Várhegyi István

INFORMÁCIÓS KÖRNYEZETVÉDELEM, INFORMÁCIÓS KATASZTRÓFA

AZ INFORMÁCIÓS KÖRNYEZET FOGALMA, HELYE ÉS SZEREPE AZ INFORMÁCIÓS TÁRSADALOMBAN

A jelen előadásban a konferencia tisztelt hallgatói számos új és még nemigen ismert fogalmakról fognak hallani. Az információs környezet védelme NATO-szövetségi és magyar össznemzeti társadalmi, politikai, gazdasági, biztonsági és védelmi feladat, amelyben mindenkinek meg van a maga helye és szerepe, valamint személyre szóló feladata. Terjedelmi okoknál fogva a témának csak a lényeges kérdéseire tudtunk összpontosítani. Célunk a figyelemfelkeltés és a továbbgondolkodás beindításának elérése volt. Az anyag korlátozott terjedelme ellenére meggyőződésünk, hogy az elhangzottak képesek betölteni a „szellemi indító töltet" szerepét témákat érintően.

Az információs környezetvédelem új fogalom, nemzetbiztonságot, ország-teljesítményt, ország-védelmet és vállalati versenyképességet érintő tevékenység.

Az információs környezet fogalma

A magyar közgondolkozásban már egyre inkább elfogadottá váltak az olyan fogalmak, mint *információs forradalom, információs korszak, információs társadalom.* Ez az új társadalmi formáció világszerte kialakulóban van: az Európai Unió és Magyarország is ilyen típusú társadalom felépítésére törekszik. Az információs társadalom az innovatív tudásra épül, amelynek alapját a minőségi információk képezik. Az információs és tudásforradalom új tudományos és ipari képességeket és ezáltal új lehetőségeket teremtettek a fejlett országok számára. A tudásközpontú gazdaság jövőbeli növekedése attól függ, hogy milyen mennyiségű és minőségű új információt és ezáltal milyen fajta új tudást tudunk biztosítani a társadalom szereplőinek. A tudomány legújabb eredményeire támaszkodó új tudományos és ipari teljesítő képességek kialakítása lehetővé teszi egy fejlett társadalom számára, hogy sikeres piaci verseny folytasson, amit viszont csak hatékony innovációs folyamat segítségével lehet elérni. Az innováció nem más, mint a megnövelt teljesítő képességekre támaszkodva, az adott ország potenciális lehetőségeinek valóra váltása. Az új képességek új válaszadási lehe-

tőségeket teremtenek, ami által egy fejlett ország számára jelentős mértékben megnő a politikai és gazdasági mozgástér és a kihívásokra adható válaszlehetőségek (döntési alternatívák) száma.

Az információs társadalom információs tevékenysége egy sajátos közegben zajlik, amelyet *információs környezetnek* nevezünk. Ez a környezet részben természeti, részben pedig mesterséges (művi) eredetű és számos elemből tevődik össze. A társadalom élete intenzív információcserére épül, amely információs környezet nélkül elképzelhetetlen. Az információs társadalomnak fejlett információs környezete van, amely lehetővé teszi, hogy a társadalom működéséhez szükséges információkat rövid idő alatt: *megszerezzék, előállítsák, értékét növeljék, biztonságát fokozzák és óvják, gyorsan szállítsák és az érintettek számára terítsék*, mely tevékenységek az információs környezet *információs infrastruktúrájának* igénybevételével történik.

Mivel az információs környezet a társadalom számára nélkülözhetetlen, fejlesztése és védelme alapvetően fontos társadalmi feladat, amelyben valamennyi szektornak megvan a sajátos feladata. Az információs környezet védelmében az állami, vállalati (állami + magán), a civil (NGO nonprofit) közösségi, nemzetbiztonsági, közbiztonsági, honvédelmi, gazdasági szférának és a társadalom minden egyes polgárának meghatározott — eddig még kevésbé hangsúlyozott — feladata van, amelynek tudatosítása mindenki számára fontos. Ezek a feladatok az információs társadalmat érintő globális, regionális, körzeti, helyi és perszonális kihívások és veszélyek formájában jelentkeznek, amelyek többsége az információs környezet zavartalan működése ellen irányul.

Az információs környezet összetevői

Az információs környezet számos elemből áll, a gyakorlati életben azonban közöttük rendszerint csak a következő fontosabb összetevőket sorolják fel:

— *Információs humán erőforrások,* amely a társadalom informatikailag képzett polgárait jelenti, alkalmazói, szoftver és hardver fejlesztői, gyártói, karbantartói és rendszergazda minőségű szakképzettséggel. Az informatikailag professzionálisan képzett szakembergárda az ország *„informatikai aranytartalékát”* képezi. Kulcsszerepet betöltő személyeit az információs környezet kritikus humán erőforrásai közé kell sorolni, gondoskodni kell nyilvántartásba vételükről. — mint ahogy a kiemelkedően fontos orvosoknál szokás —, és szükséghelyzetben riasztani kell őket. Ezek a szakemberek képezik az *információs környezetvédelem polgári tagozatának informatikus elitrétegét*. Gondoljunk csak a rendszergazdákra, a szoftver és hardver karbantartó technikusokra, a szoftverfejlesztő mérnökökre, akik nélkül minden informatikai rendszer gyorsan összeomolna;

— Informatikai erőforrások fogalma alatt azokat a szoftver rendszereket, számítógépes hálózatokat, adatbankokat kell érteni, amelyek lehetővé teszik az információs társadalom és az elektronikusat jelentő e-jelzővel ellátott — hálózatba kötött, „on-line" — e-gazdaság, e-állam és e-közigazgatás, e-bankrendszer, e-üzleti élet, e-kereskedelem, e-vámrendszer, e-közbiztonság, e-hadsereg, e-légi irányítás, e-időjárás jelentő szolgálat stb. folyamatos és megbízható működését;
— *Információs infrastruktúrák* fogalma alatt egyrészt azokat a távközlési (kommunikációs) rendszereket kell érteni, amelyek lehetővé teszik az információk továbbítását (Ilyen rendszerek pl. a *föld felszíni* rádiós és rádiórelés rendszerek, a cellarádiós rendszerek, a *földalatti* fémes és optikai kábelhálózatok, a *vízalatti* kábelrendszerek, a *űrtávközlési* műholdak, másrészt azok a rádiótechnikai rendszerek, amelyek biztosítják a távirányítást, távellenőrzést (lokátorrendszerek), a légiforgalom és hajónavigációs rendszerek, autópálya szolgálatok, a vasút, az időjárásjelentő szolgálatok stb. folyamatos működését. Továbbá azokat az elektronikus tömegtájékoztató rendszereket (TV, rádiók), amelyek az informálás és informálódás területén a lakosság mindennapi életéhez szorosan hozzátartoznak.
— *Információs támogató és ellátó szolgáltatások* fogalma alatt azokat a szolgáltatásokat, gyárakat, üzemeket kutató és fejlesztő intézményeket, egyetemeket, nagybani elosztó raktárakat kell érteni, amelyek az információs környezett fenti három elemének zavartalan tevékenységét közvetlenül vagy közvetve biztosítják. A szolgáltatások közül kiemelkedően fontos szerepet töltenek be a villamos energetikai rendszer erőművei, transzformáló alállomásai és vezetékes hálózatai, mivel köztudott, hogy egy fejlett információs társadalomban és e-gazdaságban minden árammal működik.

Az információs környezet fenti rendszereinél olyan kulcsfontosságú szerepet betöltő elemek találhatók, amelyek nemzetgazdasági, nemzetbiztonsági, közbiztonsági és honvédelmi fontosságánál fogva az ország biztonságát közvetlenül érintik, ezért az ilyen elemeket joggal sorolják az ország működéséhez feltétlenül szükséges *kritikus információs erőforrásokhoz, kritikus információs infrastruktúrákhoz és kritikus információs szolgáltatásokhoz*. Ezek védelméről országos, körzeti (régiós) és helyi szinten egyaránt gondoskodni kell. Az ország területén található és a NATO szövetségi rendszerhez tartozó kritikus információs környezeti infrastruktúrák védelméről a magyar államnak (rendőrségnek, honvédségnek, nemzetőrségnek) kell gondoskodnia. Amikor országvédelemről beszélünk össznemzeti védelmi erőfeszítésekre kell gondolni, amely nagyobbrészt polgári elemekből, kisebb részt közbiztonsági és honvédségi elemekből épül fel. Ezért nem lehet csodálkozni azon, hogy az országos és országrégiós

vállalatok, sőt a helyi vállalatok információs kapacitását — fontos tartalék kapacitásként — számításba veszik, amikor az ország védelmi tervét előkészítik. A magánszektor egyes fontos információs infrastruktúrális központjait az *országos kritikus információs infrastruktúrák* közé sorolják és védelméről a vállalattal közösen gondoskodnak.

AZ INFORMÁCIÓS KÖRNYEZETET FENYEGETŐ FONTOSABB VESZÉLYEK

Nyilvánvaló, hogy az információs környezetet fenyegető valamennyi veszély felsorolására terjedelmi okoknál fogva nem vállalkozhatunk. Az információs környezetet fenyegető veszélyeket sokféleképpen lehet osztályozni. Rendszerint a következő veszélyforrásokat említik: információs és informatikai támadó képességből, információs terrorizmusból, számítógépes bűnözésből, különböző fajtájú katasztrófákból (természeti és ipari katasztrófákból), valamint a kezelői állomány hibáiból eredő fenyegetések és veszélyek. Az *információs fenyegetések* fogalma alatt azt kell érteni, hogy a versenytársaknál, ellenfeleknél, ellenségeknél kifejlesztenek vagy megszereznek (a nemzetközi piacon megvásárolnak) olyan információs és informatikai képességeket, amelyek *információs kihívások* formájában jelentkezhetnek. (Lásd az iraki légvédelmi rendszer vezetésének földalatti optikai kábelekkel történő korszerűsítését kínai szakértők segítségével). Ezek megválaszolására kellő odafigyeléssel és megfelelő anyagi áldozattal még fel lehet készülni. Az *információs veszélyek* a versenytársak, ellenfelek, ellenségek rosszindulata, rossz szándéka, az érdekérvényesítésben megnyilvánuló agressziós hajlama, továbbá a kialakított *információs és informatikai támadó képesség* kombinációjából alakulhat ki, melynek sikeres realizálása esetén komoly vesztességek és/vagy károk érhetik az információs környezetet.

Az információs környezetet fenyegető fontosabb veszélyek megnyilvánulási formái:

— *Információs hadviselési támadás az információs környezet ellen.* Az információs társadalom kialakulásával párhuzamosan egyre jobban növekszik az ilyen fajtájú támadás veszélye. Napjaink egyik komoly potenciális kihívása a „műholdas Pearl Harbournak" elnevezett és tartalmában a nyugati világ műholdas felderítő, navigációs és távközlési rendszereinek támadását és összeomlását célzó globális veszély növekedése. A világ fejlett hadseregei és az aszimmetrikus fejlesztésre képes egyéb haderői komolyan készülnek az információs környezet védelmére, mivel stratégiájukban ilyenfajta támadásokat, már reálisan számításba vesznek. (Lásd az amerikai össznemzeti Shriever—2001. fedőnevű hadászati mű-

holdas gyakorlat feltevését és tanulmányi kérdéseit). A Jugoszlávia elleni NATO légi hadjárat, amely számos információs célpont ellen is irányult, 10 évre vetette vissza Jugoszlávia általános és információs kapacitását. Grafitszálas és/vagy grafitporos bombák alkalmazásával egy ország elektromos hálózata teljesen megbénítható. Megelőző és/vagy lefejező információs támadással egy fejlett ország teljes e-gazdasága „leültethető", ami által elveszti tartós támadó képességét. Ilyen támadások következtében a célország térdre kényszeríthető, kialakulhat a teljes digitális összeomlás állapota: *megszűnik a ballisztikus rakétavédelem, a haderő mozgásképtelenné válik: nincs többé utánpótlás, leáll a közlekedés, szállítás, ipari termelés, bankrendszer, megszűnik a víz-, gáz-, olaj-, benzin-, elektromos és élelmiszerellátás, a kórházak nem képesek működni*. Bekövetkezik a káosz állapota.

— A korlátozott célú *információs agressziót* gyakran *információs gerillatámadásnak* álcázzák a válaszcsapás elkerülése céljából. Nehéz megállapítani, hogy a 2000 évi „I love You" globális kihatású vírus csak hacker csínytevés, vagy egy jövőbeli globális vírustámadásnak bizonyos hatalmak által „megrendelt" főpróbája volt. Az *információs környezetszennyezés* az információs támadáson belül a lélektani hadviselési hatókörébe tartozó „lágy" vagy „kemény" támadási forma, amely a lakosság különböző célcsoportjait és az általános kultúra vagy a biztonságkultúra meghatározott területeit érintheti.
— *Információs terrorizmus*. Az információs terrorizmust szervezett gerilla csoportok információs támadásra kiképzett *információs gerillái* hajtják végre meghatározott célpontok ellen az információs környezetben. Ilyen támadásokra már rendszerint igénybe veszik az Internet-világhálót és a számítógépes vírus hadviselés különböző módszereit. Az információs terrorizmus keretében egyes „magányos" infogerillák információs túszejtést is végrehajthatnak (pl. az információs hálózatok feletti ellenőrzés átvételével) különböző politikai követeléseik teljesítése érdekében.
— *Számítógépes bűnözés*. Az információs társadalom növekvő kibontakozásával fokozódik az informatikai rendszerek elleni támadások veszélye és gyakorisága, mivel ezáltal pénzhez és befolyásra lehet szert tenni a „fehérgalléros" bűnözők világában. Az internetes világhálót előszeretettel használják ilyen célokra.
— *Pusztító katasztrófák.* Az információs környezet elemeit pusztító katasztrófákat két nagy csoportra lehet felosztani, úm. *természeti katasztrófákra* (földrengés, tűzhányó kitörés, árvíz, vízbetörés, tűzvész, szélvihar stb.) és *ipari eredetű katasztrófákra.* Ez utóbbiak közül különösen nagy károkat tudnak okozni az elektromos energiatermelő és ellátó rendszerben, vagy a gyártó kapacitásokban. (Lásd a 70-es évek New York-i nagy

áramkimaradását, vagy a Japán kobei földrengés által elpusztított számítógépgyár esetét). A gondatlan piaci verseny is okozhat komoly áramkimaradásokat. (Lásd a 2001 évi kaliforniai elektromos ellátórendszer összeomlását az ellátó vállalatok közötti árháború miatt).

— *Műszaki üzemzavarok.* Ezek különböző súlyosságú és időtartamú információs rendszerkiesést idézhetnek elő. Elhárításukra felkészült szakember gárda szükséges. Ilyen esetekben rendkívül nagy jelentősége van a humán professzionális informatikai és távközlési szakember tartalékoknak. Az üzemzavarok által okozott kiesések kárait jelentősen csökkenthetik az igénybe vehető tartalékrendszerek, vagy segítségnyújtásra képes kapacitások megléte.
— *Humán eredetű veszélyek.* Az ilyen veszélyek az alkalmazottak képzetlenségéből, hanyagságából, az előírások megszegéséből, szélsőséges esetekben sértődöttségéből, vagy bosszújából származnak. Az informatikai rendszerekhez való illetéktelen hozzáférés lehetősége részben a rendszerek védelmének gyengeségéből, jelentős részben azonban az alkalmazottak „figyelmetlenségéből" származik. Háborús helyzetben humán oldali veszélyek esetén gyakran *„információs és informatikai hazaárulásról"* lehet beszélni.

Mit kell érteni az információs katasztrófa fogalma alatt?

A katasztrófa fogalmát a Hadtudományi Lexikon a következőképpen határozza meg: „Az életet, az életfeltételeket, az anyagi javakat, a természeti (*és a mesterséges)* környezetet jelentős mértékben és súlyosan károsító v. veszélyeztető, többnyire váratlan elemi csapás, természeti, ipari, civilizációs rendkívüli esemény, szerencsétlenség, amely nagy területeket, nagy tömegeket érint, és amelyek károsító hatása elleni védekezés az állami, az önkormányzati szervek, magán és jogi személyek *(vállalatok)* és egyéb *(civil)* szervezetek összehangolt együttműködését, és szükség esetén rendkívüli intézkedések megtételét igényli."

Az *információs katasztrófa,* az általános katasztrófakategória sajátos fajtája, olyan rendkívüli esemény, amely az információs környezetben következik be és idéz elő különböző méretű pusztító károkat. Méreteit tekintve az információs katasztrófa globális, regionális, országos, körzeti (országregiós), helyi és egyes személyeket érintő lehet. A globális és regionális, valamint az országos kiterjedésű információs katasztrófa elhárításában és következményeinek felszámolásában az ENSZ, EU, NATO és az érintett ország illetékes szervei vesznek részt. (Lásd az évezred váltásával kapcsolatos Y2K problémákat). A nagyobb méretű információs környezeti katasztrófa komoly kieséseket válthat ki a globális és regionális e-gazdaság működésében. (Lásd: New York-i áram kimaradást, a 2001 év eleji kaliforniai áramhiányt, az egyik nagy teljesítményű amerikai polgári műhold 72 órás üzemzavarát, a brit Skynet-műholdat ért hackertámadás hatását, az „I love You" és a „Melissa" kódnevű vírustámadásokat stb.)

A nagy kiterjedésű információs katasztrófa hatását a környezet- szennyezésből ismert Föld körüli ózon-pajzson vékonyodásához, illetve az „ózonlyuk hatás kialakulásához" lehet hasonlítani, amikor is az *„információs és informatikai védőpajzson"* nagy kiterjedésű ún. *„információs lyuk"* keletkezik, aminek következtében „*információs és tájékoztatási hiány*" lép fel. Ennek káros voltát nem lehet eléggé hangsúlyozni. Az információ ellátásban nem lehet megengedni ilyen hiány (lyuk) tartós kialakulását, illetve kialakulása esetén gyorsan be kell foltozni az információs lyukat, mivel az információellátásban sincs légüres tér. Ha nem a mi információink vannak jelen, akkor nem kívánatos információk terjedhetnek el, amelyek károsan befolyásolhatják az ország információellátásának szilárdságát. Ilyenkor van nagy jelentősége a nyilvántartásba vett információs rendszertartalékok felhasználásának.

A szándékosan előidézett információs katasztrófa — különböző szintű — információs, informatikai és tájékoztatási rendszeri összeomláshoz vezethet. (Lásd a „Digitális Pearl Harbour" és a „Műholdas Pearl Harbour" elnevezésű információs környezetvédelmi veszélyfogalmak megjelenését).

Megvédhető-e az információs környezet?

Erre a kérdésre egyértelműen igennel lehet válaszolni, ha az érintett országban erre megvan a politikai szándék, akarat és pénz, ha az e-tudomány, e-gazdaság és az e-védelmi rendszerek felkészültek és kellő gyakorlással képesek a védelemre. Az információs környezetvédelem közös érdek, „egy e-hajóban evezünk". Mit kell elsősorban megvédeni az információs környezetben?

- az adatokat, a döntéshez szükséges információkat (információbiztonsági problémák), az állami és üzleti titkokat (okmánybiztonsági problémák);
- a számítógépes rendszereket, hálózatokat, szoftvereket, hardvereket;
- a számítógép hálózatok működését lehetővé tevő távközlési rendszereket;
- a tájékoztató (TV, rádió) rendszereket;
- a támogató és háttérintézményeket, mindenek előtt az elektromos energiaellátó rendszereket;
- az informatikai rendszereket professzionálisan működtetni képes humán erőforrást.

Az információs környezetvédelem főbb feladatai

Az információs környezetvédelem főbb feladata az információs katasztrófa elhárítására való felkészülés, amely a következőket foglalja magában:

- MEGELŐZÉS, FELKÉSZÜLÉS, FEJLESZTÉS. Tartalma: információs rendszerek és eszközök felmérése, információs, informatikai tartalékképzés megszervezése, körültekintő rendszerfejlesztés;

— ELHÁRÍTÁS ELŐKÉSZÍTÉSE ÉS MŰKÖDTETÉSE. Tartalma: aktív és passzív humán-, infrastruktúrális-, információs, adat- és okmányvédelem. (Megbízható információ-biztonság, információ- és okmánykezelés, -tárolás, -hozzáférés és átvitelbiztosítás);
— RIASZTÁS. Tartalma: működési zavar-, üzemi kiesés-, katasztrófajelzés, első kárfelmérés. Az *információs védelmi pajzson*, illetve az *információs lyukon* keletkezett károk és vesztességek területi nagyságának és következményeinek gyors megállapítása, a várható károk előzetes becslése, az ideiglenes helyreállításhoz szükséges erők mozgósítása, és az eszközök megállapítása;
— GYORSELHÁRÍTÁS. Tartalma**:** az információs környezet infrastruktúrájában és az információs védelmi pajzson — az információs katasztrófa következtében keletkezett — információs lyuk gyors felszámolása az információs környezeti tartalékok igénybevételével;
— TARTÓS HELYREÁLLÍTÁS. Tartalma: az információs katasztrófa következményeinek tartós felszámolása. Tapasztalatok összegyűjtése, értékelése, értelmezése, tanulságok levonása, tervek készítése a jövőre;
— GYAKORLÁS. Tartalma: Az érintett szervezetek és információs környezeti katasztrófák hatásainak kivédésére rendelt virtuális törzsek rendszeres gyakoroltatása. Együttműködés nemzetközi, szövetségi hasonló feladatú szervezetekkel. Az elméleti és gyakorlati kutatások folytatása. Javaslatok kidolgozása az ilyen fajta katasztrófák elhárítására.

Nyitott kérdések

— Kinek az érdeke az információs környezetvédelem?
— Milyen hatóságokra, intézményekre, szervezetekre (állami, államigazgatási, minisztériumi, egyesületi, vállalati szereplőkre) hárul ez a feladat?
— Vannak-e vonatkozó törvények és jogi felhatalmazások?
— Mi a polgári, ipari, társadalmi szektor helye és szerepe az információs környezetvédelemben?
— Milyen kapcsolat áll fenn az általános (polgári) információs környezetvédelem, a szövetségi védelem és a honvédelem között?
— A felállításra tervezett nemzetőrség hogyan vehet részt az információs környezetvédelemben és az információs katasztrófa-elhárításban?

Nyilvánvaló, hogy az elhangzottak alapján a tisztelt hallgatóságban további kérdések merültek fel, amelyekre azonban már együtt kell keresnünk a válaszokat.

FELHASZNÁLT IRODALOM

[1] VÁRHEGYI—MAKKAY: Információs korszak, információs háború, biztonságkultúra, OMIKK kiadó, Bp., 2000.
[2] VÁRHEGYI—MAKKAY: Információs hadviselés alapjai, egyetemi jegyzet, ZMNE, 2000.
[3] PELÁEZ A.L.—KRUX M.: Social impact of robotics and advanced automation towards the year 2010, The IPTS report/EU, Oktober/2000. Page 34-39.