HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Sándor Miklós
sandor.miklos@zmne.hu

Kuris Zoltán
zoltan.kuris@bm.gov.hu

A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA VÉDELEM ÉS A VÉDELMI CÉLÚ KATASZTRÓFAVÉDELMI HÍRADÁS KAPCSOLATRENDSZERE

Absztrakt

Az információs társadalom működésének zavarai, katasztrófavédelmi és különböző minősített helyzet kialakulásához vezethetnek. A szerzők a társadalmi szintű megközelítést követően, részleteiben fejtik ki a kritikus információs infrastruktúra működési zavarainak hatásait a létfontosságú infrastruktúrákra. Bizonyítani szeretnék, hogy a kialakuló katasztrófavédelmi és egyéb minősített helyzetekben, különösen fontos és nélkülözhetetlen az infokommunikációs rendszerek megbízható működésére alapozott katasztrófavédelmi híradás zavarmentes üzemelése. Az információs stabilitás fogalmának bevezetésén keresztül mutatják be a rendszerközpontú működtetés alapvető irányelveit.

A catastrophe might emerge from the disorders of the informational society. The social effects are analyzed. Then the disorders of the critical infrastructure of information is described in detail, how they affect the infrastructures of vital importance the authors describe it in detail. The significance and functioning of sending news are proved as well as the significance of notifying news.

Kulcsszavak: *kritikus információs infrastruktúra védelem, minősített adat, fizikai biztonság, elektronikai biztonság, dokumentum biztonság, személyi biztonság ~ critical information infrastructure protection, sensitive data, physical security, electronic security, document security, personal safety*

BEVEZETÉS

Ma már alapvető axiómának tekinthető az, hogy a biztonság újkori értelmezésének megfelelően, a biztonság dimenzióinak rendszere – az elemek közötti kapcsolatrendszer – alapvetően átalakult. Bizonyos biztonsági dimenziók felértékelődtek, más dimenziók pedig veszítettek súlyukból. Különösen igaz ez, amikor az utóbbi évtized változásait, az információs társadalom működésének tükrében vizsgáljuk. Ma a modern társadalmak nagy része felismerte annak jelentőségét, hogy a társadalom zavartalan működését biztosító „létfontosságú infrastruktúrák" működtetése alapvető biztonságpolitikai cél. Ennek megfelelően a modern társadalmak, a biztonsági stratégiájuk megfogalmazásakor különös figyelmet tanúsítanak az újkori kihívások, kockázatok és fenyegetések részletes feltárására. Az információs társadalmi formációban működő államoknak különös figyelemmel kell lenniük tehát a létfontosságú infrastruktúráik és információs infrastruktúráik védelmére, mert a védelmi rendszer egyenszilárdságának csökkenése alapvetően képes befolyásolni az adott ország geopolitikai és geostratégiai helyzetét egyaránt. A biztonsági stratégia a társadalom működésének biztosítására irányuló alapvető dokumentum. A hazai biztonsági stratégiát elemezve megállapítható, hogy hazánk a fent említett új kori követelményrendszerre építkező, megfelelő biztonsági stratégiával rendelkezik. Ha tovább vizsgáljuk az ágazati stratégiák rendszerét, megállapítható hogy igen ritka a pragmatikus, rendszerszemlélettel rendelkező ágazati stratégia.

Az általános biztonságpolitikai szemléletű megközelítést követően célszerű megvizsgálni azt, hogy a létfontosságú infrastruktúrák zavartalan működtetését célzó kritikus infrastruktúra védelem (a továbbiakban: KIV) milyen kapcsolatban van a katasztrófavédelmi területtel, illetve milyen szerepe van ezen a területen a kritikus információs infrastruktúrák (a továbbiakban KII) zavarmentes üzemeltetésének. Érdemes azt is vizsgálni, hogy ezen a területen hogyan valósul meg, vagy milyen igény mutatkozik a vezetési-irányítási, távközlési és informatikai, rendszerek komplex rendszerének alkalmazásának. Elfogadható állítás az, hogy a társadalom információs és infokommunikációs rendszereinek rendelkezésre állása ugrásszerűen felértékelődik, katasztrófavédelmi és a minősített időszak helyzetében. Célszerű tehát azt vizsgálni, hogy milyen jogalkotási, szabályozási és technológiai feladatok körvonalazódnak ezen a területen. A fentiekből következik, hogy azt is célszerű megvizsgálni, hogy a fentiekben kifejtett vezetés-irányítási, távközlési és informatikai rendszerek, milyen előfeltételekkel és környezetben tudják biztosítani azt az információs stabilitást, bonyolult katasztrófavédelmi és minősített helyzetben.

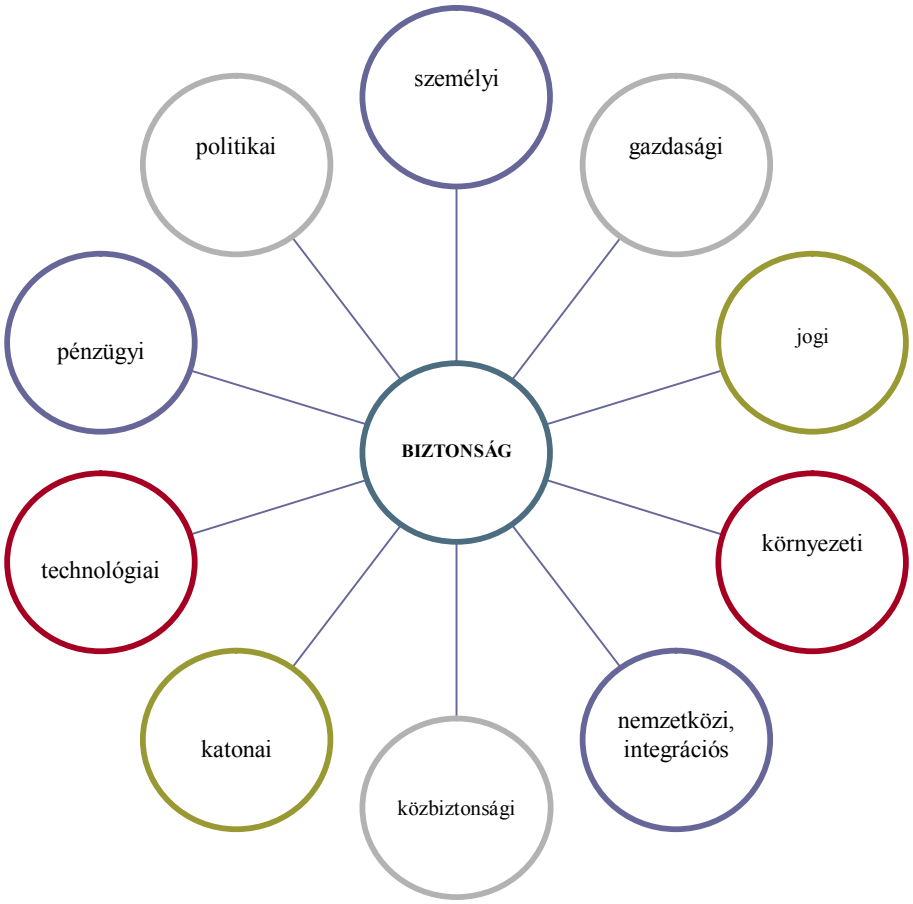
A BIZTONSÁG ÚJKORI DIMENZIÓI

A biztonságot az államok manapság komplex módon értelmezik. Az elemek fontossági sorrendben: a politikai, gazdasági szociális ökológiai és katonai területek. Természetesen ez béke állapotra jellemző fontossági sorrend és az adott körülményeknek megfelelően a súlypontok áthelyeződhetnek. A fenti elemeket megvizsgálva következtetés eredménye ként megállapítható, hogy a fenti elemek megjelenésének színterei a különböző létfontosságú infrastruktúrák és ezen belül a kiemelt fontosságú szektorok.

Ahhoz, hogy a biztonság hatókörét értelmezni tudjuk meg kell határozni a tartalmát. Ezzel összefüggésben a **biztonság szintjei**, *az egyének, csoportok, kisebbségek, nemzetek, államok, régiók és a nemzetközi rendszer.*

Ugyanakkor a 90'-es évektől elterjedt a biztonság fogalmának parttalan használata, kiterjedt azon jelenségek köre, amelyek kiváltói lehetnek a már elemzett biztonsági

hiányérzetnek. Ezért szükséges és elégséges értelmezés szerint az alábbi biztonsági dimenziók körvonalazódnak.



1. ábra. Jellemző biztonsági változatok (szerzők)

A társadalom biztonsági érzete összességében mérhető jelenség. E mérés és a biztonsági érzetek meghatározására hívták segítségül a biztonságpolitikával foglalkozó szakemberek a szociológia eszköztárát. A TIT HABE[1] (a honvédelmi tárca megbízásából) a Szonda Ipsos-sal közösen két ízben is végzett közvélemény-kutatást e terület vonatkozásában. 1999-ben ezer, míg 2008-ban háromezer főt kérdeztek meg „az utca emberei közül". A következő táblázat ennek rövid összefoglalását szemlélteti.

[1] A TIT Hadtudományi és Biztonságpolitikai Közhasznú Egyesületet életünk legfontosabb kérdéseivel, a biztonsággal és biztonságpolitikával foglalkozik az ország egész területén. A TIT HABE 1996-os megalakulása óta aktívan részt vesz az ország kül-és biztonságpolitikájával, NATO- és EU-tagságával és a nemzetközi biztonság erősítése érdekében végzett egyéb tevékenységével összefüggő kérdések elemzésében és publikálásában, hazai és nemzetközi rendezvények szervezésében, a lakosság különböző célcsoportjainak a tájékoztatásában és felkészítésében.

***2.* ábra.** (Forrás: Gondolatok és vélemények a biztonságunkról – a biztonságkultúra kérdései, TIT HABE, 2008)[2]

A biztonság a fejlődés előfeltétele

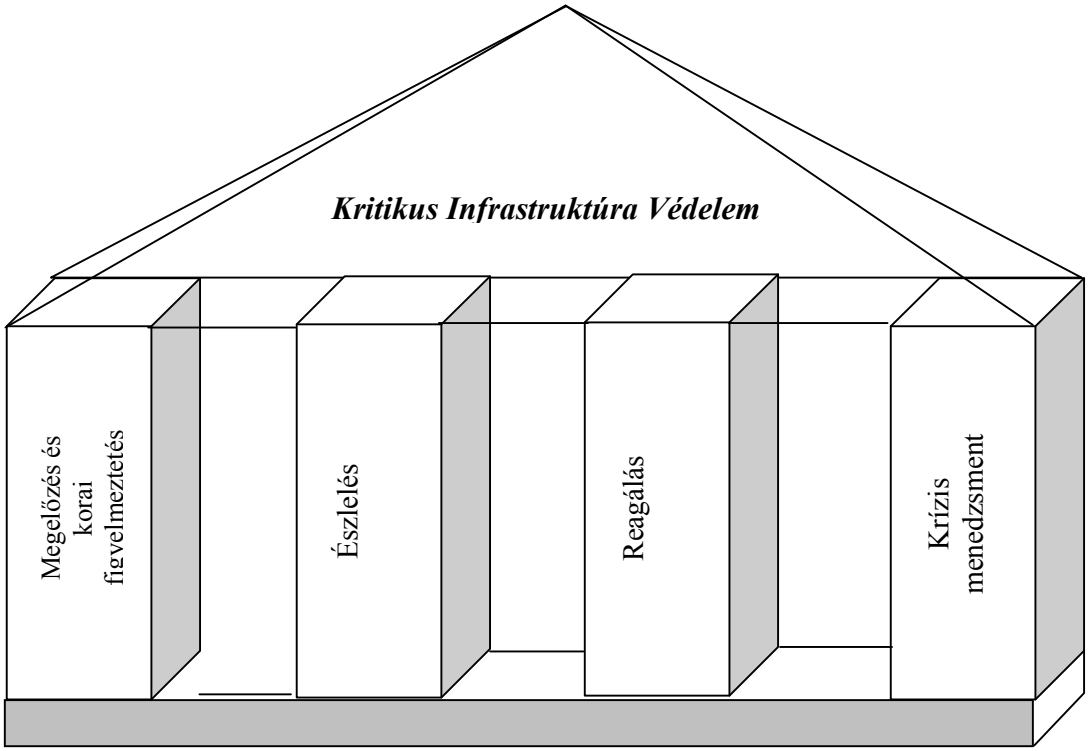
A konfliktusok nemcsak az infrastruktúrákat – így a szociális infrastruktúrákat – teszik tönkre, hanem ösztönzik a bűnözést, eltántorítják a befektetőket és lehetetlenné teszik valamennyi szokásos gazdasági tevékenység gyakorlását is. Számos ország és régió a konfliktus–bizonytalanság–szegénység ördögi körének a foglya.

A fenti rövid áttekintés jól példázza, hogy a társadalom működését biztosító infrastruktúrák működésében előforduló zavarok visszahatnak a társadalom biztonsági érzetére és alapvető hatással vannak a társalmi fejlődésre is!

A kritikus infrastruktúra védelmének négy alappillérét (3. ábra) értelmezve megállapítható, hogy a megelőzéstől a krízis menedzseléséig terjedő teljes vertikumban alkalmazásra kerülnek a különböző kritikus információs infrastruktúra elemek,(kommunikációs, infokommunikációs rendszerek).

Sok Európai Uniós tagállamban – köztük Magyarországon is – találkozunk kormányzati CERT–el, melynek feladata az állami információs rendszerek elleni támadásokra történő reagálás. A CERT-ek fontosságát alátámasztja az is, hogy irányadó szakemberek szerint a kritikus információs infrastruktúrák védelmének megvalósítása is a megelőzés és korai észlelés, valamint a reagálás és a krízismenedzsment négy pillérén kell hogy alapuljon.

[2] Dr. Radványi Lajos szociológus, biztonságpolitikai szakértő, a TIT Hadtudományi és Biztonságpolitikai Közhasznú Egyesület alelnöke *„A magyar lakosság biztonságfelfogásának változásai 1999 – 2008”* című előadásából. Veszélyhelyzetek kezelésének kormányzati koordinációja – munkaműhely, Göd, 2009. március 10.



3. ábra. A kritikus infrastruktúra védelem négy alappillére

Egy az amerikai kongresszus számára készült jelentés megállapítja, hogy a kritikus infrastruktúra besorolások nem olyan listák, amelyek örök érvényűek, és amelyeken nem lehetne változtatni attól függően, hogy milyen veszély fenyeget, illetve ezek milyen hatásokkal járnának a különböző szektorok vonatkozásában. [14]

A tanulmány táblázatban (4.. táblázat) foglalja össze azokat a szektorokat, amelyek a meghatározott kritériumok alapján kritikus infrastruktúrának minősülhetnek.

Infrastruktúra	**Kritériumok, amelyek meghatározzák a kritikusságot**			
	nemzetvédelem	***gazdasági***	***biztonság***	***közegészségügy***
telekommunikációs és információs hálózatok	***X***	***X***		
energia	***X***	***X***		
bank/pénzügy		***X***		
szállítás	***X***	***X***		
víz			***X***	
készenléti szervek			***X***	
kormányzat			***X***	
egészségügyi szolgáltatások			***X***	
nemzetvédelem	***X***			
külföldi hírszerzés	***X***			
igazságügy			***X***	
külügyi kapcsolatok	***X***			
nukleáris létesítmények és erőművek			***X***	
különleges események				***X***
élelmiszer/mezőgazdaság			***X***	
	nemzetvédelem	***gazdasági***	***biztonság***	***közegészségügy***

ipari gyártás		***X***		
vegyipar			***X***	
védelmi ipar	***X***			
Postai szolgáltatások			***X***	
nemzeti emlékművek és emlékhelyek				***X***

4. ábra. Szektorok értékelése és besorolása

AZ INFOKOMMUNIKÁCIÓS RENDSZEREK INFORMÁCIÓBIZTONSÁGI STABILITÁSÁT BIZTOSÍTÓ ÖSSZETEVŐINEK ELEMZÉSE

Az információs társadalom nagyon fejlett és hatékony társadalom, ugyanakkor meglehetősen sebezhető is. Sebezhetőségének alapját az adja, hogy működése szorosan kapcsolódik a globális, nemzeti, regionális és lokális információs környezethez [h 67.old.] Irányadó szakemberek szerint, napjainkban várhatóan felértékelődik az információs környezet átfogó védelme. A Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló 2073/2004. (IV.15.) Korm. határozat [3] a fenyegetések, kockázatok, kihívások szakaszában (II.) nevesíti az információs társadalom kihívásait, ezen belül a telekommunikációs hálózatok sebezhetőségét és kockázatait emeli ki. A terrorizmus elleni védekezés szakaszban (III.3.1) külön kiemeli a kritikus infrastruktúrák védelmének feladatait is. Az információs rendszerek védelme szakaszban (III.3.7) pedig hangsúlyozza a kormányzati információs rendszerek védelmének szükségességét és felhívja a figyelmet a sikeres védelem érdekében szükséges együttműködésre, az érintett informatikai és távközlési szolgáltatókkal. Sajnos a Magyar Köztársság Nemzeti Biztonsági Stratégiájával összefüggő ágazati (távközlés, informatika) területét fellelő gyűjtő néven infokommunikációs doktrínának [8] nevezhető dokumentum a mai napig nem került kidolgozásra.

A Magyar Köztársaság kritikus információs infrastruktúrái az alábbiak:

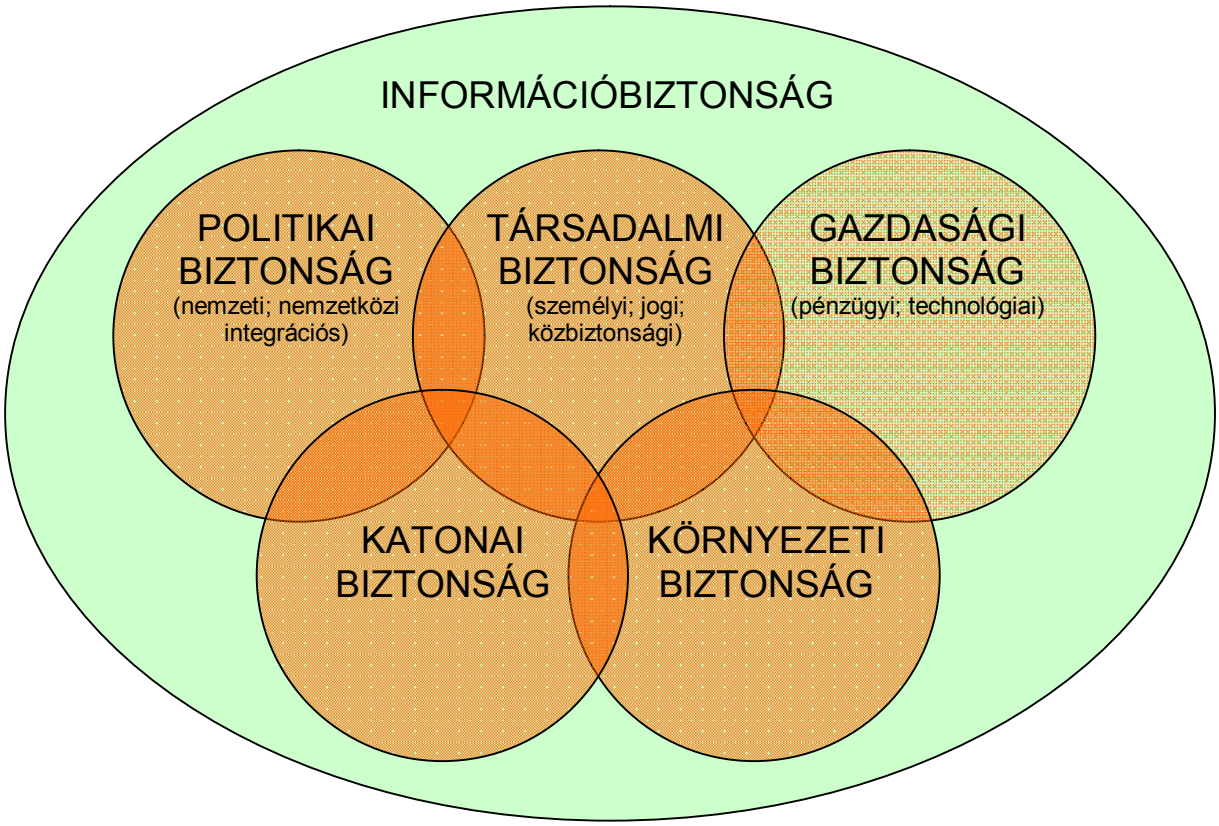
- Informatikai rendszerek és hálózatok,
- automatizálási, vezérlési és ellenőrzési (SCADA, távmérő, távérzékelő és telemetriai) rendszerek,
- internet szolgáltatás és infrastruktúrája,
- vezetékes távközlési szolgáltatások és infrastruktúrái,
- mobil távközlési szolgáltatások és infrastruktúrái,
- műholdas távközlési szolgáltatás és infrastruktúrái,
- földfelszíni műsorszórás és infrastruktúrája,
- közigazgatási informatika és kommunikáció és infrastruktúrái,
- a kritikus infrastruktúrák létfontosságú infokommunikációs rendszerei.

A biztonság dimenzióiban értelmezett információbiztonsággal összefüggésben megállapítható, hogy a KIV szektoraiban gyűjtött, feldolgozott tárolt és továbbított információkat a különféle infokommunikációs eszközök alkalmazásával kezeljük. Infokommunikációs eszközök gyűjtőfogalom kőré csoportosíthatóak, az informatikai és a távközlés, illetve az egyéb információtechnológiai eszközök konvergenciájának következményeként alkalmazott „informatizálódott” eszközök. A fenti infokommunikációs rendszerek információbiztonsági stabilitásának biztosítása alapfeltétel, a katasztrófavédelmi

és egyéb minősített időszaki helyzetekben is. Az előző gondolatot tovább fűzve megállapítható, hogy a kritikus információs infrastruktúra azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftverek, internet, GPS,stb.) [8]

A kritikus információs infrastruktúrák védelme tehát a tulajdonosok, gyártók, és felhasználók, valamint a hatóságok programjai és tevékenységei, melyek célja fenntartani a kritikus információs infrastruktúra teljesítményét meghibásodás, támadás vagy baleset esetén a meghatározott minimális szolgáltatási szint felett, illetve, illetve minimálisra csökkenteni a helyreállításhoz szükséges időt, valamint a károkat. [8] Az információs stabilitás elérésének érdekében komplex információbiztonsági elveket kell alkalmazni. Ezeket a komplex és integrált védelmi intézkedéseket tudati, információs és fizikai dimenziókban is érvényesíteni kell a kritikus információk védelmének érdekében. Ezzel összefüggésben elmondható, hogy ezen a területen a minősített adat védelméről szóló 2009. évi CLV. Törvény (a továbbiakban: MAV törvény) már egységes irányelveket szab.

A MAV törvény nyomán, a Nemzeti Biztonsági felügyelet működésének, valamint a minősítet adat kezelésének rendjéről szóló 90/2010.(III.26.) Kormányrendelet, és a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Kormányrendelet, viszont már egységes alapokra helyezi a minősített adatok védelme érdekében érvényesítendő, személyi, fizikai, dokumentum és elektronikai védelem komplex rendszerét.[10] Az elektronikai védelmi intézkedések keretei között megjelenik az átvitel út védelme, számítógép (szoftver, hardver és hálózat) védelme. [11] Egységesítésre kerültek a rejtjelzéssel összefüggő követelmények és megjelennek a kompromittáló kisugárzással kapcsolatos alapvető irányelvek. Sajnos a kompromittáló kisugárzás védelmének részletes szabályozását illetően megállapítható, hogy a magas színvonalú védelmi intézkedésekkel összefüggő követelményrendszert nem sikerült érvényesíteni. Ennek az is lehet az oka, hogy – ez a viszonylag új és bonyolult terület – a leg költségigényesebb védelmi intézkedések megvalósítását feltételezi és ezen a területen hazai tapasztalatok hiányában a nemzetközi irányelvekre figyelemmel kell kialakítani a hazai szabályozást! Ezen a területen, az irányadó hazai információvédelmi szakemberek bevonásával, további lépések szükségesek ahhoz, hogy az elektronikai védelem területén a maradvány kockázatot optimalizáljuk és növeljük az elektronikai rendszerek egyenszilárdságát. Az viszont egyértelmű eredménye a fenti törvényben és kormányrendeletekben megfogalmazott szabályrendszernek, hogy a minősített adat védelmével összefüggő komplex védelmi intézkedések többé-kevésbé koherensek lettek a nemzetközi szabályokkal, ennek okán az Európai Uniós és a NATO rendszereken belüli információáramlás (bizonyos szintig) egységessé és lehetővé vált.



5. ábra. A biztonsági dimenziók és az információbiztonság kapcsolata.

AZ ORSZÁGOS TÁVKÖZLŐ HÁLÓZAT (OTH) FELHASZNÁLÁSA A VÉDELMI FELADATOKKAL ÖSZEFÜGGÉSBEN

Annak érdekében, hogy a rendszerben keletkezett kritikus információk kellően támogassák a döntési helyzetben lévő felelős vezetőket, az információ továbbítására alkalmas és képes nemzeti Országos kommunikációs távközlési hálózat magas szintű rendelkezésre állását kell biztosítani. Meg kell határozni a szükséges és elégséges szolgáltatás mértékét. Ennek előfeltétele a megfelelő szintű és tartalmú törvényi szabályozás, amely lehetővé teszi ezt a rendelkezésre állást a bonyolult nemzetközi tulajdonosi rendszer esetén is. Különösen fontos abban az esetben jól szabályozni ezt a területet, amikor például a védelmi szektor zártcélú vezeték nélküli kommunikációját biztosító rendszer szolgáltatója egy olyan egyetemes szolgáltató, amely külföldi tulajdonosi rendszerben üzleti alapokon szolgáltat. Ezt a részterületet hivatott szabályozni a Miniszterelnöki Hivatalt vezető miniszter 4/2010. (III. 26.) MeHVM rendelete a védelmi feladatokban részt vevő elektronikus hírközlési szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról.

Az elektronikus hírközlésről szóló 2003. évi C. törvény 182. § (4) bekezdés l) pontjában kapott felhatalmazás alapján a Miniszterelnöki Hivatalt vezető miniszter feladat- és hatásköréről szóló 29/2008. (II. 19.) Korm. rendelet 1. § j) pontjában meghatározott feladatkörében eljárva, a miniszterelnöki hivatalt vezető miniszter az alábbiakat rendelte el [12]:

Az elektronikus hírközlés szolgáltatási tevékenységének a minősített időszakban történő ellátásához szükséges védelmi felkészülési feladatok előkészítésében és végrehajtásában való részvételre kijelölt, valamint az informatikai és elektronikus hírközlési, továbbá postai ágazat (a továbbiakban: ágazat) ügyeleti rendszerébe bevont elektronikus hírközlési tevékenységet

végző szervezetek (a továbbiak ban: szolgáltatók) felsorolását a rendelet 1. melléklete tartalmazza.

A riasztási és tájékoztatási feladat ellátásában részt vevő nem közszolgálati műsort sugárzó országos, körzeti, helyi rádió és televízióadók, az adókat üzemeltetők (engedélyesek) jegyzékét a rendelet 2. melléklete tartalmazza.

A kijelölés alapján a szolgáltatók a tevékenységi körüket érintően ellátják a minősített időszakban bekövetkező rendkívüli események megelőzésére, elhárítására, a következményeik csökkentésére, illetve megszüntetésére, valamint a helyreállításra irányuló védelmi felkészülési és végrehajtási feladatokat.

A rendelet alkalmazásában minősített időszak a Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény 19. §-a (3) bekezdésének h) pontjában meghatározott rendkívüli állapot és i) pontjában meghatározott szükségállapot, az Alkotmány 35. § (1) bekezdésének i) pontja és a polgári védelemről szóló 1996. évi XXXVII. törvény 2. § (2) bekezdése szerinti veszélyhelyzet, valamint az Alkotmány 19. § (3) bekezdés n) pontjában meghatározott megelőző védelmi helyzet, továbbá a 19/E. § (1) bekezdésében foglalt, a szükségállapot vagy a rendkívüli állapot kihirdetésére vonatkozó döntésig terjedő időszak.

Az elektronikus hírközlésért felelős miniszter (a továbbiakban: Miniszter), illetve a Nemzeti Hírközlési Hatóság (a továbbiakban: NHH) a védelmi felkészülés és a végrehajtás időszakában felmerülő egyedi védelmi feladatokat az érintett szolgáltatók számára külön jogszabály szerint határozza meg.

A védelmi felkészülési feladatok végrehajtásáért minden esetben a szolgáltató vezető tisztségviselője felelős.

A szolgáltatók – a minősített időszakra történő felkészülés keretében – az alábbiakban meghatározott tevékenységi körökből a saját szervezetük szakmai feladat- és hatáskörébe tartozó védelmi feladatokat látják el:

- a szervezeti készenlét előkészítésének és fenntartásának körében:
  - a védelmi felkészülési feladatok ellátásához szükséges személyi, szervezeti és anyagi-technikai feltételek megteremtése, folyamatos biztosítása,
- a védelmi felkészüléssel, műszaki, forgalmi, katasztrófa vagy egyéb veszély miatt keletkező üzemzavar elhárításával kapcsolatos intézkedések kidolgozása, tervek készítése és azok folyamatos aktualizálása,
  - a védelmi felkészüléssel összefüggő rendszeres képzési, továbbképzési és gyakoroltatási feladatok meghatározása és végrehajtása,
  - az ügyeleti szolgálatnak a külön jogszabályban foglaltak szerinti működtetése,
  - a külön jogszabály alapján a meghagyással kapcsolatos feladatok végrehajtása;
- a hálózatok felkészítésének és irányításának terén:
  - a gerinchálózati struktúra és az elektronikus hírközlési létesítmények védelmi, biztonsági feltételeinek biztosítása,
  - a zártcélú hálózatokhoz szükséges összeköttetések és kapcsolódó szolgáltatások előkészítésének és alkalmazásának biztosítása,
  - a meghatározó szerepű elektronikus hírközlési csomópontok, illetve felhasználók több útvonalon történő elérhetőségét segítő megoldások kialakítása,
  - a riasztási és tájékoztatási feladat ellátására létrehozott rendszerben szükséges elektronikus hírközlési összeköttetések biztosításában való közreműködés,
  - be) a honvédségi, kormányzati, rendvédelmi elektronikus hírközlési eszközöknek a szolgáltató hálózatához történő csatlakoztatásához szükséges hozzáférési pontok és jogosultságok biztosítása;
- az üzemviteli és tartalékolási rendszer kialakítása terén:
  - a nemzeti és a nemzetközi gerinchálózati irányító és üzemviteli funkciók működésének összehangolása,

- az illetékes hazai, valamint nemzetközi szervek és szervezetek közötti védelmi jellegű kapcsolattartás feltételeinek kialakításában és végrehajtásában való közreműködés,
- az elektronikus hírközlési szolgáltatások területén elrendelhető korlátozó vagy szüneteltető rendelkezések végrehajtására és következményeik kezelésére történő felkészülés,
- a védelmi feladatok ellátásához szükséges mértékű és összetételű tartalékkészletek biztosítása,
- a hálózati létesítmények és eszközök meghibásodása, rongálódása, sérülése, megsemmisülése esetére az elsődleges helyreállításhoz és az üzemszerű állapot visszaállításához szükséges feladatok megtervezése és végrehajtási feltételeinek folyamatos biztosítása;

❖ a szolgáltatási igények kielégítése terén:
- a védelmi felkészülésben részt vevő, külön jogszabályban meghatározott követelménytámasztó szervek minősített időszakra vonatkozó szolgáltatási igényeinek kielégítéséhez szükséges feltételek biztosítása, az összefüggő tervezési, szervezési tevékenység ellátása, szolgáltatási feladatok végrehajtása,
- a lakosság minősített időszaki elektronikus hírközlési igényeinek az egyetemes szolgáltatási, illetve koncessziós szerződésben meghatározott szinten és tartalommal történő kielégítéséhez szükséges feltételek biztosítása,
- a védelmi felkészüléssel kapcsolatos jogszabályok által meghatározott gazdasági és anyagi szolgáltatási kötelezettségek teljesítésére, illetve kezelésére való felkészülés,
- da kormányzat minősített időszaki szolgáltatási igényeinek kielégítéséhez és kommunikációs tevékenységéhez szükséges feltételek megteremtésében, fenntartásában való közreműködés,
- a Befogadó Nemzeti Támogatás tervezési és végrehajtási feladataiban történő részvétel;

❖ a nyilvántartások vezetése és az adatkezelés terén:
- a védelmi felkészülési feladatokkal kapcsolatos jogszabályokban meghatározott adatszolgáltatási kötelezettség teljesítéséhez szükséges nyilvántartási rendszer kialakítása és adatainak a követelményekhez igazodó pontosságú karbantartása;

❖ a műsorszórási tevékenység körében:
- a műsorszórási tevékenység folyamatosságához szükséges technikai és biztonsági feltételek megteremtése, a meghatározó szerepű létesítmények őrzés-védelmének biztosítása,
- a műsorszóró hálózaton a lakosság légi-, illetve katasztrófariasztásra és tájékoztatására létrehozott rendszer működésében való közreműködés,
- a lakosság légi-, illetve katasztrófariasztásának és tájékoztatásának elrendelésére illetékes szervek intézkedésére a riasztási és tájékoztatási közlemények leadásának – az elrendelő szervekkel kötött megállapodás szerinti, saját eszközökkel történő – biztosítása.

A riasztási és tájékoztatási feladat ellátásában külön jogszabály alapján – az illetékes honvédelmi és rendvédelmi szervek, valamint a közszolgálati rádió és televízió műsorszolgáltatók, műsorszóró adók és az adókat üzemeltető szolgáltatók mellett – részt vesznek:

❖ a Miniszter és az NHH;
❖ a rendelet 2. mellékletében meghatározott nem közszolgálati országos, körzeti és helyi rádió és televízió műsorokat sugárzó adók, az adókat üzemeltetők (engedélyesek);
❖ azok az elektronikus hírközlési szolgáltatók, amelyek összeköttetést, illetőleg modulációs vonalat biztosítanak

- a riasztási és tájékoztatási közlemény leadását kezdeményező szerv és az érintett rádió, televízió stúdiója között,
- a riasztási és tájékoztatási feladatban részt vevő stúdió és a részére sugárzást végző rádió, televízió adóállomás között, valamint
- a műsorszolgáltatók és a műsorszóró adók között;

❖ a riasztási rendszer technikai elemeit, a riasztási és tájékoztatási közlemények átvételére és továbbítására szolgáló átkapcsoló berendezések fenntartását ellátó gazdálkodó szervezet;

AZ EURÓPAI UNIÓ LÉTFONTOSSÁGÚ INFRASTRUKTÚRÁK FIGYELMEZTETŐ ÉS INFORMÁCIÓS HÁLÓZATA (CIWIN)

Vezetés irányítási rendszerek alapvető megközelítése

Az információbiztonsági stabilitást alapvetően befolyásoló OTH, magas szintű rendelkezésre állása és a minősített adatok védelmével összefüggő részterülteken túl, az alábbiakban célszerű megvizsgálni a globális, nemzetközi, nemzeti és regionális infokommunikációs rendszerekre épülő vezetés-irányítási rendszerekkel összefüggő alapvető ismereteket és követelményeket. Ennek nyomán célszerű áttekinteni - egy a kritikus infrastruktúra védelmével összefüggő- adattovábbítási értesítési és riasztási rendszerrel szembeni alapvető igényeket is. Különösen indokolt ez, annak fényében, hogy az összekapcsolódó (adott esetben globális) infrastruktúrákon keresztül – az incidens bekövetkezését követően- a működési zavarok felhalmozódnak, hatványozódnak az interdependencia jelenség miatt. Ebben a helyzetben indokolt egy nemzetközi (európai) adatok cseréjére alkalmas megosztott figyelmeztető és tájékoztató rendszer alkalmazása, amelynek segítségével a döntéshozók, az egységes és valós idejű adatok alapján rövid idő alatt a helyzettel összefüggő széleskörű adatszolgáltatás alapján képesek meghozni az optimális döntéseket. Az információs társadalomban alapvető igény fogalmazódik meg az infokommunikációs eszközökre épülő valós idejű globális döntés támogató rendszerek üzemeltetésére. Ezzel összefüggően megállapítható, hogy a kritikus infrastruktúra védelem területén is alapvető igény az információs fölény birtoklása, annak érdekében, hogy a fenyegetések előrejelzése, majd annak realizálódását követően a kár elhárítás és a működőképesség helyreállításának időszakában is optimális szinten tartható legyen a szükséges és elégséges szintű védelmi intézkedések alkalmazása.

A CIWIN kezdeményezés

A CIWIN létrehozására irányuló kezdeményezések már 2006 decemberére nyúlnak vissza. A létfontosságú infrastruktúra védelem Európai Programja (EPCIP) javaslatok célkitűzések értelmében fogalmazódott meg egy az infrastruktúra védelemmel összefüggő, biztonságos információcserére alkalmas eljárás kidolgozása. Ez a kezdeti lépés alapozta meg egy tagállamok közötti kölcsönös tájékoztató rendszer létrejöttét, illetve fogalmazta meg annak igényét. Erről az Európai Bizottság határozatban is gondoskodott ugyan, de a tagállamok CIWIN- hez történő csatlakozása nem kötelező. Ugyanakkor az EPCIP-vel kapcsolatos irányelveknek megfelelően a tagállamoknak az Európai Bizottság részéről rendelkezésre bocsátott információkat hozzáférhetővé kell tenniük a kijelölt ágazatok részére. A tagállamoknak viszont a saját területéről gyűjtenie kell az adatokat az európai létfontosságú infrastruktúrákról, a sebezhetőségi és függőségi pontjairól, a védelmi fejlesztésekről és ezt elérhetővé kell tenni az EU részére.

A CIWIN (szerver / kliens) rendszer funkcionalitását illetően, a Bizottság és a tagállamok közötti viszonylatban alkalmasnak kell lennie a két vagy többoldalú információ megosztásra,

illetve gyors riasztási funkció megvalósítására. A bizottsági felületen az ágazati területek jelennek meg. A rendszer kötött és dinamikus területi adatkezelésre egyaránt alkalmas.

A kötött területen jelennek meg a tagállami, szektor, vezetői, külső együttműködési területek és egy gyors információcserét biztosító RAS alrendszer.

Egy speciális esemény, vagy tagállami projektek, szakértői munkacsoport terület részésze, igény szerint dinamikus területek hozhatók létre.

Az elrendelt figyelmeztetés esetén lehetőség van egy ideiglenes RAS terület létrehozására, amely az együttműködés színtere az adott projektre vonatkozóan.

A kritikus infrastruktúra védelmével összefüggő és rejtelzéssel védeni rendelt, minősített információk megosztására speciális terület áll rendelkezésre azok számára, akik a „muszáj tudni" elv alapján azokhoz jogosultak hozzáférni.

A CIWIN rendszer (MS SharePoint 2007), piaci alkalmazásra épül és beépített, minden nyelvre automatikus fordítóprogramot, illetve „off the shelf" tartalomkezelőt használ. Funkcióit illetően megtalálhatóak benne a vitafórum, kalendárium, és a személyes belső levelező funkciók is.

A TESTA rendszeren történő elérést megelőzően, minősített információk továbbítására nem alkalmas. Az elérést követően korlátozott terjesztésű minősített adatok továbbítására alkalmas, de középtávon - sTESTA hálózaton - Bizalmas minősítésű információk megosztására lesz alkalmas.

A TESTA (Trans European Services for Telematics between Administrations) egy független zártcélú (publikus hálózatoktól független) gerinchálózat, amely az Európai Unió adminisztrációja és a tagállamok közötti kommunikációs hálózat. A TESTA rendszer, információvédelmi szempontból továbbfejlesztett változata az sTESTA, amely már megfelelő egyenszilárdságú rejtjelző eszközöket és algoritmusokat használ. A tagállamok részére a CIWIN rendszerre történő csatlakozás opcionális, azonban a rendszerhez csatlakozó tagállamoknak a minősített adatkezeléssel összefüggő kötelezettség alapján az elektronikai, dokumentum, személyi és fizikai védelmi követelményeknek meg kell felelni. Az előzőekben már kifejtett EU minősített adatvédelmi követelményekkel koherens szabályozási rendszer, különösen ezen a területen nyit új távlatokat, melyeket az Európai Bizottság, a tagállamokkal kötött többoldalú szerződésekkel is megalapozott.

Az elérést követően korlátozott terjesztésű minősített adatok továbbítására alkalmas, de középtávon Bizalmas minősítésű információk megosztására lesz alkalmas.

Információvédelmi kérdések

Az Európai Bizottság által kiadott irányelv 9. cikkelyében megfogalmazottaknak megfelelően., a minősített információt kezelő személyeknek, személyi biztonsági tanúsítvánnyal kell rendelkezniük. Ennek előfeltétele a megfelelő szintű nemzetbiztonsági átvizsgálást követő kockázatmentesség megállapítása. A tagállamoknak, a Bizottságnak és az illetékes felügyeleti szerveknek (ez hazánkban a Nemzeti Biztonsági Felügyelet) biztosítaniuk kell, hogy a minősített információkhoz a létfontosságú infrastruktúrák védelme céljából jussanak hozzá, az arra jogosult személyek. Ezzel összefüggésben elengedhetetlen a nemzeti és nemzetközi jog harmonizációja (ez meg is történt) valamint az egységes jogértelmezésen alapuló jogkövető magatartás érvényesítése. Az egyes tagállamoknak és a bizottságnak egyaránt tiszteletben kell tartania a minősített adat minősítője által megállapított minősítési szintet.

A CIWIN rendszer információs funkciója biztosítja, hogy az adathoz való hozzáférés alapja a már említett"tudnia kell" elv alkalmazása. A rendszeren belül az információ birtokosa dönti el azt, hogy ki és milyen biztonsági szinten férhet hozzá az adathoz. A tagállamok jogosultsága és felelőssége az, hogy tagállamon belül hogyan szabályozzák a hozzáférést az adathoz. Természetesen itt vissza kell utalni a koherens EU és nemzeti szabályokra, melynek

rendelkezéseit maradéktalanul be kell tartani. A tagállamnak minden alkalommal ki kell jelölnie egy arra jogosult vezetőt, aki a jogosultságokat illetően dönteni tud. Ez az egyszemélyi vezető jogosult ezeket a jogokat – korlátozott mértékben- a tagállam más tisztségviselőjére delegálni. A szabályoknak megfelelő szintű személyi biztonsági tanúsítványokkal a kezelőknek és felhasználóknak egyaránt rendelkezniük kell.

Hazai rendszerek együttműködése a CIWIN rendszerrel

A nemzeti KIV hatókörében, az irányadó szakemberek szerint nem szükséges külön riasztási és értesítési rendszereket létrehozni. Azt azonban célszerű elemezni, hogy a jelenleg működő riasztási és értesítési rendszerek, hogyan tudják támogatni a nemzeti KIV-ben érintett szektorok és az állami szektor döntésképes vezetőit. Ha a vizsgálat eredménye ként erre a jelenlegi rendszerek nem alkalmasak, akkor (és csak is akkor) szükséges új, különálló rendszerek fejlesztésében gondolkodni. Ugyanakkor védelmi vezetéstechnikai rendszerszervezési szempontokat figyelembe véve, nem indokolt sok sziget rendszerű riasztási rendszert üzemeltetni. Célszerű a jövőben megvizsgálni annak a lehetőségét is, hogy a meglévő nemzeti rendszereket (Marathon Terra; K-600/KTIR) illetve azok bizonyos adatbázisait (amelyek nem sértenek nemzeti érdekeket) egy funkcionális interfészen keresztül, hogyan lehet elérhetővé tenni a CIWIN számára, egységes és redundáns platformra helyezve ezzel a nemzeti és európai KIV figyelmeztető és információs rendszereit.

ÖSSZEFOGLALÁS

A biztonság újkori értelmezéséből kiindulva - elfogadva azt, hogy a dimenziók átalakultak és némely dimenziók felértékelődtek – megállapítható, hogy az információs társadalom kritikus infrastruktúrának és ezen belül a kritikus információs infrastruktúra védelmével összefüggő kérdések a biztonsági stratégiába épülő és annak szerves részét képező elemei. Megállapítható, hogy a társadalom zavartalan működésén túl, a katasztrófa helyzetben és a különböző minősített időszaki helyzetekben súlyponti kérdés a kritikus információs infrastruktúrák rendelkezésre állása. Az mára bizonyított tény, hogy az információk gyors, hiteles és változatlan formában történő áramlása alapvetően befolyásolja a védelmi intézkedések hatékonyságát. A fentiekből azt a végkövetkeztetést lehet levonni, hogy ezen a területen is fontos az információs fölény elérése.

A külföldi és hazai jogi és technológiai környezetet elemezve az a végkövetkeztetés vonható le, hogy a hazai szabályozás – a hazai doktrínák rendszerét vizsgálva – ugyan igyekszik követni az európai folyamatokat, de különösen technológiai területen az útkeresés fázisában lévő folyamat érzékelhető. A felhasználók igénye az információs rendszerek használatával kapcsolatban nagyon határozott és jól érzékelhető, de különösen az érzékeny, vagy minősített adatok gyors, hiteles és változatlan továbbítására alkalmas hazai rendszerek kialakítása még várat magára. Ezen a területen több párhuzamos fejlesztési folyamat érzékelhető. Ezért is különösen fontos annak a problémának a feloldása, hogy a hazai és nemzetközi értesítési rendszerek egységes platformon és egységes elvek alapján képesek legyenek a hatékony együttműködésre. A fentieket összefoglalva, irányadó szakemberek szerint az információs társadalom zavartalan működését veszélyeztető fenyegetésekkel szembeni védelmi intézkedések foganatosítása az információs dimenzióban, meghatározó szerepet töltenek be.

FELHASZNÁLT IRODALOM

[1] Egyesült Nemzetek Nevelésügyi és Kulturális Szervezete (UNESCO) társadalomtudományi szótár

[2] Amerikai nemzetbiztonság c. könyv (1981)

[3] A Magyar Köztársaság nemzeti Biztonsági Stratégiájáról szóló 2073/2004.(IV.15) korm. határozat.

[4] Kőszegvári Tibor: A hadtudomány mai problémái, területei és új fogalma (Hadtudomány, Magyar

Hadtudományi Társaság, Budapest XVII. évfolyam 2007/1. szám) 13. oldal

[5] Farkasné dr. Zádeczky Ibolya: A biztonságot veszélyeztető globális kihívások (Hadtudomány, MHTT. Budapest XVI. évfolyam 3. szám, 2006. szeptember) 41. oldal.

[6] Wörterbch zur sicherheitspolitik, Mitter Kiadó, 1985. 113. o.

[7] Szabó József::Hadtudományi Lexikon, Magyar Hadtudományi Társaság, 1995. 144. o.

[8] Muha Lajos A Magyar Köztársaság Kritikus Információs Infrastruktúráinak védelme doktori (Phd) értekezés 2007.

[9] a minősített adat védelméről szóló 2009. évi CLV. Törvény

[10] a Nemzeti Biztonsági felügyelet működésének, valamint a minősítet adat kezelésének rendjéről szóló 90/2010.(III.26.) Kormányrendelet

[11] a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Kormányrendelet

[12] Az elektronikus hírközlésről szóló 2003. évi C. törvény

[13] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf 4. (210. 09.10) 4.oldal

[14] MOTEFF, JOHN– COPELAND, CLAUDIA– FISCHER, JOHN: Report for Congress, Received through the CRS Web, Critical Infrastructures: What Makes an Infrastructure Critical?, January 29, 2003.