HADMÉRNÖK

VII. Évfolyam 4. szám - 2012. december

Kassai Károly
kassai.karoly@hm.gov.hu

KIBERVESZÉLY ÉS A MAGYAR HONVÉDSÉG

Absztrakt

A korszerű élet és társadalom erősen függ a különböző információs rendszerektől és szolgáltatásoktól. Az összekapcsolt magánhálózatoknak, telekommunikációs szolgáltatásoknak, kormányzati hálózatoknak és az internetnek kölcsönös függőségei vannak, illetve a kibertérben lévő hálózatokat és szolgáltatásokat és adatokat érhetik belső vagy külső forrásból eredő negatív hatások.
A Magyar Honvédség katonai szervezeteinek rendszer és szervezet specifikus információs rendszerei, kritikus infrastruktúrái (benne kritikus információs infrastruktúrák) találhatók a nemzeti és globális kibertérnek, így a kiber fenyegetések, sérülékenység illetve a kiberbiztonsággal kapcsolatos kérdések vizsgálata fontos és aktuális feladat a jobb és biztonságosabb katonai elektronikus adatkezelő szolgáltatások érdekében.

Modern life and society highly depends upon different information systems and information capabilities. The interconnected private networks, telecommunication services, governmental networks and the Internet have some interdependency and the services, networks and information may have some negative impacts in the cyberspace from internal and external sources.
The military organisations of Hungarian Defence Forces have system and organisation specified information services and critical infrastructures, including critical information infrastructures in the national and global cyberspace, so the study of cyber threats, vulnerabilities and cyber security related issues is real important and actual task for the better and secure military information services.

Kulcsszavak: *információvédelem, kiberbiztonság, kiberfenyegetés, kritikus információs infrastruktúra ~ information security, cyber security, cyber threat, critical information infrastructure.*

A „KIBER” ÉS FENYEGETÉSEI

Napjaink egyre népszerűbb témája a „kiberhadviselés” (cyberwar), a „kibertámadás” (cyber attack; a továbbiakban a „cyber” előtag napjaink gyakorlata szerint „kiber”-ként szerepel), illetve az ehhez kapcsolódó kérdések. Hazánkban e területen egységes álláspont, központi szabályozás nem azonosítható, a magyar szakkifejezések sem alakultak ki, így a Magyar Honvédségnél is indokolt kiberveszéllyel kapcsolatos általános kérdések vizsgálata.

Az elektronikus adatkezelés területén a *veszélyek megállapítása a fenyegetések és a sebezhetőség felmérésének, a bekövetkezés gyakoriságának és súlyosságának elemzésének rendjéből áll*, minden esetben adott elektronikus adatkezelési szolgáltatásra, infrastruktúrára, vagy annak elemére vonatkoztatva, így célszerű ezt a sorrendet követni a kiberveszély általános értelmezése esetében is.

A „kibertér”-en (cyberspace) lényegi megfogalmazás szerint az összekapcsolt hálózatok világát célszerű érteni, mely megfogalmazás legfontosabb eleme az *összekapcsolás*. A német Kiber Stratégia pontosan megfogalmazza, hogy a külső kapcsolatokkal nem rendelkező elektronikus adatkezelés nem része a kibertérnek. [1.] Az összekapcsolás történhet azonos vagy különböző szintű védelmi rendszabályokkal rendelkező hálózatok között, tartalmazhat teljes vagy részleges szolgáltatás elérést, illetve önmagában az internet csatlakoztatása is összekapcsolás (nyilvános hálózattal történő összekapcsolás). Láncszerűen összekapcsolt hálózatok esetében elképzelhető, hogy egy hálózat felé nem a közvetlenül csatlakozó hálózatból érkezik a fenyegetés, hanem azon keresztül egy további hálózatból. A kibertér értelmezésénél a szolgáltatás hardver és szoftver összetevőin kívül *magát az adatot is elemként kell figyelembe venni*.

A „kiberművelet” (cyber operation) a kibertérben végzett elektronikus adatkezelés és az adatkezelő képességek működésével kapcsolatos tevékenységek, illetve tágan értelmezve az ezek védelmére, befolyásolására vagy támadására (pl. kibertámadás; cyber attack) irányuló tevékenységek, folyamatok.

A „kiberbiztonság” (cyber security) a kibertérben lévő szolgáltatás vagy adat meghatározott (kiber)fenyegetések (cyber threats) ellen, előre meghatározott védelmi szintű állapotát jelenti.

A „kibertér” vagy a „kiberinfrastruktúra” (cyber infrastructure) fogalom tartalma esetenként térben, vagy fizikai jellemzőkkel nehezen meghatározható, a képességek alakulása szerint dinamikusan változó tartalommal bír, beleértve az adatok és hozzáférési lehetőségek sokféleségét, valamint az adat, vagy infrastruktúra hozzáférési lehetőséggel rendelkező személyek körét is.

A kiberfenyegetéseknél *célszerű a fenyegetések eredetét tisztázni, ami támpontot adhat a kihívások kezeléséhez szükséges szervezetek azonosításához is*. Egy Európa Parlament számára készített tanulmány szerint alapvetően a hacker tevékenység, a szervezett bűnözés, az ideológiai vagy politikai szélsőségesség és az állami szereplők által támogatott kiber területű agresszió képezi a fenyegetések forrását.

A Nemzetközi Távközlési Szövetség (International Telecommunication Union; ITU) számára készített szakterületi tanulmány is ehhez hasonlóan fogalmaz (az „állami szereplők” megfogalmazás helyett „hírszerző szervezetek”-et alkalmazva), az előbbiek mellett külön kategóriában említve az oknyomozó riportereket és az elégedetlen alkalmazottakat (ez utóbbi kategóriát a korábbi forrás egyszerűen a hacker kategóriába sorolta). [2.]

A fenyegetések eredetét egy nemzetközi információbiztonsági szabvány [3.] a következőként azonosítja: hacker, cracker; szervezett bűnözők; terroristák; ipari kémek és belső szereplő.

A kiberfenyegetés a Világ Gazdasági Fórum tavalyi évre vonatkozó tanulmánya szerint lehet:

- *Kiberlopás*, ami egyre erősödő iparággá válik, különösen ahol a gazdasági fejlődés a globális kommunikációs technológia hozzáférésével párosul.
- K*iberkémkedés*, a magán és közszférában egyaránt értelmezve, benne a hírszerzés új formáival, amely fenyegetés nem csak az ellenséges, hanem a szövetséges államokból is származik.
- *Kiberháború*, figyelembe véve a háború értelmezése körüli téves civil értelmezéseket. Háború a kibertérben is lehetséges, illetve a hagyományos és kiberháború kölcsönhatásának egyre nagyobb kockázata van a társadalmakra; az online agresszió nem csak támogatása, hanem hagyományos támadások lehetséges provokálása is lehet.
- *Kiberterrorizmus*, ami az internet nyitottsága, a biztonság és a magánjellegű adatok szempontjából kevésbé ismert. A terrorista szervezetek az elmúlt években egyre szélesebb körben használják az internetet elméleti megalapozásra, toborzásra, műveleti kommunikációra, valamint kiberlopásra.

A fenti szándékos vagy rosszindulatú fenyegetésekből adódó kockázatok hatásának fokozását jelenti az internethez csatlakoztatott „okos” rendszerek hiányosságainak széles skálájából adódó kockázat. [4.]

A kiberfenyegetés célja más ITU források szerint lehet:

- adatok vagy erőforrások megsemmisítése;
- adatok illetéktelen módosítása vagy megismerése;
- adatok vagy erőforrások eltulajdonítása, eltávolítása vagy elvesztése;
- adatok illetéktelen felfedése;
- szolgáltatások megszakítása vagy korlátozása; [5.]
- megszemélyesítés, feljogosított személy adataival történő visszaélés. [6.]

Egyéb ITU forrás szerint a fenyegetések lehetnek *véletlenek* (hardver vagy szoftver hiba, kiszolgáló elemek meghibásodásai) vagy *szándékosak* (vírusok és egyéb rosszindulatú programok), *aktívak* (adat és erőforrás megváltoztatása) vagy *passzívak* (erőforrást nem változtató lehallgatás, forgalomelemzés), illetve el kell különíteni a (hálózat szempontjából) *külső és a belső eredetű* (valamilyen feljogosítással, helyi ismeretekkel rendelkező személy) támadásokat. [7.]

Az ISACA (Information Systems Audit and Control Association; Információrendszer Ellenőrök Egyesülete) Európára vonatkozó 2012-es biztonsági felmérés alapján a szervezeti szempontból legmagasabb kockázatú felhasználói tevékenységek: felhasználói jelszavak tárolása fájlban, magántulajdonú eszközön (80%), on-line fájlmegosztási szolgáltatások igénybevétele szervezeti adatok kezelésére (71%) szervezeti tulajdonú számítógép vagy okostelefon elvesztése (65%), személyes fájlok, zene, alkalmazások letöltése szervezeti tulajdonú számítógépre vagy okostelefonra (53%), felhasználói jelszavak tárolása fájlban, szervezeti tulajdonú eszközön (48%), szervezeti tulajdonú számítógép vagy okostelefon használata hivatalos levelezésre, adatkezelésre (43%). [8.]

Az Európai Unió államaiból jelentett incidensek alapján az Európai Hálózatbiztonsági Központ (European Network and Information Agency; ENISA) 2011-es évre vonatkozóan az állandó telefon, állandó internet szolgáltatások, mobil telefon (benne szöveges üzenet szolgáltatás) és mobil internet szolgáltatások bontásban értékelte a veszélyeket. Az incidensek okai: hardver és szoftverhiba (41%), áramellátás (20%), kábelhiba (14%), változáskezelési probléma (10%), vihar (6%), karbantartási hiányosság (6%), hóvihar (4%), humán hiba (4%),

áramingadozás (4%), kábellopás (2%), árvíz (2%), kibertámadás (2%), szolgáltatás túlcsordulás (2%), fizikai támadás (2%). Az éves elemzés alapján a tanúságok a következők:

- A mobil hálózatok veszélyeztetése a legmagasabb (az incidens bejelentések 60%-a erre a területre vonatkozott).
- Az üzemkiesések a mobil szolgáltatások felhasználóit érinti a legnagyobb számban (összhangban a behatolások legnagyobb arányával).
- A hardver, szoftverhiba valamint a harmadik fél miatt (pl. áramszünet, szoftver javítócsomag hiány, külső üzemeltető hiányosságai) bekövetkezett hibák okozzák a kiesések túlnyomó részét. A hardver, szoftverhiba kiemelten veszélyezteti a mobil szolgáltatásokat (a komplexitás és a redundancia hiánya miatt).
- A természeti katasztrófák (kiemelten: vihar, árvíz, hóvihar) okozták a leghosszabb kieséseket (átlag: 45 óra).
- Az elektromos hálózattól való függés egyaránt kimutatható az állandó és a mobil rendszereknél. [9.]

Stratégiai szintű összefoglalásnak tekinthető az EU Biztonsági Stratégia megfogalmazása, mely szerint a kereskedelem, a befektetések, a technikai fejlődés erősítik Európa függőségét – így sebezhetőségét – az összekapcsolt szállítási, energetikai, információs és egyéb infrastruktúrákon keresztül. [10.] Ehhez hasonlítható a NATO megközelítés is, mert a NATO Stratégiai Koncepció szerint *a kibertámadások egyre gyakoribbá, szervezettebbé vállnak* és *egyre nagyobb károkat okoznak* a közigazgatásban, az üzleti életben és a gazdaságban, veszélyeztethetik a szállítást, az energetikai rendszereket és egyéb kritikus infrastruktúrát is. A támadások elérték azt a küszöböt, amikor már a nemzeti és Euro-Atlanti jólétet, biztonságot és stabilitást fenyegetik. A támadások eredhetnek külföldi fegyveres erőktől és hírszerző szolgálatoktól, a szervezett bűnözés köreiből, terrorista és egyéb extrém csoportoktól. [11.]

A magyar felső szintű megfogalmazás a nemzetközi megfogalmazásokkal összhangban van. A Nemzeti Biztonsági Stratégia megállapítja, hogy az állam és a társadalom működése mind meghatározóbb módon a számítástechnikára épül. 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 rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését. Emiatt a kibertérben növekvő mértékben jelentkező nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmi vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kell állnia. A nemzeti szintű védelem a Magyar Honvédség számára is iránymutatóan kettős feladatot jelent:

- *a tényleges vagy potenciális fenyegetések és kockázatok rendszeres felmérése és priorizálása, a kormányzati koordináció erősítése, a társadalmi tudatosság fokozása, valamint a nemzetközi együttműködési lehetőségek kiaknázása;*
- *a nemzeti kritikus információs infrastruktúra védelmének erősítése mellett a szövetségesekkel és EU-partnerekkel együtt az információs rendszerek biztonságának erősítése, a megfelelő szintű kibervédelem* kialakításában való részvétel. [12.]

Az ISACA magyarországi tagozat által végzett, a 2011-es évet elemző tanulmánya szerint – az auditálások tapasztalata alapján – a leggyakrabban előforduló információbiztonsági problémák: túlzott jogosultságok (52%), nem megfelelő naplózás (42%), nem kielégítő változáskezelés (36%), összeférhetetlen szerepkörök (24%), az üzletmenet folytonosság nem megfelelő biztosítása (23%), és a fizikai biztonság hiányossága (17%). (A felmérés 114 magyar cég és intézmény bevonásával történt; 1/3 - 2/3 arányban költségvetési és magánszférából.) [13.]

A Puskás Tivadar Közalapítvány (Nemzeti Hálózatbiztonsági Központ, PTA CERT HUN) 2012. évi harmadik negyedéves jelentése szerint a magyar vállalati szférában tavaly az észlelt biztonsági incidensek megoszlása: eszközlopás (26%), bizalmas adatok kompromittálása (16%), belső behatolási kísérlet (8%), külső behatolási kísérlet (5%), csalás (4.5%). Egy másik hivatkozott felmérés szerint a magyar vállalati rendszeradminisztrátorok szerinti legfontosabb fenyegetések: a vírusfertőzés vagy hálózati támadás miatti leállás (31%), célzott külső támadás miatti adatvesztés (30%), hardverhiba vagy szándékos/véletlen törlés miatti adatvesztés (26%), felhő szolgáltatások biztonsága (24%), illetéktelen fizikai hozzáférés a belső hálózathoz (22%), tabletek és okostelefonok vállalati használata (20%). [14.]

A bemutatott fenyegetések illetve veszélyek az utóbbi időszak valamilyen gyakorlata alapján összeállítottak (statisztikák, interjúk), de a fenyegetések felméréséhez nemzetközi szabvány is nyújthat általános segítséget. [15.] Az általános fenyegetéslista a következő fő csoportokat tartalmazza:

- fizikai károk;
- természeti csapás;
- kritikus szolgáltatások kimaradása;
- sugárzás okozta károk;
- kompromittálódás;
- technikai meghibásodás;
- engedély nélküli műveletek;
- funkciók veszélyeztetése.

A fentiek alapján megállapítható, hogy *a kiberfenyegetés eltérő veszélyű, széles skálán értelmezhető fogalom*. Hazánkban – más államokhoz hasonlóan – a közigazgatásban egy szervezet nem azonosítható, mint e fenyegetésekkel szemben a védelemért felelős szervezet. Feladata van a bűnüldözésnek és megelőzésnek, a nemzetbiztonsági tevékenységeknek és a terrorelhárításnak, az adóhatóságnak, a katonai felderítésnek. A védelem és helyreállítás területén eltérő feladata van a különböző szakmai feladatokkal megbízott szervezeteknek, mint a CERT-nek (Computer Emergency Response Team, Nemzeti Hálózatbiztonsági Központ), a minősített adatkezelés biztonsági felügyeletéért felelős Nemzeti Biztonsági Felügyeletnek, a közigazgatási rendszerek üzemeltetőinek és az önálló hálózatokat üzemeltető tárcáknak, a katasztrófavédelmi feladatokat végző szervezeteknek. Széles körben értelmezve említeni kell még a hardver és szoftverfejlesztésben, gyártásban érintett cégeket, tanácsadó cégeket, oktatási intézményeket, de szerepe van az igazságügyi szereplőknek, egyéb hatóságoknak és a jogszabályalkotóknak is.

A gyakorlati statisztikák láthatóan illeszthetők a szabvány alapú fenyegetések témaköreihez, illetve az is megállapítható, hogy *az általános fenyegetések a Magyar Honvédség elektronikus adatkezelő rendszerei nagy részénél értelmezhetők*, így az üzemeltetési sajátosságok figyelembe vételével ezek az eredmények hasznosíthatók.

SEBEZHETŐSÉG ÉS KOCKÁZATMENEDZSMENT

Az eddig említett általános fenyegetések után következik a sebezhetőség, az adatkezelő képességek értelmezésének és ismeretének, illetve a kockázatok menedzselésének kérdése.

A sebezhetőség vizsgálat adott elektronikus adatkezelő szolgáltatáshoz, infrastruktúrához köthető *szisztematikus, visszatérő jellegű felmérés és értékelés*. A vizsgálat összetett szervezeti, technikai, adminisztratív és szabályozási kérdésekre irányuló feladat, ami az szolgáltatás összetettsége, kiterjedése, fontossága szerint *felosztható, strukturálható*. A sebezhetőség vizsgálatát célszerű két lépcsőre bontani. Az első lépcső feladata valamilyen

általános módszertan, bevált gyakorlat alapján az általános sebezhetőségek azonosítása és csoportosítása, amit második lépcsőben követhet az adott helyszíneknek és rendszereknek megfelelő specifikus adatokkal történő kiegészítés (ami már nagy valószínűséggel az üzemeltető szervezet által bizalmasan kezelt adatok kategóriájába fog esni).

A sebezhetőség vizsgálat területén hazánkban jogszabály pontos követelményt nem azonosít, csak az valószínűsíthető, hogy a készülő elektronikus információbiztonsági törvény végrehajtási rendeletei valamilyen szinten az MSZ ISO 27000 szabványcsaládhoz fognak igazodni. Az általános sebezhetőségi szempontrendszert ezek alapján az ISO/IEC 27005:2011 szabvány ajánlása szerint célszerű kialakítani [16.], melynek fontosabb területei a következők:

- *Hardver terület:* karbantartási hiányosságok, telepítési problémák, konfiguráció felügyelet hiánya, páratartalomra, porra vagy egyéb szennyeződésre való érzékenység, elektromágneses sugárzásra való érzékenység, hatékony konfiguráció felügyelet hiánya, áramellátás ingadozásra vagy kiesésre való érzékenység, hőmérsékletváltozásra való érzékenység, engedély nélküli módosítás, tárolási hiányosságok.
- *Szoftver terület:* szoftver tesztelési hiányosság, ismert szoftver hiba, kijelentkezés nélküli távozás lehetősége, megfelelő szintű törlés nélküli adathordozó használatra történő átadása vagy újrafelhasználása, szoftver kiadás hiányosságai, a hozzáférési jogosultságok nem megfelelő alkalmazása, naplózási hiányosság, nem megfelelő alkalmazások használata, túl bonyolult felhasználói felületek, üzemeltetési vagy felhasználói dokumentumok hiánya, az adatkezelő rendszer nem megfelelő beállításai, azonosítási és hitelesítési hiányosságok, jelszóbiztonsági menedzsment hiányosságai, felesleges szolgáltatások biztosítása, fejlesztés alatt álló vagy új szoftver alkalmazása, változáskezelés hiánya, kontroll nélküli szoftver letöltések, illetve illegális szoftverek alkalmazása, biztonsági mentések hiánya.
- *Hálózati terület:* nem megfelelően védett kommunikációs csatorna alkalmazása, érzékeny adatok védelem nélküli továbbítása, hibás kábelcsatlakozások, tartalék nélküli elem meghibásodása, az üzenet küldőjének vagy fogadójának nem megfelelő azonosítása és hitelesítése, nem biztonságosan kialakított hálózati architektúra, a jelszavak nyílt formában történő továbbítása, nem kielégítően működő hálózati menedzsment, nem megfelelően védett nyilvános hálózathoz való csatlakozás hiányosságai.
- *Személyi sebezhetőség:* személy távolléte, nem megfelelően kialakított eljárások, nem elégséges biztonsági képzés, hardver vagy szoftver nem megfelelő használata, hiányos biztonságtudatosság, külső fél vagy karbantartó, takarító személyzet felügyelet nélküli tevékenysége, eszköz vagy szolgáltatás használatának hiányos szabályozása.
- *Helyszín:* épületekbe vagy helyiségekbe történő belépés szabályozatlansága, áradásra érzékeny vagy talajvíz által fenyegetett helyen történő kialakítás, nem stabil áramellátás, épületek, ajtók vagy ablakok hiányos fizikai védelme.
- *Szervezet:* felhasználói jogosultságot szabályozó eljárások hiányosságai, szerződő felekkel, harmadik partnerrel kapcsolatos intézkedések hiányosságai, szabályozott audit vagy felügyeleti tevékenység hiánya, a kockázatok azonosítására és felmérésére vonatkozó eljárások hiánya, a bejelentett hibák rögzítésének hiánya, változáskezelési eljárások hiánya, üzemeltetési vagy biztonsági dokumentumok menedzselési hiányosságai, felelősségek meghatározásának hiányosságai, az adatkezelés szabályozási hiányosságai, a biztonsági incidensek esetén alkalmazandó fegyelmező intézkedések hiánya, a mobil adatkezelő eszközök használatának szabályozatlansága, helyiségen kívüli alkalmazás felügyeletének hiánya, a szerzői jogok védelmére vonatkozó eljárások hiánya.

A sebezhetőség vizsgálat és értékelés történhet *az üzemeltető szervezet által* (belső ellenőrzés), *jogszabályban meghatározott felügyeleti szerv által*, illetve ezt kiegészítően (és nem a komplex szempontú ellenőrzés helyett), történhet *belső vagy külső szervezet által* végzett technikai jellegű, specializált mérnöki szintű vizsgálat. Ezeket a vizsgálatokat egyes esetekben kiválthatja egy *független szervezet által végzett biztonsági audit*, melynek szabvány alapon történő megvalósítása az említett szabványcsaládon belül – erőforrások függvényében – hazánkban is megvalósítható.

A sebezhetőség kérdésénél gyakran félreértelmezett feladat a szolgáltatást biztosító elemek, pontosabban *az információs vagyontárgyak (assets) azonosítása*. A pontos konfiguráció ismerete, az azonnal alkalmazható tartalék eszközök és a raktárban lévő eszközök nyilvántartása nélkül javítási vagy helyreállítási lépések nem képzelhetők el. A kérdés további értelmezése elvezet a *kritikus infrastruktúra védelem*, ezen belül a *kritikus információs infrastruktúra védelem* témaköréhez. Hosszabb kifejtés nélkül is belátható a kritikus szolgáltatások azonosításának – és azok védelmére szervezett feladatok meghatározásának – fontossága. Az üzemeltető állománynak pontosan tudnia kell, hogy meghibásodások esetén milyen sorrendben kell helyreállítani a szolgáltatásokat – kiemelt figyelemmel a kritikus fontosságú felhasználók munkájának támogatására –, ami a pontos hardver és szoftver helyzet ismerete mellett már a vészhelyzeti és helyreállítási tervezési és képzési, gyakorlási feladatokra is rámutat. A már hivatkozott nemzetközi szabvány információs vagyontárgyakra vonatkozóan elsődleges és másodlagos vagyontárgyakat különít el. Elsődlegesek az szervezeti folyamatok és tevékenységek másodlagosak a hardver, szoftver, hálózat, személyek, helyszínek és szervezeti struktúra. [17.]

Az adott infrastruktúrához, elemekhez köthető fenyegetések és sebezhetőség az előfordulás gyakorisága, súlyossága figyelembevételével valamilyen kockázatelemzési módszertannal határozható meg, de célszerű a feladatot tovább gondolni. Az adott szolgáltatásra kimutatott veszély önmagában még nem teljes értékű adat, *a katonai képességek szempontjából kulcsfontosságúnak inkább a működési hatáselemzés* (Business Impact Analysis; BIA) e*redménye tekinthető*. A hatáselemzés azt mutatja meg, hogy az adott híradó és informatikai rendszer szolgáltatásainak kiesése vagy a szolgáltatási szint csökkenése mely műveleti képességekre milyen negatív hatást fejt ki. A felgyorsult élet veszélyeit jól szemlélteti, hogy egy német információbiztonsági kormányzati ajánlás a működési hatáselemzés dokumentumaira egyedileg azonosított változáskezelési eljárást javasol, illetve önmagát a hatáselemzést féléves gyakorisággal tartja szükségesnek. [18.]

A kibervédelmi helyzet tanulmányozása, a teendők azonosítása hazánkban is megkezdődött, egyik oldalról jól azonosíthatóan kritikus infrastruktúra védelem és kritikus információs infrastruktúra védelem irányultsággal. Egy magyar kritikus infrastruktúra védelmet elemző tanulmány az információs hadviselés tárgyalásánál a támadások célterületeiként a *tudati*, *fizikai* és *információs* dimenziót azonosítja. A tudati dimenziónál felsorolt tényezők elgondolkodtató, társadalmi szintű jelenségekre mutatnak rá, mint a *tudatlanság*, az *információs technológia vívmányaihoz való hozzáférés hiánya*, az *innoválható tudás hiánya*, a *rejtett tudás kihasználatlansága*, az *információs túlterheltség hatásai*, az *információs technológiákkal szembeni idegenkedés, bizalmatlanság, iszony*.

A tanulmány a fenyegetéseket a korábban ismertetett módon külső és belső fenyegetésekre bontja, ezen belül *magasan és alacsonyan szervezett fenyegetettségeket* különböztet meg.

A kritikus infrastruktúra védelem kialakítása a szerzők javaslata szerint a következő témakörökre tagolható (a témakörök önmagukban is összetett feladatokat tartalmaznak):

- a védelmi célok meghatározása;
- a kritikus infrastruktúrák meghatározása és azonosítása;
- a feltárt kritikus infrastruktúrák kritikus információs infrastruktúráinak meghatározása és azonosítása;

- a kritikus infrastruktúrák priorizálása;
- a veszélyek és sérülékenységek feltárása;
- az ideális védelmi megoldások és akciótervek kidolgozása;
- az ideális védelmi megoldások és az aktuálisan alkalmazott védelmi megoldások összehasonlítása, és az esetleges hiányok vagy meg nem felelés pótlása vagy megszüntetése.

E feladatok támogatásához kiemelendő *az azonos szempontrendszer szükségessége meghatározáshoz, besoroláshoz*, valamint a *sérülékenység illetve a kockázatelemzés területén egységes módszertan, elvek alkalmazása*, ami kormányzati *szintű kutatási és fejlesztési támogatást igényel.* [19.]

Egy másik magyar tanulmányban Haig Zsolt és Kovács László – akár összegzésnek is értelmezhető megállapítása – szerint az említett három dimenzióban „a komplex információs támadások egymás után vagy egymással párhuzamosan, egyszerre több színtéren, dimenzióban realizálódhatnak". [20.]

E miatt az összetettség miatt – mint Nagyné Takács Veronika cikkében megállapította – kiemelt fontosságú, hogy a *védelem tervezése minél több szempont figyelembe vételével történjen, a védelmi rendszer többszintű és több elemből álló legyen, illetve a helyi és központi feladatok, felelősségi körök legyenek összehangolva*. [21.]

A kiberveszély általános összefoglalása, illetve az ehhez szükséges lépések átfogó ismertetése mellett megemlítendő, hogy az *időszakosan végzett, vagy egyedi változáshoz rendelt kockázatelemzés napjainkban már nem elégséges* a kellően rugalmas védelem kialakításához, illetve az incidenskezeléshez. A hálózatokba integrált szenzorok, adatfeldolgozó eljárások, automatikus értékelő megoldások és döntéstámogató alkalmazások már *lehetővé teszik a dinamikus kockázatelemzést*, az incidens során történő valós idejű beavatkozást, ami lényegesen eredményesebb lehet, mint a hálózati katasztrófa vagy információs károkozás utókezelése. A közel valós idejű információbiztonsági helyzetismeret (situation awareness) feltárja a negatív eseményeket, megmutatja a lehetséges kimeneteket, és segít annak a döntésnek meghozatalában, melynek eredménye lehet a szolgáltatás azonnali változtatása, szüneteltetése, az adatok hozzáférésének azonnali letiltása vagy korlátozása, illetve a bizonyíték szolgáltatás érdekében már az ellenséges műveletekkel párhuzamosan is megtörténhet naplózás, együttműködő partner riasztása, hatósági bejelentés.

KATONAI SAJÁTOSSÁGOK

A Magyar Honvédség szervezeteinek irányításához, vezetéséhez és működéséhez szükséges elektronikus adatkezelő szolgáltatások biztonsága (vagy kiberbiztonsága) publikus formában részletesen nem tárgyalható, de az általános helyzetmegítéléshez szükséges áttekintéshez erre nincs is szükség. A honvédelmi feladatok ellátásához a következő típusú információs infrastruktúra elemeket kell megkülönböztetni:

- EU vagy NATO tulajdonú EU, vagy NATO adatot kezelő rendszer;
- nemzeti tulajdonú EU, vagy NATO adatot kezelő rendszer;
- kormányzati rendszer;
- honvédelmi ágazati állandó (stacioner) rendszer (MH Kormányzati Célú Elkülönült Hírközlő Hálózat és hozzá csatlakozó, vagy önállóan üzemelő helyi hálózat), vagy honvédelmi ágazati tábori rendszer;
- honvédelmi szervezettel együttműködő szervezet rendszere;
- nyilvános hálózat.

A felsorolás átfogalmazható úgy is, hogy az MH Kormányzati Célú Elkülönült Hírközlő Hálózat (annak célrendszerei, a központi szolgáltatásokat kiegészítő helyi szolgáltatások és tábori rendszerek), illetve az ezekhez csatlakozó más szervezetek hálózatainak és nyilvános hálózatok összekapcsolásainak összességéből kialakított kibertér alkotja a magyar katonai kiberteret, amely fogalom *a vizsgálati szempont szélesítésével magyar védelmi ágazati kibertérré bővíthető.*

Az MH Kormányzati Célú Elkülönült Hírközlő Hálózat jogszabályban meghatározott feltételek szerint [22.] üzemeltetett *kormányzati célú elkülönült hírközlő hálózat*, melynek hálózatgazdája a honvédelmi ágazatért felelős miniszter. Ez az elkülönülés üzemeltetési és biztonsági szempontból lényeges szempont, illetve megvilágítja azt a tényt is, hogy a *katonai képességeket biztosító szervezetek térben és időben dinamikusan más-más szolgáltatásokat vesznek igénybe*, más a függőségi viszonyuk a különböző célrendszerektől, vagy éppen az internettől. Emiatt nagyon nehezen értelmezhető a „Magyar Honvédség kibervédelme" és ehhez hasonló általános megfogalmazás, ami tízes nagyságrendű stratégiai, hadműveleti és harcászati szintű honvédelmi szervezet, háttérintézmény és tevékenységüket kiszolgáló hálózatok egységes értelmezését jelenti.

Megállapítható az is, hogy a katonai képességek működtetése a közszférában megszokotthoz képest *lényegesen nagyobb arányban tartalmaz minősített adatkezelést* (az ezzel járó kiegészítő védelmi rendszabályokkal együtt), haderőnemenként specializált tábori mobil eszközöket, egyéb katonai szolgáltatásokat, melyeket összefoglalóan nem lehet értelmezni, tárgyalásuk csak specifikusan lehetséges. Ebbe a körbe tartozik például a radaradat, a föld-levegő azonosításhoz szükséges speciális kommunikáció, a fegyverirányítási rendszerek vagy a harcászati rendszerek egyedileg kialakított jelkészlete, ahol a hagyományosan értelmezett „minősítő" és a minősítési folyamat követelményei közvetlenül nem alkalmazhatók.

További – nem csak a Honvédséget érintő – sajátosság, hogy hazánkban jelenleg *a minősített és a nem minősített elektronikus adatkezelésre nincs egységes szabályozási követelményrendszer meghatározva*. A nem minősített adatkezelésre jelenleg nincs jogszabályban megfogalmazott egyértelmű, végrehajtható követelmény. Minősített elektronikus adatkezelésre vonatkozóan átfogó megfogalmazású követelmény áll rendelkezésre, mely szerint „biztonsági követelményeket" kell meghatározni – és jóváhagyni, és ennek alapján „üzemeltetés biztonsági szabályzat"-ot kell készíteni és jóváhagyni. [23.]

A fentiek mellett szükség van a katonai sajátosságok értelmezésére. A stratégiai szintű adatkezelés a közigazgatásban még könnyen azonosítható elvek alapján működik, bár itt már megjelenik a szövetségi tagsággal kapcsolatos adatkezelés bonyolultsága. A Magyar Honvédségnél egyes esetekben tisztán azonosíthatók a NATO, EU (vagy egyéb két, vagy többoldalú nemzetközi kötelezettségvállalás alapján védendő) adatok halmaza, más esetben ezen adatok dinamikus változása, egymásba történő átalakulása könnyen megkeseríti a felhasználók életét. A katonai sajátosságoknál további *fontos tényező a mobilitás szükségességének és fontosságának megértése, támogatása*. Stratégiai vagy hadműveleti szinten is szükség van a felhasználók mobil kommunikációjának biztosítása, de ez lényegesen különbözik a harcászati jellegű mobil, kézi, vagy hordozható képességektől, ahol az adatkezelés jellege eltolódik az alacsonyabb minősítésű, rövid elévülési idejű adatok felé, jellemzően a harcászati rádiókommunikációra támaszkodva.

Napjainkban katonai területen nem ritkaság *a NATO, EU vagy egyéb nemzetközi együttműködés, amit elektronikus minősített adatkezelő képességekkel is támogatni kell* (itt jelennek meg egyszerű esetben a „milyen nyilvántartásba kell venni", vagy a „milyen akkreditált rendszeren tudom megoldani a feladatot" kérdések). Az adat identitás kezelése mellett a másik jellegzetes kihívás *a rövid elévülési idejű adatok kérdése*. A nemzeti légtérhelyzet pillanatnyi állapota érzékeny adat, ami átadás után már egy EU vagy NATO

egységes légihelyzet információ szerves részét képezi. Az ilyen jellegű minősített adat kezelése, vagy harcászati környezetben egy parancs, intézkedés kiadása nem egyenértékű a hagyományos irodai alkalmazású adatkezeléssel, így nyilvánvaló, hogy szükség van ezen esetek pontos meghatározására és *az adatkezelés sajátosságainak megfelelő specializált védelmi rendszabályok kialakítására*.

A Honvédség alkalmazása nem csak békeidőszakban, a közigazgatási rend szerinti körülmények között történhet. Az Alaptörvény különleges jogrendre vonatkozó fejezetében megfogalmazott esetekben kijelölt személy, vagy testület rendeletet alkothat, amellyel egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat. Ennek megfelelően a kibervédelem területén is meg kell tenni azokat az előkészítő lépéseket, melyek az adott biztonsági helyzetnek megfelelően a legjobban támogatják a katonai szervezetek híradó és informatikai rendszereinek védelmét speciális helyzetekben is.

A Honvédség esetében jogszabály fogalmazza meg a lehetőséget, hogy különleges jogrend időszakában az általános katonai híradó és informatikai szolgáltatások kiegészíthetők tömegkommunikációs létesítmények, berendezések igénybevételével, használatba történő átvételével. Elrendelhető elektronikus hírközlési szolgáltatás szüneteltetése, korlátozása vagy ellenőrzésének módosítása, illetve megtörténhet ezek használatra történő átvétele is. [24.] A jogszabályban megfogalmazott változtatások eredményeként módosult híradó és informatikai szolgáltatások *megkövetelik az üzemfelügyeleti és biztonságfelügyeleti rend átalakítását, kiegészítését, illetve szükségessé válhat új szervezési, műszaki megoldások kialakítása is*.

Az adatkezelésre vonatkozó jogszabályok változásai érinthetik az elektronikus adatkezelésre vonatkozó *biztonsági követelményeket, a hatósági eljárásokat, az üzemeltetésre vagy felügyeletre vonatkozó szabályokat*.

Az országvédelemhez szükséges egyedi helyzetek kezelése az elektronikus adatkezelő szolgáltatások, védelmi igények és megoldások naprakész ismeretét igényli, illetve *megköveteli azt a tudást is, ami lehetővé teszi a katonai szervezetek működéséhez szükséges jogszabályi változtatási javaslatok megtételét, új megoldások gyors és kreatív kialakítását*. Rendkívüli helyzetek szövetségesi kötelezettségvállalás teljesítése közben is előfordulhatnak, ahol - akár egy másik földrészen, hiányos infrastrukturális feltételek között – szükség van szövetségi, vagy más nemzeti szolgáltatásokkal történő gyors együttműködés megszervezésére, szolgáltatások kölcsönös igénybevételére, ami – különösen minősített elektronikus adatok esetén – nem mindig tekinthető egyszerű esetnek.

AKTUÁLIS KIBERVÉDELMI FELADATOK

A Magyar Honvédségnél az információbiztonsági átfogó követelmények, irányelvek és feladatok miniszteri utasításban megfogalmazott információ biztonságpolitikában rögzítettek. [25.] *A kibervédelem feladatainak értelmezése az eddigi elektronikus információbiztonsági követelmények és eljárásrend erőforrások szerinti továbbfejlesztését jelenti, az eddig megtett szakmai lépések, feladatok átszervezésére vagy visszavonására nincs szükség*. A továbblépéshez szükséges feladatok lényege a következő:

A szükséges szabályozási környezet kialakítása. A meglévő szabályozási renden belül az üzemeltető, felügyelő és biztonságért felelős szervek és szervezetek hatáskörének, kibervédelmi feladatainak – benne a külső-belső együttműködési feladatainak – kidolgozása, a kritikus információs infrastruktúra védelem ágazati feladatrendjének kidolgozása, a különleges jogrendben alkalmazható eljárások irányelveinek meghatározása.

Az elektronikus adatkezelő hálózatok biztonsági szintjének emelése. A hálózatok biztonságának növelése érdekében szabvány és bevált gyakorlat alapú módszereket kell alkalmazni a biztonsági követelmények megfogalmazása és a védelmi rendszabályok

kialakítása, alkalmazása, felülvizsgálata és továbbfejlesztése során. Specializált módszertant kell kialakítani a védelmi rendszabályok ellenőrzéséhez. Kiegészítő védelmi rendszabályokat kell meghatározni, alkalmazni a magas kockázatú szolgáltatások biztonsága érdekében. Az infrastruktúra meghatározott elemeinél meghatározott szintű tanúsított terméket lehet alkalmazni, illetve az architektúra menedzselése során a központi szolgáltatásokat kell előtérbe helyezni és központi biztonsági mechanizmusokat kell alkalmazni helyi megoldások helyett. A hálózati szintű csatlakozásoknál fel kell használni a Nemzeti Távközlési Gerinchálózat adta lehetőségeket (tartalék útvonalak, illetve elsődleges védelmi vonal). Fel kell tárni a szolgáltatások életciklusa során az üzemeltetéssel és fejlesztéssel kapcsolatos biztonsági réseket, azonosítani kell az ellátási láncban rejlő kockázatokat (supply chain risks), és ellensúlyozni kell azokat. Specializáltan erősíteni kell a biztonságtudatosságot (security awareness) a felhasználóknál, az üzemeltetőknél (beleértve a tervezést és az üzemeltetés irányítást), a biztonságért felelős állománynál, a kibervédelem kialakításában és fejlesztésében érintett vezetői és döntéshozó állománynál. A rendelkezésre álló kommunikációs lehetőségek kihasználásával ezeket a mozzanatokat figyelemfelhívó programokkal, időszakos tájékoztatásokkal kell erősíteni.

A kibertámadások elleni képességek kialakítása és fejlesztése. Időszakosan és változáshoz kötötten elemezni és értékelni kell a kiberbiztonsággal kapcsolatos kockázatokat. Naprakészen kell tartani a kiberbiztonság aktuális állapotának megítéléséhez szükséges adatok körét és folyamatosan fejleszteni kell a szervezeten belüli és a szervezetek közötti együttműködés rendjét és feladatait. A védelmi rendszabályokon belül a detektálásra és jelzésre épülő mechanizmusok mellett folyamatosan fejleszteni kell a valós idejű döntéstámogatást és előkészítést, a reagálást, illetve a bizonyítékszolgáltatást és helyreállítást is támogató eljárásokat. Az üzemeltető, a biztonsági felügyeleti feladatokat ellátó, illetve a kibervédelmi eljárásokat irányító állomány számára specializált képzési és továbbképzési rendszert kell fenntartani. A reagáló képesség értékelésének érdekében komplex – a váratlan ellenőrzéseket is tartalmazó – ellenőrzési módszertant kell kialakítani és fenntartani. Ki kell használni az önkéntes szervezetekkel, oktatási és kutatási intézményekkel kapcsolatos nemzeti és nemzetközi együttműködési lehetőségeket (tanácsadás és konzultáció).

A szaktudás növelése. Az általános katonai képzésekbe a lehető legjobban integrálni kell az információbiztonsági ismereteket. A szükséges képességek kialakítása és fenntartása érdekében a biztonsági és üzemeltető állomány számára specializált, valósághű gyakorlási lehetőségeket kell biztosítani. A biztonsági incidensek, üzemeltetési tapasztalatok, gyakorlások alapján szerzett tudást fel kell használni és be kell építeni a híradó és informatikai rendszerek védelmébe.

Kutatás és fejlesztés. Ki kell használni a központi kutatási programokban való részvétel, valamint a nemzeti és nemzetközi programokban, projektekben, K+F folyamatokban és feladatokban, illetve az ezeket megvalósító szervezetekben való részvétel lehetőségét. Figyelemmel kell kísérni az adatkezelési igényeket, folyamatosan elemezni kell a rendelkezésre álló megoldásokat, és elemezni kell alkalmazhatóságukat. A kibervédelmi feladatok tervezését az újonnan felbukkanó technológiák és azok hatásainak vizsgálatával, a technológiai trendek előrejelzésével kell támogatni.

Együttműködés. Az illetékes tárcákkal, nemzeti hatóságokkal és kibervédelmi feladatokat ellátó szervezetekkel szoros, specializált együttműködést kell kialakítani, valamint ki kell használni az oktatási és tudományos intézményekkel, szervezetekkel való együttműködésből adódó lehetséges szinergikus hatásokat. Kapcsolatokat kell tartani a kiberbiztonság szempontjából jelentős gyártókkal, forgalmazókkal, auditor és tanácsadó szervezetekkel. Hatékonyan működő kapcsolatokat kell fenntartani a honvédelmi érdekből összekapcsolt nemzeti és nemzetközi hálózatok üzemeltető, illetve menedzsment állományával.

Az azonosított kiberveszélyek kezeléséhez szükséges feladatok megtervezése, megfogalmazása a Magyar Honvédségnél felső szinten *háromfokozatú rendben képzelhető el*. Első lépésként a honvédelmi tárca információbiztonsági politikájának felülvizsgálatára és szükség szerinti módosítására van szükség, figyelembe véve a kiberbiztonsági, illetve a már jogszabályban megfogalmazott kritikus infrastruktúra védelmi szempontokat.

A szükséges mértékű hatásokat garantáló képességek megtervezése érdekében – figyelembe véve a kibertér és a kibervédelem összetettségét – második lépésként az MH szintű kibervédelmi feladatokat megalapozó koncepciót kell kialakítani és jóváhagyni.

Harmadik lépésként a jóváhagyott koncepció alapján a megvalósításhoz szükséges feladatokat megfogalmazó, szakmai és erőforrási tervezési lépéseket, programokat tartalmazó stratégia kialakítására van szükség. A Magyar Honvédség eddigi szabályozási rendjének megfelelően – amíg jogszabály ettől eltérő követelményt nem határoz meg – a stratégiai feladatok megfogalmazására alkalmas eszköz az MH Informatikai Stratégia, illetve ennek alapján a fejlesztési és üzemeltetési feladatok tízéves, rövid távú (négyéves), és éves beszerzési tervekben történő megjelenítése. A stratégiában rögzítetteket (képességeket) a haderőfejlesztési eljárások rendje szerint kell tervezni, kialakítani és használatba venni, kiegészítve a szükséges szabályozási és képzési feladatokkal.

A kifejezetten kibertámadás elleni védelem megfogalmazása során szintén lehetőség van a szabvány alapú megközelítésre. A logikai vonalat az *esemény bekövetkezése* – a *detektálás és jelentés* – az *elemzés és döntés* (incidensé nyilvánítás) – a *válasz* – a *szabályozó rendszer felülvizsgálata* - és a *szolgáltatás javítás* blokkokban megfogalmazható lépések határozzák meg. [26.]

A kiberbiztonság nem csak katonai területen értelmezhető, így nyilvánvaló, hogy egy nemzeti álláspont kialakítása és fenntartása kiemelt feladat az Alaptörvényben megfogalmazott „nemzeti vagyon” (e fogalmon belül a nemzeti adatvagyon) védelme és az adatkezelő képességek rendelkezésre állás érdekében. A strukturált megközelítéshez a *nemzeti koncepció – nemzeti stratégia – megvalósítást célzó jogszabály(ok)* vonal követése látszik célszerűnek. A megoldásba beleértendő a fogalmi kérdések tisztázása, az elektronikus információ biztonság és a kiberbiztonság tartalmának, viszonyának tisztázása, mert *pontosan kidolgozott fogalmi rendszer nélkül a jogszabályalkotást nem szabad elkezdeni*. Az említett vizsgálati rendszerből hazánkban eddig egy keretjellegű elektronikus információbiztonsági törvénytervezet megfogalmazása történt meg. Ez a katonai képességek megfogalmazása területén egyrészt a nemzeti szabályozási folyamatok követésének és szükség szerinti támogatásának fontosságát jelzi, másrészt meghatározza azt a szakmai követelményt is, hogy a katonai képességek megfogalmazása a szabványok, bevált gyakorlat alkalmazásának vonalán haladjon (remélve, hogy a folyamatban lévő nemzeti szabályozás is ebben az irányban fog haladni).

ÖSSZEGZÉS

A kibertérben lévő szolgáltatások, események és incidensek összetett szempontok szerint meghatározható kiberbiztonságot eredményeznek. A szervezeti feladatok sokszínűsége, a szolgáltatások változásai nem teszik lehetővé, hogy a fenyegetések, sebezhetőségek hosszabb távra érvényes biztonsági szinten legyenek kezelhetők.

A változó kibervilágot fenyegetések területén egyre komplexebb és súlyosabb kihívások érik, miközben a védelemre fordított erőforrások csökkennek. Emiatt a kibervédelem területén *kiemelt jelentősége van a szolgáltatások, hálózati erőforrások, hozzáférésre feljogosítottak minimalizálására és szervezeti működéshez igazítására, a kritikus infrastruktúra és kritikus információs infrastruktúra pontos kijelölésére*.

A szolgáltatások, információs vagyontárgyak azonosítása mellett *létfontosságú a fenyegetések és sebezhetőségek azonosítása* (nem lehet minden ellen védekezni), az eseményekből a biztonsági incidensek helyes kiválasztása (nem minden eset kibertámadás), és a célkitűzéseknek megfelelő eljárások kialakítása, bevezetése és folyamatos felülvizsgálata.

A Magyar Honvédség szervezeteinek működéséhez szükséges kiberbiztonság megteremtése az erőforrásokhoz kötött, *folyamatban elképzelhető feladatrendszer.* A vázolt katonai elektronikus adatkezelő környezet meglehetősen összetett és változó, esetenként még a hálózat szempontjából „kívül" és „belül" megközelítések is értelmezést igényelnek, ami a terminológiai kérdések mellett kiemeli a *szolgáltatások szervezésének, biztosításának fontosságát*, illetve aláhúzza a *magas szintű felhasználói tudatosság szükségességét*.

A bemutatott fenyegetések és sebezhetőségek jó része a katonai elektronikus adatkezelő képességek esetében is értelmezhető, így igazolható, hogy a katonai képességek kialakításához létfontosságú a *nemzetközi trendek, folyamatok ismerete*, a *szabványok és bevált gyakorlat alapú tudás alkalmazása* és specializálása a hadműveleti és alkalmazói követelmények kiszolgálása érdekében.

A vázolt megoldás szerint csoportosított biztonsági célkitűzések mutatják, hogy a színesnek mondható sebezhetőségi területek miatt *a védelem kialakítása és fenntartása erőforrásokat igénylő, bonyolult, katonai műveletektől erősen függő cél és feladatrendszer*.

Felhasznált irodalom

[1.] Cyber Security Strategy for Germany, 2011, p. 9; http://www.cio.bund.de/SharedDocs/Publikationen/DE/StrategischeThemen/css_engl_download.pdf?__blob=publicationFile

[2.] ITU National Cybersecurity Strategy Guide, 2011, 2. 4. 1. p; http://www.itu.int/ITUD/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

[3.] ISO/IEC 27005: 2011, Information technology — Security techniques — Information security risk management, C melléklet p. 43- 44. feny.

[4.] Global Risks 2011, World Economic Forum, 2012, Cyber security, p. 36. http://reports.weforum.org/global-risks-2011/

[5.] ITU X 1205. (2008) Overview of Cybersecurity 7. 3. p.

[6.] ITU Security in Telecommunications and Information Technology, 2009, p. 9; http://www.itu.int/pub/T-HDB-SEC.04-2009

[7.] ITU National Cybersecurity Strategy Guide, 2011, 2. 4. 3. p.

[8.] ISACA: 2012 IT Risk/Reward Barometer: Europe, p. 1-2; www.isaca.org/risk-reward-barometer

[9.] Annual Incident Reports 2011, ENISA, 2012 p. p. 8, 12, 15; http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011

[10.] A Secure Europe in a Better World, European Security Strategy, 2003, „The global challenges" fejezet; http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

[11.] Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation, 2010, 12. p; http://www.nato.int/cps/ en/natolive/ official_texts_68580.htm

[12.] 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, 31. p.)

[13.] Információbiztonsági helyzetkép 2011, ISACA Budapest Chapter, p. 12, http://www.kpmg.com/HU/hu/IssuesAndInsights/ArticlesPublications/Documents/Informaciobiztonsagi-helyzetkep-2011.pdf
[14.] PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ 2012. III. negyedéves jelentés, p. 9; http://www.cert-hungary.hu/sites/default/files/news/cert_2012_quart_3.pdf
[15.] ISO/IEC 27005: 2011, Information technology — Security techniques — Information security risk management, C melléklet p. 42- 43.
[16.] ISO/IEC 27005: 2011, Information technology — Security techniques — Information security risk management, D melléklet p. 45- 48.
[17.] ISO/IEC 27005: 2011, Information technology — Security techniques — Information security risk management, B melléklet p. 33.
[18.] BSI Standard 100-4, Business Continuity Management, v 1.0, 2009, p. 18; https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile
[19.] Haig Zsolt - Hajnal Béla - Kovács László - Muha Lajos - Sík Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana; ENO Advisory Kft. 2009; (p. 74, 76, 151-152 és 182-183; http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf
[20.] Haig Zsolt – Kovács László: kritikus infrastruktúrák és kritikus információs infrastruktúrák (tanulmány), NKE, 2012; p. 100. http://kovacsx.hu/download/doktorikepzes/KOVASZ_KII_Tanulmany_FINAL.pdf
[21.] Nagyné Takács Veronika: A nemzeti kritikus infrastruktúrák védelmének szabályozási és szervezési kérdései, Hadmérnök, VII. Évfolyam 1. szám - 2012. március; p. 183. http://hadmernok.hu/2012_1_takacs.pdf
[22.] 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról, 2. melléklet
[23.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 59. § (1)
[24.] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről, 68.§. (4-5.)
[25.] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról
[26.] ISO/IEC 27 035: 2011Information technology — Security techniques — Information security incident management, p. 23.