseket megtette.

Film és fényképezési előírások

A vállalat és a hozzátartozó külső létesítmények területén általános filmezési és fényképezési tilalom legyen érvényben. A vállalat munkatársai és más cégek munkatársai, akik rendelkeznek képrögzítő eszközökkel³⁶⁶ a vállalat területére bevihetik, de kép/filmfelvételeket nem készíthetnek. Film és fényképezési engedélyeket csak az érintett üzleti egység vezetője adhat ki.

A működéshez szükséges adatok és dokumentumok védelme

A vállalat biztonságos működéséhez és zavartalan üzletmenethez szükséges adatok és dokumentumok védelme gazdasági/pénzügyi okokból csak a vállalat zavartalan üzemeléséhez szükséges információkra kell, hogy korlátozódjon.

Csak olyan biztonsági intézkedéseket kell kidolgozni, amelyek alkalmazkodnak az adott üzleti egység igényeihez, hogy megfelelően biztosítsák az adatok és dokumentumok megőrzését és tárolását.³⁶⁷ Ezen adatokat és dokumentumokat az érintett üzleti egység vezetője határozza meg.

Személyvédelem

A személyvédelem kifejezést általában az angol nyelvterületről származó "Bodyguard" szóval azonosítják. Ez egy olyan terület, amelyet jellemez a különböző elemek és technikai megoldások komplex módon történő alkalmazása. A hangsúly a folyamatos védelmi képességen van. Ezzel el lehet kerülni a nyomásgyakorlást és az esetleges támadásokat.

A személyvédelem olyan tevékenység, amely garantálja a védett személy zavartalan életvitelét, a direkt és indirekt támadások elhárítását és támadás esetén gyors biztonságba helyezését. A személyvédelmi intézkedések magába foglalják a megelőző rendszabályokat, a feladatnak megfelelő taktikai elemeknek és technikai eszközöknek alkalmazását, valamint az együttműködés a bevont erőkkel és hatóságokkal.

³⁶⁶ ideértve például, a mobiltelefonokat és más képfelvételi képességgel rendelkező eszközök

³⁶⁷ például: a másolatok külső tárolása, mikrofilm felvételek készítése, tűz-, víz- és katasztrófa biztos tárolók alkalmazása

A biztosítási terület fontosabb feladatai:

- > Biztonsági helyzet elemzése,
- > Megelőző-védelmi feladatok,
- > Szállás-/munkahelybiztosítás,
- > Utazásbiztosítás,
- > Helyszínbiztosítási feladatok,
- > Logisztikai feladatok,
- > Vezetés és irányítás rendje.

A legfontosabb feladatkörök

Biztosítás parancsnoka: felelős a biztosítás megszervezéséért és személyi állomány feladat végrehajtásáért. A biztosítási feladat végrehajtását és a beosztott személyi állományt, az adott országban érvényes törvények és előírások alapján irányítja. *Személy-/helyszínbiztosító:* a védett személy közvetlen környezetében tartózkodik. Köteles megakadályozni a támadás sikeres végrehajtását, valamint a védett személy menekítését.

Biztonsági gépjárművezető: felkészültek a vészhelyzetek megoldására és képesek az esetleges menekítés gyors végrehajtására. A biztonsági gépjárművezetők részt vesznek speciális gépjárművezetői tréningeken pl.: vezetés extrém időjárási körülmények között, anti-terrorista gépjárművezető kiképzés, taktikai képzés, protokoll ismeretek.

Rendezvénybiztosítás³⁶⁸

A rendezvénybiztosítás alapját a forgatókönyv és egyéb más információk szolgáltatják. A biztonsági koncepció arra épül, hogy nagy tömeg egyidejű jelenlétének idejére meg kell szervezni a rendezvénybiztosítás feladatait, a közönség odaérkezésétől a távozásig. A tervezésnél figyelembe kell venni, hogy minden előre számítható rendkívüli helyzetet a

³⁶⁸ 23/2011. (III.8.) korm. rendelet, a zenés, táncos rendezvények működésének biztonságosabbá tételéről, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100023.KOR, (Letöltve: 2014.09.25.)

lehető legrövidebb időn belül, megfelelő beavatkozás kövessen a minden oldalú biztonság fenntartása, illetve helyreállítása érdekében.

A tervezés fázisában

A biztosítás tervezésének alapvető mutatói:

- > a prognosztizált látogatói szám,
- > a teljes területen belül az a térrész, ahol a legtöbb látogató várható,
- > az oda és elvezető, illetve a területen meghatározott közlekedés rendje,
- > az egymáshoz kapcsolódó rendezvények helyszínei és főbb paraméterei,
- > a körülzárandó terület nagysága,
- > a veszélyes létesítmények, csomópontok lezárása (tűz, robbantás, balesetveszély).

A tervezés fázisában figyelembe kell venni a különböző kockázatokat:

- > A gépjármű közlekedés ellehetetlenülése,
- > Lehetséges terrorfenyegetés, illetve közveszéllyel való fenyegetés,
- > Alkalmi bűnözők feltűnése,
- > Az azonnali veszélyhelyzeti beavatkozás időbeli elhúzódása, késése,
- > Kedvezőtlen tömeghatások (pl. pánik),
- > Extrém időjárás,
- > Kommunikációs és információs zavarok (téves információk, rémhírek, információhiány),
- > Balesetek, rosszulletek,
- > Esetleges tüzek szokásosnál nagyobb száma,
- > Köztisztasági, higiéniai, közellátás szűk kapacitásai.

A biztosítás rendszerének taktikai elemei és technikai feltételei

A helyszíntől, az adott időszak jellemzőitől, az egyes rendezvények speciális voltától függően többféle taktikai elem bevonására van szükség egy tömegrendezvény lebonyolítása során.

Biztosítás területei:

- > Közlekedésrendészeti, rendvédelmi és bűnügyi biztosítás,
- > Katasztrófavédelmi (tűzvédelmi, polgárvédelmi biztosítás),
- > Műszaki mentési biztosítás,
- > Egészségügyi biztosítás,
- > Logisztikai biztosítás,
- > Terrorfenyegetés és közveszéllyel való fenyegetés elleni védelem.

Tűzvédelem

A tűzvédelem feladata a vállalat munkatársainak és látogatóinak, valamint működésének és javainak védelme a tűz, robbanás, természeti és mesterséges katasztrófák okozta károsodásuktól.

Fő feladatok:

- > Az emberek és a vállalat vagyontárgyainak, értékeinek védelmének biztosítása,
- > A fennmaradó kockázatok csökkentése és folyamatos ellenőrzése, valamint a kockázati fedezet biztosítása a vállalat további működéséhez,
- > Mindenkor érvényes jogszabályok és a nemzetközi normák alapján kell a tűzvédelmi irányelvet kidolgozni,
- > Sérültek és vész helyzetben lévők mentése,
- > A mentőszolgálat tevékenységének támogatása,
- > Technikai segítségnyújtás a károk következményeinek felszámolásában,
- > Kapcsolat a biztosító társaságokkal,
- > A munkatársak és vezetők tűzvédelmi továbbképzése.

Biztosítani kell tűzvédelmi célok megvalósulását az épületek és berendezések átépítése vagy módosítása során már a tervezés fázisában, amelynél a gazdaságossági szempontokat is figyelembe kell venni. Ennek alapján a védelmi koncepciónak tartalmaznia kell az érvényben lévő tűzvédelmi irányelveket.

Minden kockázatot növelő változás - még ha rövid távúak is - lehetséges hatását össze kell hangolni a tűzvédelmi, a kárelhárítási és a mentési műveletekkel.

A vállalat minden munkatársának támogatása szükséges ahhoz, hogy a vonatkozó

tűzvédelmi iránymutatások megvalósuljanak. Az egyik legfontosabb eleme az azonnali jelentésre kötelezett események, mint például a balesetek és tüzesetek, egyéb esetleges technikai káresemények bejelentése.

A megelőző tűzvédelem koordinálja az együttműködést az építészeti, tűzvédelmi szakértői csoportok és hatóságok, valamint a technikai támogatást nyújtó más szakterületek és az érintett üzleti egységek között. A jogszabályokban és a szabványokban foglaltak megvalósulásának biztosítása és garantálása. Mindig meg kell felelni egy kockázat- és költséghatékony célorientált szempontoknak.

Objektumvédelem

Az objektumvédelem magába foglalja a vállalat és külső területeinek általános védelméhez szükséges építészeti, technikai és szervezeti intézkedéseket, valamint a különálló területeken lévő különleges biztonsági követelményeket igénylő létesítmények (üzembiztonsági vagy különösen értékes berendezések) minden károsodással szembeni védelmét.

Az üzletei egységek vezetői felelősek a szükséges biztonsági intézkedések bevezetéséért és kötelesek erről a Biztonsági menedzsmentet informálni.

A belépés-szabályozás része az objektumvédelmi intézkedéseknek, amely magába foglalja a vállalat külső területeinek, épületeinek vagy az egyes területeinek, helységeinek, valamint a különleges biztonsági követelmények szerint kialakított biztonsági zónák beléptetés ellenőrzésre vonatkozó építészeti, technikai, szervezeti és személyi feltételeit és a szükséges intézkedéseket.

Integrált biztonsági tervezés

Az objektumvédelmi intézkedéseket egy biztonsági koncepcióban vagy biztonsági tervben kell meghatározni. A kidolgozásáért és tartalmáért a Biztonsági tervező csoport a felelős. Ezeket az intézkedéseket az érintett üzleti egység vezetője köteles bevezetni és alkalmazni. Az adott üzleti egységre vonatkozó objektumvédelmi intézkedések kidolgozását egy rizikóanalízisnek kell megelőzni és ennek eredménye alapján kell a megfelelő biztonsági intézkedéseket alkalmazni. A Biztonsági tervező csoportot az ide vonatkozó tervek alapján időben kell informálni és be kell vonni a biztonsági tervezés támogatásába.

A tervező csoport és az érintett szakterületek támogatják az üzleti egység vezetőjét beléptetési szabályok tervezésében és bevezetésében.

Külső védelem

A vállalat területét és létesítményeit teljes körű, homogén és folyamatosan működő rendszerrel kell védeni. Külső területeknek egyszerűen őrizhetőnek, beláthatónak kell lennie.³⁶⁹

A beléptetést a bejáratoknál és kapuknál egységes kritériumok alapján kell ellenőrizni, figyelembe véve az adott ország kulturális szokásait. A vagyonvédelmi szolgálat utasításában részletesen kell meghatározni a bejáratoknál és a kapuknál alkalmazandó belépési szabályokat.

A kártya tulajdonosnak kell az automatikus beléptető rendszeren való áthaladáskor a belépési jogosultságukat igazolni. A személyazonosság ellenőrzése szűrőpróba szerűen lehetséges.

A látogatók és külső személyek a belépési ponton megkapják a részükre meghatározott belépési engedélyt személyazonosság ellenőrzése után.

Épületek védelme

Az épületek külső mechanikus védelme garantálja a biztonsági zónák/területek megfelelő, teljes és homogén elkülönítését.

A nyílások (ajtók, kapuk, ablakok), a szűrő- és szellőztető berendezések nyílásait, az installációs aknákat a zónahatároknak megfelelően mechanikus védelemmel kell ellátni. A mechanikus védelmet pontosan kell meghatározni egy biztonsági koncepcióban. A magasabb védelmi fokozatot igénylő területeken betörésjelző rendszer telepíthető, így csökkenthető a keletkező károk nagysága. A részleteket a biztonsági koncepcióban kell megjeleníteni és a veszélyforrásokat beazonosítani.

A mesterkulcsrendszert³⁷⁰ központilag kell tervezni és kezelni. A Beavatkozó erők részére mindenhol és mindenkor biztosítani kell az egyszerű belépés lehetőségét.

Az elektronikus biztonsági rendszereket csak, mint kiegészítő biztonsági intézkedéseket lehet alkalmazni a mechanikus intézkedések mellett és nem szabad önállóan felhasználni.

³⁶⁹ alacsony növényzet, lehetőleg egyszerű vonalvezetés, átmászás lehetőségének megnehezítése

³⁷⁰ A mesterkulcsos zárrendszer egyedi zárból áll, melyek kulcsa a rendszer más egyedi zárait nem működteti. A kulcsok nem másolhatóak. A rendszerhez tartozik egy főkulcs, amely a rendszer valamennyi zárját képes nyitni-zárni. A csoportkulcsok az alájuk rendelt egyedi zárat lehet nyitni-zárni.

Vagyonvédelmi feladatok

Az időben felismert lehetséges veszélyforrást folyamatosan kell védeni. Az ilyen feladatokra egy gyorsan alkalmazható felelős Beavatkozó egység³⁷¹ kerül kijelölésre a vagyonvédelem vezetője által.

Az őrzés támogatásához és hatékonyságához elektronikus védelmi rendszereket lehet telepíteni a szükséges helyeken és ezekkel a SitCen-nel kell közvetlen összeköttetést létesíteni.

A Beavatkozó erők között a folyamatos összeköttetést és a riaszthatóságot fenn kell tartani.

A közlekedési szabályok

A közlekedési szabályozás foglalja magában a gyár területére való belépés- és behajtás ellenőrzésére vonatkozó építészeti, technikai, szervezeti és személyi feltételeket és az ezekre vonatkozó intézkedéseket.

A szabályozás célja az üzem működésével és az érvényes belépési jogosultságokkal összefüggésben a személyek és gépjárművek be- és kiléptetésének ellenőrzése.

Személyek és járművek csak a vagyonvédelem ellenőrzése és nyilvántartása mellett közlekedhetnek. A KRESZ³⁷² szabályai szerinti közlekedés és parkolás a vállalaton belül, illetve a külső parkolókból minden járművezető részére kötelező. A külső cégek tulajdonában és személyi tulajdonban lévő, valamint a gyár területén munkát végző más vállalatok gépjárműveit belépővel kell ellátni, melyet jól látható helyen kell elhelyezni.

A tűzoltó, mentő és rendőrségi gépjárművek belépése esetén csak a be –és kilépési idejét kell nyilvántartani.

A gépjárművezetőket kétnyelvű, a terület legfontosabb biztonsági és munkavédelmi kérdéseit, az üzemszabályokat, objektumok, a gyáron belül lévő parkolók helyét, valamint az orvosi rendelő, tisztálkodási lehetőségek helyét tartalmazó tájékoztatóval kell ellátni.

³⁷¹ Beavatkozó csoport

³⁷² **K**özúti **R**endelkezések **E**gységes **S**zabályozása

Parkolási rend

A vállalat külső és belső parkolóiban a parkolási rendet mindenki köteles betartani. A parkolási rend betartását a vagyonvédelmi szolgálat köteles ellenőrizni. A parkolóban a közlekedés rendjét közúti jelzőtáblák mutatják. Mivel a parkoló nem őrzött, ezért a gyár nem vállal felelősséget az esetlegesen keletkező károkért, lopásokért.

A vállalat biztonságához kapcsolódó feladatok

A vállalattal megkötött szerződés alapján a különböző szolgálatokat ellátó külső cégek a biztonsági szabályok és a Tűzvédelmi terv alapján kötelesek a vállalat objektumainak, vagyonának külső és belső őrzését, tűzvédelmét biztosítani.

A biztonsági szervezeteken kívül a vállalat minden munkatársának kötelessége a kezelésére bízott vállalati tulajdont fokozott gondossággal kezelése és azt minden károsodástól megóvása.

A vállalat minden munkatársa köteles a vállalati tulajdon sérelmére elkövetett cselekményt jelenteni. Ha erre irányuló cselekményről, vagy más erőszakos esetről tudomást szerez, vagy észlel, a SitCen munkatársainak és közvetlen vezetőjének informálása a szükséges intézkedések megtétele érdekében.

Zárt üzemrészek, nemzetközileg ellenőrzött termékek és technológiák védelme

Minden munkatárs csak azon a területen tartózkodhat, ahová beosztásra került. A munkaterületet csak közvetlen vezetője engedélyével hagyhatja el. Az engedély nélkül más munkaterületen tartózkodókkal tisztázni kell a jogosultságot és az ott létük okát.

A kiemelt biztonsági zónákban dolgozó személyeken kívül más személyek, csak az adott üzleti egység vezetőjének külön engedélyével léphetnek be.

A nemzetközileg ellenőrzött termékek és technológiák kezelését és védelmét az Információbiztonsági irányelvben meghatározottak szerint kell az arra feljogosított munkatársaknak végrehajtani.

Ezen termékek és technológiák iránti érdeklődésről azonnal tájékoztatni kell a Biztonság- és védelempolitika szakterületet.

Fokozott biztonsági intézkedések alkalmazása

Jelentősebb események (védett személyek látogatása), rendezvények az állandó biztonsági előírásokon túl a Válságkezelő Tervben rögzített fokozott biztonsági intézkedéseket kell bevezetni.

A fokozott biztonsági intézkedések rendszabályait az esemény jellegének megfelelően a Biztonsági menedzsmenst vezetője állítja össze a megbízott szakterületek bevonásával. Alkalmazásukra a felsővezetés jóváhagyása után kerülhet sor.

Munkafegyelem és magatartás szabályai

A vállalatnál az Üzemi Szabályzat tartalmazza minden munkatársra kötelező érvényű munkafegyelmi és magatartásbeli általános szabályokat, amelyek betartását a munkaszerződés aláírásával magára vállal. A vállalatnál a munkavédelem szervezése, irányítása és végrehajtása a Munkavédelmi politikában és egyéb más szabályzatokban kerültek meghatározásra.

A biztonsági rendszereket úgy kell kiépíteni, hogy - a munkavédelmi és a biztonsági előírásoknak megfelelően - a menekülési útvonalak és vészkijáratok működését ne befolyásolja. A vészkijáratok technikai biztosítását betörés és jogtalan belépés ellen védeni kell.

Megsértések

Aki e szabályokat megsérti, munka / büntetőjogi és adatvédelmi szempontok figyelembevételével kell egyénileg kivizsgálni és megfelelő szankciót alkalmazni, valamint a hatóságokat informálni.

3.3.3. Biztonság- és védelempolitika

A biztonság- és védelempolitika szakterület legfontosabb feladatai a vállalati biztonság alapjainak meghatározása. Kidolgozza az irányelveket, rendelkezéseket és az egyéb más védelmi feladatokat, valamint nyílt eszközökkel adatokat gyűjt a vállalat biztonságát érintő információkról, amelyeket értékel és terjeszt a felsővezetés részére.

A globális szinten működő vállalatoknál fontos cél a válsághelyzetek időbeni felismerése, kezelése, megoldása és felszámolása. Már a tervezés időszakában a „Troubleshooting”³⁷³ szerint kell a legrosszabb alternatívával számolni. Ennek célja a megelőző megközelítés és ezzel megakadályozható vagy mérsékelhető a kár mértéke. A válságok kialakulása befolyásolja a vállalat stratégiai döntéseit és védelmi intézkedéseit. A XXI. században egyre nagyobb jelentőséggel bír a „Security Risk Management” (továbbiakban Biztonsági Rizikó Menedzsment)³⁷⁴. A globalizáció kihívásai miatt a „hagyományos” vállalati kockázat elemző szervezetek már nem képesek kezelni a jelenkor fenyegetéseit, veszélyeit és rizikóit.³⁷⁵ A tervezett beruházások pénzügyi értékeléséhez és a jogi kockázatok meghatározásához szükséges a biztonság- és védelempolitikai tudomány eredményeinek figyelembevétele, amely számol a globális, regionális és helyi politikai stabilitással, lehetséges környezeti kockázatokkal és egyéb más biztonsági kihívásokkal.

A biztonság- és védelempolitika szakterület vezetője a vállalat menedzsmentjének tagja és közvetlenül a vállalat első számú vezetőjének alárendeltségébe tartozik.³⁷⁶

Funkció

Felvetődik az a szervezeti kérdés, hogy a biztonság- és védelempolitika önálló szervezeti egység vagy része legyen-e egy nagyobb üzleti egységnek? Erre egyértelmű választ nem lehet adni. Ez függ az adott vállalat nagyságától, tevékenységi körétől, a vállalati kultúrától és nem utolsósorban a vállalat telephelyének otthont adó ország geopolitikai helyzetétől.

Feladatrendszer:

- > Biztonsági helyzet folyamatos elemzése, értékelése, jelentések összeállítása,
- > Védelmi tervek előkészítése és kidolgozása a szakterületekkel közösen,
- > Terrorelhárítási feladatok előkészítése a hatóságokkal együttműködve,
- > Információvédelmi feladatok koordinálása (titoktartás, know-how védelem, prototípusvédelem, üzleti hírszerzés elhárítása ...),
- > Adatvédelem és adatbiztonság,
- > Event Security,³⁷⁷
- > Személyvédelem koordinálása.

³⁷³ Hibakeresés, hibajavítás, eredeti helyzet visszaállítás folyamata

³⁷⁴ Stratégiai szintű válságkezelés

³⁷⁵ http://www.verismo.ch/sites/default/files/Verismo_Publikationen_04_0.pdf (Letöltve: 2014.10.01.)

³⁷⁶ KOVACICH & HALOBOZEK: *The Manager's Handbook for Corporate Security*, Imprint Butterworth-Heinemann, 2003, ISBN: 9780750674874, pp. 117

³⁷⁷ rendezvénybiztosítás

3.4. BIZTONSÁGI SZERVEZETEK OPERATÍV FELADATAI

3.4.1. Tűzvédelem

A tűzvédelem magába foglalja a vállalat és külső területeinek megfelelő szintű tűzbiztonságát megalapozó tervezési és létesítési folyamatok felügyeletét, az általános használati szabályok érvényre juttatását, a biztonságos üzemeltetést lehetővé tevő – az adott vállalatra vonatkozó – szabályrendszer kidolgozását és gyakorlati megvalósítását, a szükséges folyamat felügyeleti és szankcionálási tevékenységeket. A jogszabályokban és belső irányelvekben, szabályzatokban foglaltak betartatásával és betartásával, az építészeti, technikai és szervezeti intézkedések, valamint a különleges biztonsági követelmények és intézkedések kidolgozásával garantálja a létesítmények minden tüzesettel és az egyéb ebből eredő károkkal szembeni védelmét.

A 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról (továbbiakban: tűzvédelmi törvény): „3. § A hivatásos tűzoltóság, az önkormányzati tűzoltóság, a létesítményi tűzoltóság és a beavatkozó önkéntes tűzoltó egyesület (a továbbiakban együtt: tűzoltóság) a tűz oltása és a műszaki mentés érdekében a személyes szabadságra, a magánlakás sérthetlenségére és a tulajdonra vonatkozó alkotmányos jogokat - az e törvényben meghatározottak szerint - olyan mértékben korlátozhatja, amely arányban áll az élet, a testi épség és anyagi javak védelmével.”

Tűzvédelmi filozófia

A tűzvédelmi intézkedések kidolgozásához szükséges a komplex üzleti környezet ismerete. A különböző üzleti egységek és szakterületek problémamentes és jól összehangolt együttműködése - menedzsment, szervezet, technológia szintjén -, elengedhetetlen előfeltétele a tűzvédelmi koncepció teljes körű megvalósulásának, melyet szükségszerűen ki kell egészíteni egyedi intézkedésekkel.

A gazdálkodó szervezetek elemi érdeke, a tűz megelőzési tevékenység filozófiájának hangsúlyos megjelenítése, elvárásainak kommunikálása minden saját munkavállaló, és a létesítmény területén tevékenykedő fél irányába. Erre jogszabályi megalapozás és kötelezés alapján legalkalmasabb felület a Tűzvédelmi Szabályzat.

Biztosítani kell, hogy minden üzleti egység minden egyes munkatársát tájékoztassák tűzvédelmi feladatairól és részvételüket a kötelező tűzvédelmi oktatásokon.

Cél

A tüzesetek a gazdaság és a közélet minden területén reális veszélyt jelentenek. A tűz az egyes személyek testi épségének veszélyeztetésén túl súlyos károkat okozhat a gazdasági élet és a technológiai folyamatok egymásra épülő részelemeiben. A dominó elv alapján a folyamat térben és időben egymástól jól elkülönített, de nem függetlenül működő részfolyamatainak megakadását, leállítását is előidézhetheti. Ennek gyakorlati megjelenése a szállítás kiesése, határidőtől történő elmaradása, a piacok elvesztése. Kapcsolódó károk lehetnek az image veszteség vagy a hátrányos jogkövetkezmények, amelyek együttesen már a vállalkozások biztonságos működését is veszélyeztethetik.

Megelőző tűzvédelem

A törvényi szabályozás, jogszabályi előírások, hatósági határozatok és a biztosítók ajánlásai alapján kell a tűzvédelmi rendszereket tervezni, kiépíteni és üzemeltetni.

Tevékenysége során:

- > Meghatározza a gazdálkodó szervezet tűzvédelmi filozófiáját, tűzvédelmi céljait
- > Kidolgozza a Tűzvédelmi szabályzatot és a további intézkedéseket, munkautasításokat, melyek segítségével lehetővé válik a tűzvédelmi filozófia és célrendszer érvényre juttatása,
- > Részt vesz a tervezésben, a fejlesztések és beruházások előkészítésében, megvalósításában, hogy a tűzvédelmi szabályok és előírások érvényre jussanak,
- > Tűzvédelmi rendszerek használati szabályainak betartásának ellenőrzése, hiányosságok esetén szükség szerint kezdeményezi a megfelelő intézkedéseket,
- > Folyamatosan vizsgálja és értékeli a vállalat tűzvédelmi helyzetét, javaslatokat fogalmaz meg, illetőleg meghatározott körben intézkedéseket tesz a hiányosságok megszüntetésére vagy folyamatok módosítására.

A megelőző tűzvédelem teremti meg a hatékony beavatkozó tűzvédelem (Létesítményi tűzoltóság) működési feltételeit:

- > A munkavállalók tűzvédelmi felkészítése és továbbképzése,
- > Dohányzási szabályok betartásának ellenőrzése,
- > Alkalomszerű tűzveszélyes tevékenységek ellenőrzése,

- > Éghető anyagok tárolásának és kezelésének ellenőrzése,
- > Használati szabályok betartásának ellenőrzése.

Létesítményi tűzoltóság³⁷⁸ (beavatkozó tűzvédelem)

A tűzvédelmi törvény szerint a Létesítményi tűzoltóság a gazdálkodó szervezet tevékenységével összefüggő tűzoltási és más műszaki mentési feladatok elsődleges ellátására létrehozott és fenntartott szervezet. A Létesítményi tűzoltóság a fenntartó szervezetén belül, annak szervezeti egységeként, gazdasági- vagy kooperációs társaságként, illetve más nonprofit gazdasági társaságként is működhet.

A fenntartó szervezetén belüli Létesítményi tűzoltóság főfoglalkozású, továbbá alkalmasszerűen igénybe vehető létesítményi tűzoltókból is állhat. Készenléti jellegű szolgálatot a fenntartó által meghatározottak szerint lát el.

A vállalatnál SitCen-ből irányítják, támogatják és ellenőrzik az objektumok biztosításában közreműködők tevékenységét, felügyelik a tűzvédelmi rendszereket.

A Létesítményi tűzoltóság elsősorban operatív tűzvédelmi, tűzoltási, műszaki -mentési feladatokat lát el, továbbá részt vesz a stratégiai szintű tűzvédelmi feladatok tervezésében, megvalósításában a vállalat megelőző tűzvédeleméért felelős vezetője koordinálásával.

A Létesítményi tűzoltóságot oly módon kell megalapítani és felszerelni, hogy képes legyen működése során a területén keletkezett bármilyen tűz önálló eloltására az elsőfokú hatóság előírásainak megfelelő erővel és eszközökkel. A személyi állományt, a tűzoltó gépjárműveket, a felszerelést, az egyéni és kollektív védelem eszközeit, a tűzoltáshoz és a tűzmegeelőzéshez szükséges anyagokat, valamint az előírt tartalékokat készenlétben kell tartani és szükség szerint bevetni.

³⁷⁸ 239/2011. (XI. 18.) Kormányrendelet, az önkormányzati és létesítményi tűzoltóságokra, valamint a hivatásos tűzoltóság, önkormányzati tűzoltóság és önkéntes tűzoltó egyesület fenntartásához való hozzájárulásra vonatkozó szabályokról

Létesítményi tűzoltóság feladata

A létesítményi tűzoltóság tűz megelőzési tevékenysége során:

- > Figyelemmel kíséri és segíti a létesítmény területén a tűzvédelmi jogszabályokban, kötelezően alkalmazandó szabványokban és a hatósági előírásokban foglaltak érvényesülését, különös tekintettel a tűzoltás alapvető feltételeit biztosító szabályokra,
- > Jelzi a tűzvédelmi szabálytalanságokat a létesítmény vezetőjének,
- > Közreműködik a munkavállalók tűzvédelmi felkészítésében, a tűzoltó eszközök és felszerelések használatának ismertetésében,
- > Szükség szerint ellátja az alkalmoszerű tűzveszélyes munkák végzésénél a tűzoltói felügyeletet.

A Létesítményi tűzoltóság tűzoltási és műszaki-mentési tevékenysége érdekében:

- > Gondoskodik a készenléti jellegű szolgálat ellátásáról,
- > Gondoskodik a tűzoltás előfeltételeinek biztosításáról,
- > Külön jogszabályban foglaltak szerint tűzoltási és műszaki-mentési feladatokat lát el,
- > Gondoskodik szakfelszereléseinek és egyéni védőeszközeinek karbantartásáról,
- > A rendelkezésre álló eszközökkel, felszerelésekkel elvégzi az elsődleges tűzoltási – mentési feladatokat,
- > Az objektum területén vizsgálja a tűzvédelmi rendszabályok, előírások betartását,
- > Véleményezi, engedélyezi a vállalat területén a tűzveszélyes tevékenységet, szükség szerint gondoskodik a felügyeleti szolgálat biztosításáról, eseti előírások megtételéről, ellenőrzéséről,
- > Folyamatosan figyelemmel kíséri, vizsgálja a tűzvédelmi szabályok és előírások betartását,
- > A rendezvénybiztosítás tűzvédelmi feladatainak végrehajtása, a tűzveszélyes tevékenységnél ügyeleti, illetőleg felügyeleti szolgálat ellátása,
- > Közreműködnek a munkatársak tűzvédelmi oktatásában és továbbképzésében, a rendelkezésre álló tűzoltó-felszerelések használatának elsajátításában,
- > Biztosítják a készenléti felszerelések állandó üzemképességét,

- > Biztosítja a riaszthatóságot, közreműködik a tűzoltás előfeltételeinek biztosításában,
- > Együttműködik a tüzesetek körülményeinek felderítése érdekében végzett tűzvizsgálatban, a tűzoltás ideje alatt biztosítja a tűz keletkezésére utaló körülményeket és jelenségeket, valamint a tűzvizsgálat befejezéséig biztosítja a helyszínt,
- > Kezeli az automatikus tűzjelző-, és tűzoltóberendezésekről érkező jelzéseket, valamint napi ellenőrzésekkel felügyeli a tűzvédelmi rendszerek folyamatos üzemképességét.

Létesítményi tűzoltókkal szembeni elvárások

A vonatkozó jogszabály alapján, a főfoglalkozású Létesítményi tűzoltóság tagjainak a készenléti jellegű szolgálatot ellátó hivatásos katasztrófavédelmi szervek tűzoltósági szakterületének tagjaival megegyező, szakmai tartalmú képesítéssel kell rendelkezniük.

3.4.2. Katasztrófavédelem

A katasztrófák olyan előre nem látható események, amelyek előrejelzése bizonytalan, eseményeik nem kiszámíthatóak. A katasztrófák lehetnek természetes vagy mesterséges eredetűek, veszélyeztetik az emberi életet és kárt okozhatnak a környezetben. A katasztrófák okozta következmények megelőzése és enyhítése a megfelelő biztonsági szabályok kialakításával és alkalmazásával, valamint a kialakított vállalati szervezetek és hatóságok együttműködésével valósítható meg.

„...a különböző katasztrófák elleni védekezésben azon tervezési, szervezési, összehangolási, végrehajtási, irányítási, létesítési, működtetési, tájékoztatási, riasztási, adatközlési és ellenőrzési tevékenységek összessége, amelyek a katasztrófa kialakulásának megelőzését, közvetlen veszélyek elhárítását, az előidéző okok megszüntetését, a károsító hatásuk csökkentését, a lakosság élet- és anyagi javainak védelmét, az alapvető

életfeltételek biztosítását, valamint a mentés végrehajtását, továbbá a helyreállítás feltételeinek megteremtését szolgálják.”³⁷⁹

A munkatársak nem tudják magukat megvédeni minden lehetséges katasztrófától. Szükségük van elsősegélynyújtásra, egészségügyi és egyéb más beavatkozásra/támogatásra, súlyos balesetek, természeti katasztrófák és minden más veszélyeztetés esetén, amelyeket már önmaguk nem tudnak megoldani. Ezért indokolt a vállalati és állami/önkormányzati biztonsági szervezetek szoros együttműködése, hogy szükség esetén egy közös és hadrafogható kárelhárítási rendszer álljon rendelkezésre.

Katasztrófavédelem fő feladatai:

- > Tűz elleni védekezés feladatai,
- > Természeti és mesterséges (civilizációs) katasztrófák elhárítása, kár felszámolása, eredeti helyzet visszaállítása,
- > Extrém időjárás hatásainak csökkentése,
- > együttműködve az iparbiztonsággal és más egyéb fegyveres és rendvédelmi szervvel, valamint hatósággal
- > Felkészülés és felkészítés az üzem tevékenységéből és a terület fekvéséből feltételezett katasztrófavédelemhelyzetekre.
- > vállalati szinten kapcsolódó szakterületekkel (iparbiztonság, környezetvédelem, munkavédelem, megelőző tűzvédelem és Létesítményi tűzoltóság, veszélyes áru menedzsment...) való együttműködés.
- > Katasztrófavédelmi hatósággal (helyi, területi és országos szinten) kapcsolattartás.

A fennmaradó kockázatokat a vállalatnak ki kell egészíteni biztosítások megkötésével, hogy kár esetén finanszírozzák a veszteségeket. Nagyon fontos szabály, hogy erre a problémára nem lehet teljes megoldást találni, mivel a teljes veszteség költsége gyakran jelentősen meghaladja a várható biztosítási összeget. A baleset által okozott termelés kiesés költségei - gyakran nagymértékben meghaladják - a járulékos költségeket (például „image” veszteség, vevői bizalom elvesztése...).

³⁷⁹ 2011. évi. CXXVIII. törvény, a katasztrófavédelemről és a hozzákapcsolódó egyes törvények módosításáról, 3.§ 8.

3.4.3. Iparbiztonság

Az Európai Parlament és Tanács (korábban Európai Gazdasági Közösségek Tanácsa, SEVESO³⁸⁰ I.³⁸¹) a SEVESO irányelv sorozatokban szabályozta a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezelését. A SEVESO II.³⁸² irányelvet módosították és hatályon kívül helyezték a 2012/18/EU irányelvvel a SEVESO III-mal, melyet a tagállamoknak 2015. május 31-ig kellett beépíteni saját jogrendjébe.

A SEVESO irányelv sorozat meghatározza a szereplők felelősségét és kötelességeit:

- > állami kötelezettségek,
- > önkormányzati kötelezettségek,
- > üzemeltetői kötelezettségek.

SEVESO szabályozás hatálya alá tartozás esetén a vállalat köteles:

- > Az üzembiztonsági dokumentációját (küszöbértéktől függően: súlyos káresemény elhárítási terv, biztonsági elemzés vagy jelentés) naprakészen tartani,
- > Belső védelmi terv-et³⁸³ készíteni, azt az illetékes hatósággal jóváhagyatni, naprakészen tartatni, gyakoroltatni és oktatni
- > A kapcsolódó szakterületekkel (Környezetvédelem, Munkavédelem, Megelőző Tűzvédelem és Létesítményi Tűzoltóság, Egészségmenedzsment) együttműködni,
- > Az Iparbiztonsági hatóságokkal (helyi, területi és országos szinten) kapcsolatot tartani, hatósági eljárások lebonyolításában együttműködni,
- > Az Iparbiztonsági (megbízott, felelős) szakterület feladatait és kötelességeit meghatározó jogszabályok ismerete, előírásainak betartása és betartatása.

³⁸⁰ 1976-ban Olaszországban, Seveso-ban egy növényvédőszer került ki a környezetbe. Haláleset nem történt, de több mint 2000 embert kezeltek mérgezéssel.

³⁸¹ 82/501 EGK számú irányelv

³⁸² 96/82. EK irányelv

³⁸³ 219/2011. (X.20.) Kormányrendelet, a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről, 20.§ (1-2)

3.4.4. Vagyonvédelem³⁸⁴

A vagyonvédelem magába foglalja az objektumok és a külső területek általános védelméhez szükséges építészeti, technikai és szervezeti intézkedéseket, valamint a különálló területeken lévő különleges biztonsági követelményeket igénylő létesítmények védelmét.

Cél

A vagyonvédelem célja, hogy gazdaságilag tartható költségekkel, nagyobb időráfordítás nélkül megakadályozhatók legyenek az engedély nélküli behatolások, az illetéktelen információ és termék eltulajdonítások, valamint a szándékos rongálások.

Speciális objektumvédelmi intézkedéseket kell foganatosítani magasabb veszélyeztetettségi fok fennállása esetén, mint például:

- > fontos üzemi, ellátó- és kiszolgálórendszereknél
- > kommunikációs rendszereknél
- > számítógépközpontoknál és irattáraknál
- > termékfejlesztő területeken
- > pénztáraknál
- > értékes nyersanyagok vagy üzemanyagok tárolóhelyénél.

Megelőző vagyonvédelem

A biztonsági koncepciót a Biztonsági tervezői csoport és a megelőző tűzvédelem dolgozza ki az üzleti egység vezetőjétől kapott információk, valamint az építészeti és infrastrukturális adottságok alapján. Átépítések vagy új létesítések esetén a biztonsági tervezés felülvizsgálja, módosítja, illetve kiegészíti a tervezett/meglévő biztonsági intézkedéseket.

A biztonsági koncepciót az üzleti egység vezetőjének kell előterjeszteni. Ő ellenőrzi, hogy megvalósulnak-e az elvárásai és egyetért-e a kidolgozott részletek tekintetében a Biztonsági tervező csoporttal.

A tervezés alapját a vállalati stratégiában kinyilatkoztatott „vállalat biztonsági modell”³⁸⁵ alapján kell megtervezni és kiépíteni.

³⁸⁴ 2005. Évi CXXXIII. Törvény, a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

Beavatkozó vagyonvédelem

Az őrzés-védelem egy folyamatos tevékenység. Fő feladata a vállalat területének és berendezéseinek őrzés-védelme, őr-, porta-, járőr- és beavatkozó szolgálattal. A vállalati rend megsértésekor - beleértve a bűncselekményeket - az eset dokumentálása, a cselekmény megszakítása. Az adatvédelem, környezetvédelem, munkavédelem és tűzvédelem területeit érintő üzemi káresetek esetén alkalmazásra kerülő intézkedések megismerése és alkalmazása, együttműködés az üzemi katasztrófák elhárításában.

Őrszolgálat tevékenysége:

- > személyek és anyagok védelme,
- > a környezetvédelmi veszély-, vagy kárelhárítási intézkedések végrehajtása,
- > károk keletkezésének megakadályozása vagy a megtörtént esemény negatív hatásainak behatárolása,
- > a megfelelő veszélyelhárító szolgálatok riasztása,
- > a vállalat területén tartózkodó személyek ott-tartózkodási jogosultságának megállapítása.

Portaszolgálat

- > személyek be- és kiléptetése, valamint ellenőrzése,
- > gépjárművek be- és kiléptetése, valamint ellenőrzése,
- > szállítmányok, csomagok be- és kiszállításának ellenőrzése,
- > a biztonságtechnikai eszközök³⁸⁶ szabályos használatának felügyelete,
- > talált tárgyak átvétele és megőrzése,
- > a szolgálati okmányok munkautasításoknak megfelelő vezetése.

Járőrszolgálat

A járőr feladata a szolgálati utasítás szerinti folyamatos járőrözések végrehajtása. A járőrözés végrehajtását a szolgálati naplóban kell rögzíteni.

- > A járőr kijelölt járőrútvonalon ellenőrzi a csarnokok, épületek zártságát,
- > betartatja a parkolási rendet a vállalat területén.

³⁸⁵1. számú melléklet: A vállalat biztonsági stratégiája, p. 7.

³⁸⁶ Beléptető rendszer, fémkereső kapuk...

Beavatkozó erő:

A szolgálat megnevezése: Beavatkozó csoport

A szolgálat rendeltetése: Előre nem látható feladatok végrehajtása, ezen belül kiemelt feladatként a vezetés és információvédelmi szempontból fontos objektumok, valamint a vállalat anyagi készleteit tároló raktárak őrzése és a kerítésen áthatoló személyek feltartóztatása.

A szolgálat alárendeltsége: A Beavatkozó csoport közvetlenül a SitCen-nek van alárendelve.

Definíciók

Alkalmazási körlet: Azon terület, ahol az elektronikus jelzőrendszer illegálisan ott - tartózkodó személyeket jelzett.

Figyelőpont: A vállalat területén lévő azon pont, melyet a járőr külön utasításra megfigyelés céljából elfoglal.

Személyazonosság ellenőrzése: Az őrzött területen tartózkodó személyek megállítása, személyazonosságának és a területen való tartózkodás jogosságának ellenőrzése.

Elfogás: A SitCen utasítására – biztonsági rendszer riasztása – a vállalat adott területén jogtalanul tartózkodó vagy személyazonosságát igazolni nem tudó vagy az igazoltatást megtagadó személy elleni intézkedés, a SitCen által meghatározott helyre történő kíséréssel.

Alkalmazás elvei

A vállalatnál a felderítési és őrzési feladatokat a vagyonvédelem szervezetébe tartozó Beavatkozó csoport hajtja végre. A felkészített és állandó készenlétben lévő Beavatkozó csoport adatokat szerez be a riasztás helyéről, feltartóztatja az ott-tartózkodó személyeket, biztosítja a helyszínt, majd ezeket az információkat meghatározott rendben továbbítja a SitCen-nek.

Az Beavatkozó csoport a vagyonvédelem állományába tartozó biztonsági őrökből kerül kijelölésre. A járőrök elhelyezési körletét olyan helyen kell kijelölni, amely biztosítja a járőrözésre beosztott biztonsági őrök gyors gyülekezését, valamint az alkalmazási körlet gyors elérését. A Beavatkozó csoport olyan végrehajtó alegység, amely a vállalat területén

és közvetlen környezetében (parkolók és a kerítések mentén) képes felderítési, illetve különleges feladatok végrehajtására, a megszerzett adatok rövid időn belüli jelentésére.

A Beavatkozó csoport alkalmazását a vállalat SitCen munkatársai szervezik és tervezik. A feladatra történő kijelölést és felkészítést, valamint a járőr közvetlen irányítását is a SitCen munkatársai végzik.

A) A Beavatkozó csoport minimális létszáma 2 fő. A járőr állományaiba minden körülmények között tartozzon parancsnok és 1 fő biztonsági őr.

B) A kijuttatás módja az alkalmazási körletbe: személygépkocsi vagy egyéb más közlekedési eszköz

C) A Beavatkozó csoport alkalmazását befolyásolja:

- > Járőrözési feladat,
- > Riasztási feladat esetében:
 - behatoló elfogása,
 - behatoló szándéka,
 - a tiltott területet belülről megközelítő személyek feltartóztatása,
 - rendelkezésre álló idő,
 - a kijuttatás módja.

A Beavatkozó csoport feladatai:

- > Az őrzés-védelmi tevékenység meghatározott járőrözési útvonalon a SitCen munkatársai által kijelölt pontok érintésével, a kijelölt objektumok körbejárásával az őrzés-védelmi, járőrözési-ellenőrzési feladatok végrehajtása.
- > A vállalat területén ott-tartózkodók jogosultságának szűrőpróbaszerű ellenőrzése (jogosulatlan személyek feltartóztatása).
- > A járőrözés alkalmával az útvonalukba eső épületek bejárati ajtóinál és nyílászáróinál azok zártságának, sértetlenségének ellenőrzése.
- > Amennyiben gyanús dolgot észlelnek, abban az esetben a járőrparancsnok biztosítja a helyszínt és haladéktalanul jelentést tesz a SitCen-nek.
- > Különleges esetekben helyszínbiztosításba kerülnek bevonásra.

A vagyonvédelem egyéb feladatai

- > A gyártáshoz nem kapcsolódó csomagokat és személyes tárgyakat a munkatársaknak a kapunál le kell adniuk, a szolgálat átveszi és megőrzi azokat,
- > Ellenőrzik az információ- és adatvédelmi szabályok betartását,

- > Környezetvédelmi károk felszámolásában vesznek részt,
- > Közlekedési baleseteket dokumentálják,
- > Forgalmirányítási feladatokat látnak el,
- > A parkolási rendet ellenőrzik (a mentő és tűzoltó útvonalakat szabadon tartatják),
- > Kárfelvételi jegyzőkönyveket készítenek,
- > Helyismerettel nem rendelkező személyeket kísérik,
- > Beavatkozási és riasztási terv szerinti feladatok végrehajtása,
- > A sürgősségi szolgálatok részére útbaigazítást és biztosítási tevékenységet végeznek,
- > Előzetes intézkedéseket vezetnek be lopás, rongálás, szabotázs, technikai károk, tűz és más egyéb, előre nem látható események esetére,
- > Szükség szerinti különleges szolgálatot és őrzési feladatokat végeznek,
- > Jegyzeteket és jelentéseket készítenek.

3.5. BIZTONSÁGI RENDSZEREK INTEGRÁLT ALKALMAZÁSA

3.5.1. Tűzvédelmi rendszerek

A tűzvédelmi rendszereket a nemzetközi és nemzeti jogszabályokban, szabványokban és irányelvekben meghatározottak szerint kell kiépíteni. A jogszabályokban foglaltaktól eltérő létesítéshez szükséges a Belügyminisztérium OKF vagy Megyei Katasztrófavédelmi Igazgatóság (MKI)³⁸⁷ (továbbiakban hatóság) engedélye³⁸⁸. Az OTSZ 3.§ 1. bekezdése meghatározza, hogy milyen előírások alól nem lehet eltérést engedélyezni. Az ott meg nem nevezett pontok alól lehet kérni eltérési engedélyt a 259/2011 Korm. rendelet 1.§ 2. bekezdés k) pontja alapján a hivatásos katasztrófavédelmi szerv területi egységétől. A hatóság az épületek, építmények tűzvédelmi használati előírásai, valamint a tűzoltóságok beavatkozásával kapcsolatos követelmények alól eltérést engedélyezhet. A 3. bekezdés b) pontja alapján a hivatásos katasztrófavédelmi szerv központi szerve - az OKF - az épületek és építmények tűzvédelmi létesítési előírásai alól eltérést engedélyezhet. A tervezés és kiépítés során felmerült további kérdéseket, egyeztetéseket az illetékes hatóság megfelelő osztályán kell lefolytatni. Az új épületek tervezésénél figyelembe kell venni a biztonsági

³⁸⁷ Megyei Katasztrófavédelmi Igazgatóság

³⁸⁸ 259/2011 Korm rendelet

célt és szintet, amelyet teljesíteni³⁸⁹. A kockázatelemzés elvégzése után kell a megfelelő biztonsági és építészeti előírásokat alkalmazni a tervezés és építés során. Ezek figyelembevételével a jogszabályban meghatározott esetekben „az építészeti-műszaki tervdokumentáció része a tűzvédelmi dokumentáció, amely tartalmazza törvény és annak végrehajtási rendeletében előírt tűzvédelmi követelményeknek való megfelelés dokumentálását tervekkel és műszaki leírásokkal tűzvédelmi tervet elkészíteni”³⁹⁰. A tűzvédelmi terv kidolgozásánál is a vállalat biztonsági stratégiájában meghatározott vállalati biztonsági modell³⁹¹ szerint kell eljárni. (3. számú melléklet)

“3/A. § (1) Az Országos Tűzvédelmi Szabályzat meghatározza az épületek, építmények létesítési és használati, valamint a tűzoltóságok beavatkozásával kapcsolatos tűzvédelmi követelményeket, az elérendő biztonsági szintet.

(2) A tűzvédelmi műszaki irányelvek kidolgozásáért felelős bizottság kidolgozza az Országos Tűzvédelmi Szabályzatban meghatározott biztonsági szintnek megfelelő egyes műszaki megoldásokat, számítási módszereket tartalmazó tűzvédelmi műszaki irányelveket.

(3) Az Országos Tűzvédelmi Szabályzatban meghatározott biztonsági szint elérhető

a) tűzvédelmet érintő nemzeti szabvány betartásával.

b) a tűzvédelmi műszaki irányelvekben kidolgozott műszaki megoldások, számítási módszerek alkalmazásával, vagy

c) a tűzvédelmi műszaki irányelvektől vagy a nemzeti szabványtól részben vagy teljesen eltérő megoldással, ha az azonos biztonsági szintet a tervező igazolja.

A kötelezettség alapját a vonatkozó jogszabályi rendelkezések jelentik. A jogszabályi követelmények figyelembevételével kell a tűzvédelemnek kialakítani a biztonsági előírásokat, amely megfelel a vállalat által elvárt védelmi szintnek.”³⁹²

³⁸⁹ 1996. évi XXXI. törvény 3/A §(1) Az Országos Tűzvédelmi Szabályzat - 54/2014 BM rendelet - meghatározza az épületek, építmények létesítési és használati, valamint a tűzoltóságok beavatkozásával kapcsolatos tűzvédelmi követelményeket, az elérendő biztonsági szintet.

³⁹⁰ 1996. évi XXXI. Törvény, 21. § (1)

³⁹¹ ... számú melléklet: A vállalat biztonsági stratégiája, p. 7.

³⁹² 1996. évi XXXI. törvény tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

“Jogszabályban meghatározott esetben az építészeti-műszaki tervdokumentáció része a tűzvédelmi dokumentáció, amely tartalmazza törvény és annak végrehajtási rendeletében előírt tűzvédelmi követelményeknek való megfelelés dokumentálását tervekkel és műszaki leírásokkal.

(2) Az (1) bekezdésben meghatározott tűzvédelmi dokumentációt csak az a természetes személy készítheti, aki tűzvédelmi szakértő, vagy tűzvédelmi tervezői jogosultsággal rendelkezik.”³⁹³

Mechanikai tűzvédelmi berendezések és eszközök (épület szerkezetek)

A jogszabályi előírások meghatároznak több előfeltételt ahhoz, hogy az épület szerkezeti elemei, kialakítása és az alkalmazott technológiák biztosítsák a létesítmény biztonságos működését és működtetését, hogy káresemény bekövetkezése esetén a bent tartózkodó személyek ne sérüljenek meg, az épületbe beépített berendezésekben és vagyontárgyakban kár ne keletkezzen.

Mechanikai tűzvédelem követelményei:

- > Megfelelő tűzállósággal rendelkező építési anyagok, szerkezetek és technológiák alkalmazása,
- > Kiegészítő tűzgátló elemek (falak, ajtók, kapuk) beépítése,
- > Tűzállóság növelő anyagok alkalmazása a különböző szerkezeti elemeken.

Elektronikus (automata) tűzjelzőrendszerek

Tűzjelző központok

„ Beépített tűzjelző berendezés: az építményben vagy szabadtéren elhelyezett, helyhez kötött, a tűz kifejlődésének korai szakaszában észlelést, jelzést és megfelelő tűzvédelmi intézkedést önműködően végző berendezés,”³⁹⁴

A tűzjelző központok önálló egységet képeznek és szünetmentesítettek. Nagyobb kiterjedésű rendszereknél moduláris rendszert alkalmazunk, amely esetben alközpontokat telepítünk. Ez esetben az alközpontokhoz vannak kapcsolva az érzékelő csoportok és az

³⁹³ 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról 4§. 10

³⁹⁴ 1996. évi XXXI. Törvény, 6.§ 4.

egyéb más tűzvédelmi rendszerek (külső kezelők, nyomtatók, modemek, fény- és hangjelzést adó berendezések). A biztonságos működés alapfeltétele a redundancia³⁹⁵.

A tűzjelző központ (alközpont) legfontosabb feladatai:

- > Alrendszerek áramellátása,
- > Érzékelők jelének fogadása,
- > Tűzjelzés és a pozíció továbbítása,
- > Tűzriasztás jelzése,
- > Rendszer szintű felügyeleti tevékenység (például: hibajelzések továbbítása), naplózás,
- > Tűzvédelmi rendszerek vezérlése (automatikus oltórendszerek, hő- és füstelvezetők).

Automatikus érzékelők³⁹⁶

Az automatikus érzékelő része a tűzjelző rendszernek, amely figyeli a térben, helyiségben a megfelelő fizikai és/vagy kémiai paramétereket. Egy előre programozott érték elérése esetén jelzést ad a tűzjelzőközpontnak. Az érzékelők telepítésénél figyelembe kell venni a veszélyeztetett terület rendeltetését, alapterületének nagyságát, valamint a helyiség építészeti sajátosságait (belmagasság, a födém dőlésszöge, gerendázat):

Érzékelők típusai lehetnek: füstérzékelők, lángérzékelők, hőérzékelők, gázérzékelők, többfunkciós érzékelők.

Automata gázzal oltó berendezések³⁹⁷

Bizonyos helyiségekben³⁹⁸ és technológiáknál a vízzel való oltás nem megengedett vagy nagy másodlagos kárt okozna. Ezért a legtöbb helyen oltógázokat alkalmaznak. Ezen automata oltórendszerek két elven működnek. A legelterjedtebb az oxigén kiszorításon alapuló rendszerek, a kevésbé alkalmazott technológia kémiai úton szünteti meg az égési folyamatot. A rendszerek tervezésénél, telepítésénél, üzemeltetésénél és karbantartásánál az MSZ EN15004-1 és a MSZ EN 9783 szabvány előírásai irányadóak.

³⁹⁵ A komponensek és részegységek duplikált alkalmazása.

³⁹⁶ MSZ EN 54

³⁹⁷ 28/2011. (IX.6) BM rendelet a beépített tűzoltó rendszerekről

³⁹⁸ Szervertermek, IT-berendezések, megmunkáló gépek, dokumentum tárolók

Automata oltóberendezéseknél alkalmazott gázok:

- > Oxigén kiszorításon alapuló rendszereknél: szén-dioxid, argon, nitrogén, inert gázok és ezek keveréke,
- > Kémiai hatású gázok: Novec, HFC-125 vagy 227, halotronok.³⁹⁹

SPRINKLER

A sprinkler automata oltóberendezés⁴⁰⁰ egy beépített, önműködő, vízzel oltó berendezés, amely tűzoltó közegként vizet és/vagy bekevert habképző anyagot használ fel és tűzjelző funkcióval is rendelkezik. A védendő területeket oltókörökre osztják fel, amelyeknek csőhálózatot építenek ki. A csővezetékbe szórófejeket építenek be, amelyekben egy hő hatására széttörő ampulla⁴⁰¹ található, ami ha szétrobban, akkor a csővezetékben lévő oltóanyag szabadon távozik. Az oltóanyagot a szórófejre szerelt terelőtányér osztja el. A rendszerek tervezésénél, telepítésénél, üzemeltetésénél és karbantartásánál az MSZ EN 12845 szabvány előírásai a mérvadóak.⁴⁰²

Fontosabb elemei:

- > SPINKLER központ: vezérlőegység, riasztó szelep, víztartály, szivattyúk, kiegyenlítő tartály, légkompresszor, áramlásjelzők,
- > Csővezeték hálózat a szórófejekkel és szabályzó szelepekkel,
- > Habanyag tároló.

Tűzoltókészülékek

A készülékben lévő oltóanyagot a benne levő nyomás hatására irányíthatóan lehet a tűzre juttatni. Az épületekben, csarnokokban, továbbá szabadterén a jogszabályban meghatározott követelményeket kielégítő és az ott keletkezett tűz oltására alkalmas tűzoltó készüléket kell elhelyezni.

³⁹⁹ halon helyettesítők

⁴⁰⁰ 28/2011. (IX.6) BM rendelet a beépített tűzoltó rendszerekről,

⁴⁰¹ Folyadékkal töltött ampulla és melyben folyadék kémiai összetétele határozza meg az ampulla szétrobbanásának hőmérsékletét

⁴⁰² Dr. KUTI Rajmund – Dr. FÖLDI László: *A beépített vízköddel oltó rendszerek újabb alkalmazási lehetőségeinek feltárása*, Hadmánök, III. Évfolyam 2. szám - 2008. Június, pp. 61 - 63.

A tűzoltó készülékeken fel kell tüntetni:

- > milyen tűz oltására alkalmas
- > a készülék megnevezését
- > rajzos és szöveges kezelési utasítást
- > az oltható tűzosztályok jelképét
- > a veszélyekre történő figyelmeztetést
- > a gyártót
- > gyártás- és felülvizsgálat időpontját.

A vonatkozó jogszabály alapján a tűzoltó készülékekről nyilvántartási napló⁴⁰³ vezetése kötelező, amely tartalmazza a tűzoltó készülék: típusát, készenléti helyét, az ellenőrzés és a javítás időpontját.

Az MSZ EN 3 szabványsorozat szerint gyártott készülékeket évente kell ellenőriztetni.

Tűzcsapok és falitűzcsapok⁴⁰⁴

A tűz oltásához szükséges vízvételi lehetőségek, olyan csatlakozási pontok, ahol a tűzoltók a tűzivíz hálózatra tudnak kapcsolódni. Ipari környezetben a tervezéskor meghatározott és kivitelezés előtt pontosított, a lefedettséget biztosító pontokra telepítik. Tűzcsapok felülvizsgálatáról, ellenőrzéséről külön nyilvántartást kell vezetni.

Hő és füstelvezető rendszer

A hő és füstelvezető rendszer feladata – nyitott állapotban – hogy lehetővé tegye az épületben vagy helyiségben keletkezett füst és forró égésgázok természetes vagy mesterséges úton történő kiáramlását a szabadba. A rendszerek tervezésénél, telepítésnél, üzemeltetésénél és karbantartásánál az OTSZ és az MSZ EN 12101: 1- 10 szabvány előírásait kell alkalmazni. A szellőztetést csak tűz esetén szabad működtetni. Telepítése és működtetése elhatárolt füstszakaszonként történik.

Feladata tűz esetén:

- > A menekülési utak és útvonalak füstmentességének biztosítása,
- > Épületszerkezetek és berendezések tűzterhelés elleni védelme,

⁴⁰³ MSZ 1040, MSZ EN-3

⁴⁰⁴ MSZ EN 671-3, Beépített tűzoltó berendezések. Tömlőberendezések

- > A füst és égésgázok okozta egészségkárosodások csökkentése.

3.5.2. Vagyonvédelmi rendszerek

A vagyonvédelmi rendszerek tervezésénél, kivitelezésénél és üzemeltetésénél figyelembe kell venni az integrált biztonsági koncepcióban meghatározott elveket és a vállalat biztonsági modelljének irányelvét⁴⁰⁵. (2. számú melléklet)

Mechanikai védelem elemei

3.5.2.1.1. Kerítések⁴⁰⁶

A kerítések feladata – mint a vagyonvédelem egyik legfontosabb eleme –, hogy az őrzött területre illetéktelenek ne tudjanak behatolni. A kerítések kialakítása megfelelő mechanikai védelmet nyújt az illetéktelen behatolókkal szemben, mert csak komoly erőfeszítéssel, illetve különböző segédeszközök alkalmazásával küzdhető le. A kerítés megvilágítása biztosítja az őrök számára a folyamatos megfigyelés lehetőségét.

A kerítések elektronikus védelme mozgásérzékelő és videó megfigyelő rendszerből áll és teljesen automatikusan működik. A videó megfigyelő rendszer folyamatos megfigyelését a SitCen munkatársai végzik. A közvilágítás megszűnése esetén a kerítés megfigyelésére lehetőség van a videó megfigyelő rendszer infravörös üzem módjában. A kerítésvédelmi rendszerhez tartozik a vagyonvédelmi szolgálatától kijelölt 2-3 biztonsági őrből álló Beavatkozó csoport.

Követelmények

- > Általános behatolás elleni védelem (III. szintű⁴⁰⁷: még emberi erővel szállítható szerszámok ellen véd, a tettesek csak megfelelő előkészítés után tudják tervezett cselekményeiket végrehajtani),
- > Mechanikai ellenálló képessége minimum 5 perc,
- > A kerítés elemeit csavarozással kell rögzíteni a védett oldalról, a kötőelemeknek nehezen megtalálhatónak kell lenniük és csak speciális szerszámmal bonthatónak.

⁴⁰⁵ 2. számú melléklet: A vállalat biztonsági stratégiája, p. 7.

⁴⁰⁶ VdS Schadenverhütung GmbH Verlag,

⁴⁰⁷ BOOBERG Verlag GmbH: Unternehmensschutz, Kapitel: D1

Bejáratok, nyílászárók mechanikai védelme

- > Megerősített biztonsági ajtók, ablakok,
- > Mechanikus főkulcsrendszer,⁴⁰⁸
- > Felügyelt menekülő ajtók és kapuk,⁴⁰⁹
- > Biztonsági fóliák,
- > Rácsok,
- > Személyi forgalmat korlátozó eszközök, korlátrendszerek.

Mechanikai akadályok

- > Fél- vagy teljes sorompók,
- > Motoros kapuk,
- > Pollerek,⁴¹⁰
- > Gumiabroncs szagattók.

Elektronikus vagyónvédelmi rendszerek

Videó megfigyelő rendszer⁴¹¹

Egy videó megfigyelő rendszer arra szolgál, hogy az objektum területén egy központi helyről folyamatosan diszkrét megfigyelést biztosítson a biztonsági személyzet részére, egy esetleges támadó számára pedig kiszámíthatatlan kell lennie. A beavatkozási idő és a beavatkozási taktika kiválasztása lényegesen lerövidül, ha riasztás esetén a helyszínről „élőkép” közvetítésére van mód.

A videó megfigyelő rendszer a belső területeken és a perifériákon installált statikus és dinamikus kamerák együtteséből tevődik össze.

A dinamikus kamerák mozgathatók és az objektív funkciók vezérelhetőek.

⁴⁰⁸ A főkulcsra alapuló zárrendszerben a zárbetétek csoportokat alkotnak. Minden csoportnak saját csoportkulccsal rendelkezik. Egy főkulcs, ami nyitja az összes a rendszerben levő ajtót, lakatot vagy egyéb zárbetétet. Az egyedi zárbetétek saját kulccsal is rendelkezhetnek. Bizonyos csoportkulcsok nyithatnak más csoportba tartozó zárbetéteket is, így biztosítva a mátrix rendszer kialakítását. A kulcsok nem másolhatóak, csak a gyártótól lehet beszerezni és/vagy utánrendelni.

⁴⁰⁹ BOOBERG Verlag GmbH: Unternehmensschutz, Kapitel: D1, pp. 60

⁴¹⁰ Útból kiemelkedő „bak”

⁴¹¹ DIN EN ISO 22311, Videó megfigyelő rendszerek

A videó megfigyelő rendszert önállóan mint elektronikus védelmi eszközt nem használhatjuk, csak az ellenőrzés kiegészítéseként és a riasztás ellenőrzésére. Egy kamera képe önmagában a helyszínről nem elégséges. Hatékonyabb a beavatkozás, ha a több érzékelőtől érkező riasztás jelzéseket automatikusan összekapcsoljuk a kamerákkal és azok képeit egy vagy több monitoron megjelenítjük.

Beléptető rendszer

A beléptető rendszert - ami lehetővé teszi a vállalat területére és a biztonsági területekre történő belépést - egy automatikus azonosító rendszer támogatja.

- > Az automatikus beléptető funkcióval ellátott ajtónak vagy kapunak fizikailag meg kell tudni akadályozni a bejutást. A félsorompó nem fogadható el!
- > A SitCen-nek lehetősége van felülbírálni az automata beléptető rendszert, hogy megakadályozza a belépést,
- > Az „elsődleges” beléptető rendszer kiegészíthető egy „másodlagos” személyazonosító rendszerrel (PIN kód vagy különböző biometrikus azonosítók).

Az „elsődleges” rendszer kizárólagos használatából eredő hiányosság, hogy nem a személyhez kötődik a jogosultság, hanem a kártyához. Kártya elhagyása vagy annak ellopás esetén illetéktelen is beléphet a védett területre.

Belépőkártyák

Egyértelmű azonosítási és beléptetés-ellenőrzési rendszer szükséges, hogy garantálni tudjuk az illetéktelenek belépésének megakadályozását és elősegítsük a szabályszerű belépést a biztonsági zónákba. Ez elérhető személyes felismeréssel, azonban sokkal hatékonyabban elérhető egy biztonsági igazolványrendszerrel. A kiadott igazolványok nyilvántartását naprakészen kell tartani.

Az igazolványokkal szembeni követelmények:

- > Sorszámozott,
- > Tartalmaz a tulajdonosról azonosító adatokat és fényképet,
- > Egyedi és azonosítható maga a szervezet,
- > Kódolt alakban mutatja az engedélyezett hozzáférési területet vagy típust.

Biometrikus azonosítás⁴¹²

A biometrikus azonosítás adatait⁴¹³ ugyanolyan szintű biztonsági védelemben kell részesíteni, mint azokat a minősített anyagokat, amelyeket védenek. A biometrikus azonosító rendszerek napjainkban a legbiztonságosabbaknak tekinthetők.

Az RFID⁴¹⁴ kártyák és a biometrikus azonosítás kombinációjának tipikus megjelenési formája, amikor a biometrikus sablont (template-et) az RFID kártyán tárolják, így az azonosítás során csak a frissen képzett és a kártyán tárolt sablon összehasonlítása történik meg. Ez gyorsabb és működése off-line üzemmódban is megvalósítható. Az RFID kártyák egy praktikus megjelenési módja, amikor kulcstestbe építik be az RFID chipet (tag). Ekkor ugyanaz a kulcs szolgál hagyományos zárral és biometrikus azonosítással védett ajtók nyitására is (utóbbi esetben természetesen a biometrikus jellemzővel együtt).

Az elektronikus megoldások ugyanakkor felvetik az alkalmazásra kerülő elektromos zárok (zárfogadók, elektromechanikus zárok stb.) biztonságosságát, mint lehetséges gyenge pontok kiküszöbölési kényszerének kérdését.

Betörésjelzők és központok

Behatolásjelző rendszer (továbbiakban BJR) használható a biztonság erősítésére vagy az őrzés helyett, de nem az ügyeletes őrség helyett. Ennek különösen ott van jelentősége, ahol az őrség nem léphet be a biztonsági zónába. A BJR az őrző helyett működhet, ha rendelkezik a következő jellemzőkkel:

- > Biztosítsa a terület teljes terjedelmének védelméről,
- > Kapcsolódjon biztonsági központhoz (távfelügyelet), ahonnan irányítani lehet a Beavatkozó csoportokat,
- > Folyamatos felügyelet biztosított,
- > Rendelkezzen szünetmentes tápegységgel,
- > A központi egységet fizikai védelemmel kell ellátni,
- > A rendszernek képesnek kell lennie manipulálás vagy hibás működés esetén figyelmeztető jelzés adására.

⁴¹² A személy egyedi fizikai és testi jellemzői méri, rögzíti és folyamatosan frissíti

⁴¹³ Ujjnyomat, tenyérynymat, kézgeometria, írisz, aláírás, hang, arcfelismerés ...

⁴¹⁴ Radio Frequency Identification, Rádió frekvenciás azonosítás és adatközlés

Egyéb vagyonvédelmi rendszerek és eszközök:

- > Fémkereső kapuk vagy átjárók,
- > kézi fémkeresők,
- > Robbanóanyag detektorok,
- > Csomagátvizsgáló berendezések,
- > Biztonsági zónák lehallgatás elleni védelmét megakadályozó, azt detektáló és elhárító eszközök,
- > Drónok⁴¹⁵ behatolását felderítő és elhárító eszközök,
- > Videó (kép) alapú mozgásérzékelők, tűzjelzők, vészjelzők,

3.5.3. Telekommunikációs rendszerek

Vonalas/hálózatos telefonrendszer

A SitCen fő kommunikációs eszközei a telefonok, melyek a vállalat telefonközpontjára vannak kapcsolva. Ha IP⁴¹⁶-telefon rendszer üzemel a vállalatnál, az azt jelenti, hogy a hang továbbítását IP hálózaton keresztül biztosítják. Az IP alapú hangszolgáltatások összefoglaló neve VoIP⁴¹⁷. Veszély esetére (segélyhívás) a vállalat egész területére vonatkozóan hívószámokat kell megadni, melyeknek legalább három számból állnak⁴¹⁸. A segélykérő mellékállomás vagy mobiltelefon hívószáma megjelenik a képernyőn és így szükség esetén a hívót az elektronikus telefonkönyvben visszakereshetjük. A segélyhívások dokumentálására vagy ismételt visszahallgatására a hívásokat egy arra alkalmas felvevő készüléken kell rögzíteni. Más hívásokat manuálisan is lehet rögzíteni akkor, ha azt a hívó kéri vagy arra szükség van pl. közveszéllyel való fenyegetés esetén.

Tartalékkészülékként – ha a telefonközpont nem működik vagy az IP-hálózat – kell egy közvetlen fővonalra csatlakozás a nyilvános telefonhálózatra egy erre a célra elkülönített készülékkel. A telefonszámot a szolgáltatónál titkosítani kell és a vállalaton belül CSAK az ügyeleti szolgálatot adók ismerhetik.

⁴¹⁵ Pilóta nélküli repülő szerkezet

⁴¹⁶ IP – Internet Protokoll, hálózati szabvány

⁴¹⁷ Voice over IP - internet használatával működő hangátvitelt

⁴¹⁸ Általános segélyhívó szám, üzemorvosi rendelő/vállalati mentőszolgálat, Létesítményi tűzoltóság

Egységes Digitális Rádiótávközlő Rendszer (továbbiakban EDR)⁴¹⁹

Egy fontos kommunikációs eszköz az EDR rendszer, amely biztosítja a SitCen összeköttetését a védelmi szervezetekkel, hatóságokkal és a saját beavatkozó erőkkal. A SitCen-ben minden munkaállomás rendelkezzen stabil (beépített) eszközzel, illetve kézi készülékekkel.

Egyéb kommunikációs rendszerek, mint mobiltelefon hálózat,⁴²⁰ biztonsági vonalas összeköttetés,⁴²¹ Műholdas telefonok.

3.5.4. Biztonsági rendszerek integrálása⁴²²

A biztonsági rendszereknél szükséges a különböző tűz-, vagyonvédelmi- és egyéb más védelmi célokat szolgáló rendszerek integrálása. A rendszer alkotórészeivel - SitCen mint központi vezérlőrendszer⁴²³ - a vállalat külső és belső területein, épületeiben, csarnokaiban elhelyezett rendszerek együttesen szavatolják a vállalat biztonságát. A *biztonsági rendszerek integrálása* csak akkor váltja be a hozzáfűzött reményeket, ha egy *integrált biztonsági koncepcióba* illesztjük be.

Ma Magyarországon egyre inkább teret nyernek azok gondolatok, hogy integrálni kell a biztonsági rendszereket, amit jó megoldásnak tartok a rendszerek nagysága és összetettsége miatt. Több tanulmányban megjelent, hogy a háztechnikai és más épületautomatizálási, vezérlési funkciókat is *be kell kapcsolni az integrált biztonsági rendszerbe*. A különböző jogszabályok és hatósági előírások lehetővé teszik a tűzvédelmi rendszerek és háztechnikai alrendszerek kapcsolatát, de ez nem jelenti azt, hogy a rendszerek *minden elemét⁴²⁴ összekapcsolhatjuk*. Ezt mindig az adott épület/objektum szerkezeti (építészeti) kialakítása, funkciója és az ott alkalmazott technológia határozza meg. A *jogszabályoktól való eltéréseket* mindig a *hatóságokkal egyeztetve* és az általuk előírt *ellensúlyozó intézkedések* alkalmazásával kell megvalósítani.

⁴¹⁹ 450 MHz-es tartományban működő analóg rendszer

⁴²⁰ Telefon, amely egy bázisállomásból álló mobil kommunikációs hálózathoz kapcsolódik

⁴²¹ A vállalat tartalék kommunikációs rendszere, amely kiegészíti a vállalat kommunikációs rendszerét (direkt vezetékes összeköttetés). Ebben a rendszerben szerepel az összes biztonsági szereplő, (SitCen, Létesítményi tűzoltóság, vagyonvédelem szolgálati helyei, üzemorvosi rendelő, háztechnikai (épület menedzsment), szolgálat, Energiaközpont és a vállalat működése szempontjából fontos létesítmények vezérlő/irányító központjai.

⁴²² Kálmán László – Pataki János: Integrált technikai objektum védelem, Zrínyi Miklós Nemzetvédelmi Egyetem, LKBM-2732, 2007.11.15., Budapest, tanulmány – elérhető a szerzőknél

⁴²³ biztonsági menedzsment rendszerrel (továbbiakban BMR)

⁴²⁴ Légtechnika, tűzszakasz határoló ajtók/kapuk, liftek vezérlése, menekülő ajtók/kapuk nyitása, vészvilágítás bekapcsolása...

Fontos az integrált központ irányítása és kezelése, valamint az ott dolgozó munkatársak oktatása, illetve az oktatás színvonala és rendszeressége. *Egy vállalat biztonsági stratégiája szerint az elektronika és a humán erőforrás együtt képes megoldani a biztonsági feladatokat.*

A különféle gyengeáramú rendszerek (ház- és biztonságtechnika) összekötése eredményeként az elvárt irányítási rendhez maximálisan illeszkedő, azt hatékonyan kiszolgálni képes kezelői és naplózási felület szükséges. Ez nem csak a jelzések elvárt megjelenítési formáját és a jelzésekre adható meghatározott reakciókat jelenti, hanem az egyéb forrásokból beérkező (telefon, EDR ...) jelzések naplózási lehetőségét és a különféle gyengeáramú rendszerektől érkező információk naplózásban való (össze) csatolási lehetőségét is. Egy esemény bekövetkeztekor az integrált biztonsági rendszerjelzést ad, ezáltal segíti a káresemény megelőzési feladatait és a nyomozati munkát.

A BMR megjelenítésnél mindig magas prioritással rendelkeznek a tűzvédelmi rendszerek, amelyek alkalmasak arra, hogy univerzális veszélyjelző rendszerként működjenek, a riasztásokat megjelenítse és riadóztassa a beavatkozó erőket.

A BMR-rel szemben támasztott legfontosabb követelmények:

- > A különböző alrendszerek jelzéseit egységes ábrázolási módon jeleníti meg,
- > Az egyes riasztási típusokhoz tartozó tevékenységi rend a háttérben jelenik meg,
- > A különböző munkahelyeken⁴²⁵ egyedileg meghatározott prioritásokkal lehet a különböző biztonsági rendszerek riasztásait megjeleníteni és kezelni,
- > Az épületek és helyiségek grafikus megjelenítése (a riasztás helye és oka, a helyiségek, ott tartózkodók létszáma és a veszélyforrások megjelenítése ...),
- > A kiértékelési rend közvetlen összeköttetésben van a riasztási renddel, de manuálisan is elérhető, aktiválható,
- > A kezelők számára a riasztások grafikus megjelenítése miatt könnyen beazonosíthatóak a helyszínek. A terület és a különböző épületek pontosított, ellenőrzött adatait a vállalat megfelelő adatbázisaiból kell importálni.

3.6. Objektumok és épületek terrorrobbantás elleni védelme

⁴²⁵ Tűzvédelmi rendszerek kezelője (pl.: Létesítményi tűzoltóság Híradó ügyelete), vagyonvédelmi és egyéb más rendszerek kezelője ...

Az Egyesült Államok Védelmi Minisztériuma (Department of Defense, a továbbiakban DoD) adta ki az „Anti-terrorista minimum szabályozás az épületek védelméhez”⁴²⁶ című ajánlást, amely része az „Egységes Létesítési Szempontok” (Unified facilities Criteria, a továbbiakban UFC) szabályozási rendszernek.

Az objektumok és épületek terrorrobbantások elleni védelmét biztonságtechnikai szervező mérnöki szempontokból vizsgáltam. A magyar szabályok csak építészeti előírásokkal foglalkoznak. Egy alkalommal a Műszaki Katonai Közlönyben jelent meg egy publikáció „Építészeti tervezés robbantásos cselekmények ellen”⁴²⁷ címmel. A robbantásos cselekmények elleni védekezés integrált védelmi előírásairól nem elérhető jogszabályi előírások vagy irányelvek.

Ma Magyarországon még nem általánosan elfogadott, az az Európai Unióban már működő gyakorlat, hogy már a projekt indításakor a különböző biztonsági szervezeteket bevonják előkészítésébe, illetve a projekt költségvetésének tervezésébe. Ebben a folyamatban már megjelennek⁴²⁸ a biztonsági rendszerek várható költségei.

A DoD ajánlása a fő hangsúlyt a szervezeti biztonsági intézkedésekre helyezi az épületeknél és objektumoknál.

Az 1. fejezetben az általános elveket fogalmazzák meg, amelyekkel a kitűzött célok teljesíthetők.

A 2. fejezet már azokat a konkrét előírásokat tartalmazza, amelyek alkalmazásával végrehajthatóak az 1. fejezetben meghatározott minimum elvárásokat.

A dokumentum mellékletei tartalmazzák a fogalmak meghatározását, DoD minimális anti-terrorista előírásokat, az ajánlott kiegészítő anti-terrorista intézkedéseket és a minimum anti-terrorista intézkedéseket expedíciós és ideiglenes létesítmények védelméhez. A megfelelő védelem nem csak az épületek robbanásállóságának növelésével érhető el, hanem:

- > adminisztratív és megelőző intézkedések alkalmazásával
- > kiegészítő mechanikai és elektronikus védelmi intézkedésekkel
- > a személyi állomány továbbképzésével.

⁴²⁶ www.dod.wbdg.org (Letöltve: 2011.10.01.)

⁴²⁷ Műszaki Katonai Közlöny XVIII. évf. 1-4. szám, 2008.

⁴²⁸ Lásd: 2.2.3. Védelmi képességfejlesztés és beruházás költségeinek viszonya, pp. 60 - 67

3.6.1. Anti-terrorista minimum szabályozás az épületek védelméhez

A rendszabályokat és a leghatékonyabb védelmi intézkedéseket egységesen kell alkalmazni, amelyekkel minimalizálható a terrortámadások lehetősége a vállalat épületei és az ott tartózkodó személyek ellen.

Dinamikusan változó biztonsági környezet

A terrorizmus az egész világot behálózza és fejlődik, amelyet a terrorcselekmények és az áldozatok számának folyamatosan emelkedése jellemez. A terroristák tevékenysége kiszámíthatatlan. A megfelelően képzett, felszerelt és céltudatos biztonsági személyzet elrettentheti a terroristákat eredeti céljaik megvalósításától. A terroristák elkövetési eszköztára sokrétű, legtöbbször robbanóeszközöket alkalmaznak, ha tömeg ellen terveznek támadást. Magyarországon a legtöbb vállalat, objektum nem rendelkezik megfelelő védelemmel. Az anti-terrorista védelem minimális szabályainak betartása csökkenti az épületek veszélyeztetettségét.

Munkatársak és a vállalattal kapcsolatban lévő személyek védelme

Minden munkatárs, beszállító vagy a velük kapcsolatban álló személyek elleni terrorista támadások lehetőségének minimalizálása a cél a vállalt területén és az általa fenntartott objektumokban és létesítményekben.

Biztonság- és védelempolitika szakterület felelőssége

A szakterület feladata, hogy a munkatársak és a vállalat elleni terrortámadások kockázatát csökkentse. Ez csak a hatóságokkal együttműködve valósítható meg.

3.6.1. Anti-terrorista intézkedések integrált megvalósítása

Tervezés és integráció

Egy megfelelően kialakított védelmi rendszerrel csökkenthető a támadások bekövetkeztének valószínűsége és a lehetséges károk nagysága. A hatékony tervezési folyamat megkönnyíti a szükséges döntések meghozatalát, tisztázza a szerepeket és a

felelősséget, valamint a tervszerű gyakorlatok biztosítják a védelmi feladatok sikeres végrehajtását.

A vállalat terrorrobbantások elleni védelme csak az integrált biztonsági koncepció teljes körű alkalmazásával valósítható meg. A széleskörűen alkalmazott „klasszikus” biztonsági feladatok⁴²⁹ közül a vagyonvédelmet kell megerősíteni szervezeten belül, ellátni megfelelő biztonságtechnikai eszközökkel és biztosítani kell a személyi állomány szak- és továbbképzését, amellyel biztosítható a vállalat terrorrobbantások elleni védelme.

„Közveszéllyel (robbantással) fenyegetés

338. § (1) Aki a köznyugalom megzavarására alkalmas olyan valótlan tényről állít, híresztel, vagy azt a látszatot kelti, hogy közveszéllyel járó esemény bekövetkezése fenyeget, büntetett miatt három évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha a közveszéllyel fenyegetés a köznyugalom súlyosan megzavarta.”⁴³⁰

A vállalat Védelmi terve részeként jelennek meg azok az intézkedések, amelyek meghatározzák közveszéllyel való fenyegetés esetén a különböző szervezeti egységek biztonsági feladatait. Véleményem szerint külön tervet nem kell készíteni, mert a „Védelmi terv” mint koncepció tartalmazza mindazon intézkedéseket, melyek alapján az érintett terület kiüríthető, elkülöníthető és biztosítja a belső beavatkozó erők és hatóságok együttműködését.

A Védelmi terv alapján el kell készíteni egy munkautasítást a belső beavatkozó erők részére és ez képezi alapját a bevont erők felkészítésének (megelőzés), kiképzésének és a feladatok gyakoroltatásának. A munkautasításból kiemelnék néhány fontos elemet, amit fél évente legalább egy alkalommal gyakoroltatni kell, de csak az érintett állománnyal. Ez részemként megjelenhet a vállalat Krízismenedzsment törzsvezetési gyakorlatában.

A fenyegető üzenetek eljuttatásának módjai:

Telefonon:

⁴²⁹ 3.2. - 3.5 Alfejezetekben szereplő feladatok, mint például Információbiztonság, Tűzvédelem, vagyonvédelem, munkavédelem, egészségvédelem, IT-biztonság...

⁴³⁰ 16/1999. (II.5.) Korm. rendelet a rendőrség ellenérték fejében végezhető szolgáltató tevékenységéről, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99900016.KOR
(Letöltve: 2014.10.24.)

- > rögzíteni kell a telefonbeszélgetést,
- > fel kell jegyezni minden háttérzajt és releváns információt a hívóról és a környezeti zajokról,
- > a hívót minél hosszabb ideig kell beszéltetni, ha lehetőség van rá összezavarni.

Postai úton:

Óvni kell az üzenetet (levél, boríték, stb.) a szükségtelen kezeléstől, hogy megőrizze a bizonyítékokat a rendőrségi helyszíni szemléig.

- > Informálni kell a biztonsági menedzsment vezetőjét, illetve a rendőrséget,
- > Tájékoztatni kell a kiérkező tűzszerészeket, a helyi rendőrséget, tűzoltókat és a mentőszolgálatot, ha szükséges,
- > Készültségi karbantartó személyzet tájékoztatása (Facility Management⁴³¹),
- > A rendőrség dönt a teljes vagy részleges kiürítésről,
- > Kiürítés után szükséges a gyülekezési helyen tartózkodók létszámenőrzése,
- > Az utasításokat úgy kell kiadni, hogy ne keltsünk pánikot,
- > A minősített információk biztonságos tárolását meg kell szervezni az érintett terület kiürítése előtt,
- > Az átvizsgálást (Bomb Check)⁴³² a Védelmi terv megfelelő pontjai szerint kell végrehajtani,
- > A veszélyhelyzetben a liftek használata TILOS!

Robbanóanyag felderítése / megtalálása esetén:

- > Ne nyúljunk hozzá, ne mozdítsuk meg,
- > Ne veszélyeztessük a személyzetet, kerítsük körbe kordonnal (szalaggal),
- > Helyezzenek el homokzsákokat, védőeszközöket és más hasonló tűzálló eszközöket a feltételezett robbanószerkezet mellett,
- > Alakítsunk ki egy biztonsági területet és őriztessük,
- > A Beavatkozó erőket egy magasabb készenlétbe kell helyezni,
- > Ellenőrizzük, hogy a kiürítési útvonalon és a gyülekezési területen vannak-e további gyanús tárgyak, csomagok,
- > Biztosítani kell az érintett területen tárolt minősített információkat,

⁴³¹ Létesítmény gazdálkodás

⁴³² Bomba ellenőrzés/átvizsgálás

- > Meg kell szüntetni az elektromos-, a gáz- és a tüzelőanyag ellátást, amelyek a lezárt területre vezetnek vagy áthaladnak rajta,
- > A környékről el kell távolítani a gyúlékony és a veszélyes anyagokat,
- > Mivel a robbanószerkezetek általában rádiójelek által is működtethetőek, ezért minden állomást kb. 200 – 300 m belül le kell kapcsolni, kivéve a tűzszerész rádióhálót.

Robbanás esetén (ha megtörtént):

- > Riasszuk a belső és külső beavatkozó erőket,
- > Az érintett területről a személyzet eltávolítása, miután a kiürítési útvonalakat és a gyülekező helyeket leellenőrizték, ha az gyanús eszközöktől/csomagoktól mentes,
- > Az érintett területeken továbbra is biztosítani kell a minősített információk védelmét,
- > Biztosítani kell a robbanás helyszínét a rendőrség kiérkezéséig.

Védelem szintjei⁴³³

A különböző utasítások alkalmazásával egy alap szintű biztonságot érhetünk el, melyet a környezet biztonsági kihívásaihoz kell igazítani további biztonsági intézkedések alkalmazásával. Konkrét terrorfenyegetés esetén a vállalat felsővezetése más szigorúbb intézkedéseket vezethet be.

Kritikus létesítmények olyan épületek, amelyek magasabb szintű védelemmel rendelkeznek, hogy egy esetleges terrortámadás után is megtartsák működőképességüket.

3.7. OBJEKTUMOK TERRORTÁMADÁSOK ELLENEI VÉDELME⁴³⁴

Terrortámadások célja, hogy bizonyos személyeket megöljenek, elraboljanak, túszoikat ejtsenek, vagy objektumokat/épületeket foglaljanak el vagy fontos berendezéseket semmisítsenek meg, mindezt minél nagyobb média nyilvánosság mellett úgy, hogy a lakosság körében minél nagyobb pánikot keltsenek.

⁴³³ Lásd: 3.7.2. Védelmi fokozatok, pp.

⁴³⁴ 9/2007. (IK 8.) IRM-ÖTM együttes utasítás, a terrorizmus elleni egységes végrehajtására, Minősítés törölve IRM/TÜK/40322/2008. sz. alapján – a szerző birtokában

A célpont kiválasztása nem csak ideológiai szempontok alapján történik. A sikeres támadást figyelmeztetés nélkül hajtják végre, amely előtt a célpontok és annak védelmét pontosan felderítik.

3.7.1. Terrorelhárítás elvei

A Védelmi tervben kell meghatározni az alapvető és minimális biztonsági intézkedéseket, amelyek fenyegetés mentes időszakban érvényesek és biztosítják a vállalat munkatársainak és minősített információinak védelmét, valamint a működőképesség fenntartását. Fokozott terrorfenyegetettség idején a Védelmi tervben meghatározott magasabb biztonsági szintű intézkedéseket kell bevezetni, amelyek szükségesek a folyamatos működéshez. Az objektumon belül meg kell határozni a kiemelten fontos épületeket, területeket és zónákat, amelyek őrzés-védelme döntő jelentőségű a vállalat biztonságának szempontjából. Az érintett hatóságoktól javaslatot kell kérni a terv kiegészítéséhez, hogy az adott objektum biztonsági szervezetei milyen belső vagy külső védelmi intézkedéseket alkalmazzanak. Így a védelem egy összehangolt folyamatként valósul meg és egy magasabb biztonsági/védelmi szint érhető el. (5. számú melléklet)

A védelmi terv tartalmazza:

- > A bevezetendő kiegészítő biztonsági/védelmi intézkedések leírását minden egyes szükségállapotnál,
- > A felelős hatóságok megnevezését,
- > A terv különböző szintjeinek kihirdetéséért, bevezetéséért felelős személyek megnevezését,
- > A felelősségi körök egyértelmű meghatározását (parancsadási és ellenőrzési),
- > A beavatkozó és a támogató erőkre vonatkozó folyamatosan kiadandó intézkedéseket,
- > Az összekötetés módjait,
- > A sérültek mentési tervét, valamint a személyi állomány védelméről és minden oldalú ellátásáról kidolgozott feladatokat.⁴³⁵

⁴³⁵ Force Protection

Az objektumon kívüli védelmi intézkedések

Az objektum és a belső épületek/létesítmények rendelkeznek megfelelő védelemmel, így azok védettsége egy jól megtervezett támadásnak is képes ellenállni. A vállalat közös védelme⁴³⁶ nem terjeszthető ki a vállalaton kívülre. A terrortámadások megtervezésénél a „puhább” célpontokat⁴³⁷ fogják keresni, így nem zárható ki a személyek elleni támadás sem. A szálláshelybiztosítási és utazásbiztosítási feladatoknak ebben az esetben megnő a jelentősége. A külföldi tulajdonban lévő magyarországi nagyvállalatok vezetői biztonságánál figyelembe kell venni az érintett személyek származási országából fakadó kockázatokat is. Ezért szükséges a hatóságok bevonása a személyvédelmi intézkedések megtervezéséhez, bevezetéséhez és fenntartásához.

Személyvédelmi intézkedések

Az objektumvédelmi intézkedések mellett nagyon fontos feladat az objektum vezetőjének személyvédelmi feladatának megszervezése és végrehajtása.⁴³⁸

A szálláshelybiztosításánál figyelembe kell venni az integrált vagyon- és tűzvédelmi rendszerek tervezésénél és megvalósításánál felsorolt elemeket és feladatokat, amelyet a „biztonsági piramis” elvének betartásával kell kialakítani.

Az utazásbiztosításnál⁴³⁹ a szükséges taktikai elemeket, technikai eszközöket és speciális gépjárműveket kell alkalmazni.

Világszerte egyre több merényletet követtek el politikusok és nem kormányzati szereplők ellen, ezért a fenyegetettségi szintnek megfelelő védelem érdekében olyan koncepciókat dolgoztak ki, melyek alkalmazásával a védett vezetők biztonságát egyre magasabb szintre tudták emelni. A védelem meghatározó eleme a korszerű technikai eszközök és berendezések alkalmazása. A különleges védelemmel felszerelt gépjárművek meghatározó elemévé váltak az utazásbiztosításnak.⁴⁴⁰

⁴³⁶ Belső beavatkozó erők és hatóságok (külső beavatkozó erők)

⁴³⁷ Könnyebb lehetőségek

⁴³⁸ 3.3.2. Általános biztonsági intézkedések, p. 69 -70.

⁴³⁹ PATAKI János: *Különleges védelemmel felszerelt gépjárművek*, ZMNE BOLYAI JÁNOS HADMÉRNÖKI KAR ÉS A HADMÉRNÖKI DOKTORI ISKOLA, ONLINE TUDOMÁNYOS KIADVÁNYA, IX. Évfolyam 2. Szám, 2014.június

⁴⁴⁰ Reinhard SCHOLZEN: *Personenschutz*, Motorbuch Verlag, Stuttgart, 2004, pp.8-25 ISBN 3-613-02185-4

Korunkban egyre nagyobb az érdeklődés a különleges védelemmel felszerelt gépjárművek iránt. Itt két fontos felhasználói kör alakult ki, a kormányzati és a privát szféra (managerek, hírességek) szereplői. A járművek egy új generációját jelentik, amelyeknél új anyagokat használtak fel, mint a kevlár⁴⁴¹, az aramid⁴⁴² és a kerámia⁴⁴³.

A különleges védelemmel ellátott gépjárműveket különböző védettségi, illetve lövés/robbanás állósági osztályokba sorolták. Fontos hangsúlyozni, hogy nem mindig az egész gépjárműre értendő a védelmi képesség, hanem az alkalmazott anyagok védelmi képességére kell gondolni⁴⁴⁴.

Az új különleges védelemmel ellátott luxus limuzinok megfelelnek azoknak a legszigorúbb irányelveknek, amelyek a civil járművekre vonatkoznak. Számos speciális biztonsági felszereltség egészíti ki az egyébként is erős kiegészítő mechanikai védelmet. Ezek a gépjárművek minden hivatalos tanúsítvánnyal rendelkeznek, amelyek azt bizonyítják, hogy megfelelnek az elvárt biztonsági követelményeknek. A különböző tanúsító intézetek tesztelik a járművek lövedékálló, robbanásokkal szembeni ellenálló képességét. A gyártók pedig átfogó szerviz kínálattal és speciális tréningekkel támogatják vásárlóikat.

Taktikai elemek

A védett személyek a különböző helyszínek közötti közlekedésükhöz a legtöbb esetben gépjárműveket használnak. Az utazásbiztosítás végrehajtásához szükség van a megfelelő gépjárműflottára és az ehhez tartozó szerelő- és karbantartó személyi állományra. A gépkocsioszlopot a személybiztosítás parancsnoka határozza meg, állítja össze és irányítja. Az első gépjármű a rendőrségi felvezető gépjármű, amely feladata, hogy jelezze a többi közlekedő számára a zárt gépjárműoszlop közlekedését az adott útvonalon, valamint felderíti az útvonalat. A felvezető gépjármű után a protokoll gépjármű halad a szervezésért felelős személyekkel, amelyet a védett személy gépjárműve(i) és a biztonsági feladatot ellátó gépjárművek követik.

(5. számú melléklet: Utazásbiztosítás)

⁴⁴¹ <http://www.dupont.de/produkte-und-dienstleistungen/materialien-fasern-vliesstoffe/fasern/marken/kevlar/produkte/kevlar-acv.html> (Letöltve: 2013.10.29)

⁴⁴² http://portal.zmne.hu/download/bjkmk/bsz/bszemle2009/3/07_franggyorgy.pdf (Letöltve: 2013.10.29.)

⁴⁴³ http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/3/09_franggyorgy.pdf (Letöltve: 2013.10.29.)

⁴⁴⁴ A védelmi fokozatokat a DIN és az Euronorm szerint osztályozzák

A különleges védelemmel ellátott gépjárművek önmagában még nem biztosítják a védett személyek biztonságát. Ezért mindenképpen szükséges a kiegészítő intézkedések megtervezése és alkalmazása. A „gyárilag” épített különleges védelemmel ellátott gépjárműveket – általában – kormányzati szervek alkalmazzák.

A védelem biztosításához szükséges feltételek:

1. Kidolgozott védelmi terv
2. Kiképzett és begyakorlott biztonsági személyzet
3. Egyértelmű irányítás és vezetés
4. Fontosabb intézkedések:
 - > VIP⁴⁴⁵ program, „csak akire tartozik”,
 - > Biztonsági rendszerek folyamatos üzemeltetése,
 - > A terrorcselekmény helyének azonnali elhagyása, lezárása,
 - > Biztonsági szolgálatok tájékoztatása,
 - > Kiemelt biztonsági zónák védelmének megerősítése biztonsági személyzettel,
 - > Gépjármű- és személyi forgalom korlátozása, esetleges leállítása,
 - > Felkészülés a sérültek ellátására, mobil ellátópont telepítése,
 - > A terrorcselekmény helyszínén rekedt személyek (túszok) élelemmel és vízzel való ellátása.

3.7.2. Védelmi fokozatok

A rendészetért felelős miniszter⁴⁴⁶ joga és kötelessége a különböző fokozatok elrendelése, módosítása és visszavonása. A vállalatok védelmét biztosító normál biztonsági

⁴⁴⁵ Very Important Person (**VIP**) - különleges elbánásban részesítendő személy (vendég)

intézkedéseket a helyi vagy az országos biztonsági szervezetekkel együttműködve kell kidolgozni és végrehajtani.

A-fokozat: ha EU vagy NATO tagállamok ellen lehetséges terrorcselekmények általános fenyegetettsége áll fenn, amely jellege és nagysága előre nem meghatározható, illetve ha a körülmények nem indokolják a B-fokozat rendszabályainak teljes körű alkalmazását.

B-fokozat: ha EU vagy NATO tagállamban terrortámadást hajtottak végre vagy egy megnövekedett és jobban előrelátható terrorcselekmény fenyegetéséről van szó. Huzamosabb ideig is fenntartható, ha a várható cselekmény hatása kiszámíthatatlan, hogy érinteni fogja-e Magyarországot, azonban magasabb fokozat bevezetése nem indokolt.

C-fokozat: olyan ellenőrzött vagy részben ellenőrzött információk állnak rendelkezésre, melyek szerint valószínűsíthető magyarországi objektum(ok) vagy személy(ek) ellen irányuló valamilyen formájú terrorcselekmény közeli bekövetkezése, amelyről ellenőrzött információkkal rendelkezünk.

D-fokozat: akkor kell alkalmazni, ha terrorcselekmény történt vagy olyan információkat kap a hírszerzés, hogy egy meghatározott objektumban vagy személy elleni terrorcselekmény bekövetkezése nagyon valószínű. Ez azt jelenti, hogy a következő 24 órában valószínű egy terrortámadás. Ez esetben a fokozatot fenn kell tartani a felszámolás idejére vagy a fenyegetettségi szint fennmaradásáig.

ALPHA – SZÜKSÉGÁLLAPOT

Az ALPHA Szükségállapot általános figyelmeztetést akkor hirdetnek meg, ha felmerül a lehetősége egy terrortámadásnak, amely jellege és nagysága előre nem látható és a körülmények nem indokolják a magasabb fokú szükségállapothoz tartozó rendszabályok bevezetését. Adott esetben a BRAVO szükségállapot egyes elemeinek alkalmazására is van lehetőség. A végrehajtás ideje a feladat vételétől a 00:00 – 06:00-ig.

1. Intézkedés Minden munkatársat - beleértve a vagyónvédelmi személyzetet is - rendszeres képzések keretében figyelmeztetni kell, hogy az idegenek felé legyenek gyanakvóak. Különösen akkor, ha az öltözetükhöz nem illő táskát vagy megszokottól eltérő ruházati kiegészítőt viselnek, ha ismeretlen jármű van a vállalat területén vagy

⁴⁴⁶ Jelenleg a belügyminiszter (szerző megjegyzése)

közelében, elhagyott csomagot, táskákat, valamint a szokásostól eltérő eseményt észlelnek.

2. Intézkedés

A szolgálatban lévő biztonsági- vagy más ügyeleti rendszerben résztvevő munkatársaknak mindig elérhetőeknek kell lenniük. Ők intézkedhetnek az épületek és területek kiürítésére, valamint a robbanás vagy támadás színhelyének lezárására a rendelkezésre álló tervek alapján.

3. Intézkedés

Munkaidőn kívül az épületeket, irodákat és szekrényeket zárva kell tartani.

4. Intézkedés

Fokozott biztonsági ellenőrzést kell végrehajtani azon személyeknél és járműveknél, amelyek a vállalat minősített területeire és épületébe/biztonsági zónáiba lépnek/hajtanak be.

5. Intézkedés

A járművek és a személyek számára az áthaladási pontok számát csökkenteni kell.

6. Intézkedés

Szükség esetén a BRAVO szükségállapotból a veszélyeztetettség függvényében a következő rendszabályok valamelyikét alkalmazhatjuk:

(A). Minden épületet, irodát és szekrényt, melyek nincsenek rendszeresen használva, le kell zárni és rendszeresen ellenőrizni is kell. (14. Intézkedés)

(B). A folyamatosan használt épületeket/zónákat belül és kívül át kell vizsgálni, hogy van-e ott gyanús csomag vagy a megszokottól eltérő tevékenység. (15. Intézkedés)

(C). Minden az üzemi étkezdébe, kávézóba, stb. beszállított küldeményt, valamint a munkatársak csomagjait is át kell vizsgálni. (17. Intézkedés)

(D). A felsővezetés lakásainak, iskoláknak és más a vállalat területén kívül lévő védtelen („puha”) célpontoknak a

felügyeletét fokozni kell. Így növelhetjük az elrettentést és a munkatársak biztonságérzetét. (18. Intézkedés)

7. Intézkedés A terveket, a rendszabályokat, a biztonsági személyzetre vonatkozó adatokat és a logisztikai követelményeket, a magasabb szükségállapot bevezetéséhez kapcsolódó dokumentumokat felül kell vizsgálni.

8-9. Intézkedés Fenntartott

BRAVO SZÜKSÉGÁLLAPOT

BRAVO szükségállapotot hirdetnek ki, ha fokozott a terrorveszély és előrelátható terrorcselekmény fenyegetettsége áll fenn, viszont a célpontot nem lehet beazonosítani. A végrehajtás ideje a feladat vételétől 06:00 – 12:00-ig.

10. Intézkedés Az 1. Intézkedést végrehajtani és a biztonsági személyzetet figyelmeztetni kell a terrorista támadás esetleges formáira.

11. Intézkedés Minden ügyeleti rendszerbe tartozó munkatársnak, akik a terrorvédelmi terv végrehajtásában részt vesznek, készenlétben kell lennie.

12. Intézkedés A következő fokozathoz tartozó rendelkezések végrehajtásának terveit és feltételeit ellenőrizni kell.

13. Intézkedés A gépjárművek és szeméttárolók, stb. 50 m-nél közelebb nem lehetnek az épületekhez - különösen a biztonsági zónáknál -, ezért a tárolókat le kell szerelni, valamint a gépjárművek részére ki kell jelölni egy vagy több központi parkolót.

14. Intézkedés Minden épületet, irodát és szekrényt, melyek nincsenek rendszeresen használva, le kell zárni és rendszeresen ellenőrizni is kell.

15. Intézkedés A folyamatosan használt épületeket/zónákat belül és kívül át kell vizsgálni, hogy van-e ott gyanús csomag vagy a megszokottól eltérő tevékenység.

16. Intézkedés Minden postai küldeményt át kell vizsgálni az esetleges levél/csomag bombák ellen, ezzel kiegészítve a megszokott ellenőrzést.
17. Intézkedés Minden az üzemi étkezdébe, kázinba, stb. beszállított küldeményt, valamint a munkatársak csomagjait is át kell vizsgálni.
18. Intézkedés A felsővezetés lakásainak, iskoláknak és más a vállalat területén kívül lévő védtelen („puha”) célpontoknak a felügyeletét fokozni kell. Így növelhetjük az elrettentést és a munkatársak biztonságérzetét.
19. Intézkedés A bevezetett intézkedésekről és az általános helyzetről informálni kell a munkatársakat, így elkerülhetjük a rémhíreket és a pánikot.
20. Intézkedés A vállalat Válságkezelő szervezet tagjait időben kell informálni az akciókról/műveletekről és azok kiváltó okairól.
21. Intézkedés A vállalathoz belépő látogatók ruházatát, táskáikat és csomagjaikat át kell vizsgálni.
22. Intézkedés A biztonsági zónákat és környéküket, valamint az ott tartózkodó személyeket és járműveket véletlenszerű időpontokban kell ellenőrizni.
23. Intézkedés A szolgálati úton lévő munkatársakat figyelmeztetni kell arra, hogy őrzött parkolóban tárolják a járművet, indulás előtt alaposan vizsgálják át. Ezen intézkedés nem vonatkozik a VIP programokban résztvevő gépjárművezetőkre.
- 24-29. Intézkedés Fenntartott

CHARLIE SZÜKSÉGÁLLAPOT

A CHARLIE Szükségállapot alkalmazandó, ha egy incidens történt vagy olyan információkkal rendelkezünk, hogy valamilyen terrorcselekmény közeli bekövetkezése valószínűsíthető. A végrehajtás ideje a feladat

vételétől 12:00 – 24:00-ig.

30. Intézkedés ALPHA és BRAVO szükségállapot intézkedéseit fenn kell tartani.
31. Intézkedés Minden szakterület ügyeletesének, akik felelősek a Védelmi terv végrehajtásában, a szolgálati helyükön kell tartózkodniuk.
32. Intézkedés A belépési és behajtási pontok számát minimalizálni kell.
33. Intézkedés A beléptetés szabályait szigorúan kell végrehajtani. Minden járművet át kell vizsgálni, ami magába foglalja a technikai átvizsgálást is.
34. Intézkedés Alkalmazni kell a járművek központosított parkolását és csak a kijelölt helyen lehet parkolni.
35. Intézkedés Belépési pontonként minimum két fegyveres biztonsági őrt szükséges alkalmazni.
36. Intézkedés Fokozni kell a vállalat területén a járőrtevékenységet.
37. Intézkedés A vállalati kritikus infrastruktúra minden elemét kiemelten kell védeni, amelyek a vállalat területén belül vannak.
38. Intézkedés A műszaki akadályokat kell telepíteni a belépési pontoknál.
39. Intézkedés Fenntartott

DELTA SZÜKSÉGÁLLAPOT

A DELTA Szükségállapot alkalmazandó akkor, ha a terrorcselekmény már megtörtént vagy a hírszerzés olyan információkat kap, mely szerint egy bizonyos hely (objektum) vagy személyek elleni terrorcselekmény bekövetkezésének valószínűsége nagyon nagy. Ezt a szükségállapotot CSAK helyi riasztásként adják ki. A végrehajtás ideje a feladat vételétől 24:00 – 2. nap 24:00-ig.

40. Intézkedés ALPHA, BRAVO és CHARLEI szükségállapot intézkedéseit fenn kell tartani.
41. Szabály Az őrzés-védelmet meg kell erősíteni.

42. Intézkedés A vállalat területén lévő minden járművet azonosítani kell.
43. Intézkedés A vállalat területére minden belépő személyt és behajtó járművet át kell vizsgálni technikai eszközök alkalmazásával.
44. Intézkedés A kommunikációs hozzáférési pontokat folyamatosan ellenőrizni kell.
45. Intézkedés Látogatási tilalmat kell bevezetni.
46. Intézkedés Adott esetben a TEK átveszi a vállalat biztonsági szervezeteinek és a védelemi feladatok végrehajtásának irányítását.
47. Intézkedés Az épületek külső részét gyakori ellenőrzés alá kell vonni.
48. Intézkedés A szolgálati utakat lehetőség szerint minimalizálni kell.
49. Intézkedés Konzultáció a helyi hatóságokkal a vállalathoz vezető utak lezárásáról, amely terrortámadások szempontjából sebezhetővé teheti az objektumot.
50. Intézkedés Fenntartott

Védelem megszervezéséhez szükséges dokumentumok:

- > Térképek: A, B, C, D biztonsági intézkedések végrehajtásához.
- > Utasítások a biztonsági szervezetek részére:
 - SitCen Válságkezelési terve,
 - Őrzés-védelemi terv,
 - Létesítményi tűzoltóság beavatkozási terve,
 - Mentő- és Üzemorvosi szolgálat feladatterve,
 - Háztechnikai és épületfelügyelet feladatterve,
 - Számítástechnikai központ ügyeletesek feladatai,
 - Logisztikai feladatok biztosítási terve.
- > Erő és eszköz számvetés,
- > Híradás vázlat,

> Force Protection.⁴⁴⁷

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A fejezetben bemutattam, hogy egy nagyvállalat milyen sok szálon kapcsolódik az ország kritikus infrastruktúráihoz, melynek saját működési prioritásai (termelési/piaci/működési képesség) szinte teljes egészében leképezik az EU kritériumok szerinti elsődleges (energia ellátás, infokommunikáció, közlekedés) és az ágazati kritériumok szerinti NKIV szektorokat. Így a felsővezetés felelősségének szerves része a vállalati biztonsági stratégia és biztonságpolitika kialakítása és az érvényre juttatása. Ezt szakértők készítik elő a döntések meghozatalához azokat a kérdéseket, amelyek a KIV-re vonatkozó jogszabályi előírásokkal kapcsolatban, valamint a belső kritikus infrastruktúra és a termelési feltételek megengedhető kockázatokkal való működtetése során felmerülnek.

Nagyon fontos elemnek tartom, hogy a különböző „biztonsági szervezetek és hatóságok” egyformán értelmezzék a részükre meghatározott biztonsági- és védelmi feladatokat, azok kapcsolódási pontjait, valamint a kritikus infrastruktúrák létesítéséhez és működtetéséhez szükséges új biztonságtechnikai- és taktikai elemek alkalmazását. Ezekkel valósítható meg a kritikus infrastruktúrák integrált védelme. A biztonsági szakfeladatok jelentős részét belső erőkkel nem lehet gazdaságosan megoldani. Ezért szükséges külső erőforrások igénybevétele, amelyek rendelkeznek a nemzeti hatóságok által kiadott biztonsági minősítésekkel.

A mai magyar gazdaság kitettsége igen magas, mert a GDP 80%-át a TOP50 magyar vállalat állítja elő. Az 50 gazdasági társaságból „csak” 24 termelő vállalat. A további 26 - nem termelő - vállalat tartozik a kritikus infrastruktúrák sorába a 2080/2008. kormányhatározat 2. számú melléklete szerint.

Javaslom, hogy VIII. Ipar ágazat felsorolt gazdasági társaságok körét ki kell egészíteni azokkal a termelő vállalatokkal, amelyek a GDP legalább 2 %-át egy telephelyen állítják elő. Ezért tartom indokoltnak a jogszabály módosítását.

⁴⁴⁷ Erők (beavatkozó) védelme

Véleményem szerint egy nagyvállalat biztonsági szabályainak, előírásainak kidolgozásánál és biztonsági szervezeteinek kialakításánál maximálisan figyelembe kell venni az adott ország nemzeti biztonsági stratégiáját, valamint egy multinacionális vállalatnál az „anya” vállalat „worldwide”⁴⁴⁸ érvényes biztonsági intézkedéseit. A biztonsági és védelmi rendszerek tervezésénél, kiépítésénél és működtetésénél a vállalat biztonsági stratégiája az az alap dokumentum, amelyben meghatározzák a felsővezetés vállalatra vonatkozó közép- és hosszú távú biztonsági elvárásait.

A fejezet utolsó részében ismertettem azokat a törekvéseket, amelyek révén a terrorrobbantások és a terrortámadások biztonsági kérdéseit vizsgálhatjuk. Különös tekintettel a terrortámadások biztonsági kihívásaira a védelmi intézkedések végrehajtása során. Véleményem szerint ma Magyarországon az épületek/objektumok terrorrobbantások biztonsági/védelmi aspektusa nem kap a súlyának megfelelő figyelmet, mivel kutatásaim során sem találtam a témában jogszabályi háttérrel.

Ezért értekezésemben az amerikai tapasztalatokra és törvényszerűségekre alapozva olyan megoldási lehetőségeket kívántam bemutatni, amelyek integrált módon alkalmazható elemei révén hatékonyan végrehajthatóak a terrorrobbantások elleni védelem műveletei. A civil szféra terrortámadások elleni védekezéséről nincs jogszabály vagy iránymutatás, ezért dolgoztam ki a fejezet végén egy külön pontot az objektumok/épületek terrortámadások elleni védekezés általános elveinek megfogalmazására.

⁴⁴⁸ világszerte

4. FEJEZET: EGY NEMZETKÖZI VÁLLALATI HELYZETELEMZŐ ÉS VÁLSÁGKEZELŐ KÖZPONT MŰKÖDTETÉSE

4.1. HELYZETELEMZŐ ÉS VÁLSÁGKEZELŐ KÖZPONT

4.1.1. Vállalati válságkezelés elve

Válságkezelés

A krízis⁴⁴⁹ szót a korábbi civilizációkban orvosi szakkifejezésként használták. Napjainkban az angol nyelvből származó „crisis”⁴⁵⁰ kifejezést alkalmazzák, amely jelentése már átalakult és az általánosan jelentkező, a tömegeket hátrányosan érintő társadalmi problémák, események megnevezésére alkalmazzák.

A XX. század első felében történt világháborúk utáni korszakra a béke és stabilitás volt jellemző. Ez Európa történelmében példa nélkül álló időszaknak számít. A bipoláris világrend felbomlása után jelentek meg Európában a regionális konfliktusok és az ezek okozta válságok⁴⁵¹.

Európa fejlettségi szintje meghaladta és ma is meghaladja a világ átlagát, ezért érzékenyebben érinti az európai társadalmakat azok az események, amelyek befolyásolják az itt élő emberek komfort érzetét.⁴⁵² A krízist definiálhatjuk, mint az egyén, csoport vagy társadalom életében jelentkező működési zavart, amelyek lehetnek konfliktusok, válságok, katasztrófhelyzetek. Ezek a zavarok kihatnak a személyek és a csoportok biztonságérzetére⁴⁵³.

⁴⁴⁹ válság, fordulópont, görög, latin, orvosi

⁴⁵⁰ kritikus állapot, kialakult helyzet, válság

⁴⁵¹ Jugoszlávia felbomlása, Szlovénia és Horvátország kiválásával kezdődött 1991-ben, 2008-ban már hét utódállam volt az egykori Jugoszlávia területén. (szerző megjegyzése)

⁴⁵² Extrém időjárás, járványok, gazdasági válság, munkanélküliség, terrortámadások....

⁴⁵³ PATAKI János: *Az Európai Unió biztonság- és védelempolitikája, a tagállamok és Magyarország felajánlásai tükrében*, diplomamunka, Zrínyi Miklós Nemzetvédelmi Egyetem, 2007: „A biztonság nehezen meghatározható fogalom, meghatározza az állam biztonság politikája, valamint az állampolgárok olyan közösségének olyan biztonsági igényeit elégíti ki: mint a fizikai túlélés, gazdasági – politikai cselekvési szabadság. Nagyon leegyszerűsítve, „A FÉLELEM HIÁNYA”. A biztonság mindig valamilyen fenyegetés, veszély megjelenése kapcsán felmerülő igény. A biztonság végső soron értékek védelmét és biztonságát jelenti, amelyeket egy közösség tagjai elfogadnak, igényelnek és fontosnak tartanak.” Diplomamunka, Pataki

A XXI. század új kihívásokat, veszélyeket és kockázatokat hozott az egyének, a csoportok és a nemzetállamok vonatkozásában.⁴⁵⁴

Válságkezelés hadtudomány szerinti megközelítése

„Minden olyan intézkedés, amely a válság esetén arra irányul, hogy egy fegyveres konfliktus kialakulását, kiterjesztését megakadályozzuk, anélkül, hogy alapvető nemzeti érdekeinkről lemondanánk [...] körütekintő előkészületek után a döntések meghozatala. Ez utóbbiak célja a megfelelő politikai, diplomáciai, gazdasági és esetleg katonai lépések időbeni és összehangolt alkalmazása.”⁴⁵⁵

A nemzeti válságkezelés kormányzati feladat, amely alapját a Nemzeti Biztonsági Stratégia képezi. A különböző kormányzati szervek ezen elvek alapján dolgozzák ki saját irányelveiket/szakpolitikáikat.

A biztonság szavatolása kormányzati szintű feladatrendszer, amelynek meghatározó elemei a védelmi feladatokra felkészült és működőképes államigazgatás, a védelem- gazdaság feltételeinek megteremtése, a kor kihívásainak megfelelő polgári védelmi rendszer, a fegyveres erő és a biztonsági, rendvédelmi szervezetek/szolgálatok.

A válságreagáló műveletek/feladatok alapját a célok egyértelmű meghatározása, az egységesen kiépített, működtetett és hiteles vezetési rendszer, az egységes és rugalmas erő kifejtés, valamint az erők megóvásának biztosítása képezik.

Válságkezelő központok

A műveleteket a válságreagáló központokból irányítják, amelyek működésének alapját az információk⁴⁵⁶ gyűjtése, elemzése, értékelése és terjesztése, a döntések meghozatala, a feladatok meghatározása, a végrehajtás eredményeinek értékelése adja. A különböző

János, Biztonsági és biztosítási feladatok Magyarország az Európai Unió soros elnöksége idején 2011-ben, Zrínyi Mikós Nemzetvédelmi Egyetem, 2008.

⁴⁵⁴PATAKI János: *Az Európai Unió biztonság- és védelempolitikája, a tagállamok és Magyarország felajánlásai tükrében*, diplomamunka, Zrínyi Miklós Nemzetvédelmi Egyetem, 2007 „...A regionális stabilitást fenyegetik az erőszakos vagy lappangó konfliktusok, amilyeneket közvetlen környezetünkben is találhatunk. Emberi életet veszélyeztetnek, rombolják a szociális és anyagi infrastruktúrákat, fenyegetést jelentenek a kisebbségeknek, az alapvető szabadságjogok és az emberi jogok számára. A konfliktusok szélsőségekhez, terrorizmushoz és az állam működésképtelenségéhez vezethetnek, lehetőségeket biztosítanak a szervezett bűnözés számára.”... ,

⁴⁵⁵ KŐSZERGVÁRI Tibor: *A válságkezelés aktuális problémái*, Akadémiai közlemények, 1994, pp. 217

⁴⁵⁶ Felderítési és hírszerzési adatok

nemzetközi szervezetek és nemzetek rendelkeznek helyzetelemző központok rendszerével, ahonnan irányítják a válságreagáló műveleteket.

A NATO HQ SITUATION CENTER fő feladatai⁴⁵⁷

- > Válságok előrejelzése, a bekövetkezett események követése,
- > Felderítési adatok gyűjtése és értékelése,
- > Az adatok titkosított/zárt terjesztésének biztosítása,
- > A híradó központ működtetése és ellenőrzése,
- > Információk terjesztése „akire tartozik” elv betartásával,
- > Döntés-előkészítés támogatása,
- > Direktívák előkészítése, tervezése és támogatása.

EU INTCEN⁴⁵⁸ feladata:

- > A bekövetkezett események nyomon követése az EU érdekszférájában,
- > Hírszerző beszámolók készítése,
- > A hírszerzési információk feldolgozása és terjesztése válsághelyzetben,
- > Jelentések és helyzetértékelések készítése országokról és térségekről, ahol az EU műveleteket hajt végre.

EU SITUATION ROOM⁴⁵⁹

Az EU érdekszférájában történt események globális, átfogó és időszerű értékeléséhez szükséges információk gyűjtése, értékelése és terjesztése az érintett európai intézmények számára.

A Helyzetelemző „Részleg” 7/24⁴⁶⁰ működési rendje lehetővé teszi, hogy világszerte nyomon kövesse a kialakult helyzetet és időben felismerje a potenciális válságforrásokat. A SITUATION ROOM az elsődleges információs központ az európai intézmények és a tagállamok számára, valamint folyamatos kapcsolatot tart fenn az EU-műveleti egységeivel és a nemzetközi szervezetekkel.

⁴⁵⁷ NATO HQ Situation Centre (SITCEN), Security Standard Operating Procedures (SOPs), Revision 1. 16 February 2010, „NATO UNCLASSIFIED”, – a szerző birtokában

⁴⁵⁸ EU Intelligence and Situation Centre

⁴⁵⁹ Helyzetelemző „Részleg”), http://www.eeas.europa.eu/crisis-response/what-we-do/eu-situation-room/index_en.htm (Letöltve: 2015.10.12.)

⁴⁶⁰ az év minden napján 24 órában áll rendelkezésre

SITUATION ROOM feladatai:

- > Folyamatosan figyelemmel kíséri a világszerte történő eseményeket, amelyek jelentős hatással vannak az Európai Unióra és tagállamaira,
- > Folyamatos kapcsolattartás az EU misszióival és műveleti erőivel,
- > Támogatja az EU intézményrendszerét,
- > A politikai döntéshozatal előkészítése,
- > Eleme az EU integrált válságkezelési folyamatainak (IPCR),⁴⁶¹
- > Folyamatos kapcsolatot tart fenn és összehangolja a tagállamok nemzeti válságkezelő és válság koordinációs központjait,
- > Kapcsolatban áll a regionális és a nemzetközi szervezetek válságkezelő szervezeteivel és központjaival.

Megítélésem szerint a NATO és az EU helyzetelemző központjaiban alkalmazott módszerek alkalmazhatóak a civil szférában hasonló feladatokkal megbízott szervezeteknél, azzal a kitételrel, hogy a civil központok csak nyilvános források⁴⁶² felhasználásával működhetnek.

4.1.2. SitCen szervezeti felépítése és feladatai

Nemcsak a folyamatosan változó világ nehezíti meg a nemzetközi nagyvállalatok helyzetét, hanem az a tény is, hogy a nemzetközi rendszerben a nem kormányzati szereplők (nGO) száma évről évre nő. Ma már nem elég csak megfelelni az általános gazdasági és közgazdasági törvényszerűségeknek, hanem megkülönböztetett figyelmet kell fordítani az aktualitásokra, a piac ágazati politikájára, stratégiájára, kapcsolataira, és mindezt be kell illeszteni egy komplex és folyamatosan változó környezetbe.

Egy nagyvállalatnak már nem csupán a szakmai szempontok, hanem a trendek ismerete alapján kell döntenie. Számítania kell váratlanul felbukkanó lehetőségekre, fenyegetésekre, amelyek mind több bizonytalansági tényezőt jelentenek. Így a döntések megvalósításának kockázata megsokszorozódik.

⁴⁶¹ Integrated Political Crisis Response – Integrált Politikai Válságkezelés

⁴⁶² OSINT

Ennek következtében megnövekedett az információvédelem szerepe a döntéshozatali mechanizmusokban. Információk hiányában a nagyvállalat egyre kevésbé tud hatékonyan reagálni az előre nem látható eseményekre, vagyis nehezebb felkészülnie a jövő kihívásaira.

SitCen

A nap 24 órájában, a hét 7 napján kell működtetni a SitCen-t. Ha a világ bármely pontján történik egy esemény, katasztrófa vagy más veszélyhelyzet keletkezik, az kihathat a vállalat biztonságos működésére és a piacok megtartására. A SitCen munkatársai rögzítik az információkat, ezzel egyidejűleg tudják teljesíteni riasztási és jelentési kötelezettségüket.

A rendelkezésre álló információk alapján el tudják dönteni, hogy milyen üzleti egységet érinthet, illetve érdekelhet az információ. Az információforrások lehetnek a különböző mértékadó hírportálok és televízió csatornák. Természetesen szükség lehet tolmácsok alkalmazására is, ha a hírforrás megértéséhez szükséges a szakszerű fordítás. Ezért elkerülhetetlen ezen személyek részére a készenléti szolgálat elrendelése.

A fontos információkat azonnal továbbítani kell. A SitCen rendelkezésére áll minden kommunikációs csatorna (telefon, fax, e-mail, rádió...). Természetesen a minősített információkat csak kódolt vagy védett vonalon lehet továbbítani.

A SitCen munkatársai értesítik a Riasztási tervben megadott esetekben az érintett személyeket és döntésük alapján összehívja a már előre kijelölt válságkezelő szervezetet.

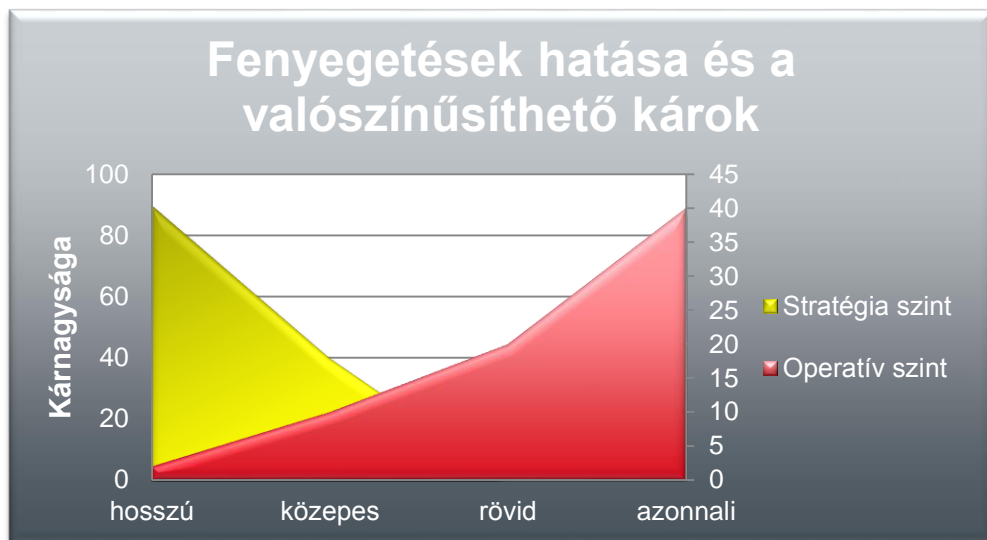
A SitCen alárendeltségébe tartoznak a különböző külső objektumok alközpontjai.

Egy multinacionális vállalatnál javasolt a különböző telephelyeken SitCen-eket telepíteni és üzemeltetni, amelyek működtetését egy elfogadott és egységesen alkalmazott módszer alapján kell szervezni.

4.1.3. Válságkezelő szervezetek felépítése és feladatai

A multinacionális vállalatoknál fontos feladat a válsághelyzetek időbeni felismerése, kezelése, megoldása és azok felszámolása. A válságok kialakulásánál mindig a legrosszabb alternatívával számolunk, így a megelőző intézkedésekkel megakadályozható vagy mérsékelhető a fellépő kár mértéke. A valószínűsíthető válságok befolyásolhatják a vállalat stratégiai döntéseit és biztonságos működését. A XXI. században egy multinacionális vállalat sem működhet eredményesen Biztonsági rizikó menedzsment nélkül. A kor kihívásait és fenyegetéseit a hagyományos vállalati kockázatelemzési szervezetek már nem képesek kezelni és feldolgozni. A tervezett beruházások pénzügyi értékeléséhez és a jogi kockázatok meghatározásához szükséges a biztonság- és védelempolitika tudomány eredményeinek figyelembevétele, amelyek számolnak a globális, regionális és helyi politikai stabilitással, a lehetséges környezeti kockázatokkal és az egyéb más biztonsági kihívásokkal.

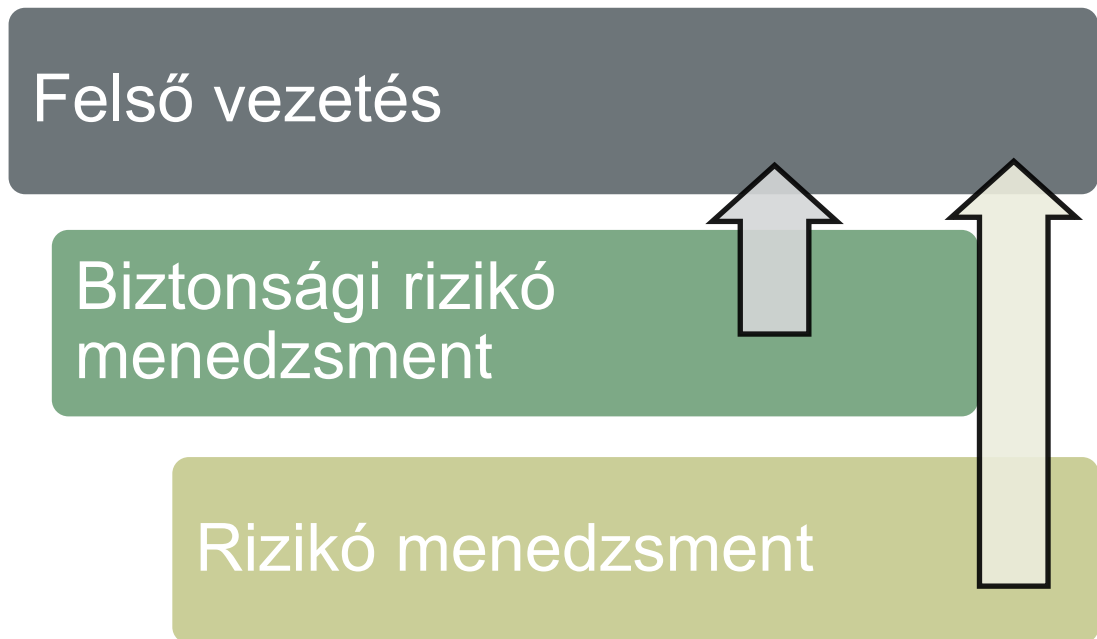
Egy nemzetközi nagyvállalatnál a válságkezelést két szinten célszerű megvalósítani és számításba kell venni a bekövetkezés valószínűségét és a várható kár nagyságát.



14. számú ábra, Fenyegetések hatása a valószínűsíthető károk, a szerző szerkesztésében

Stratégiai szintű válságkezelés

Egy nemzetközi nagyvállalatnál a hosszú távú, folyamatosan fennálló fenyegetések⁴⁶³ bekövetkezésének valószínűsége a legkisebb, de a várható kár nagysága magas és hosszútávon befolyásolja a vállalat működőképességét és jövedelmezőségét. Ezen fenyegetések elemzését és értékelését a vállalat Biztonsági rizikó menedzsment hajtja végre.



15. számú ábra: A vállalat válságkezelő szervezetei, a szerző szerkesztésében

Operatív (napi) szintű válságkezelés

Az azonnal jelentkező veszélyek csak rövid ideig befolyásolják a vállalat működését és a károk nagysága a legrosszabb esetben is közepes szinten realizálódik, amelyet a megfelelő biztonsági és védelmi intézkedések mellett, kiegészítő biztosításokkal⁴⁶⁴ lehetséges kompenzálni. Az azonnali vészhelyzetek kezelése a Krízismenedzsment felelőssége és feladata.

Biztonsági rizikó menedzsment A hosszú távú tervezés jelenti az előre nem látható, a jövőben várható eseményekre való felkészülést és a megfelelő előzetes tervek elkészítését

⁴⁶³ Globális kihívások, fenyegetések, (lásd: 1. számú ábra)

⁴⁶⁴ Általános- és felelősség biztosítás

azokra az eseményekre, amelyek zavarják a vállalat biztonságos üzletmenetét. Ez magába foglalja az átfogó, koordinált és döntési folyamatokat, amelyek részei a menedzsment folyamatoknak. A hosszú távú tervezést az előre elkészített forgatókönyvek tartalmazzák.

Cél

A Biztonsági rizikó menedzsment célja a különböző nemzetközi szervezetek és intézetek hosszú távú előrejelzéseinek folyamatos követése, a kiadott tanulmányok értékelése és trendek meghatározása, amelyek hosszú távon befolyásolhatják a nagyvállalat fejlesztéseit és működését.

Felhatalmazás

A vállalat felsővezetésének elnökének döntése alapján a Biztonság- és védelempolitika vezetője koordinálja a Biztonsági rizikó menedzsment működését, javaslatait a felsővezetésen keresztül adja ki az üzleti egységek részére utasítás vagy iránymutatást formájában.

Felelősség

A Biztonsági rizikó menedzsment felelős a stratégiai szintű kihívások elemzéséért és értékeléséért, a stratégiai szintű tervezésért, a biztonsági intézkedések és projektek kezdeményezéséért, indításáért és ellenőrzéséért. A Biztonsági rizikó menedzsment egy ideiglenes szervezet, melyet a Biztonság- és védelempolitika szakterület vezetője irányít és egy lehetséges válság esetén a felelős szakterület javaslatára hív össze. Tagjai a különböző szakterületek vezetői és bizonyos esetekben az érintett üzleti egység első számú vezetője.

Szervezeti kapcsolat

Olyan folyamatos kapcsolattartás, amely a magyarországi biztonsági szervezetek és intézetek, valamint a konszern más országokban lévő telephelyein működő biztonsági szervezetei között valósul meg.

Biztonsági rizikó menedzsment szervezeti felépítése, összetétele:

- > Biztonság- és védelempolitika vezetője,
- > Munkavédelem vezetője,
- > Környezetvédelem vezetője,
- > Egészségmenedzsment vezetője,
- > IT-biztonság vezetője,
- > Érintett üzleti egység első számú vezetője (opció).

Biztonsági rizikó menedzsment feladatai:

- > A vállalatot érintő globális trendek meghatározása évente,
- > A vállalat biztonsági stratégiájának évenkénti felülvizsgálata,
- > Negyed éves összefoglaló jelentések készítése a vállalat felsővezetés részére,
- > A bekövetkezett eseményekről előzetes helyzetértékelő jelentések készítése,
- > Összefoglaló jelentések és javaslatok tétele a felsővezetés részére.

Biztonsági rizikó menedzsment működési rendje és módszerei⁴⁶⁵:

- > Probléma felismerését a SitCen munkatársai hajtják végre,
- > SitCen munkatársainak feladata a helyzet tisztázása kapcsán:
 - Mi van?
 - Mi várható?
 - Információk gyűjtése, visszaellenőrzése (belföld, külföld).
- > Azonnal alkalmazandó rendszabályok
 - Szakterület vezető informálása,
 - Szakterület vezető informálja a Biztonság- és védelempolitika vezetőjét és elrendelik vagy nem a BRM összehívását,
 - További információk gyűjtése, informálás,
 - Szakterület vezetőinek beérkezése, egyeztetés,
 - Kríziskommunikáció, média első tájékoztatása (opció).
- > Időszámvetés készítése,
- > Helyzet megítélése, probléma feldolgozása, elemzése,
- > Célkitűzések meghatározása:

⁴⁶⁵ WALKER, W.E.: *The use of scenarios and gaming in crisis management planning and training*, (RAND 1995) p.7, <https://www.rand.org/content/dam/rand/pubs/papers/2009/P7897.pdf> (Letöltve: 2015.09.21.)

- Mit akarunk elérni?
 - Mit akarunk elkerülni?
 - A helyzet kulcsának megfogalmazása
 - Kríziskommunikáció, média második tájékoztatása (opció).
- > Cselekvési változatok kidolgozása
 - Legjobb,
 - Legvalószínűbb,
 - Legrosszabb, mindig erre tervezünk!
 - > Utasítások / javaslatok kidolgozása, kiadása:
 - Döntés, koordináció,
 - Tervezés.
 - > Végrehajtás ellenőrzése.

Krízismenedzsment⁴⁶⁶

Feladata

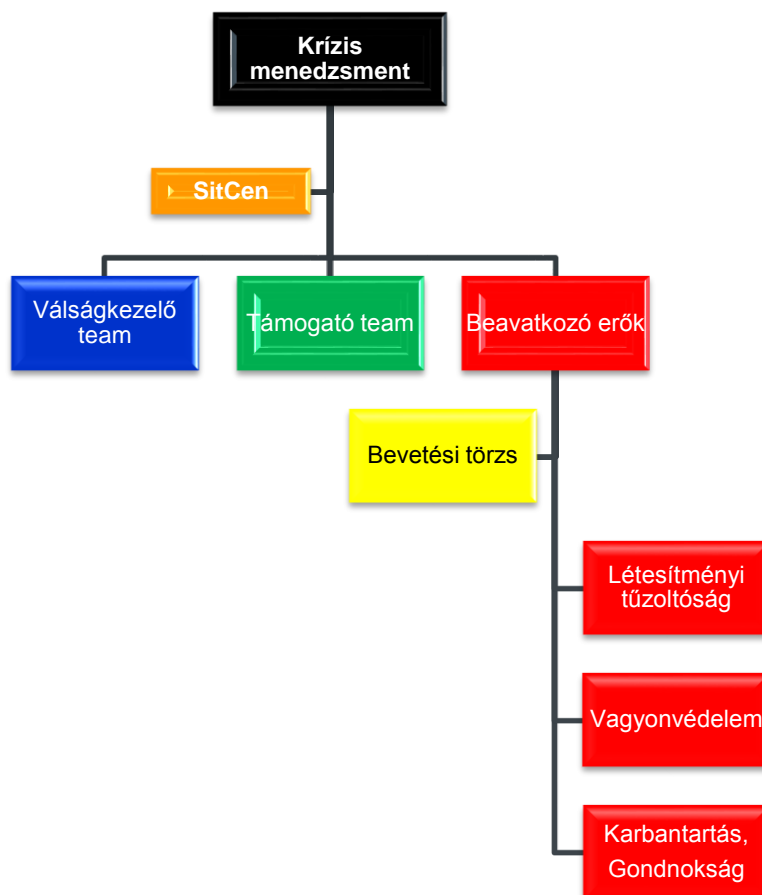
Az előre nem látható események és katasztrófák hatásainak csökkentése, megelőzése, felszámolása, valamint az eredeti helyzet visszaállítása.⁴⁶⁷

Célja

Megfelelő megelőző intézkedések alkalmazásával az előre nem látható eseményekkel, katasztrófákkal járó személyi sérüléseket és anyagi károkat a lehetséges szinten minimalizálja és azok előfordulásának lehetőségét lecsökkenti.

⁴⁶⁶ BARLAI Róbert – KŐVÁGÓ György: *Krízismenedzsment, kríziskommunikáció*, © Századvég Kiadó, 2004, pp. 366

⁴⁶⁷ ISO 31000: Risk management – Principles and guidelines



16. számú ábra: A vállalat Krízismenedzsmentje, a szerző szerkesztésében

Krízismenedzsment vezető feladata

- > Folyamatos riaszthatóság biztosítása és ennek ellenőrzése,
- > Dönt a katasztrófahelyzet kihirdetéséről,
- > Dönt a Válságkezelő vagy Támogató team összehívásáról,
- > Dönt a külső Beavatkozó erők bevonásáról,
- > Irányítja a krízis kommunikációt,
- > Kihirdeti a katasztrófahelyzet végét.

Válságkezelő team

A Válságkezelő team specialistákból áll, akiket esemény bekövetkezése esetén a Krízismenedzsment vezető döntése alapján a SitCen munkatársa értesíti ki. A specialisták

szakmai ismereteik segítségével, megfelelő előkészítés után tanácsokkal támogatják a Krízismenedzsment vezetőjét a gyors és megbízható döntések meghozatalában.

SitCen szolgálatban lévő munkatársai irányítják a Beavatkozó erőket⁴⁶⁸ a Krízismenedzsment vezetőjének beérkezéséig.

A Válságkezelő team támogatja a Krízismenedzsment vezető feladatának végrehajtásában és megoldásokat dolgoz ki az okozott károk felszámolására, a káresetek behatárolására, a vállalat működőképességének fenntartására. A team az eredeti helyzet visszaállításáig működik.

Válságkezelő team tagjai:

Vezető: Biztonsági menedzsment vezetője

Tagjai:

- > Katasztrófavédelmi/ Iparvédelmi ügyeletes,
- > Tűzvédelmi ügyeletes,
- > Vagyonvédelmi ügyeletes,
- > Munkavédelmi ügyeletes,
- > Egészség menedzsment ügyeletes,
- > Környezetvédelmi ügyeletes,
- > Épületkarbantartás ügyeletes,
- > Személyügyi ügyeletes,
- > IT-biztonság ügyeletes,
- > Központi logisztika ügyeletes,
- > Kommunikációs osztály ügyeletes.⁴⁶⁹

Támogató team feladatai:

- > Alaprendeltetésből adódó legfontosabb feladata az eredeti helyzet visszaállításának megkezdése,
- > A Krízismenedzsment vezető tanácsokkal való támogatása,

⁴⁶⁸ döntési jogkörrel

⁴⁶⁹ Krízis kommunikáció

- > Az esemény, katasztrófa helyzet folyamatos figyelemmel kísérése,
- > Minden válsághír és jelentés gyűjtése, vizsgálata és továbbítása az érintetteknek,
- > Helyzetértékelő megbeszélések szervezése,
- > A munkafolyamatok irányítása és a szükséges dokumentumok elkészítése (jegyzőkönyvek),
- > Külső tanácsadók bevonása (opció),
- > Biztosítja az információ áramlást a felső vezetés és a Krízismenedzsment vezető között.

A Támogató team a következő területek munkáját irányítja:

- > Személyügy,
- > Érintett üzleti egységek,
- > Logisztika és ellátás,
- > Kommunikáció.

Beavatkozó erők vezetője⁴⁷⁰

- > Beavatkozó erők vezetőjét a Krízismenedzsment vezető jelöli ki, akinek személyét az esemény vagy a katasztrófa helyzet jellege és hatásai határozzák meg,
- > Beavatkozó erők vezetője a helyszínen megszervezi a Beavatkozó erők és egységek feladatait, a katasztrófa helyzet felszámolását,
- > Beavatkozó erők vezetőjét feladatának végrehajtásában egy Bevetési törzs támogatja, amelybe folyamatosan a szakmai támogatás érdekében további szakembereket is bevonhat,
- > A Bevetési törzs közvetlenül a Beavatkozó erők vezetőjének van alárendelve.

Bevetési erők, egységek

Egységek alatt mindig egy olyan ideiglenes szervezeti egységet kell érteni, amelynek összetételét a feladat határozza meg. A Bevetési erők azok az egységek, akik megkezdik a kialakult helyzet felszámolását. A Krízismenedzsment vezetőnek vannak alárendelve és a Beavatkozó erők vezetője támogatja alkalmazásukat. A Beavatkozó erők vezetője irányítja a kárhelyen tartózkodó szakemberek feladatait.

⁴⁷⁰ A helyszínrre kiérkező szervezet vezetője/parancsnoka

Az egységek belső vagy külső erőkkel történő megerősítését a Krízismenedzsment vezető határozza meg a Beavatkozó erők vezetője javaslata alapján.

Riasztás módjai

- > A Riadó tervtől csak a Krízismenedzsment vezető térhet el. Ez nem zárja ki azt, hogy a különböző a Beavatkozó erők már más riasztások alapján⁴⁷¹ a helyszínen legyenek,
- > A Riadó terv biztosítja, hogy a Krízismenedzsment tagjai bármikor riaszthatóak legyenek,
- > A riasztást a SitCen hajtja végre,
- > A riaszthatóság folyamatos biztosítása érdekében, a Riadó tervben történt változtatásokat és kiegészítéseket a SitCen-nel írásban kell tudatni.

Krízismenedzsment helységeinek védelme

A Krízismenedzsment védelmét az integrált biztonsági koncepció alapján kell tervezni, szervezni, kiépíteni és működtetni. A biztonsági koncepciónak biztosítani kell, hogy csak a megfelelő jogosultsággal rendelkező személyek léphetnek a Krízismenedzsment helyiségeibe.

Már a tervezés fázisában figyelembe kell venni a vonatkozó jogszabályokat, szabványokat és egyéb belső előírásokat, irányelveket. A Krízismenedzsment biztonsága érdekében a vállalatoknál a legmagasabb szintű védelmet kell biztosítani részére.

SitCen funkciói:

- > Információk gyűjtése,
- > Információk kezelése,
- > Médiafigyelés,
- > Elemzés,
- > Várható kihatások felmérése,
- > Szakértők bevonása,
- > Információk szolgáltatása a döntés előkészítéshez,

⁴⁷¹ Tűzjelzés, munkatársi bejelentés, stb. ...

- > Koordináció,
- > Kapcsolattartás,
- > Értesítés, riasztás,
- > Működési feltételek fenntartásának biztosítása és ellenőrzése.

4.2. HELYZETELEMZŐ ÉS VÁLSÁGKEZELŐ KÖZPONT RENDSZEREI

4.2.1. Biztonsági rendszerek felügyelete

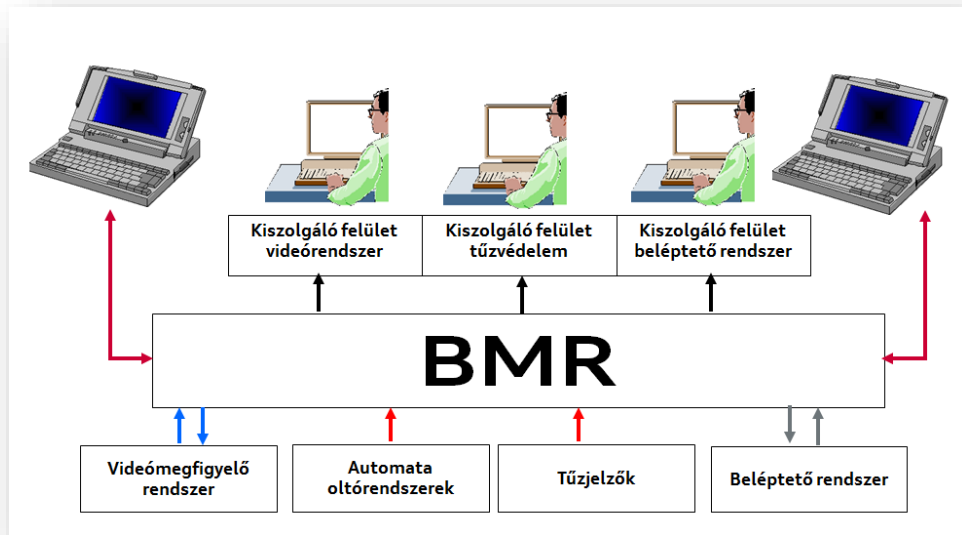
A SitCen-be kell telepíteni az integrált biztonsági rendszereket. Az összekapcsolt rendszerek egy lényegesen magasabb szintű biztonságot tudnak megvalósítani. Így az ott szolgálatot teljesítő személyi állomány leterheltsége csökken és költséghatékonyabb módon teljesülhetnek a biztosítási és védelmi feladatok.

Telepített biztonsági rendszerek:

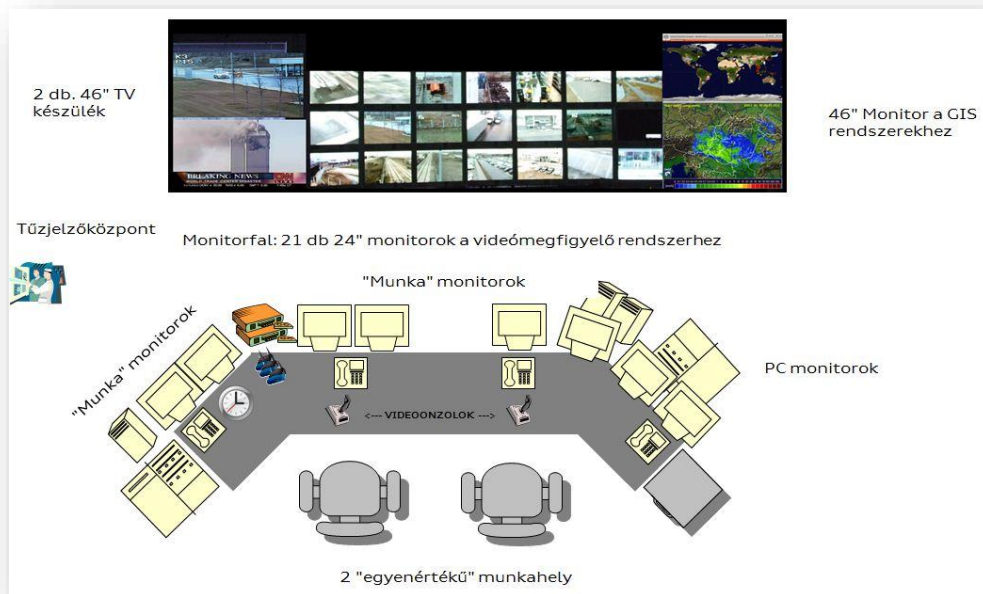
- > A Biztonsági Management Rendszer, ami a legmagasabb integrációja a különböző biztonsági rendszereknek,
- > Univerzális veszély- és tűzjelzőrendszerek,
- > Videó megfigyelő berendezés az objektum területének, környezetének, kerítésének és a bejáratainak megfigyelésére és ellenőrzésére,
- > Belépés ellenőrző rendszer,
- > Gépjármű behajtás ellenőrző rendszer,
- > Behatolásjelző rendszerek,
- > Látogató nyilvántartó rendszer,
- > Járórellenőrző rendszer,
- > EDR,
- > Biztonsági hangos bemondó (riasztó rendszer⁴⁷²) rendszer,
- > A telefonkészülékek (vállalati hálózat) mint fő kommunikációs eszközök,

⁴⁷² Például sziréna és/vagy hangszóró

- > Telefon (külső, a száma titkosított), direkt fő csatlakozással a nyilvános telefonhálózathoz,
- > Vészvilágítás és a szünetmentes tápegység felügyelő rendszer,
- > Pánik és segélykérő jelzések fogadása.



17. számú ábra: SitCen biztonsági rendszereinek kapcsolata, a szerző szerkesztésében



18. számú ábra: SitCen munkahelyek kialakítása, a szerző szerkesztésében

A külön-külön működő (elszigetelt) biztonsági rendszerek alkalmazása nem felel meg a XXI. században a biztonsági rendszerekkel szemben támasztott követelményeknek. Egy vészhelyzetben az emberi hibák csökkenthetőek a biztonsági rendszerek integrálásával, mert a rendszer telepítésénél a „leendő” felhasználók definiálják elvárásaikat a tervező részére.

Előre meghatározásra kerül:

- > A különböző rendszerek riasztó és hiba jelzéseinek a felhasználó általi prioritizálhatósága
- > Megjelenítés formái:
 - Riasztás „szöveges” formában,
 - Grafikusan: minimum 2 méretben,
 - A riasztás helyén tárolt anyagok felsorolása, különös tekintettel a veszélyes anyagokra,
 - Az ott tartózkodók létszáma,
 - Beavatkozási tervek megjelenítése.
- > Automatikus riasztások meghatározása (Kit, mikor, hogyan, milyen esetekben?)

SitCen munkatársak feladata jelzések vétele esetén:

- > Vészjelzés értelmezése,
- > Beavatkozó erők riasztása,
- > Az érintett területen tartózkodók értesítése,
- > Egyéb riasztási feladatok végrehajtása,
- > Beavatkozó erők irányítása és támogatása,
- > Esemény dokumentálása a rendszerben,
- > Előzetes jelentés összeállítása,
- > Jelentés a beavatkozás befejezéséről az üzleti egységek vezetőinek.

Az integrált biztonsági rendszerek alkalmazásával hatékonyan és gyorsan értékelhetőek a riasztások, mert a vészjelzések automatikusan már kiértékelődnek, így csökkenthetőek az emberi hibák és elkülöníthetőek a különböző „alrendszerek” téves jelzései is. A riasztások feldolgozása előre definiált folyamat, amit az adott felhasználó a rendszerbe való

bejelentkezéskor meghatároz. Így a munkatársaknak lépésről lépésre kell a logikailag már meghatározott feladatokat végrehajtani. Ezzel elkerülhető a munkatársak rossz döntése.

4.2.2. Térinformatikai⁴⁷³ és egyéb információs rendszerek alkalmazása

A válságkezelés alapja a megfelelő és időszerű információk rendelkezésre állása, amely segítségével végrehajtható a veszélyek felderítése, beazonosítása és az információk terjesztése.

A térinformatikai rendszerek modellezésével készíthetünk előre kidolgozott védelmi terveket, scenáriókat, jelzéseket és kiadhatunk figyelmeztetéseket, riasztásokat.

Ezen rendszerek segítségével készíthetünk közép- és hosszú távú kockázati modelleket és szimulációkat, amelyek alapján trendeket tudunk meghatározni.

Behatárolhatjuk a lehetséges veszélyforrások okait és helyét, amelyet megjeleníthetünk tematikus térképen vagy légi(űr) felvételeken.

A veszélyt (riasztást) ábrázoló térképeket az interneten nem mindig egységes formában érhetőek el. Digitális térképek alkalmazásával készíthetünk térmodelleket (DTM)⁴⁷⁴. Egy adott területről több tematikus térképet „rétegenként”⁴⁷⁵ egymásra helyezve kaphatunk egy „általános” veszélyforrás térképet.

A SitCen-ben leggyakrabban használt térinformatikai és vészhelyzeti térképek:

- Global Incident Map, <http://www.globalincidentmap.com/>
- RSOE EDIS - Emergency and Disaster Information Service, <http://hisz.rsoe.hu/alertmap/index2.php>
- OKF: Rendkívüli események Magyarország területén, http://www.katasztrofavedelem.hu/index2.php?pageid=lakossag_esemeny_terkep
- OMSZ⁴⁷⁶: Vészjelzés, riasztás <http://www.met.hu/idojaras/veszelyjelzes/riasztas/>
- Időkép: Radarkép, riasztás: <https://www.idokep.hu/radar>

⁴⁷³ tér(geo)informatikai rendszer

⁴⁷⁴ DTM: Digital Terrain Modell, digitális térmodell

⁴⁷⁵

⁴⁷⁶ Országos Meteorológiai Szolgálat

- OVF⁴⁷⁷: Árvíz-, belvízvédelmi készültségi fokozatok:
<http://www.vizugy.hu/?mapModule=OpArviz&mapData=ArvizTajekoztatok>
- Útinform: Magyar Közút Nonprofit Zrt., <http://www.utinform.hu/terkep>
- Stb. ...

4.2.3. Riasztási feladatok

Nyilvános információ források lehetnek a vállalat számára a különböző mértékadó hírportálok és televízió adók. Természetesen szükség lehet tolmácsok alkalmazására is, ha a hírforrás megértéséhez szükséges a szakszerű fordítás. Ezért elkerülhetetlen, hogy ezen személyek részére készenléti szolgálatot rendeljenek el.

A rendelkezésre álló információk alapján lehet eldönteni, hogy milyen szervezetet érinthet, illetve érdekelhet az információ. Ha globális kihívásokat vagy regionális fenyegetéseket észlelnek, abban az esetben ez stratégiai szintű válságkezelést igényel. A Biztonság- és védelempolitika vezetőjét kell értesíteni és ő dönt a Biztonsági rizikó menedzsment esetleges összehívásáról, kiértékeléséről (6. számú ábra, A válságkezelés folyamata).

A helyi (lokális) események esetén (baleset, tüzeset, katasztrófahelyzet, környezeti károsodás... stb.) a Biztonsági menedzsment vezetőjét kell értesíteni, aki dönt az operatív Válságkezelő team vagy Krízismenedzsment összehívásáról. A válságkezelő team-be bevont szakterületek ügyeleti rendszert tartanak fenn (7. számú ábra, A vészhelyzetkezelés folyamata).

Riasztási feladatok:

- Legyenek felkészülve a hatáskörükbe utalt szolgálatok riasztására, ellenőrizzék az alárendelt szolgálatok ilyen irányú felkészültségét
- Folyamatosan tartsák nyilván a Biztonsági menedzsment vezetőjének, helyettesének és a területek (szervezetek) vezetőinek tartózkodási helyét
- Tartsanak állandó összeköttetést az alárendelt szolgálatokkal és a szakterületek ügyeleteseivel

⁴⁷⁷ Országos Vízügyi Hatóság

4.3. SitCen VÉDELME⁴⁷⁸

A vállalat biztonsági stratégiájában meghatározott biztonsági filozófiája alapján kell az integrált védelmi rendszert kiépíteni a lehetséges fenyegetések, a felmerülő költségek figyelembe vételével, amely mellett azonban a megfelelő szintű védelmet is biztosítani kell. A megfelelő védelmi szint kialakításának célja, hogy csökkentse a lehetséges kockázatokat.

A SitCen biztonságos működésének előfeltétele annak védelme. Az integrált biztonsági koncepció alapján kell a SitCen védelmét tervezni, szervezni, kiépíteni és működtetni. A SitCen Védelmi terve biztosítja az információk és anyagai javak biztonságát az engedély nélküli behatolókkal, a jogosulatlan információ szerzéssel és más elkövetőkkel szemben.

A tervezés fázisában a „biztonsági piramisnak” megfelelően a vonatkozó jogszabályok, szabványok és egyéb belső előírások és irányelvek alapján kell meghatározni a védelmi szinteket. A SitCen biztonsági besorolásának a vállalatoknál a legmagasabb szintűnek kell lennie, amelyet egy előzetes rizikó- analízis alapján határozunk meg.

4.3.1. Szervezeti intézkedések

A SitCen olyan terület, ahol Bizalmas és TITKOS minősítésű információkat kezelnek és tárolnak, a vállalat biztonsági rendszereit irányítják és ellenőrzik, valamint válság helyzetekben irányítják a Beavatkozó erőket.

A megvalósítás során szükséges a jövőbeli használó (megrendelő) folyamatos jelenléte, hogy ellenőrzött legyen a tervekben meghatározottak megvalósulása, valamint az, hogy „egyéb más eszköz”⁴⁷⁹ ne kerüljön beépítésre.

A védelem első lépcsője az adminisztratív védelem, amely magába foglalja a vonatkozó törvényi előírásokat, rendeleteket, szabványokat, az egész vállalatra vonatkozó irányelveket és utasításokat, a Biztonsági menedzsment vezetője által jóváhagyott szabályzatokat és munkautasításokat, valamint az adott szolgálati helyre és feladatokra vonatkozó folyamatokat.

⁴⁷⁸ A Helyzetelemző és Válságkezelő Központ védelménél kiemelten fontos a „3.3.2.Általános biztonsági intézkedések” pontban felsorolt biztonsági elemek következetes megvalósítása, p.

⁴⁷⁹ Lehallgató, megfigyelőrendszerek ...

A szakmai feladatok eredményes végrehajtása érdekében szükséges, hogy az együttműködő SitCen-ek személyi állománya egységesen értelmezze a biztonsági feladatokat és szabályokat.

Parkolási módok

Parkolni a SitCen közvetlen környezetében csak a Biztonsági menedzsmenthez tartozó szolgálati és bevetési gépjárművekkel lehet. A gépjárművek műszerfalára ki kell helyezni a gépjárművek parkolási engedélyét és azok részére saját parkoló helyet kell kijelölni. Ez elsősorban a lehallgatások és terrorcselekmények megelőzését szolgálja.

Növényzet

Sűrű bokrokat, futónövényeket az épület közvetlen közelében alacsonyra kell vágni, hogy csökkentsék a lehetőségét az illetéktelen behatolók rejtőzködését. A fákat az épület környezetében úgy kell telepíteni, hogy a fákról ne lehessen az épület ablakain és egyéb nyílásain behatolni, továbbá az ablakokban virágládákat és virágkosarakat TILOS elhelyezni. Ezeket a vagyonvédelmi szolgálatnak rendszeresen ellenőrizni kell, ha rendellenességet tapasztalnak, azonnal jelentik a SitCen-nek.

4.3.2. Mechanikai védelem

A biztonsági és Beavatkozó erők szolgálati helyéül szolgáló épület tervezése során figyelembe kell venni az épület statikai és mechanikai ellenálló képességét, természeti csapások és terrorrobbantások elleni védelmét. Az alkalmazott anyagoknak és technológiáknak meg kell felelni ezen előzetes elvárásoknak.

Építészeti kialakításnál az alagútzsalus technológiával megépített épületek a legellenállóbbak a robbanásakor keletkező lökő hullámokkal szemben, amelyeknél a vasalással megerősített teherhordó elemek (falak, födémek) viselik a robbanásakor keletkező energiákat. Továbbá javasolt a SitCen helységeinek az épület első emeletén történő elhelyezése, mert az erőszakos behatolásoknál alkalmazható eszközök köre - méretükből adódóan - korlátozott.

A földszinten lévő ajtókat, kapukat (kivéve a főbejárat) és ablakokat úgy kell kialakítani, hogy csak belülről legyen nyithatóak. A földszinten lévő ablakok ne rendelkezzenek nyitó

szerkezettel. A helyiségekbe – minimum – A1 típusú biztonsági ablakokat⁴⁸⁰ kell felszerelni, amelyeket biztonsági fóliákkal kell ellátni.

Az épület kétszintes legyen, a földszinten a Beavatkozó erők (Létesítményi tűzoltóság, vagyonvédelem) szolgálati- és szociális helyiségei, valamint szerállásai legyenek. A felső szinten kapjanak helyet a Biztonsági menedzsment irodái, raktárai és tárgyalói, illetve külön biztonsági zónában a SitCen szolgálati és kiszolgáló helyiségei.

Kulcsrend és zárási feladatok

A kulcsrend és a zárási feladatok szervesen illeszkednek a vállalat „Beléptetési és zárási koncepciója” című szabályzatában meghatározottakhoz. A koncepció külön fejezete foglalkozik a SitCen épületkomplexum kulcsrendjével és zárási feladataival. A SitCen kulcsait a zónán belüli biztonsági kulcstároló szekrényben kell tárolni és **csak** a beléptető rendszer üzemképtelensége estén használhatóak. A használatukhoz szükséges a Biztonsági menedzsment vezetőjének engedélye. Ezen állapot csak addig tartható fenn, amíg a beléptető rendszer újra működőképes állapotba nem kerül.

4.3.3. Elektronikus biztonsági rendszerek

Az installálásra kerülő elektronikus védelmi eszközök riadó jelzései a SitCen-be érkeznek és kapcsolódnak az BMR-hez. Riasztás esetén a SitCen személyzete riasztja a Beavatkozó erőket.

Az elektronikus védelmi rendszereket el kell látni 72 órás szünetmentes tápegységgel.

Betörés jelzők

A földszinten minden olyan helyiséget fel kell szerelni olyan duális elven működő mozgásérzékelővel, amelyek külterületre nyíló nyílászáróval (ajtók, kapuk, szellőzők stb.) rendelkeznek. A felszerelésük a várható behatolási irányt ismerve a jellemző érzékenységi karakterisztikájuk figyelembevételével a legoptimálisabb helyre történjen.

Az alkalmazott duális mozgásérzékelők rendelkezzenek szabotázs védelemmel, a visszajelző LED⁴⁸¹ letiltásának lehetőségével, dual piroelemmel, hőkompenzációval.

⁴⁸⁰ MSZ EN 1063 Építési üveg. Biztonsági üvegezés. MSZ EN 1630 Bejárati ajtók, ablakok, függönyfalak, rácsok és redőnyök. Betörésállóság. Vizsgálati módszer a kézi betörési kísérlettel szembeni ellenálló képesség meghatározására

⁴⁸¹ LED - Light-Emitting Diode (fényt kibocsátó dióda)

Lehetőség van kiegészítő érzékelők telepítésére például: falbontás-, üvegtörés-, rezgésérzékelő, pánik jelző.

A földszinten lévő nyílászárókat fel kell szerelni nyitás érzékelőkkel. Az épületen belüli biztonsági zónák bejárati ajtóit el kell látni beléptető rendszerrel, amely illetéktelen behatolás esetén riasztó berendezésként is funkcionál.

Beléptető rendszer

A SitCen bejáratainál egységes beléptető rendszert kell alkalmazni, amely az RFID kártyák és a biometrikus azonosítás kombinációját (opció) egyesíti. Jogosultságok kiadása és visszavonása a SitCen vezetőjének feladata és felelőssége.

Videó megfigyelőrendszer

Videó kamerákat kell elhelyezni a földszinten a nyitás érzékelővel ellátott nyílászáróknál, a főbejáratnál, a folyosókon, a kiemelt biztonsági védelemmel rendelkező helységek bejáratánál. A videó rendszernek folyamatos képet kell továbbítania a SitCen-be folyamatos rögzítés mellett. Ha a betörésjelzőtől riasztás érkezik, grafikuson jelzi a SitCen munkatársának a riasztás helyét és jellegét. A munkatárs riasztja a Beavatkozó erőket.

4.3.4. Beléptetés rendje

A SitCen beléptetési rendszere szervesen kapcsolódik a vállalat beléptetési rendszeréhez. A Biztonsági Konceptió „A beléptetés rendje” című fejezete tartalmazza az általános szabályozást az egész vállalatra vonatkozóan, de ezt ki kell egészíteni a speciális szabályozással, amely csak a SitCen-re érvényes.

A SitCen területén 4 belépési kategóriát különböztetünk meg:

- 1) Állandó személyzet, akiket le kell ellenőrizni és a titkos ügyvitel végzéséhez szükséges engedéllyel kell rendelkezniük.
- 2) Más üzleti egységhez tartozó személyek (saját munkatársak), akik rendelkeznek megfelelő biztonsági ellenőrzéssel, határozott időre szóló belépési jogosultságot kapnak és kíséret nélkül közlekedhetnek. A látogatók csak kísérettel engedhetők be.
- 3) A hatóságok nem engedhetők be megszokásból a SitCen területére, csak ha rendelkeznek megfelelő felhatalmazással.

- 4) A valamely vállalkozáshoz tartozó személyzetnek (például a karbantartók vagy a takarítók) mindig kíséretet kell biztosítani.

Az 1) és 2) kategóriába tartozó személyek állandó belépési engedélyt kapnak, a 3) és 4) kategóriába tartozó személyek pedig „VISITOR” feliratú kártyát. Az állandó belépési engedéllyel rendelkezők a földszinten lévő forgóajtónál elhelyezett terminálon keresztül léphetnek be az épületbe a portaszolgálat ellenőrzése mellett. A be- és kiléptetésnél a portaszolgálat köteles a csomagokat és a beérkező anyagokat ellenőrizni.

Anyagok, dokumentumok és elektronikus adathordozók be- és kiszállítása csak szállítólevéllel történhet, a SitCen vezetőjének engedélyével.

SitCen portaszolgálata

A megfelelő portaszolgálat fontos prevenciós tényező, a szolgálat 2 biztonsági őrből áll. Az épületen belül külön járőr ellenőrző rendszert kell kiépíteni, amely jól elkülöníthető a vállalat általános járőr ellenőrző rendszerétől. Ezt a rendszert is a SitCen munkatársai felügyelik és ellenőrzik.

A vagyonvédelmi szolgálat Beavatkozó csoportját és a portaszolgálatot riasztani kell, ha gyanúsán viselkedő személyekre figyelnek fel, illetve ha gyanúsnak tűnő tárgyakat találnak.

Gondnokság⁴⁸²

A háztechnikának meg kell adni a SitCen vezetőjének a gondnoksági feladatok ellátására kijelölt személyek névsorát és adatait, majd az ellenőrzés után csak kísérettel léphetnek az épületbe⁴⁸³.

A SitCen területére csak munkaidőben léphetnek be karbantartási célból (pl.: takarítás, hibaelhárítás) a gondnokság munkatársai, az ott szolgálatot teljesítő munkatársak felügyelete mellett. Külső cégek munkatársai állandó belépési engedélyt nem kaphatnak a SitCen területére.

⁴⁸² Épületgazdálkodás (karbantartás, javítások, takarítás ...)

⁴⁸³ A SitCen helységeit célszerű a biztonsági menedzsment épületében elhelyezni. A biztonsági menedzsment által használt helyiségek 1-es biztonsági zónába tartozzanak, így megvalósítható a SitCen „külső védelemi gyűrűje”.

4.3.5. Információvédelem

A SitCen információvédelme magába foglalja a titoktartást, a SitCen működéséhez szükséges adatok és tervek védelmét, valamint a feladat végrehajtása során keletkezett információt, illetve az adatok megőrzési feltételeit és határidejét.

A SitCen-ben speciális információvédelmi szabályokat kell alkalmazni, amelyek megakadályozzák:

- > a SitCen-re vonatkozó információk felderítését (hírszerzés) és a gondatlan információkezelést
- > a visszaéléseket a személyekre vonatkozó adatok feldolgozásánál
- > a Biztonsági menedzsment működéséhez szükséges adatok és tervek megsemmisülését, pld. vis major,

és biztosítják az adatok és dokumentumok megőrzését és rendelkezésre állását.

Felelősség

A SitCen vezetője felelős a biztonsági intézkedések végrehajtásáért és betartatásáért. A Biztonság- és védelempolitika tanácsadással támogatja a SitCen vezetőjét a fent említett feladatok végrehajtásában.

Titoktartás hatálya

A titoktartás vonatkozik a SitCen-ben keletkezett és a hatóságoktól kapott információkra, különös tekintettel az állami (hatósági) és működési titkokra, amelyeket a SitCen vagy harmadik személy érdekében bizalmasan vagy titkosan kell kezelni. A titoktartási kötelezettség kiterjed a SitCen személyi állományára, amely a munkaszerződésükben szerepel.

Minősítés

Az információk minősítését az határozza meg, hogy ha jogtalanul használják fel, akkor fenn áll-e a SitCen alaprendeltetéséből adódó feladatainak sikeres végrehajtásának veszélyeztetése.

Azokról az információkról, amelyek tartósan veszélyeztethetik a SitCen céljainak megvalósítását, név szerinti nyilvántartást kell vezetni. Minden más információt „NEM NYILVÁNOS” használatú dokumentumként kell kezelni.

Titoktartási megállapodás

A SitCen vezetője titoktartási szerződést köt a beosztott személyi állománnyal, ami a beosztás betöltéséhez szükséges. A személyi állomány szolgálatba lépése előtt a Biztonság- és védelempolitika köteles a pályázó által megadott adatokat ellenőrizni.

Ha a külső cégek munkatársai, alvállalkozói stb. TITKOS vagy bizalmas projektről, feladatokról ismereteket szerezhetnek, titoktartási szerződést kell kötni.

Minősített információk továbbítása

Technikai eszközökön történő információ továbbításánál (pl.: telefon, telefax, videó vonal, e-mail) biztosítani kell, hogy csak a címzett kapja meg. Minősített információt csak kódolt vonalon lehet továbbítani. A továbbítás után le kell ellenőrizni, hogy a címzett valóban megkapta-e az adott információt.

Minősített iratok megsemmisítése

A SitCen területén szükséges egy iratmegsemmisítő⁴⁸⁴ telepítése. Az iratmegsemmisítőt csak a papíralapú adatoknál alkalmazhatjuk. DIN32757 szabvány szerint választhatjuk ki az adatok minősítésének megfelelő iratmegsemmisítő eszközt.

Elektronikusan tárolt adatoknál az adatok törlése nem elégséges, mert a megfelelő eszközök birtokában visszaállíthatóak. Ezért a végleges adatmegsemmisítés az elfogadott módszer az ilyen módon tárolt minősített adatoknál:

- > fizikai megsemmisítés (az adathordozó feldarabolás, demagnetizálás ...)
- > egyéb más adatmegsemmisítő eszközök használata.

Fotózási és filmezési tilalom a SitCen területén

A SitCen területén nem engedélyezett fotózási és filmezési tevékenység.

A fényképezésre alkalmas készülékeket⁴⁸⁵ a biztonsági zónába nem szabad bevinni, illetve azok elhelyezéséért a biztonsági területen kívül mindenki **saját maga** felelős.

⁴⁸⁴ <http://iratdaralas.hu/din-3-iratmegsemmisites/> (Letöltve: 2014.11.14.)

⁴⁸⁵

4.4. ÖSSZEGZÉS

A multinacionális vállalatoknak számos új kihívással kell számolni működésük során. A vállalatok biztonsági kérdésekkel foglalkozó menedzsment tagjainak és munkatársainak folyamatosan figyelemmel kell kísérni a saját szakterületükön bekövetkezett változásokat. Ennek megfelelően új eljárásokat és módszereket kell kidolgozniuk és alkalmazniuk annak érdekében, hogy a vállalat felsővezetése időszerű és megfelelő információk birtokában tudja meghozni döntéseit.

Ezen alapvetések szerint egy multinacionális vállalatnak rendelkeznie kell a kor színvonalán álló válságkezelő szervezetekkel és módszerekkel, amelyek fontos részét képezik a menedzsment folyamatoknak.

Véleményem szerint ez a típusú válságkezelés – vállalati szinten – még nem elterjedt vagy teljesen más „rég” módszerek vannak alkalmazásban. Általában a mai Magyarországon történni „kell” egy eseménynek, amely rávilágít a válságkezelő szervezetek hiányára vagy a nem megfelelően támogatott és szervezett működésre. Ebben nagy felelőssége van a biztonsági szervezetek vezetőinek, hogy felhívják a vállalat felsővezetésének figyelmét a potenciális veszélyekre, amelyeket esettanulmányokkal tudnak megerősíteni, alátámasztani.

A SitCen időben való tájékoztatása nélkül – vagy hiányában – a válságkezelő szervezetek nem tudják tevékenységüket megkezdeni és a válságot megoldani. A válságkezelés feladatait a SitCen-ből irányítják, amelynek működésének alapját az információk gyűjtése, elemzése, értékelése és terjesztése, a döntések meghozatala, a feladatok meghatározása és a végrehajtás eredményeinek értékelése jelenti.

Az előre kidolgozott biztosítási, védelmi tervek és scenáriók alapján kell a kialakult fenyegetéseket kezelni a térinformatikai rendszerek alkalmazásával. Ezek a rendszerek alkalmasak az előre nem látható események időbeni felderítésére, amely lehetővé teszi a válságkezelő szervezetek és a bevetési erők figyelmeztetését, riasztását.

Az integrált biztonsági rendszerekkel lényegesen magasabb szintű biztonságot lehet megvalósítani. Ezzel a személyi állomány leterheltsége és a kezelői (emberi) hibák nagymértékben csökkenthetőek.

A kétszintű válságkezelés módszere lehetőséget ad az új kihívások időbeni előre jelzésére, elemzésére és értékelésére, valamint a jelentések, trendek terjesztésére. A hatásos válságkezelés így megvalósítható, mert az erre a feladatra kijelölt és rendelkezésre álló munkatársak feladata nem duplikálódik. Ezért szükséges a két válságkezelő szervezet szétválasztása, hogy működésük során ne akadályozzák egymás munkáját. A rendelkezésre álló információk alapján hajtják végre riasztási és jelentési feladataikat. Ha globális kihívásokat vagy regionális fenyegetéseket észlelnek, akkor a stratégiai szintű válságkezelési szervezetet riasztják. A stratégiai válságkezelő szervezet tagjai a különböző szakterületek vezetői, akik egyben a vállalat menedzsmentjének tagjai is.

A lokális események bekövetkezése esetén a Krízismenedzsment vezetőjét kell informálni. Az operatív válságkezelő szervezetet a Biztonsági menedzsment vezetője irányítja és tagjai a szakterületek ügyeleti rendszert adó munkatársai (mérnökei).

A SitCen integrált védelmét is a vállalat biztonsági stratégiájában meghatározott biztonsági filozófia alapján kell kiépíteni. A SitCen megfelelően megtervezett, kiépített és működtetett védelme biztosítja a zavartalan működését. A „biztonsági piramis” minden elemének alkalmazásával garantálható a legmagasabb szintű védelem.

A SitCen biztonságos működése megköveteli a különleges információvédelmi intézkedések alkalmazását, úgy mint a titoktartást, az adatvédelmet és az adatbiztonságot, valamint a működéshez szükséges adatok és tervek, illetve a működés során keletkezett és továbbított információk védelmét, illetve az adatok megőrzési feltételeit és határidejét.

BEFEJEZÉS

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A kutatómunka összefoglalása

Az értekezés *első fejezetében* bemutattam a biztonsági kihívásokat, fenyegetéseket és kockázatokat, illetve a terrorizmus stratégiai céljait, működésének általános elveit és az alkalmazott módszereit. A *második fejezetben* elemeztem a terrorizmus hatását a világgazdaságra és a kritikus infrastruktúra működésére, valamint áttekintést adtam a terrortámadások elleni védekezés állami és civil feladatairól. A *harmadik fejezetben* ismertettem a kritikus infrastruktúrák nemzetközi- és nemzeti védelmi feladatait, amely egy integrált biztonsági koncepció alkalmazásával valósítható meg. Kidolgoztam azokat a szervezeti, építészeti és technikai eljárásokat, amelyek alkalmazásával megvalósítható a kritikus infrastruktúrák létesítményeinek védelme. A *negyedik fejezetben* áttekintést adtam a válságkezelés alapfeltételeiről és az ezekhez szükséges technikai eszközökről. Továbbá ismertettem a nemzetközi biztonsági szervezetek és intézmények válságkezelő mechanizmusait, valamint tanulmányoztam, hogy hogyan lehet a civil társadalom hasonló szervezeteinél, objektumainál alkalmazni a „kormányzati” (GO) válságkezelés elveit.

Összevont következtetések

- > A globalizáció hatásai világszerte, regionális és lokális szinten jelennek meg, amelyek direkt vagy indirekt módon okoznak biztonsági problémákat.
- > Egy helyi konfliktus hatással lehet a közeli és a távoli régiókra vagy akár az egész világra.
- > Európa nem tudja magát a világ eseményeitől függetleníteni sem gazdaságilag, sem politikailag. A világ országaiban és kontinensein bekövetkező események - közvetve vagy közvetlenül - érintik földrészünk biztonságát és gazdaságát, illetve a lakosság jólétét. Ezért fontos, hogy Európa ezekre a veszélyekre megfelelő és egységes válaszokat adjon.
- > A globálisan jelentkező terrorizmus és a civilizációs ellentétek csak tovább növekedtek, melyet a kulturális és vallási különbségek felerősödése okozott. A terrorizmus egyre tudatosabban használja ki a média adta lehetőségeket, amely segítségével fenyegeti és terrortámadásaival sokkolja a világ közvéleményét.

- > A hidegháborúban az ideológiai különbségeket használta ki a terrorizmus, ezt a XXI. században már a vallási és a kulturális különbségeken alapuló filozófia váltotta fel.
- > A terrorizmus kihasználja a globalizáció technikai vívmányait és vissza is él ezekkel.
- > Magyarország biztonsági helyzetét nagyban befolyásolják a válságövezetek, amelyek egyre jobban megközelítették határainkat, mint például az Ukrajnai konfliktus, az Észak-Afrikában és a Közel-Keleten fennálló polgárháborús helyzet és a szegénység okozta migrációs válság a mediterrán térségben, valamint a Balkánon.
- > A kritikus infrastruktúra megléte és működőképessége jelentősen befolyásolta és befolyásolja ma is egy civilizáció fejlődését és fennmaradását.
- > Fontos, hogy a különböző „biztonsági szervezetek és hatóságok” egyformán értelmezzék a biztonsági és védelmi feladatokat és azok kapcsolódási pontjait, valamint a kritikus infrastruktúrák létesítéséhez és működtetéséhez szükséges új biztonságtechnikai és taktikai elemek alkalmazását. Így megvalósítható a kritikus infrastruktúrák integrált védelme.
- > A kritikus infrastruktúra folyamatos működéséhez szükséges rendszerek vagy létesítmények elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, úgy mint az egészségügyhöz, a biztonsághoz, a *gazdasági és szociális jóléthez*.
- > A GDP 80%-át a TOP50 magyar vállalat állítja elő. Az 50 gazdasági társaságból 24 termelő vállalat. *Csak 26 - nem termelő - vállalat tartozik a kritikus infrastruktúrák sorába a 2080/2008. kormányhatározat 2. számú melléklete szerint. A kormányrendelet mellékletében a VIII-as (Ipar ágazat) pontját ki kell egészíteni azokkal a termelő vállalatokkal, amelyek a GDP legalább 2 %-át egy telephelyen állítják elő.*
- > A vállalati biztonsági szabályzatrendszerét elsősorban az adott ország nemzeti biztonsági stratégiája - ahol mint „leányvállalat” működik -, másodsorban az „anyavállalat” „worldwide” érvényes biztonsági intézkedései alapján kell kidolgozni.
- > A vállalat biztonságpolitikája számba veszi az értékeket és érdekeket, valamint a biztonsági környezet elemzése alapján meghatározza azokat a vállalati célokat, feladatokat és eszközöket, amelyekkel a vállalat a globalizált világban szavatolni

tudja a munkatársak életét és egészségét, illetve a vállalat biztonságos működését. A szakpolitikákat a biztonságpolitikából származtatják és egészítik ki az adott területre vonatkozó speciális feladatokkal.

- > Egy nagyvállalat biztonsági rendszerét a „*hatalom-megosztás*” elve jellemzi. Az *üzleti egységek* biztonsági felelőssége szétválasztódik a *szakterületek* és *Biztonsági menedzsment* biztonsági felelősségétől.
- > Az általános biztonsági intézkedések az egész vállalatra érvényesek. A kollektív szerződéssel együtt határozzák meg a munkavállalókra nézve kötelezően betartandó szabályokat.
- > Biztonsági szervezetek kialakításánál két szintet kell meghatározni. A stratégiai szint, amelybe a szakterületek tartoznak, valamint az operatív szint, ahol a napi rutinszerű biztosítási és védelmi feladatokat látják el a SitCen, Beavatkozó erők és egyéb más szolgáltató szervezetek.
- > A stratégiai szintű biztonsági szervezetek határozzák meg a közép- és hosszútávú védelmi feladatokat, kapcsolatban állnak az országos hatáskörű szervekkel és hatóságokkal, valamint egyéb nemzetközi szervezetekkel.
- > Az operatív biztonsági szervezetek határozzák meg az egész vállalatra érvényes szabályrendszereket, illetve ezek a területek tartják a kapcsolatot a helyi hatóságokkal.
- > A különböző *biztonsági rendszereknél* szükséges a tűz-, vagyonvédelmi és egyéb más védelmi célokat szolgáló rendszerek *integrálása*. Ez teszi lehetővé, hogy a SitCen mint központi irányító szervezet működjön. A biztonsági rendszerek integrálása és az infokommunikációs rendszerek alkalmazása képezi az alapját a SitCen működésének.
- > A terrorrobbantások és a terrortámadások biztonsági kérdéseinek vizsgálata során megállapítottam, hogy ma Magyarországon az épületek/objektumok terrorrobbantások és terrortámadások elleni védelmi aspektusa nem kap a súlyának megfelelő figyelmet, mert a jogszabályi háttér hiányos vagy nem létezik.
- > A nemzetközi tapasztalatokra, törvényszerűségekre alapozva olyan megoldási lehetőségeket kívántam bemutatni, amelyek integrált módon alkalmazott elemei révén hatékonyan végrehajthatóak a terrorrobbantások és -támadások elleni védelmi műveletei. A civil szférában alkalmazható terrortámadások elleni védekezésről nincs jogszabály vagy iránymutatás. Ezért tartottam fontosnak két

külön pontban az objektumok/épületek terrortámadások elleni védekezésének általános elveit megfogalmazni.

- > A nemzeti válságkezelés kormányzati feladat. A válságreagáló központ feladata az információk gyűjtése, elemzése, értékelése és terjesztése. A nemzetközi szervezetek helyzetelemző központjaiban alkalmazott módszerek felhasználhatóak a civil szféra hasonló központjaiban is.
- > Egy multinacionális vállalat válságkezelését két szinten célszerű tervezni és végrehajtani. A globális kihívásokat vagy regionális fenyegetéseket a stratégiai szintű válságkezelési szervezet látja el. A helyi események kezelése az operatív Krízismenedzsment feladata.
- > SitCen -t a nap 24 órájában, a hét minden napján kell működtetni. A SitCen személyi állománya figyelemmel kíséri a világban történt fontosabb eseményeket, illetve fogadja a biztonsági rendszerek riasztásait, rögzíti az információkat, ezzel egyidejűleg teljesíti riasztási és jelentési kötelezettségeit.
- > A biztonsági rendszerek integrálása révén magasabb szintű biztonságot lehet megvalósítani, mert a vészjelzések kiértékelése (priorizálása) automatikus. Így csökkenthetőek az emberi hibák, a személyi állomány leterheltsége és kiszűrhető a rendszerek téves jelzései.
- > Az interneten elérhető térinformatikai rendszerek alkalmazásával veszélyt (riasztást) megjelenítő térképek segítségével a SitCen személyi állománya elrendelheti a válságkezelő szervezetek vagy Beavatkozó erők magasabb készségi fokozatba helyezését. A térinformatikai modellek segítségével készíthetünk közép- és hosszútávú kockázati modelleket és szimulációkat, amelyek alapján trendeket tudunk meghatározni, illetve előre kidolgozott scenáriókat és védelmi terveket.
- > A SitCen védelmét az integrált biztonsági koncepció alkalmazásával kell megvalósítani. A tervezés, építés és a biztonsági rendszerek telepítése során különös figyelmet kell fordítani az információvédelmi intézkedések betartására és betartatására, amelyet a működés során is kiemelten kell kezelni.

Tudományos eredmények

- 1) A globalizáció hatási világszerte biztonsági problémákat okozhatnak, illetve veszélyeket jelelhetnek regionális vagy helyi szinten, direkt vagy indirekt módon. A társadalmi kihívások és egyéb fegyveres konfliktusok, természetes és mesterséges katasztrófák menekülthullámot eredményezhetnek a környező országokba, régiókba. Az érintett területeken több olyan biztonságpolitikai fenyegetés és kockázat alakulhat ki, amely befolyásolja az érintett területek gazdaságát, mert a befektetők tevékenységét és szándékait a legjobban a stabilitás és a biztonság hiánya vagy megléte befolyásolja.

A terrorizmus hatását a világgazdaságra a 2001-es terrortámadások utáni tanulmányok és elemzések alapján mutattam be, mert ezen események elemzéséről áll rendelkezésre megfelelő mennyiségű szakirodalom. A terrortámadások nemzetközi trendekre gyakorolt hatása függ a támadások helyétől és idejétől. A hatások leggyorsabban a kereskedelemben és a turizmusban jelentkeznek, illetve a későbbiekben a tranzakciós költségnél okoznak jelentős növekedést. További hatások várhatóak még, mint például bizonytalanság a pénzpiacon és a befektetők körében, a külkereskedelem lassulása, a költségek üzleti életben történő növekedése, befektetők bizonytalansága, fogyasztás csökkenése, biztosítás költségeinek növekedése, a bevezetett biztonsági intézkedések lassíthatják a külkereskedelmi folyamatokat, a biztonsági költségek az állami és nem állami szereplőknél növekednek, a szállítási útvonalak megváltozása, illetve a szállítási határidők és költségek növekedése.

A kritikus infrastruktúrák elleni terrortámadások kieséseket és zavarokat okozhatnak az állam és a gazdaság (termelés, szolgáltatások), valamint a lakosság ellátásában.

- 2) Bemutattam értekezésem második részében, hogy a biztonságpolitika különböző dimenziói kapcsolatban állnak egymással és kihatnak egymás működési mechanizmusára. A XXI. században a gazdasági dimenzió a leghangsúlyosabb. A biztonságpolitikai irányelvek meghatározása a kormány politikájának fontos részét jelenti, amelyet a Nemzeti Biztonsági Stratégiában deklarálnak.

A kritikus infrastruktúrák védelmének tervezési fázisában figyelembe kell venni a „dominó hatást”, amely következtében a károk eszkalálódhatnak és a bekövetkezett események hatására másodlagos, harmadlagos károk is keletkezhetnek.

A terrorellenes küzdelem különböző aspektusaival foglalkozó biztonsági intézmények és szervezetek szereplői közötti koordináció napi és közigazgatási szinten megfelelő. Arra a következtetésre jutottam, hogy a jövőbeni nemzeti biztosítási műveletekben történő szerepvállalás elérte a magyar rendvédelmi szervek lehetőségének határát (pl.: minősített időszakban a kritikus és létfontosságú infrastruktúrák védelme). A biztosítási és védelmi feladatok végrehajtásába be kell vonni azokat a biztonsági profilú civil vállalatokat, amelyek rendelkeznek a nemzeti hatóságok által kiadott biztonsági minősítéssel.

Megvizsgáltam a nemzetközi és nemzeti jogszabályokat és hatósági állásfoglalásokat, milyen módon garantálható az objektumok teljeskörű védelme. A Magyarországon kialakult biztonsági irányzatok vizsgálata során megállapítottam, hogy az *integrált biztonsági koncepció* követeli meg az összes biztonsági elem alkalmazását (adminisztratív, monitoring rendszer, mechanikai védelem, elektronikai eszközök, Beavatkozó erők, válságkezelés, biztosítások). Az integrált biztonsági koncepcióban határozzák meg a biztonsági szakterületek és üzleti egységek feladatát és kötelezettségeit, valamint a telepített biztonsági rendszerek teljes körű integrációját.

Az objektumok/vállalatok fejlesztésnél és/vagy új „zöld mezős” beruházásoknál már a tervezés időszakában figyelembe kell venni a biztonsági kihívásokat, fenyegetéseket és kockázatokat, amelyek meghatározzák a védelmi költségeket. A biztonsági rendszerek kialakítása egy tudatos folyamat, amely a megállapított veszélyekhez igazodó rendszer kiépítését követeli meg.

A Helyzetelemző és válságkezelő központ feladata az információk gyűjtése, előzetes elemzése, értékelése és terjesztése. Megállapítottam, hogy a nemzetközi szervezetek helyzetelemző központjainak módszerei alkalmazhatóak a vállalatok hasonló központjaiban is.

A válság kezelését kétszintűvé kell tenni, mert a globális kihívásokat és regionális fenyegetéseket a stratégiai szintű válságkezelési szervezet tudja kezelni, mely a különböző biztonsági szakterületek vezetőiből tevődik össze. A

lokális események kezelése az operatív Krízismenedzsment feladata, amelynek részei a Beavatkozó erők, a szakterületek ügyeletet adó munkatársai és az üzleti egységek delegált vezetői.

Javaslatok

A kutatásaim alapján négy javaslatot fogalmaztam meg:

- > Szükségesnek A terrortámadások időbeni előrejelzése, megelőzése, megelőző intézkedések és forgatókönyvek (standard-ok) kidolgozása, terjesztése és alkalmazása.
- > Az elvégzett kutatómunka alapján megítélésem szerint a kritikus infrastruktúrák védelme egy integrált biztonsági rendszer teljes körű kiépítésével és üzemeltetésével valósítható meg, így csökkenthető a kritikus infrastruktúrák veszélyeztetettsége.
- > A 2080/2008. kormányrendelet 2. mellékletét módosítani, hogy a *gazdasági jólétet biztosító* szervezetek is kritikus infrastruktúra besorolással rendelkezzenek.
- > A nemzetközi biztonsági szervezetek és a nemzeti válságkezelő központokban alkalmazott módszerek és folyamatok alkalmazhatóak a civil szféra ilyen jellegű központjaiban.

Ajánlások

Az értekezés kutatási eredményeinek két felhasználási területet javasolok. Felhasználható oktatási célokra, a felsőoktatásban, a hadtudomány és a katonai műszaki tudományok területén.

Véleményem szerint a tudományos eredmények és módszerek hasznos információkat tartalmaznak a civil biztonsági területen dolgozó szakembereknek és háttér információként szolgálnak az állami biztonsági szervezetek és intézmények munkatársai számára.

FELHASZNÁLT IRODALOM

Könyvek, kiadványok, tanulmányok, publikációk, előadások

ARTNER Annamária: Globalizáció alulnézetben, Elyomott csoportok – lázadó mozgalmak, Napvilág Kiadó, @ Artner Annamária, 2006, HU ISSN 1587-6128

BARLAI Róbert – KŐVÁGÓ György: *Krizismenedzsmet, kríziskommunikáció*, © Századvég Kiadó, 2004

BENCE Balázs – Dr. DEÁK János – Dr. SZTERNÁK György: *Gondolatok a válságreagáló műveletekről II. RÉSZ, A fegyveres erő helye, feladatai a válságreagáló műveletekben*, Nemzetvédelmi egyetemi közlemények, 2005, 9. évf. 2. szám

BLEISCHWITZ, Raimund: *Internationale Rohstoffmärkte: steigende Preise und wachsendes Konfliktpotenzial*, Global Trends 2007, ©Stiftung Entwicklung und Frieden, Bonn, 2006, ISBN 3-89-331-739-2

BOLZ, Frank Jr. – DUDONIS, Kenneth J. – Schulz, David P., *The Counter-Terrorism Handbook. Tactics, Procedures, and Techniques*. New York, Elsevier, 1990

BOLGÁR Judit – SZTERNÁK György: *A terrorizmus társadalmi és személyiség-lélektani háttere*, ZMNE Hadtudományi Doktori Iskola, Publikációk, 2005, pp. 56 – 57,

BOTTORÉ, Tom: *Élites and Society*, Routledge N.Y., 1993, ISBN-13: 978-0415082716, pp. 1-7.

BRÜCK, Tilman: *The Economic Analysis of Terrorism*, Routledge, New York, 2007, ISBN1134216475,

CHANG, Gordon G.: *Blue Gold: The Coming Water Wars*, World Affairs Journal, Washington, © 2013 World Affairs Institute

CLAUSEWITZ, von Carl: *A háborúról*, Zrínyi Kiadó, Budapest, 2013

DEÁK János: *Oroszország katonai stratégiája a második világháború befejezésétől napjainkig*, Egyetemi jegyzet, Budapest, 2010

DIRMOSER, Dietmar: *Energiesicherheit*, © Friedrich-Ebert-Stiftung, Bonn/Berlin 2007, ISBN: 978-3-89892-727-7

EURÓPAI BIZOTTSÁG: *Európai Biztonsági Stratégia: Biztonságos európa egy jobb világban*, Európai Unió Kiadóhivatala, Luxemburg, 2009, pp. 12, ISBN 978-92-824-2427-8

EURÓPAI BIZOTTSÁG: *Energiapolitika*, Az Európai Unió Kiadóhivatala, Luxembourg, 2013, ISBN 978-92-79-34123-9

EURÓPAI BIZOTTSÁG: *Egészségpolitika, minden uniós polgár egészségének javításáért*, Luxembourg, Európai Unió Kiadóhivatala, 2014, ISBN 978-92-79-42343-7

Hans FRANK: *Sicherheitspolitik in neuen Dimensionen*, Bundesakademie für Sicherheitspolitik, 2001, ISBN 3-8132-0776-5

FORGÁCS Balázs - KALÓ József - NÉMETH József Lajos: *Aszimmetrikus kihívások a haderő, az állam, valamint a társadalom viszonyában*, Magyar Hadtudományi Társaság, Konferenciája – Aszimmetrikus hadviselés, 2015/1-2

FROMKIN, David: *The Strategy of Terrorism*, Foreign Affairs, Tampa, 1975, ISSN 0362-4331

FUCSKU Sándor: *A válságkezelő műveletekben résztvevő magyar kontingensek terrorfenyegetettsége, a felderítő csapatok különleges felderítő képességei*, Felderítő Szemle, 2006, január, V. évfolyam

GÁL István László: *Új biztonságpolitikai kihívás a XXI. században: A terrorizmus finanszírozása*, KNBSZ Szakmai Szemle, 2012/1

GAZDAG Ferenc: *Biztonságpolitika*, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2011, ISBN 978-615-5057-23-6,

GREGOSZ, David: *Wirtschaftspolitische Megatrends bis 2020*, Konrad-Adenauer-Stiftung, Bellin, 2012, ISBN 978-3-944015-02-6

GROSS, Emanuel: *The struggle of democracy against terrorism, lessons from the United States the United Kingdom, and Israel*, 2006 by the Rector and Visitors of University of Virginia, ISBN: 0-8139-2531-2

GUNDEL, STEPHAN, MÜLLI, LARS: *Unternehmenssicherheit*, München: Oldenbourg, 2009, ISBN 978-3-486-58712-8

HART, B.H. Liddel: *Stratégia*, Európa Könyvkiadó, Budapest, 2002

HANKISS Ágnes előadása: *Kihívások és ellentmondások a terrorizmus elleni harcban*, „A terrorizmus Rubik-kockája” avagy a fenyegetések komplex megközelítése” Nemzetközi tudományos-szakmai konferencia, Budapest, 2013. szeptember 30. – október 1.

HÁRDI István: *A terrorizmusról*, A Magyar Tudományos Akadémia folyóirata. Alapítás éve: 1840, 170. évfolyam – 2009/8. szám

HEGEDÜS Zsuzsanna: *Az Amerikai Egyesült Államok adósságválsága és okai*, MTA Közgazdaság- és Regionális Tudományi Kutatóközpont Világgazdasági Intézet. 206. sz., 2013. december

HOBIIJN, Bart: *What Will Homeland Security Cost?*, FRBNY Economic Policy Review, November, 2002

JOHNSTON, R. Barry and NEDELESCU, Oana M.: *The Impact of Terrorism on Financial Markets*, © International Monetary Fund, 2005

KAHANER, Larry: *Competitive Intelligence: How to Gather, Analyze, and Use Information to Move Your Business to the Top*, TOUCHSTONE ROCKEFELLER CENTER, New York, 1997, ISBN-13: 978-0-684-81074-4

Karen AMSTRONG: *Az iszlám*, A Weidenfeld & Nicolson book, Hungarian translation © Péri Benedek, Európa Kiadó, Budapest, 2005

KAISER Ferenc – TÁLAS Péter: *Politikai erőszakformák*, Nemzet és Biztonság 2012/5-6. szám, pp. 139

KENEDLI Tamás r.őrnagy: *Elemzőközpontú információfeldolgozás a szervezett bűnözés és a terrorizmus elleni harcban*, Doktori (PhD) értekezés

KISS Álmos Péter: *Generációk a hadviselésben – A negyedik generáció*, Hadtudományi Szemle, 2009/2.

KÁLMÁN László – PATAKI János: *Integrált technikai objektum védelem*, Zrínyi Miklós Nemzetvédelmi Egyetem, LKBM-2732, 2007.11.15., Budapest, tanulmány, (A szerző birtokában)

KIRÁLY László – PATAKI János: *Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz*, A MAGYAR HADTUDOMÁNYI TÁRSASÁG ÉS A MAGYAR TUDOMÁNYOS AKADÉMIA HADTUDOMÁNYI BIZOTTSÁGA FOLYÓIRATA, XXIII. Évfolyam, 2013/1. elektronikus lapszám

KIRÁLY – Medveczky: *Védelemgazdasági ismeretek önkormányzati (védelemi igazgatási) válság menedzsereknek*. Budapest, 2009, ZMNE, ISBN 978-963-7060-75-5

KLINGHOLZ, Reiner: *Demographische Entwicklung*, Die Zeit, Zeitverlag Gerd Bucerius GmbH & Co. KG, Hamburg, 2014/7.

KOVACICH & HALOBOZEK: *The Manager's Handbook for Corporate Security*, Imprint Butterworth-Heinemann, 2003, ISBN: 9780750674874

KÓTHAY János: *Általános logisztikai módszerek*, Katonai Logisztika, MH ATFCSF, 2. Évfolyam, 1994/1

KÖSZERGVÁRI Tibor: *A válságkezelés aktuális problémái*, Akadémiai közlemények, 1994

KUBARYCH, Roger M. “*Aftermath of the Terrorist Attack: Economic, Financial and Policy Consequences.*” *Council on Foreign Relations. council on foreign relations*, 2011, ISSN: 0015-7120

KUTI Rajmund – FÖLDI László: *A beépített vízköddel oltó rendszerek újabb alkalmazási lehetőségeinek feltárása*, Hadmánök, III. Évfolyam 2. szám - 2008. Június

Dr. KUTI Rajmund – GRÓSZ Zoltán: *Biológiai eredetű vészhelyzetek kezelése, előtérben a mentesítési feladatok*, Hadtudomány, XI. Évfolyam 1. szám, 2016, ISSN 1788-1919

LAKATOS Zsolt: *A terrorista szervezetek felépítése és csoportosítása*, Felderítő Szemle (KFH), 2007/1.

MCFARLAND, Duncan – KREHBIEL, Paul – TARG, Harry: *Vietnam, From National Liberation to 21 st Century Socialism*, Committees of Correspondence Education Fund, Inc, New York, ISBN: 978-1-304-20457-8

MÜLLER, Klaus-Rainer: *IT-Sicherheit mit System*, © Springer Fachmedien Wiesbaden, 2014, ISBN 978-3-658-04333-9

Műszaki Katonai Közlöny XVIII. évf. 1-4. szám, 2008.

NATIONAL INTELLIGENCE COUNCIL „*Mapping the Global Future - Projekt 2020*”, Pittsburgh, 2004, (p. 83 –92), ISBN 0-16-073-218-2

Report on the NATO’s, New Strategic Concept Workshop, Centre for Defence and Security Studies, University of Manitoba 2010, ISSN 1922-7027

NATO HQ Situation Centre (SITCEN), Security Standard Operating Procedures (SOPs), Revision 1. 16 February 2010, „NATO UNCLASSIFIED”, (A szerző birtokában)

OTTEN, Wolfgang: *Eigensicherung*, ISBN-10: 3-452-26276-6 , Köln, 2006

PADÁNYI József: *Az aszimmetrikus hadviselés során*, HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 25: (1-2)

PATAKI János: Biztosítási feladatok Magyarország az Európai Unió soros elnöksége idején 2011-ben, tanulmány, Zrínyi Miklós Nemzetvédelmi Egyetem, Magasabb Tanfolyami Parancsnokság, Budapest, 2009, (A szerző birtokában)

PATAKI János – SULÁNYI Péter: *Lage- und Analysezentrum bei einem internationalen Unternehmen*, ZMNE BOLYAI JÁNOS HADMÉRNÖKI KAR ÉS A HADMÉRNÖKI DOKTORI ISKOLA, ONLINE TUDOMÁNYOS KIADVÁNYA, VI. Évfolyam 3. szám 2011. szeptember

PATAKI János: *Helyzetelemző Központ*, Zrínyi Miklós Nemzetvédelmi Egyetem, LKBM-7242, Budapest, 2008.04.07., tanulmány, (A szerző birtokában)

PATAKI János: *Különleges védelemmel felszerelt gépjárművek*, ZMNE BOLYAI JÁNOS HADMÉRNÖKI KAR ÉS A HADMÉRNÖKI DOKTORI ISKOLA, ONLINE TUDOMÁNYOS KIADVÁNYA, IX. Évfolyam 2. Szám, 2014.június

PATAKI János: *Az Európai Unió biztonság- és védelempolitikája, a tagállamok és Magyarország felajánlásai tükrében*, diplomamunka, Zrínyi Miklós Nemzetvédelmi Egyetem, 2007

PHILPOTT, Don: *Terrorism and Weapons of Mass Destruction: „The Future of Terrorism Task Force”*, Homeland Defense Journal, 04/2007

PROCHOW, Stefan: *Terrorism*, Globale Herausforderungen, © Bundeszentrale für politische Bildung, Bonn, 2013, ISBN 978-3-8389-7086-8

SCHNELLNHUBER, Hans-Joachim –SCHLUZ-BALDES, Meinhard –PILADEAUX, Benno: *Umweltveränderungen und ihre Folgen*, Sicherheitspolitik in neuen Dimensionen, Bundesakademie für Sicherheitspolitik, 2001, pp. 567 - 584, ISBN 3-8132-0776-5

SCHOLZEN, Reinhard: *Personenschutz*, Motorbuch Verlag, Stuttgart, 2004, pp.8-25 ISBN 3-613-02185-4

SCHRÖDER, Helge: *Wie funktionieren Finanzmärkte? – Chancen und Gefahren globalisierter Geldströme*, Globale Herausforderungen, © Bundeszentrale für politische Bildung, Bonn, 2011, pp. 195 – 199, ISBN 978-3-8389-7042-4

SCHRÖDER, Helge: *Wie viele werden wir werden? Demographische Entwicklungen*, Globale Herausforderungen, © Bundeszentrale für politische Bildung, Bonn, 2010, pp. 13 - 30, ISBN 978-3-8389-7056-1

SIMICSKÓ István: előadása *A magyar védelempolitika aktuális kérdései és jövőbeni tervei* címmel 2015. november 13-án a Nemzeti Közsolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Felsőfokú Vezetőképző Tanfolyam hallgatóinak. <http://www.defence.hu/cikk/54098>, (Letöltve:2016.01.21.)

RESPERGER István: *Az iszlám világ és hatása a biztonságra*, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003

RESPERGER István mk. ezredes: *Biztonsági Kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig*, KNBSZ, Felderítő Szemle, 2013/3

RESPERGER István – KISS Álmos Péter – SOMKUTI Bálint: *Gerillaharc a betonzsungelban*, Hadtudomány, A Magyar Hadtudományi Társaság folyóirata, 2013

RESPERGER István ezredes – KISS Álmos Péter – SOMKUTI Bálint: *Negyedik generációs hadviselés: Néhány alapfogalom*, Zrínyi Kiadó, ISBN 9789633275924

ROZMAN Tamás: *Tananyag a TÁMOP-2.4.8-12/1-2012-0001, „ A munkahelyi egészség és biztonság fejlesztése, a munkaügyi ellenőrzés fejlesztése című projekt keretében a Nemzeti Munkaügyi Hivatal megbízásából került kidolgozásra*, BMGE, Budapest, 2014, ISBN 978-963-313-122-0, II. rész

Samuel P. HUNTINGTON: *A civilizációk összecsapása és a világtrend átalakulása*, Európa Kiadó, 2006, pp. 58-61,

SARDAR, Ziauddin – MALIK Zafar Abbas: *Introducing Islam*, Icon Books UK - Totem Books USA, © SZAKÁCS Gergely – Hungarian translation, Edge 2000 Kiadó, ISBN 963 86450 7 5, p.4

SENZ, Anja-Désirée – HEBERER, Th.: *Deutschland und China, Zusammenarbeit und Wettbewerb*, in: Bundesakademie für Sicherheitspolitik: *Sicherheitspolitik in neuen Dimensionen, Ergänzungsband II*, Verlag E.S. Mittler & Sohn GmbH, Hamburg, 2004, ISBN 3-8132-0823-0

STIFTUNG ENTWICKLUNG UND FRIEDEN: *Globale Trends 2007*, Bonn 2006, ISBN 3-89331-739-2

SZEPESI György: *A pénzügyi világválság néhány eddigi tanulsága II. Köz-gazdaság*, 4 (3)., 2009, pp. 73 -75. ISSN 1788-0696

SZTERNÁK György: *A fegyveres erő feladatai valamint fejlesztése közötti kapcsolat*, Ludovika Digitális Tudástár és Archívum, Hadtudomány, 2011

SZTERNÁK György: *A geopolitikai, geostratégiai elemzés következtetései*, Ludovika Digitális Tudástár és Archívum, Hadtudomány, 2011

SZTERNÁK György: *A terrorizmus, mint hadtudományi probléma I. rész*, NEMZETVÉDELMI EGYETEMI KÖZLEMÉNYEK , 2005/1

SZUN CE: *A hadviselés tudománya*, Göncöl Kiadó, Budapest, 2012, ISBN: 9789639183742

TÁLAS Péter: *A nemzetközi terrorizmus és a szervezett bűnözés hatása a nemzetközi biztonságra és Magyarország biztonságára*, MTA Társadalomtudományi Kutatóközpont **Kisebbségkutató Intézet**, 2007. január

THOMAS, Jeffrey E.: *Do the Costs Justify the Benefits?* Symposium: The Law and Economics of Providing Compensation for Harm Caused by Terrorism, Indiana University–Purdue University Indianapolis, 2003/2

TOMOLYA János – PADÁNYI József: *A terrorizmus és a gerilla-hadviselés azonosságai és különbségei*, HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 24: (1)

TÚRI Viktória: *Az intrapszichés megküzdés típusai*, Gazdasági élet és társadalom, Wekerle Sándor Üzleti Főiskola Tudományos Folyóirata, 2013. I-II. szám, ISSN: 2060-7466

ÜVEGES László: *A Magyar Köztársaság katasztrófa-veszélyeztetettsége és az arra adandó válaszok*, ZMNE, – Ph D értekezés –, Budapest, 2002

VARGHA Ferenc: *A terror pszichológiája*, MAGYAR JOGI SZEMLE KÖNYVTÁRA, PALLAS RÉSZVÉNYTÁRSASÁG NYOMDÁJA, 1921

VARGA Henriett – BAGDI Róbert: *A terrorizmus hatása a nemzetközi idegenforgalomra*, Károly Róbert Főiskola Tudományos Tanácsa, Acta Carolus Robertus, 2011/2

Dr. VIDA Csaba alezredes: *A jelenkori népvárdorlás hatásai*, KNBSZ Felderítő Szemle, XIV. évfolyam 3. Szám, 2015, ISSN 1588-242X

WESSEL, Jan: *Organisierte Kriminalität und soziale Kontrolle*, Springer Fachmedien Wiesbaden GmbH, 2001, ISBN 978-3-8244-441-0

Internetes források

Aramid

http://portal.zmne.hu/download/bjkmk/bsz/bszemle2009/3/07_franggyorgy.pdf

(Letöltve: 2013.10.29.)

A globalizáció kihívásai miatt a „hagyományos” vállalati kockázat elemző szervezetek

http://www.verismo.ch/sites/default/files/Verismo_Publikationen_04_0.pdf

(Letöltve: 2014.10.01.)

... „a 60-as korosztálynál” ...

<http://www.uni-miskolc.hu/~ecomojud/4neptermnepmozg.pdf>

(Letöltve: 2014.12.01.)

... „A világ népessége több mint 7 milliárd ember, ami várhatóan 2050-ben” ...

http://www.ksh.hu/szamlap/eletunk_nep.html

(Letöltve: 2014.12.01.)

... „az átlagos születési ráta” ...

<http://www.nyf.hu/others/html/kornyezettud/global/002.htm>

(Letöltve: 2014.12.01.)

Bundeszentrale für politische Bildung, <http://www.bpb.de/politik/hintergrund-aktuell/172918/autofreier-sonntag-1973> (Letöltve: 2014.12.29.)

Eco-management and Audit Scheme, Öko-menedzsment és audit rendszer, <http://www.emas.de/home/> (Letöltve:2014.11.05)

Egyesült Államok Védelmi Minisztériuma (Department of Defense)
www.dod.wbdg.org
(Letöltve: 2011.10.01.)

Energiemanagementsystem, energia menedzsment rendszer,
http://www.dnv.de/Binaries/Whitepaper_Energie_final_tcm70-447552.pdf (Letöltve: 2014.11.05.)

Environmental management, környezeti menedzsment,
<http://www.iso.org/iso/home/standards/management-standards/iso14000.htm> Letöltve: 2014.11.05.)

Európai Unió környezetvédelmi politikája,
http://europa.eu/pol/pdf/flipbook/hu/environment_hu.pdf (Letöltve: 2014.11.04.)

EU SITUATION ROOM
http://www.eeas.europa.eu/crisis-response/what-we-do/eu-situation-room/index_en.htm
(Leöltve:2016.03.14.)

Global Incident Map
<http://www.globalincidentmap.com/>
(Letöltve:2016.12.11.)

Gyermekmunka
<https://btk.ppke.hu/uploads/articles/6414/file/reinischreka.pdf>
(Letöltve: 2014.12.02.)

Hiperinfláció a küszöbön?
<http://kiszamolo.hu/hiperinflacio-a-kuszobon/>
(Letöltve: 2013.11.18.)

Időkép: Radarkép, riasztás
<https://www.idokep.hu/radar>
(Letöltve:2015.12.11.)

Iratmegsemmisítés
<http://iratdaralas.hu/din-3-iratmegsemmisites/>
(Letöltve: 2014.11.14.)

Kerámia

http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/3/09_frankgyorgy.pdf (Letöltve: 2013.10.29.)

Kevlár

<http://www.dupont.de/produkte-und-dienstleistungen/materialien-fasern-vliesstoffe/fasern/marken/kevlar/produkte/kevlar-acv.html>

(Letöltve: 2013.10.29)

Kommunikáció

<http://www.spiegel.de/kultur/gesellschaft/medien-und-terrorismus-tausendundein-missverstaendnis-a-472517.html>

(Letöltve: 2014.10.11.)

Lemezszekrények, biztonsági szekrények, bútorszéf, páncélszekrény.

<http://www.mabisz.hu/hu/component/content/article/19-biztonsagtechnika/353-biztonsagtechnikai-fogalomtar.html> (Letöltve: 2014.10.01.)

... „Magyarországon ezen irányzat a jellemző, mert 2013-ban kb. 97.000 vagonvédelmemmel foglalkozó személy kötelezett különböző szintű vizsgára”...

<http://biztonsagpiac.hu/mintegy-szazezren-vegzik-el-iden-a-kotelezo-tovabbkepzest>

(Letöltve: 2014.09.21.)

Magyar GDP eloszlása (2013)

<http://statinfo.ksh.hu/Statinfo/haViewer.jsp?wcf9e2b1f9a=x>

(Letöltve:2014.10.10.)

NATO 2020: Assured security; dynamic engagement

<http://www.nato.int/strategic-concept/expertsreport.pdf>,

(Letöltve: 2010.07.01)

www.nbf.hu , Nemzeti Biztonsági Felügyelet (NBF)

Németország GDP-jének eloszlása a szerző saját számítása alapján

<http://www.cio.de/top500>

(Letöltve: 2014.10.12.)

... „Németországban ez a szám kb. 185.000 főt jelentett 2013-ban” ...

<http://de.statista.com/statistik/daten/studie/258775/umfrage/beschaeftigten-bei-privaten-wach-und-sicherheitsdiensten-nach-bundeslaendern/>

(Letöltve: 2014.09.21.)

OKF: Rendkívüli események Magyarország területén,
http://www.katasztrofavedelem.hu/index2.php?pageid=lakossag_esemeny_terkep
(Letöltve: 2015.12.11.)

Országos Meteorológiai Szolgálat (OMSZ): *Meteorológiai világ és kontinens rekordok*
http://owww.met.hu/omsz.php?almenu_id=misc&pid=met_rekordok&pri=1&mpx=3&stt=vilagrekordok
(Letöltve: 2016.11.20.)

OMSZ: Vészjelzés, riasztás
<http://www.met.hu/idojaras/veszelyjelzes/riasztas/>
(Letöltve:2015.12.11.)

Pareto-elmélet
<http://www.absolventa.de/karriereguide/zeitmanagement/pareto-prinzip>
(Letöltve:2014.10.10.)

POLITIETS EFERRETNINGSTJENESTE, DANISH SECURITY AND INTELLIGENCE SERVICE, *The role of the Internet in relation to radicalization and terrorism*, 15.
September 2008
[Center for Terror Analysis \(CTA\)](#)
(Letöltve: 2014.10.10.)

REPORT OF THE UNITED NATIONS CONFERENCE ON THE HUMAN ENVIRONMENT, Stockholm 1972,
<http://www.unep.org/Documents.Multilingual/Default.asp?DocumentID=97>
(Letöltve: 2014.11.05.)

RSOE EDIS - Emergency and Disaster Information Service,
<http://hisz.rsoe.hu/alertmap/index2.php>
(Letöltve: 2014.07.11.)

SAXTON, Jim (R-NJ): Chairman Joint Economic Committee United States Congress: *The Economic Cost of Terrorism*, p. 11.
http://www.jec.senate.gov/public/_cache/files/79137416-2853-440b-9bbe-e1e75d40a79d/the-economic-costs-of-terrorism---may-2002.pdf
(Letöltve:2015.01.05.)

STAATSSSEKRETARIAT FÜR WIRTSCHAFT SECO: *Auswirkungen der Terroranschläge auf die Weltwirtschaft*,
<http://www.seco.admin.ch/themen/00374/00375/00381/05253/index.html>
(Letöltve:2015.01.05.)

„Seat at the Executive”

http://humanresources.about.com/strategichr/a/exec_success.htm (28.august 2011)

(Letöltve: 2014.07.11)

„szikáriusok a lat. *sica*, 'kis tör' szóból: 'törviselők'

<http://lexikon.katolikus.hu/S/szik%C3%A1riusok.html>

(Letöltve: 2014.10.11.)

The UN Refugee Agency : *Global Trend 2013*,

<http://www.unhcr.org/5399a14f9.html>

(Letöltve: 2015.01.12.)

TrendsDerZukunft.de, Heidorn GmbH: Staatsverschuldung der USA – Wer sind die Gläubiger?

<http://www.trendsderzukunft.de/staatsverschuldung-der-usa-wer-sind-die-glaebiger/2009/03/30/>

(Letöltve: 2014.12.02.) 09/2009

UNESCO, Magyar Nemzeti Bizottság: A fenntartható fejlődés fogalma, célkitűzése,

<http://www.unesco.hu/termesztudomany/fenntarthato-fejlodesre/fenntarthato-fejlodes-091214> (Letöltve: 2014.11.10.)

Verfassungsschutzbericht 2013, p. 191-205

www.verfassungsschutz.de/download/vsbericht-2013.pdf

(Letöltve: 2014.08.25.)

OVF: Árvíz-, belvízvédelmi készültségi fokozatok:

<http://www.vizugy.hu/?mapModule=OpArviz&mapData=ArvizTajekoztatok>

(Letöltve:2015.12.11.)

WALKER, W.E.: *The use of scenarios and gaming in crisis management planning and training*, (RAND 1995) p.7,

<https://www.rand.org/content/dam/rand/pubs/papers/2009/P7897.pdf> (Letöltve:

2015.09.21.)

JOGSZABÁLYOK

89/391 irányelv - A munkahelyi biztonságról és egészségvédelemről szóló "keretirányelv"

96/82/EK IRÁNYELVE, a veszélyes anyagokkal kapcsolatos súlyos baleseti veszélyek szabályozásáról

Magyarország Alaptörvénye, 2011. április 25.

1993. évi XCIII. törvény, a Munkavédelemről

1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

2005. évi CXXXIII. Törvény, a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

2011. évi CXII. törvény, az információs önrendelkezési jogról és az információszabadságról

2011. évi CXIII. törvény, a honvédelemről és a Magyar Honvédségről

2011. évi. CXXVIII. törvény, a katasztrófavédelemről és a hozzákapcsolódó egyes törvények módosításáról

2012. évi I. törvény, a munka törvénykönyvéről

2012. évi CLXVI. törvény, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2012. évi XXXVI. törvény, az Országgyűlésről

89/1995. (VII. 14.) Kormányrendelet, a foglalkozás-egészségügyi szolgálatról

16/1999. (II.5.) Kormányrendelet, a rendőrség ellenérték fejében végezhető szolgáltató tevékenységéről

128/2001. (VII.13.) Kormányrendelet, az Egyesült Nemzetek Szervezetének Európai Gazdasági Bizottság keretében létrejött, az ipari balesetek országhatáron túli hatásairól szóló Helsinkiben, 1992. március 17-én kelt Egyezmény kihirdetéséről.

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

2080/2008. (VI. 30.) Kormányhatározat, a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

295/2010. (XII. 22.) Kormányrendelet, a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól

295/2010. (XII. 22.) Kormányrendelet, a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól

1176/2010. (VIII. 19.) Kormányhatározat, a közbiztonság megerősítésével kapcsolatos egyes költségekkel összefüggésben a 2010. évi központi költségvetés általános tartalékanakelőirányzatából történő felhasználásról, valamint a terrorfelderítés műveleti koordinációjáról és a Terrorellenes Koordinációs Bizottság létrehozásáról szóló 2239/2005. (X. 28.) Korm. határozat módosításáról

1249/2010. (XI.19.) kormányhatározat, az európai kritikus infrastruktúrákról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK

23/2011. (III.8.) korm. rendelet, a zenés, táncos rendezvények működésének biztonságosabbá tételéről,

219/2011. (X.20.) Kormányrendelet, a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

234/2011. (XI.10.) kormányrendelet, a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

239/2011. (XI. 18.) Kormányrendelet, az önkormányzati és létesítményi tűzoltóságokra, valamint a hivatásos tűzoltóság, önkormányzati tűzoltóság és önkéntes tűzoltó egyesület fenntartásához való hozzájárulásra vonatkozó szabályokról

259/2011. (XII. 7.) Kormányrendelet, a tűzvédelmi hatósági feladatokat ellátó szervezetekről, a tűzvédelmi bírságról és a tűzvédelemmel foglalkozók kötelező élet- és balesetbiztosításáról

278/2011. (XII.20.) kormányrendelet, a NATO Válságreagáló Rendszerével összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről

38/2012. (III. 12.) Kormányrendelet, a kormányzati stratégiai irányításról

1035/2012. (II. 21.) Korm. határozata: Magyarország Nemzeti Biztonsági Stratégiájáról

65/2013. (III. 8.) kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

27/1995. (VII.25) NM rendelet, a foglalkozás-egészségügyi szolgáltatásról

27/1996. (VIII. 28.) NM rendelet, a foglalkozási betegségek és fokozott expozíciós esetek bejelentéséről és kivizsgálásáról

9/2007. (IK 8.) IRM-ÖTM együttes utasítás, a terrorizmus elleni egységes végrehajtására, Minősítés törölve IRM/TÜK/40322/2008. sz

28/2011. (IX.6) BM rendelet a beépített tűzoltó rendszerekről

54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról

SZABVÁNYOK, UTASÍTÁSOK:

DIN EN 50 131, Betörésjelző rendszerek

DIN EN ISO 22311, Videó megfigyelő rendszerek

ISO 31000: Risk management – Principles and guidelines

MSZ 28001:2008 (BS OHSAS 18001:2007) A szakpolitika alapját a munkahelyi egészségvédelem és biztonsági irányítási rendszerének (MEBIR:) kialakítása és tanúsítása az szerint

MSZ EN ISO 9000-es sorozatok, Minőségirányítási rendszerek.

ISO 27001:2013, Nemzetközi szabvány az Információ Biztonság Irányítási Rendszerekre

MSZ EN 3, Tűzoltó készülékek

MSZ EN 671-3, Beépített tűzoltó berendezések. Tömlőberendezések

MSZ 1040, Régi szabványú tűzoltó készülékek

MSZ EN 1630, Bejárati ajtók, ablakok, függönyfalak, rácsok és redőnyök. Betörésállóság. Vizsgálati módszer a kézi betörési kísérlettel szembeni ellenálló képesség meghatározására

MSZ EN 1063, Építési üveg. Biztonsági üvegezés.

MSZ EN 54, Tűzjelző berendezések

MSZ EN15004-1, Beépített tűzoltó berendezések. Gázzal oltó berendezések. 1. rész: Tervezés, létesítés és karbantartás (ISO 14520-1:2006, módosítva)

MSZ EN 9783, Szén-dioxiddal oltó berendezés

MSZ EN 12101, Füst- és hőszabályozó rendszerek

RÖVIDÍTÉSEK JEGYZÉKE

4G Negyedik generációs hadviselés

AH Alkotmányvédelmi Hivatal

AIDS Acquired Immune Deficiency Syndrome (angol), szerzett

immunhiányos tünetegyüttes

ABV	Atom- biológiai-vegyi
BJR	Behatolásjelző rendszer
BRM	Biztonsági Rizikó Menedzsment, Security Risk Management (angol)
CEP	Civil Emergency Planning (angol), Polgári Veszélyhelyzeti Tervezés (NATO)
CIIP	critical information infrasructure protection (angol), kritikus információs infrastruktúrák védelme
DoD	Deparment of Defense, Védelmi Minisztérium
DTM	Digital Terrain Modell, digitális térmodell
EÁP	Ellenőrző áteresztő pont
EDR	Egységes Digitális Rádiótávközlő Rendszer
EGB	Európai Gazdaság Bizottság
EMÜ	együttműködés
EN	European Standard, Európai Szabvány
ENSZ	Egyesült Nemzetek Szervezete, United Nations, (angol) rövidítése: UN
EU	Európai Unió
EU INTCEN	EU Intelligence Centre, EU Hírszerző Elemző Központ
EU SitRoom	EU SITUATION ROOM, EU Helyzetelemző „Részleg”
FED	Federal Reserve System (angol), Szövetségi Tartalék Rendszer
GATT	General Agreement on Tariff and Trade (angol), Általános Vám- és Kereskedelmi Egyezmény
GDP	Gross Domestic Product (angol), mérőszám: egy adott idő alatti gazdasági termelés

GIS	Geographical Information System (angol), térbeli adatok gyűjtése, tárolása, adatbázis kialakítása
GO	government organisation (angol), kormányzati (állami) szervezet
HJMŰ	harcjármű
HRA	Health Risk Assessment (angol), egészségügyi kockázatok
HUF	magyar forint
HUMINT	Human Intelligence, humán forrásokkal (személyekkel) hírszerzés
ICT	Information and Communication Technology (angol), Információ és Kommunikáció Technológia
ILO	International Labour Organization (angol), Nemzetközi Munkaügyi Szervezet
IP	Internet Protokoll, hálózati szabvány
IPCC	Intergovernmental Panel on Climate Change, Éghajlat-változási Kormányközi Testület
IPCR	Integrated Political Crisis Response, Integrált Politikai Válságkezelés
IS	Islamic State (angol), Iszlám Állam
ISO	International Organization for Standardization, Nemzetközi Szabványügyi Szervezet
IT	Information technology (angol), információs technológia
Itv	Információs önrendelkezési jogról és az információszabadságról szóló törvény
JIT	Just-In-Time (angol), vezetélmélet, „éppen időben”
KI	kritikus infrastruktúra
KIV	kritikus infrastruktúra védelem
KRESZ	Közúti Rendelkezők Egységes Szabályozása

LED	<i>Light-Emitting Diode</i> , fényt kibocsátó dióda
MKI	Megyei Katasztrófavédelmi Igazgatóság
MSc	master of science (angol), mesterképzés, mester diploma
MSZ	Magyar Szabvány
NATO	North Atlantic Treaty Organisation (angol), Organisation du Traité de l'Atlantique Nord, OTA (francia), Észak-atlanti Szerződés Szervezete
HQ SitCen	Headquarters SITUATION CENTER, Központi Helyzetelemző Központ (NATO)
NBF	Nemzeti Biztonsági Felügyelet
NCSR	Crisis Response System (angol), NATO Válságreakálási Rendszer
nGO	non Government Organisation (angol), nem kormányzati (állami) szervezet
NKIV	Nemzeti kritikus infrastruktúra védelem
NNI	Nemzeti Nyomozó Iroda
OKF	Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság
ORFK	Országos Rendőr-főkapitányság
OMSZ	Országos Meteorológiai Szolgálat
OSINT	Open Source Intelligence, nyílt információs források
OTSZ	Országos Tűzvédelmi Szabályzat
RENEGADE	"repülő eszköz fegyverkénti használata"
RFID	Radio Frequency Identification, Rádió frekvenciás azonosítás és adatközlés
SitCen	Situation Centre (angol), Helyzetelemző és válságkezelő központ

SCEPC	Senior Civil Emergency Planning Committee (angol), Polgári Védelmi Tervező Főbizottság (NATO)
SOF	Special Operations Forces (angol), különleges műveleti erők
TEK	Terrorelhárítási Központ
TEEO	Terrorizmus és Extrémizmus Elleni Osztály
TÜO	tűzoltó
TECHINT	Technical Intelligence, Technikai hírszerzés
TESZ	Terrorelhárító Szolgálat
UFC	Unified facilities Criteria, Egységes Létesítési Szempontok
UNHCR	United Nations High Commissioner for Refugees (angol), Egyesült Nemzetek Menekültügyi Főbiztosa
UNESCO	United Nations Educational, Scientific and Cultural Organization (angol), Egyesült Nemzetek Nevelésügyi, Tudományos és Kulturális Szervezete
USA	United States of America, Amerikai Egyesült Államok
VIP	Very Important Person, különleges elbánásban részesítendő személy
WEF	World Economic Forum (angol), Világgazdasági Fórum
WTO	World Trade Organization (angol), Kereskedelmi Világszervezet

ÁBRAGYŰJTEMÉNY

Fsz.	Cím	Forrás	Oldal
1.számú ábra	Kihívások, fenyegetések és kockázatok (szerző által átszerkesztve)	Dr. Resperger István mk. ezredes, Felderítő szemle, 2013/3, p. 6., http://www.knbsz.gov.hu/hu/letolt/es/fsz/2013-3.pdf (Letöltve: 2014.08.19.)	16
2. számú ábra	Olajár 1970-től	Bundeszentrale für politische Bildung, http://www.bpb.de/politik/hintergrund-aktuell/172918/autofreier-sonntag-1973 (Letöltve: 2014.12.29.)	47
3. számú ábra	Biztonsági modell	a szerző összeállítása	65
4. számú ábra	Biztonsági szervezetek	a szerző összeállítása	66
5. számú ábra	Biztonsági költségek megoszlása	a szerző összeállítása	67
6. számú ábra	Biztonsági területek költségeinek megoszlása	a szerző összeállítása	68
7. számú ábra	KIV fő funkciói	Dr. Király-László Medveczky: Védelemgazdasági ismeretek önkormányzati (védelemi igazgatási) válság menedzsereknek. Budapest, 2009.	79

		ZMNE. ISBN 978-963-7060-75-5., 76. oldal (a szerző szerkesztésében)	
8. számú ábra	A magyar GDP eloszlása, 2013, Forrás: GDP 2013 eloszlása a szerző saját számítása szerint	http://statinfo.ksh.hu/Statinfo/haVierwer.jsp?wcf9e2b1f9a=x (Letöltve:2014.10.10.)	81
9. számú ábra	TOP 50 magyar vállalat tevékenység szerinti megoszlása	a szerző összeállítása	82
10. számú ábra	A termelő vállalatok értékelése telephelyek száma szerint	a szerző összeállítása	83
11. számú ábra	Németország GDP-jének eloszlása a szerző saját számítása alapján	http://www.cio.de/top500 (Letöltve: 2014.10.12.)	84
12. számú ábra	Munkavédelem, mint folyamatorientált tevékenység	Rozman Tamás, BMGE, Tananyag, II. rész, p. 48)	100
13. számú ábra	A vezető feladata	Rozman Tamás, BMGE, Tananyag, II. rész, p. 50	102
14. számú ábra	Fenyegetések hatása a valószínűsíthető károk	a szerző szerkesztésében	180
15. számú ábra	A vállalat válságkezelő szervezetei	a szerző szerkesztésében	181
17. számú ábra	Krízismenedzsment szervezete	a szerző szerkesztésében	185
18. számú ábra	SitCen biztonsági rendszereinek kapcsolata	a szerző szerkesztésében	190
19. számú ábra	SitCen	a szerző szerkesztésében	191

MELLÉKLETEK

1. számú melléklet: A kritikus infrastruktúra fejlesztésénél várható biztonsági költségek
2. számú melléklet: A vállalat biztonsági stratégiája
3. számú melléklet: Tűzvédelmi rendszerek és a Létesítményi tűzoltóság
4. számú melléklet: Vagyonvédelem
5. számú melléklet: Terrorelhárítási feladatok

1. számú melléklet



A kritikus infrastruktúra fejlesztésénél várható biztonsági költségeket

A védelmi felkészítés finanszírozásának 1/20-es és 1/10 szabálya

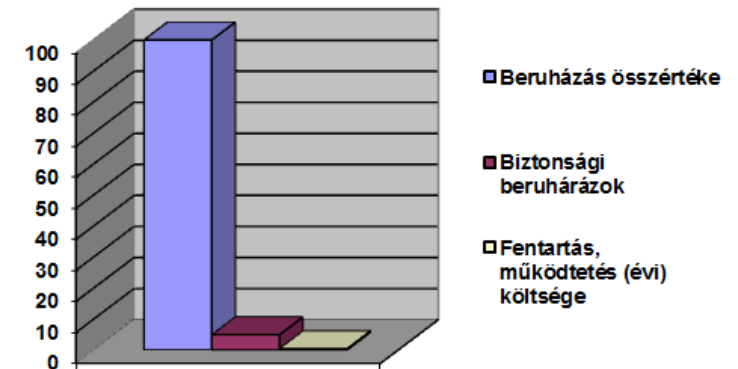


- a tervezett beruházás nagysága (K) egyrészt,
- a védelmi célú beruházásokra előirányzott fejlesztési forrás (B) másrészt és
- a folyó védekezési felkészülésre (a megelőzésre) fordítandó kiadások (V) aránya
- 100:5:0,5 vagyis 1/20 illetve 1/10-es hányadosú mértani sorozatot alkot.
- $K : B : V = 100 : 5 : 0,5$ ahol:

K – beruházás nagysága,

B – a védelmi célú beruházásokra előirányzott fejlesztési forrás,

V – a folyó védekezési felkészülésre (a megelőzésre) fordítandó kiadások



Építés fázisában



Ha egy beruházás összértéke 1000 mrd. Ft., akkor a fent említett „arany szám” alapján a biztonsági rendszer költsége 50 mrd. Ft. Természetesen ebbe az összegbe bele értendő az építés során felmerülő őrzés, tűzvédelmi és egyéb más (munka-, környezetvédelmi) költségek is.

■ Őrzés-védelem	150.000.000 Ft.
■ Tűzvédelem	200.000.000 Ft.
■ Munka-,környezetvédelem	300.000.000 Ft.



Tervezés és megvalósítás fázisában

■ Periféria védelem (kerítés, porták, beléptető és videó megfigyelő rendszer)	8 mrd. Ft.
■ Épületek, csarnokok vagyonvédelmi rendszerei	4 mrd. Ft.
■ Épületek, csarnokok tűz- és polgárvédelmi, iparbiztonsági rendszerei	10 mrd. Ft.
■ SitCen	3 mrd. Ft.
■ Létesítményi Tűzoltóság (GJMŰ-vek, felszerelések...)	1 mrd. Ft.
■ Egyéb biztonsági rendszerek (vészvilágítás, szellőztetők...)	3 mrd. Ft.
■ Munkavédelmi berendezések, felszerelések	9 mrd. Ft.
■ Környezetvédelmi berendezések, felszerelések	8 mrd. Ft.
■ Egészségügyi szolgáltatások	3 mrd. Ft.



A működtetés, fenntartás költségei

Vagyonvédelem	1.000 miO. Ft.
Tűzvédelem	1.300 miO. Ft.
Katasztrófavédelem, iparbiztonság, polgári védelem	200 miO. Ft.
Munkavédelem	800 miO. Ft.
Környezetvédelem	1.100 miO. Ft.
Egészségügyi szolgálat	600 miO. Ft.

Természetesen ezen adatok is csak tájékoztató jellegűek!

2. számú melléklet



A vállalat biztonsági stratégiája

A vállalat biztonsági stratégiája



Vízió

Konzern stabil beszállítója

Biztonságfilozófia

A vállalattal kapcsolatba került emberek biztonsága és a vállalat működőképességének biztosítása.

Biztonságkultúra



Szakterületek

Biztonságpolitika

Munkabiztonság

Környezetvédelem

Egészségvédelem

IT-biztonság

Felelősség

Munkatárs

Vezetők

Beavatkozó erők

Szakterület

Vállalat vezetés

A biztonságkultúra alapjai



- A vállalat **Biztonsági Stratégiája irányt ad**, és megmutatja a közös utunkat a **víziókhöz** „Konzern stabil beszállítója“.
- Ez képviseli a vállalat **fő célkitűzését**, amivel hozzájárul a **Vállalati Stratégia 2025 vállalati víziójához**: „Vállalat – az 1. számú prémiummárka”.
- **Víziónk** és a **biztonságfilozófiánk** közösen alkotja a működésünk **alapját**. Minden **munkatárs felelős** a biztonsági célok **végrehajtásáért** és **betartásáért**.

A vállalat veszélyforrásai



Fenyegetések

- ▶ Világgazdasági helyzet
- ▶ Források kimerülése
- ▶ Migrációs nyomás
- ▶ Demográfiai változások
- ▶ Klímaváltozás



Fenyegetések

- ▶ Források az instabil régiókban
- ▶ Járványok / fertőzések
- ▶ Fundamentalizmus
- ▶ Terrorizmus
- ▶ Ökológiai destabilizáció



Rizikók

- ▶ Extrém időjárás
- ▶ Baleset, tüzeset, katasztrófák
- ▶ Környezeti károsodás
- ▶ Információbiztonság
- ▶ Beszállítói kapacitások szűkülése



Biztonságkultúra



Szakterületek felelőssége



Tudományos alapok



Biztonságtudatos munkatársak

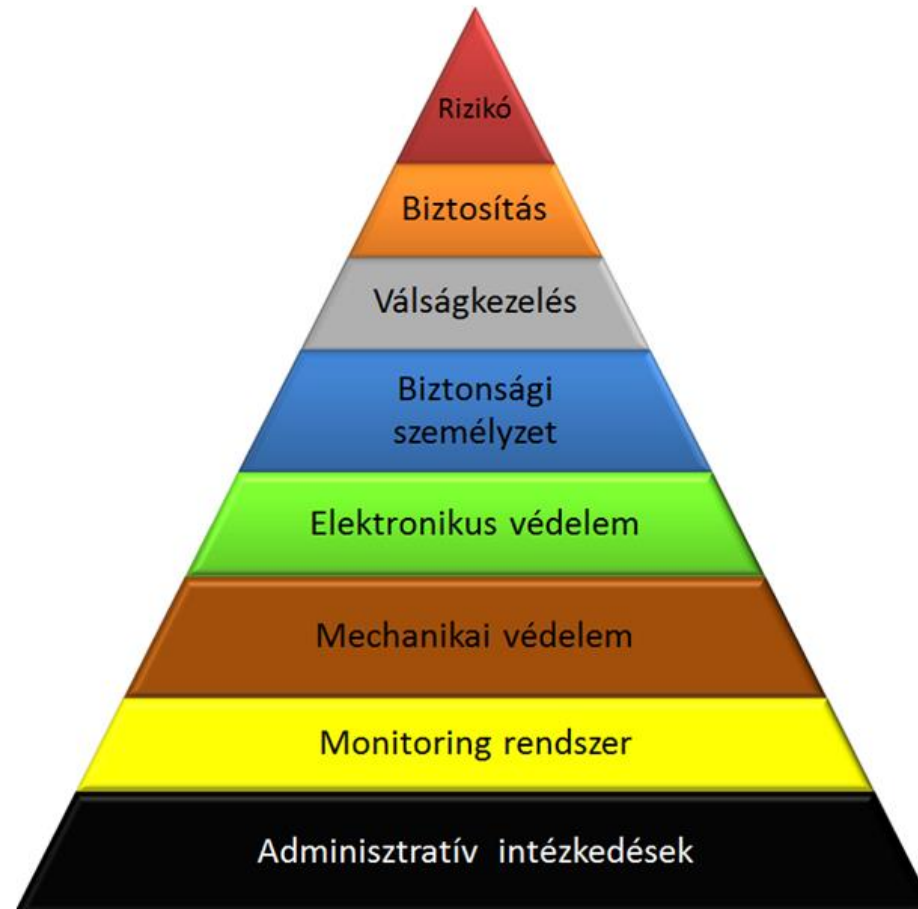


Beavatkozó erők



- A vállalat biztonságkultúrája integrálja a **négy irányvonalat, melyek eléréséhez egyedi intézkedések határozhatóak meg.**
- Ezen célok követése a stratégia **sikeres végrehajtásának alapja.**

A vállalat biztonsági modellje [1]



A vállalat biztonsági dokumentumai



■ Biztonsági stratégia

- Biztonságpolitika
- Biztonsági szervezetek
 - Munkabiztonsági politika
 - Környezetvédelmi politika
 - Egészségvédelmi politika
 - IT-biztonságpolitika
 - Vállalat vezetés belső irányelvei

■ „A konzern” biztonsági előírásai

A vállalat biztonságáért felelős személyek és szervezetek



Munkatárs



A **biztonságtudat** azt jelenti, hogy munkatárs a biztonsági intézkedéseket elfogadja, végrehajtja és alkalmazza.

Vezetők



A biztonsági felelősség része a **vezetői felelősségnek**, mely szerint a vezető feladata a biztonsági intézkedések érvényre juttatása a saját területén.

Beavatkozó erők



A beavatkozó erők feladata, hogy a káreseményeket nagyságától függetlenül időben **felismerjék**, **riasszák** az érintetteket, **kárfelszámolás** és **kármentesítés**.

Szakterületek



Az új kihívások miatt **emelkedett** mind mennyiségileg mind minőségileg a **biztonsági veszélyforrások száma**. Ezekre a kihívásokra a **megfelelő válaszokat** a szakterületek készítik el és terjesztik.

Vállalat vezetés



A vállalat vezetés a biztonsági dokumentumokat **jóváhagyta** és a belső irányelveket **kiadta**.

3. számú melléklet



Tűzvédelmi védelmi rendszerek és Létesítményi tűzoltóság

1. Tűzvédelem

1.1 Mechanikai védelem



Tűzgátló ajtó

Forrás: szerző saját felvétele



Tűzgátló tolókapu

<http://projektajto.hu/tuzgatlo-kapuk/tuzgatlo-tolokapu>

(Letöltve: 2014.10.01.)



Tűzgátló bevonatok

<http://www.anyagvedelem.hu/index.php?stilus=lap&hiv=443&forr=7>

(Letöltve: 2014.10.01.)

1. Tűzvédelem

1.2 Tűzjelzők, központok



Kézi tűzjelző

Forrás: szerző saját felvétele



Pontszerű érzékelők

http://Forrás: szerző saját felvétele



Tűzjelző központ

https://www.schrack-seconet.com/hu/products_solutions/fire_alarm/firealarm_control_panels/integral-ip-mxf/index.html

(Letöltve: 2014.10.01.)

1. Tűzvédelem

1.3 Automata oltórendszerek



Automata gázzal oltó központ

Forrás: szerző saját felvétele



SPRINKLER központ

Forrás: szerző saját felvétele



Sprinklerfej

Forrás: szerző saját felvétele

1. Tűzvédelem

1.4. Tűzoltó készülékek, fali tűzcsapok



Tűzoltó készülék

Forrás: szerző saját felvétele



**Kombinált fali tűzcsap
szekrény**

Forrás: szerző saját felvétele



Tűzcsap földfeletti

<http://www.euromix.hu/webshop/groupcontent/979/csatornazasi-anyagok/tuzcsap.html>

Forrás: szerző saját felvétele

2. Létesítményi tűzoltóság személyzete és felszerelése



Forrás: a szerző saját felvételei

4. számú melléklet



Vagyonvédelem

1. Mechanikai védelem

1.1 Kerítések



Kerítés lakóövezetben

http://luxart.hu/wp-content/uploads/2013/02/kapu-es-keritesmezo_941.jpg
(Letöltve: 2014.10.01.)



Mobilkerítés (ideiglenes)

http://www.szakaly2000.hu/termek/big/1377078737_636.jpg
(Letöltve: 2014.10.01.)



Ipari kerítés

Forrás: szerző saját felvétele

1. Mechanikai védelem

1.2. Bejáratok



Forgókapu

http://www.zaunbau-leis.de/images/drehkreuze/drehkreuz_1.jpg (Letöltve: 2014.10.01.)



Gyorskapu beléptető rendszerrel vezérelve

http://www.szakaly2000.hu/termek/big/1377078737_636.jpg
(Letöltve: 2014.10.01.)



Vészkijárat-vezérlőrendszer

<http://media1.heinze.de/media/61396/images/14765482px600x338.jpg>
(Letöltve: 2014.10.01.)

1. Mechanikai védelem

1.3 Sorompók, akadályok



Sorompó

Forrás: szerző saját felvétele



New Jersey elem

Forrás: szerző saját felvétele



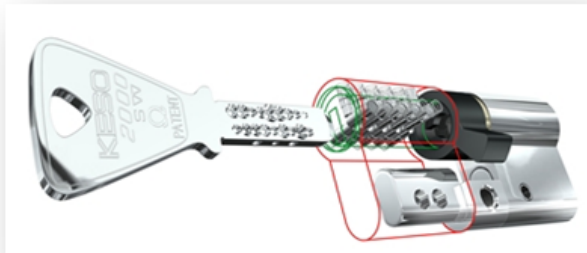
Poller

http://upload.wikimedia.org/wikipedia/commons/6/6a/Der_Homberger_Poller.jpg

(Letöltve: 2014.10.01.)

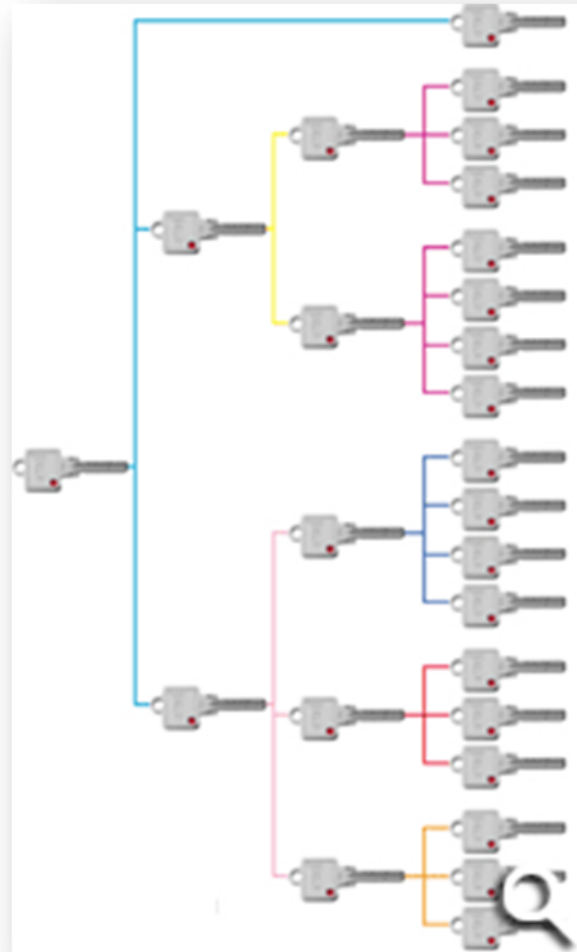
1. Mechanikai védelem

1.4. Zárak, zárrendszerek



Mechanikus kulcsrendszer

Forrás: <http://www.keso.de/de/site/keso-de/Services/Downloadcenter/Mediathek/>
(Letöltve: 2014.10.01.)

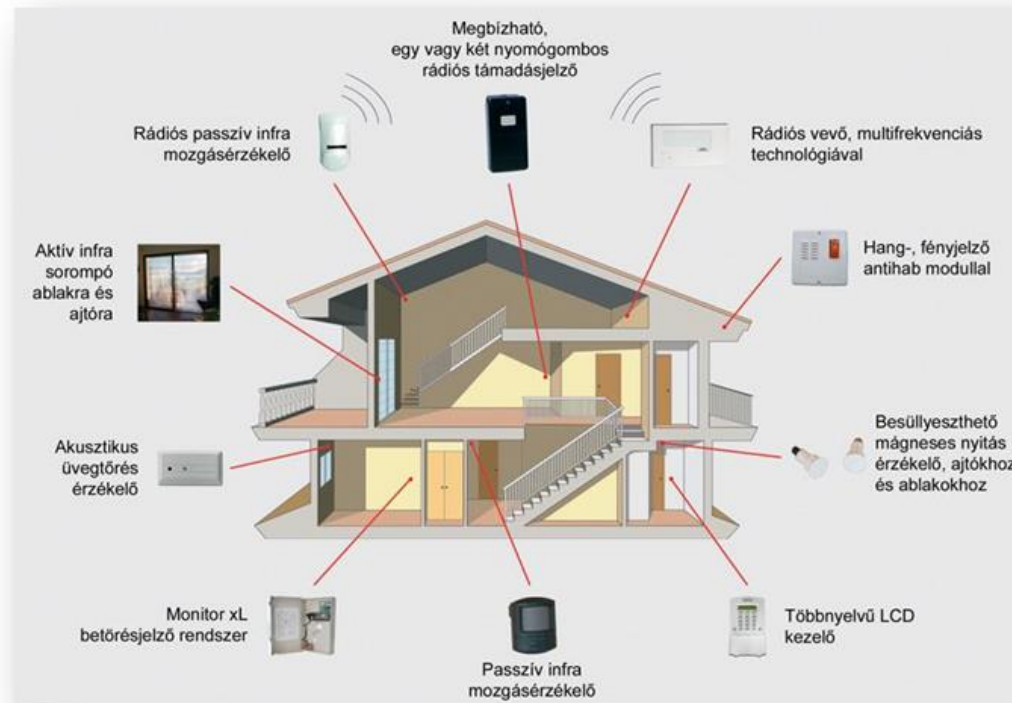


Főkulcsrendszer

<http://www.schlusseldienst-ruhrgebiet.de/schliessanlagen.htm>
(Letöltve: 2014.10.01.)

2. Technikai védelem

2.1 Behatolás jelzők, központok



Behatolás jelzők és központ

<http://www.fittich.hu/modularis-betoresjelzo-rendszer-25.html> (Letöltve: 2014.10.01.)

2. Technikai védelem

2.2. Beléptető rendszerek



Forgókereszt

Forrás: szerző saját felvétele



Beléptető rendszerrel felszerelt zónahatár

Forrás: szerző saját felvétele



Ujjlenyomat

http://www.vs-sicherheit.de/zutrittssysteme-schliess-systeme/art/444_-_buw_tse_allgemein_2_4c_ok.jpg
(Letöltve: 2014.10.01.)

2. Technikai védelem

2.3. Videómegfigyelő rendszerek



**Dinamikus kamera,
mozgásérzékelők**

Forrás: szerző saját felvétele



Speed-dome kamera

Forrás: szerző saját felvétele



Monitorfal

<http://www.avisec.ch/angebote/videoueberwachungssysteme/>

(Letöltve: 2014.10.01.)

3. Egyéb vagyonvédelem eszközök



**Sziréna, hangosbemondó,
Menekülési út jelző**

Forrás: szerző saját felvétele



Kézi fémkereső

Forrás: szerző saját felvétele



Páncélszekrény

Forrás:

<http://www.pancelszekreny.hu/>

(Letöltve: 2014.10.01.)

4. Vagyonvédeleми személyzet



Elfogó csoport, gépjárművel

Forrás: szerző saját felvétele



Portaszolgálat

Forrás: szerző saját felvétele



Bevetési erők ruházata és felszerelése

Forrás:

<http://www.511tactical.com/>

(Letöltve: 2014.10.01.)

5. számú melléklet



Terrorelhárítási feladatai

Terrortámadások célja



- Bizonyos személyeket elraboljanak, túszokat ejtsenek, vagy objektumokat foglaljanak el és/vagy fontos berendezéseket semmisítsenek meg;
- A terroristák a média, a védelem gyengítése érdekében, célpontot nem csak ideológiai szempontok alapján választanak,
- Figyelmeztetés nélkül hajtják végre a sikeres támadást.
- Előtte pontosan felderítik a célpontok védelmét.

Terrorelhárítás elvei



1. Kidolgozott védelmi terv;
2. Kiképzett és begyakorlott személyzet (biztonsági);
3. Egyértelmű irányítás és vezetés.
4. Fontosabb intézkedések:
 - VIP programok, „csak akire tartozik”;
 - Biztonsági rendszerek üzemeltetése;
 - A terrorcselekmény helyének azonnali lezárása;
 - Biztonsági szolgálatok tájékoztatása;
 - Kiemelt biztonsági zónák mechanikus védelmének megerősítése;
 - Gépjármű- és személyi forgalom korlátozása;
 - Felkészülés a sérültek ellátására;
 - A terrorcselekmény helyszínén rekedt személyek élelemmel és vízzel való ellátása.

Szükségállapotok fokozatai



Az objektumok védelmét biztosító normál biztonsági intézkedéseket a helyi biztonsági szervezetekkel együttműködve kell kidolgozni.

A-fokozat: ha az objektum vagy személy ellen, lehetséges terrorcselekmények általános fenyegetettsége áll fenn, amely jellege és nagysága előre nem meghatározható, amikor a körülmények nem indokolják a B-fokozat rendszabályainak teljes körű alkalmazását.

B-fokozat: egy megnövekedett és jobban előrelátható terrorcselekmény fenyegetéséről van szó és hosszabb ideig is fenntartható.

C-fokozat: terrorcselekmény történik vagy ha olyan információk állnak rendelkezésre, hogy valószínűsíthető az objektum vagy személy ellen valamilyen formájú terrorcselekmény közeli bekövetkezése.

D-fokozat: ott kell alkalmazni, ahol terrorcselekmény történt, vagy ha olyan információkat kap a hírszerzés, hogy egy meghatározott helyen vagy személy elleni terrorcselekmény bekövetkezése nagyon valószínű. Ezt a fokozatot helyi biztonsági szervezetek határozzák meg és ez azt jelenti, hogy a következő 24 órában valószínű egy terrortámadás.

ALPHA



Végrehajtó	Feladat
Vállalat vezetés	Igazgató <u>tanács</u> tagjainak informálása, bevezetett intézkedések ellenőrzése
Vállalat biztonsági osztály	Tervek pontosítása, kapcsolat biztonsági szervekkel, vezetők tájékoztatás
Biztonsági szolgálat	Szigorított beléptetés, csomag ellenőrzés szűrőpróba szerűen
Megerősítő erők	-
Vezetők	-
Postaszolgálat	-
Logisztika	-

BRAVO



Végrehajtó	Feladat
Vállalat vezetés	Válságkezelő team összehívása, tájékoztatása
Vállalat biztonsági osztály	Kapcsolat biztonsági szervekkel, Igazgató tanács folyamatos tájékoztatása, vezetők tájékoztatás
Biztonsági szolgálat	Szigorított beléptetés, beléptető rendszer folyamatos üzemre kapcsolása, csomag ellenőrzés szűrőpróba szerűen, Védőeszközök készenlétének fokozása
Megerősítő erők	-
Vezetők (1. Jelentési szint)	Tájékoztatják a kialakult helyzetről a beosztott vezetőket
Postaszolgálat	Küldemények ellenőrzése
Logisztika	Veszélyes anyag raktárak fokozott ellenőrzése

CHARLEI



Végrehajtó	Feladat
Vállalat vezetés	A vállalat Krízis menedzsment összehívása
Vállalat biztonsági osztály	Kapcsolat biztonsági szervekkel, Igazgató tanács folyamatos tájékoztatása, vezetők tájékoztatás
Biztonsági szolgálat	Belépők 100%-os ellenőrzése (fémkeresők alkalmazása), Vendég fogadási tilalom
Megerősítő erők	„Check-point”-ok telepítése (fegyveres őrök)
Vezetők (1. Jelentési szint)	Tájékoztatják a kialakult helyzetről a beosztott vezetőket
Postaszolgálat	Küldemények 100%-os ellenőrzése
Logisztika	Veszélyes anyagok ki- és beszállításának folyamatos ellenőrzése az üzemi tűzoltóság által

DELTA

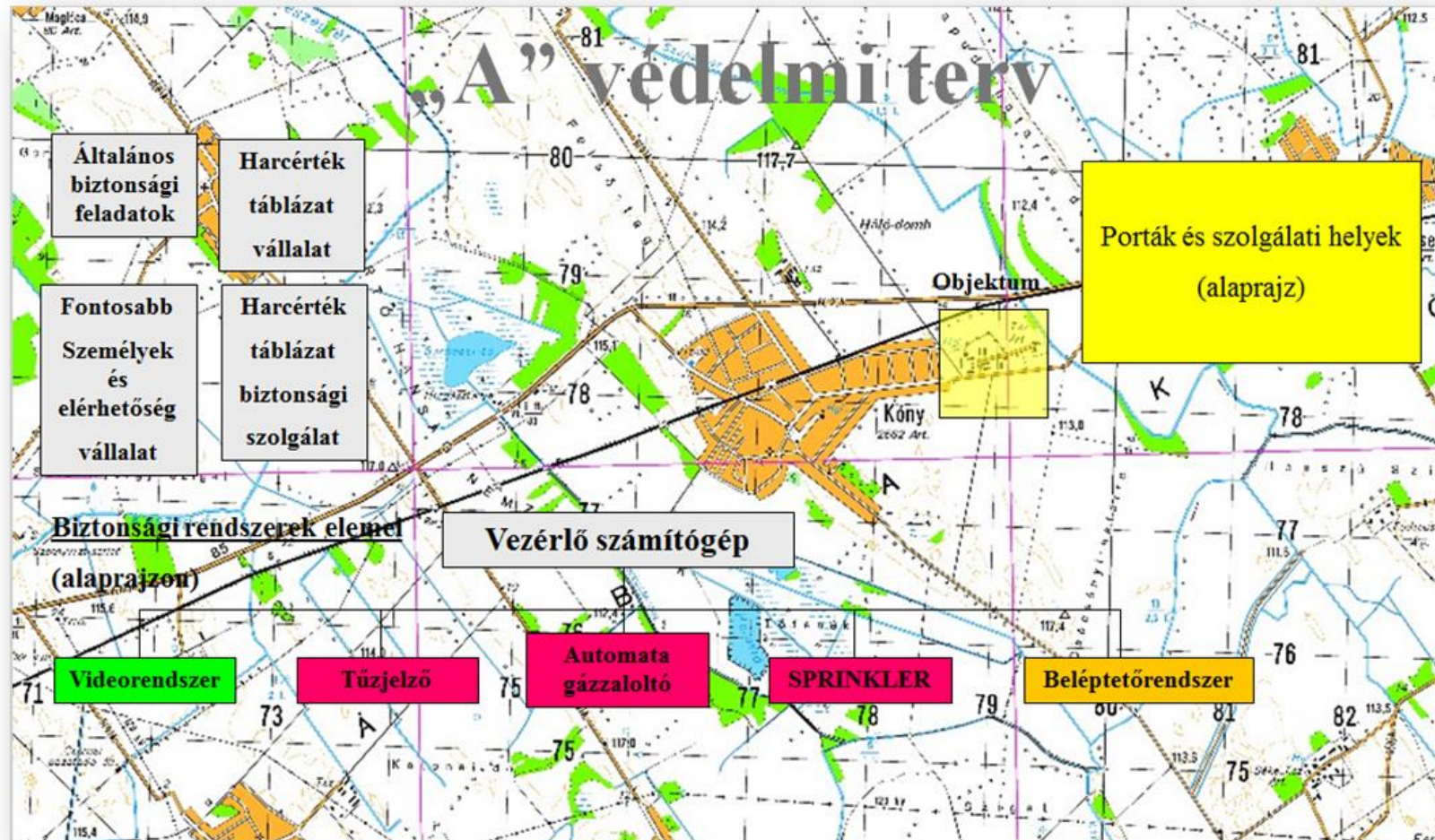


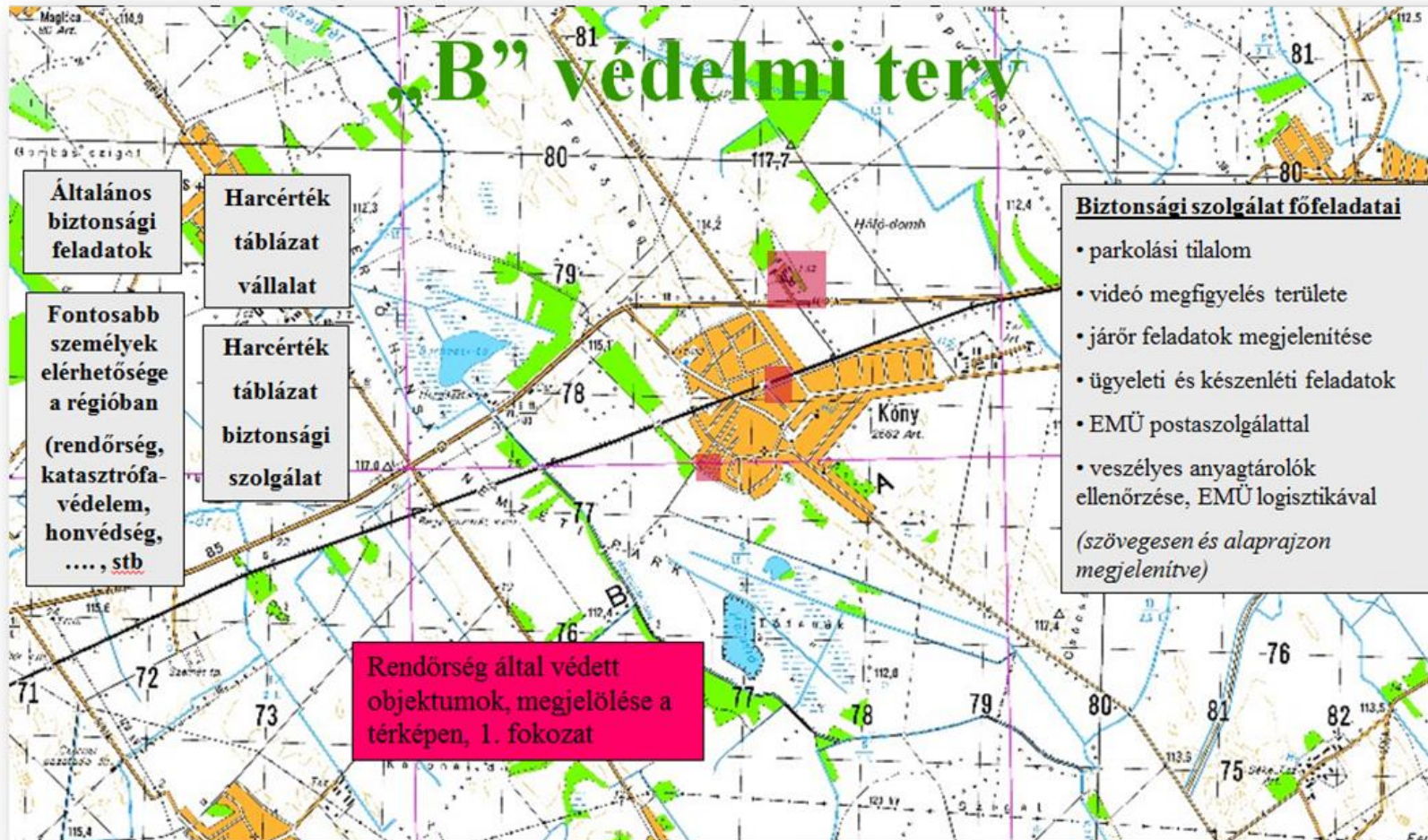
Végrehajtó	Feladat
Vállalat vezetés	A, B, C feladatok végrehajtása, Válságkezelő szervezet összehívása, munka megkezdése, üzleti utak lemondása, építőipari tevékenység szüneteltetése
Vállalat biztonsági osztálya	Kapcsolat biztonsági szervekkel, Igazgató tanács folyamatos tájékoztatása, vezetők tájékoztatás
Biztonsági szolgálat	Személyi védelem megszervezése
Megerősítő erők	Együttműködés a kirendelt biztonsági szervezetekkel
Vezetők (1. Jelentési szint)	Tájékoztatják a kialakult helyzetről a beosztott vezetőket
Postaszolgálat	Küldemények átvételének megtagadása
Logisztika	Veszélyes anyagok ki- és beszállításának megtiltása

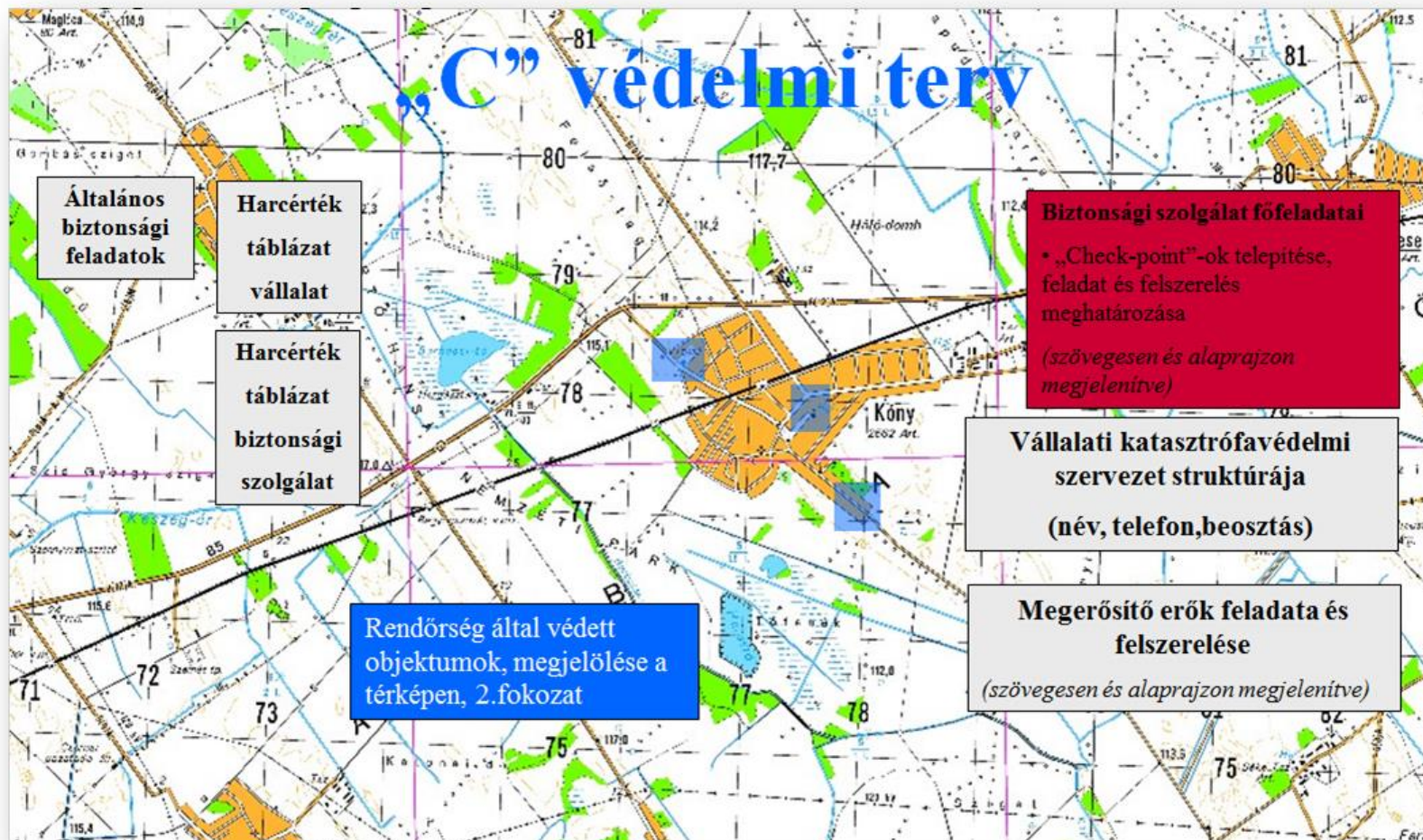
Mellékletek

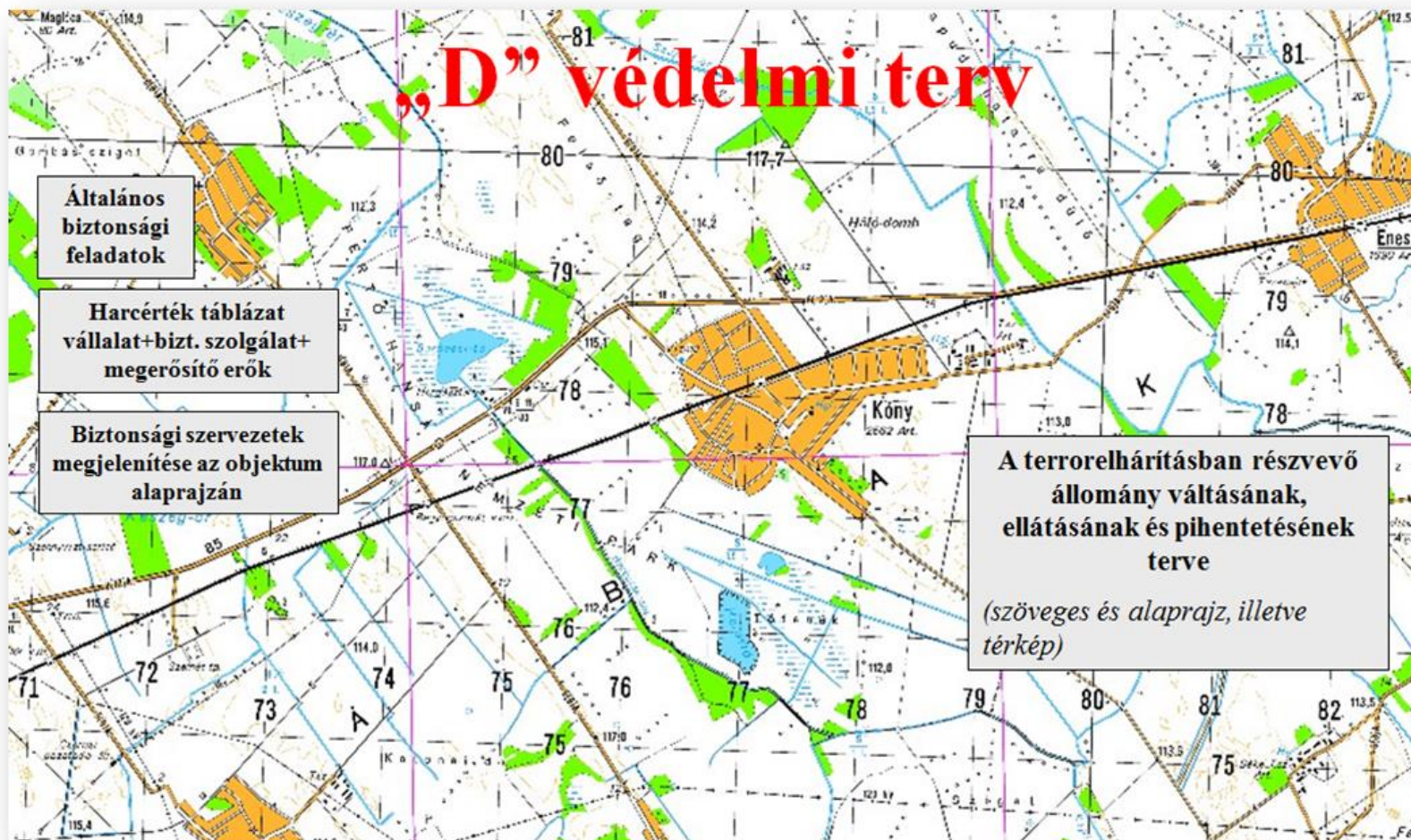


- **Térképek:** A, B, C, D biztonsági intézkedések végrehajtásához
Utasítások a biztonsági szervezetek részére: SITCEN, őrzés-védelem, létesítményi tűzoltóság, üzemorvos, háztechnikai ügyelet, számítástechnikai központ ügyeletes, logisztikai szolgáltató, környezetvédelmi szolgáltató, munkavédelmi megbízott
- **Erő és eszköz számvetés**
- **Híradás vázlata**
- **Személyi állomány pihentetése**

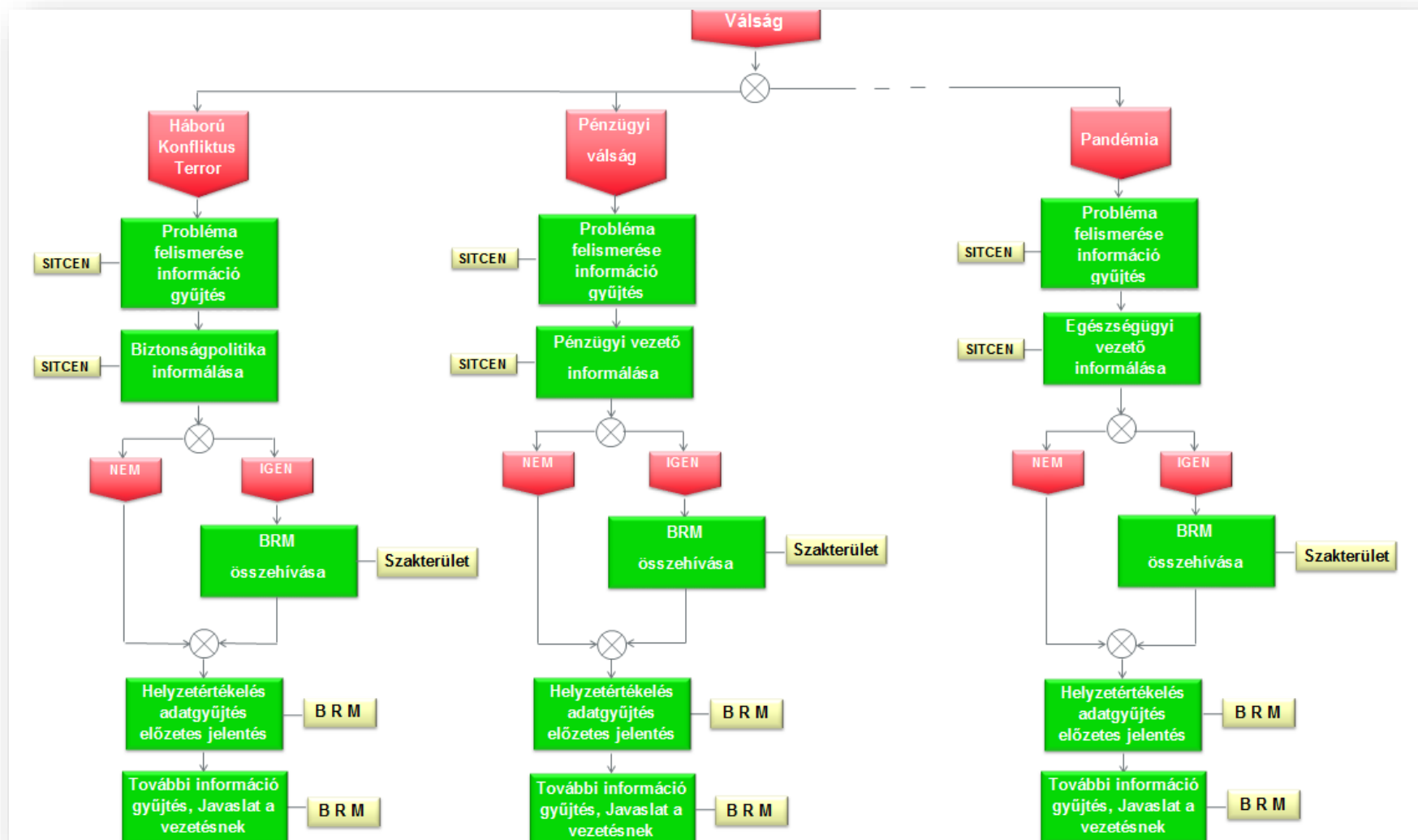




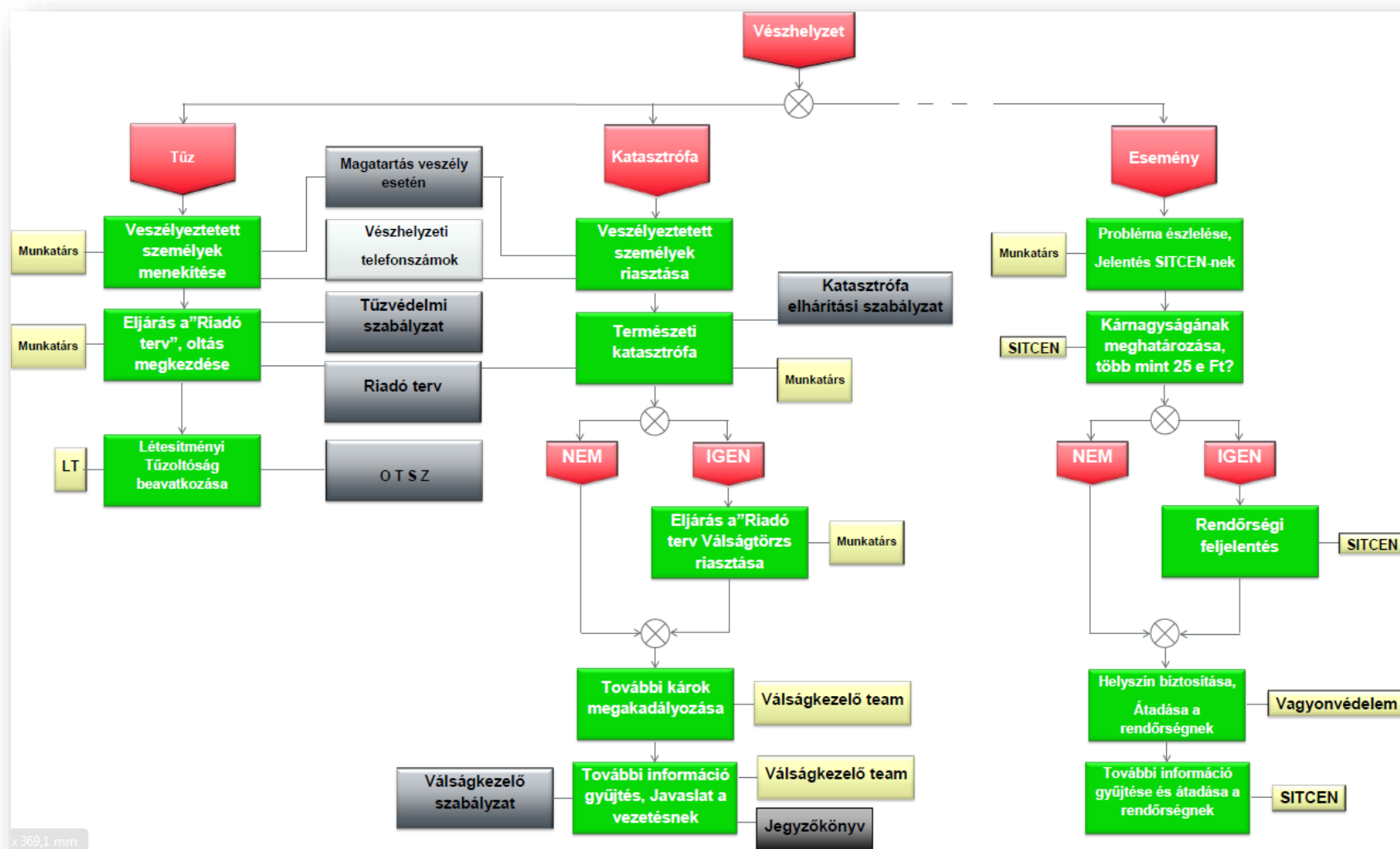




6. számú melléklet: A válságkezelés folyamata



7. számú melléklet: A vészhelyzetkezelés folyamata



PUBLIKÁCIÓS JEGYZÉK

Fsz.	Cím	Megjelenés helye	Szerzői arány
1.	Einführungsaufgaben der Sicherheitsmaßnahmen der Sicherheitsbehörde der Ungarischen EU-Ratpräsidentschaft im ersten Halbjahr 2011	Hadmérnök 2011/3. p. 154 – 160	90 %
2.	Lage- und Analysezentrum bei einem internationalen Unternehmen	Hadmérnök 2011/3. p. 161 – 168	50 %
3.	Personenschutz	Hadmérnök 2011/4. p. 261 – 269	50 %
4.	Werkschutz	Hadmérnök 2012/3. p. 26 – 32	50 %
5.	Integrierte Brandschutzeinrichtungen	Hadmérnök 2013/4. p. 150 – 165	80 %
6.	Egy multinacionális nagyvállalat kritikus infrastruktúrájának illeszkedése a hazai (vertikális és horizontális) kritikus infrastruktúrákhoz	Hadtudomány 2012/3. p. 150 – 165	90 %
7.	Aufgabenstellung und Rolle der Werkfeuerwehr bei einem multinationalen Unternehmen	Hadmérnök 2014/1.p.57 – 66	70 %
8.	Az objektumok és épületek terrorrobbantások elleni védelme	Műszaki Katonai Közlöny 2014/1. p. 72 -82	100%
9.	Különleges védelemmel felszerelt gépjárművek	Hadmérnök 2014/2.p.56 – 72	100 %

SZAKMAI-TUDOMÁNYOS ÖNÉLETRJAZ

1965-ben Szolnokon született, középfokú tanulmányait a Pálffy János Szakközépiskolában végezte. Tanulmányait 1984-ben kezdte a Kossuth Lajos Katonai Főiskolán, ahol általános felderítő szakon végzett és gépészmérnöki végzettséget szerzett. 2003-ban elvégezte a Budapesti Műszaki Egyetem Mérnök Továbbképző Intézet üzleti hírszerzés szakát, majd a Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi karán a biztonság- és védelempolitika szakot, majd a Katonai Műszaki karon a biztonságtechnikai mérnök (MSc) szakon végzett.

A doktori képzést 2010 szeptemberében kezdte a Hadtudományi Doktori Iskolában. Abszolutóriumot 2013 őszén szerzett.

Német nyelvből középfokú, angol nyelvből alacsony szintű nyelvvizsgával rendelkezik.

Fő kutatási területe a globális biztonsági kihívások, válságkezelés és a biztonsági- és védelemi feladatok, biztonsági rendszerek integrált alkalmazása.

Publikációs tevékenysége során – amelyek száma 9, ebből 7 német nyelvű – 2011-es soros magyar elnökség biztonsági kérdéseivel, személyvédelemmel, válságkezeléssel, kritikus infrastruktúrák védelmével, terrorrobbantások elleni védelemmel, vagyonvédelemmel, tűzvédelemmel, tűzvédelmi rendszerekkel, valamint a különleges védelemmel felszerelt járművekkel foglalkozik.

Jelenleg az Audi Hungaria menedzsmentjének tagja és a Biztonságpolitikai és adatvédelmi szervezeti egység szakmai vezetője.