SIK Zoltán Nándor

A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA VÉDELME ÉS A KÖZIGAZGATÁS

A kritikus infrastruktúra védelme (KIV) a mai kor kihívása, amely a globális terrorizmus terjedésével került a figyelem fókuszába világszerte. A kritikusnak minősített infrastruktúrák azok, amelyeknek köszönhetően tud alapvetően működni egy társadalom, egy gazdaság. A védelem különösen fontos ma, az ún. negyedik generációs (4GW) vagy aszimmetrikus hadviselés korában, amikor információs hadviselési eszközökkel szinte bármely érdekcsoport tudja érdekeit érvényesíteni, nála jóval nagyobb ellenfelével – tipikusan nemzetállamokkal – szemben. Ezen támadások fő célpontjai a kritikus infrastruktúrák (KI), különösen a kritikus információs infrastruktúrák (KII). Kritikusinfrastruktúra-elemek segítségével tartja nyilván állampolgárai adatait az állam, ezek igénybevételével működik a közigazgatás (nem csak az e-közigazgatás), és ezek segítségével nyújt az állam (nem csak e-kormányzati) szolgáltatásokat. Ezek védelme tehát jórészt állami feladat, a védelem megszervezése pedig kifejezetten az. Állami feladat már csak azért is, mivel az állam maga is ezekre az infrastruktúrákra támaszkodik. Egy ilyen kritikusinfrastruktúra-elem bármilyen okból történő kiesése pedig gyakorlatilag káoszba, anarchiába tudja sodorni az adott nemzetállamot. Ezért a feladatok pontos végrehajtására, a védelem folyamatos fenntartására kell az államnak koncentrálnia

Kulcsszavak: **kritikus infrastruktúra (KI), kritikus információs infrastruktúra (KII), kritikusinfrastruktúra-védelem (KIV), kritikus információs infrastruktúra-védelem (KIIV), információs hadviselés, információs műveletek**

Tetszik, nem tetszik, a világ ma magát fejlettebbnek tartó felét igenis eluralta az infokommunikáció. Alvin Toffler, amikor híres könyvében[1], a harmadik hullám társadalmairól beszél, egyértelműsíti, hogy ez az irány minden társadalom számára. Bár lehet ezzel vitatkozni, mindenesetre tény, hogy ma „információfüggő", sőt „információfeldolgozás-függő" a világ nem elhanyagolható méretű része.

Toffler szerint az első hullám társadalmai a mezőgazdasági társadalmak voltak, a második hullám az ipari társadalmaké, a harmadik hullám pedig az információs társadalmak kora. Ezek a társadalmak azonban a mai napig egymás mellett élnek, azaz a második hullám nem felváltotta az elsőt, mint ahogyan a harmadik sem a másodikat, hanem egyszerre létezik vele. Miután az egyes társadalmak fejlettsége nem egyforma, ezért találkozunk második, sőt első hullámos társadalmakkal. Ebből pedig következik, hogy ma sem minden társadalom érzékeny egyformán az információra. A jelen dolgozatban azonban nem ezekkel, hanem a harmadik hullám társadalmaival és gazdaságaival kívánunk foglalkozni.

De mielőtt erre rátérnénk, nézzük a kérdést a technika, a technológia oldaláról. A Toffler-féle felosztásban az egyes hullámokat a technológiai fejlődés „kelti". Azaz a technika, a technológia az, amely alapvetően meghatározza egy társadalom, ezzel egyidejűleg egy gazdaság fejlettségét. Az természetesen filozófiai kérdés, hogy mit is tekintünk fejlettebbnek, mit fejletlenebbnek, és mitől fejlettebb, vagy fejletlenebb ez vagy az a társadalom. Sőt az is filozófiai kérdés, hogy a fejlődésnek makroszinten csak egy útja van-e, vagy létezhetnek egymástól teljesen eltérő fejlődési utak, és ezek a fejlődési utak mind, vagy nem mind a technikai fejlődést jelentik-e. Most azonban fogadjuk el azt, hogy a technika a fejlődést hozza, időrendben ez legalábbis így van.

A technikai fejlődésnek, mint azt a történelem folyamatosan bizonyítja, vannak előnyei, de ugyanúgy vannak hátrányai is. A gőzgép feltalálásával kezdetét vette az ipari társadalmak kialakulása, de a gépesítés, a tömegtermelés mellett egyszersmind hozott nyomort, munkanélküliséget, luddista géprombolókat, de gépesített háborúkat, fejlett hagyományos és tömegpusztító fegyvereket is.

Ugyanúgy, az információs társadalom kiépülése, amellett, hogy hihetetlenül felértékeli az információt, meggyorsítja és minőségivé teszi a termelést és a szolgáltatásokat. Egyedi szolgáltatások kialakítását teszi lehetővé, felgyorsítja a pénzforgalmat, a logisztikát, áttekinthetővé és kezelhetővé tesz óriási rendszereket, még nagyobb, sőt globális rendszerek, cégek kialakulásához és hatékony működéséhez. Ezáltal óriási pénztömegek mozgatásához, mozdíthatóságához vezet, gyakorlatilag függővé teszi a társadalmat és a gazdaságot az információtól. Függővé, mégpedig „abszolút és relatív mértékben is" függővé. Abszolút mértékben annyiban, hogy azokban a társadalmakban és gazdaságokban, ahol megjelent az információtól való függés, azaz az információ hiánya vagy megléte, időbeli rendelkezésre állása, pontossága mára létkérdéssé vált, információ nélkül mára nincs gazdaság, nincs termelés, nincs szolgáltatás, de jól szervezett társadalom sincs. Más szavakkal, ahol a társadalom és a gazdaság elindult ezen az úton, ott már nincs visszaút.

A relatív mértékben való függés pedig azt jelenti, hogy az információ értéke és az információtól való függés mellett lassan minden más eltörpül, de legalábbis az információ legalább olyan fontos, mint pl. a nyersanyagok, azaz az információtól való függésnek helye van egy társadalom, egy gazdaság erőforrásai között, az információt minden más erőforrás mellett szintén súlyozni kell, szignifikáns szerepet kell neki tulajdonítani.

Emellett az információtól függő társadalmak az összes társadalom között kivívott helyük tekintetében mára relatív előnyt élveznek (legalábbis a saját maguk által állított skálák szerint). Azaz az információ, az információtól való függés pozicionálja a társadalmakat, ha nem is proporcionális alapon (hiszen pont a függés mértéke nem mérhető jól), de mindenképpen „előrébb" tartanak ezek a társadalmak a fejlődés útján, mint az információt nem ilyen mértékben és „töménységben" felhasználók.

Ha a proporcionális összefüggésre a fejlődés mértékét illetően sincs egyértelmű bizonyíték, az információtól való függés árnyoldalait vizsgálva sem tehetünk ilyen értelmű kijelentést. Mindemellett az információtól való függés hozza magával annak árnyoldalait is, azaz az ilyen függés hiánya egyszersmind ennek a „sebezhetőségi faktornak" a hiányát is jelenti. Más szóval, ha nem is kizárólag, de elsősorban a harmadik hullám társadalmai és gazdaságai sebezhetők az információ mint erőforrás miatt. A nem kizárólagosság pedig annak tudható be, hogy végül is minden társadalom fő szervezőereje az információ, és bár annak igen intenzív felhasználása csak az információs társadalmakra jellemző, az ilyen értelemben nem információfüggő társadalmakban is káoszt, veszteséget tud okozni az általuk felhasznált információ hiánya, sérülése (ezért a proporcionalitás legalább ilyen mértékben, de mégis igaznak tűnik).

És ezen a ponton értünk el egy újfajta hadviselési formához, az információs hadviseléshez (Information Warfare – IW). Ez a hadviselési forma modern felfogását tekintve a mai kor „találmánya", habár egyes területeit már a kínai Szun Ce „A háború művészete" című, az i. e. 6. században írt munkájában is megtaláljuk. De ugyanúgy megtalálunk ma az információs hadviselés körébe tartozó formákat pl. a II. világháborúban vagy a hidegháború idején.

Az információs hadviselést mindazonáltal igen nehéz definiálni. Ezzel sokan, sokszor megpróbálkoztak, sőt másképpen definiálják a katonák és másképpen a civilek. A civil definíciókra álljon itt pár példa, amelyet a Google internetes kereső definiál, a Wikipedia internetes enciklopédia, illetve az IWS – The Information Warfare Site nevű információs hadviseléssel foglalkozó internetes oldal közöl.

2007-ben a fenti internetes oldalak a következőt írták:

„Az információs hadviselés a hadviselés egy új formája, amikor is az információ, illetve támadások az információ, illetve az információs rendszerek ellen a hadviselés eszközeivé válnak."

2008-ban ugyanott a következő definíciót lehetett megtalálni:

„Információs hadviselés (information warfare – IW): az információ vagy az információtechnológia használata krízis vagy konfliktus idején, adott ellenfelet vagy ellenfeleket érintő meghatározott célok elérésére vagy azok elősegítésére."

2009-ben pedig az alábbi definíciót találjuk, szintén ugyanott:

„Információs hadviselés: az információ használata és menedzselése egy ellenfél felett való versenyelőny megszerzése érdekében."

Mindezek mellett álljon itt a katonai doktrínák által használt két definíció is. Az alábbi definíciót a MNIOE (Multinational Information Operations Experiment)

névre keresztelt, mintegy 20 országot tömörítő, német vezetésű katonai konzorcium dolgozta ki az információs műveletek leírására. Információs műveletek – Information Operations – IO kifejezéssel illetik a katonai terminológia szerint az információs hadviselést, ami inkább polgári megfogalmazás:

> *„Az információs rendszereket – beleértve a rendszerek viselkedését és lehetőségeit – érintő, olyan katonai tevékenységekre való javaslattétel, illetve ezek koordinálása, amelyekkel a kívánt hatások elérhetők."*

Ehhez kapcsolódóan definiálja az USA védelmi minisztériuma az információs fölényt, az információs hadviseléssel elérendő célt, a következőképpen:

> *„Valamely fél saját erőinek vezetésében való relatív előnye az ellenfelekhez képest. Az információs fölény vagy dominancia elérhető a saját vezetők kiképzésével úgy, hogy azok a rendelkezésükre bocsátott, fölényt biztosító technikai információk segítségével gyors és megfelelő döntéseket tudjanak hozni, illetve annak érdekében tett erőfeszítések az ellenfél ugyanilyen képességeinek rombolására és lehetetlenné tételére, egyidejűleg a saját képességek védelmével."*

A fenti definíciók mellett mind a polgári életben[2], mind a katonai doktrínákban[3],[4] megjelenik az információs hadviselés egyfajta felosztása. Ezek taglalása helyett az információs hadviselés megértéséhez érdemes inkább egy kis kitérőt tennünk. Az információs hadviselés mai formájában való megjelenését gyakorlatilag 1991-től, az első – Sivatagi Vihar (Desert Storm) fedőnevű – öbölháborútól számítják. Az USA hadserege vetette be ezt a hadviselési formát az iraki erők ellen, amelynek eredményeként az óriási technikai fölény és a jól szervezettség sebészi pontosságú találatokat, kevés amerikai áldozatot és hatékony műveletvégrehajtást, a háború megnyerését eredményezte.

Ez azonban más oldalról azt jelentette, hogy az amerikaiak, akik birtokában voltak az információnak, egyszersmind előnyükre tudták azt kihasználni. Miért mondjuk azt mégis, hogy ők a sebezhetőek? Elemezzük ezért egy kicsit a helyzetet! Az amerikaiak az információs hadviselési eszközökkel a hagyományos (ún. kinetikus) hadviselési technikájukat támogatták, és a hagyományos értelemben vett hadviselés területén értelmezett győzelmet arattak vele (azaz a háborús jogi terminológia szerint rombolást és sérüléseket okoztak vele). Természetesen az iraki erők sem viseltek hadat információk nélkül, azonban ennek hatékonysága alulmúlta az amerikaiakét, akik előnyüket ún. információs dominanciává tudták fejleszteni (azaz huzamos ideig meg tudták tartani előnyüket). Azaz az amerikaiak képesek voltak arra, hogy a saját információikat pontosan és hatékonyan tudják felhasználni, míg az irakiakat „távol tartották" ezektől az információktól, sőt az irakiak információellátását is akadályozták, bénították (azaz mégiscsak győzelmet arattak felettük információs hadviselési értelemben is).

Az amerikaiak mégis úgy érezték, hogy igen sérülékenyek, és ezt már akkor jól érezték. Ugyanis rájöttek arra, hogy információs hadviselési eszközeikre olyan mértékben támaszkodnak a győzelem megszerzése érdekében, hogy ezek nélkül hadseregük hatékonyságát teljes mértékben elvesztené. Azaz az információs hadviselésnek már nem volt alternatívája. Más szóval, ha az ellenség pont az ő információs hadviselési technológiájukat támadná, az náluk okozna káoszt. Olyan sebezhetőséggel szembesültek tehát, amely addig nem létezett.

Az amerikai hadsereg ennek nyomán 1995-ben tesztelte azt, hogy információs hadviselési eszközökkel milyen és mekkora károkat lehetne okozni az amúgy a világ GDP-jének mintegy 40%-át előállító saját gazdaságának, társadalmának.[5] A teszt eredménye meglepő volt: eszerint mintegy négy nap alatt lehetne kvázi romba dönteni az amerikai gazdaságot annak – a későbbiekben kifejtendő – ún. kritikus infrastruktúra elemei ellen intézett információs hadviselési támadással. Ami a még meglepőbb volt, az az, hogy ehhez nincs szükség sok százmilliárd dolláros technikai fejlesztésre, azaz egy közepesen fejlett, sőt akár fejletlenebb állam is hatékonyan szembe tudna szállni az amerikai szuperhatalommal. Az amerikai hadsereg egy, az USA ellen irányuló információs hadviselési támadás valószínűségét akkor 10 éves távlatra, 2005-re tette. Nem kellett eddig várniuk, már 1999-ben érték az USA-t és Nagy-Britanniát, állítólag Oroszországból érkező támadások. Ezek közül az első, nagyobb port felvert akció az ún. Holdfénylabirintus (Moonlight Maze) fedőnevű támadássorozat volt. Egy másik, ismertté vált esetben pedig 2003-ban az USA védelmi minisztériuma és több más kormányszerv ellen nagy valószínűséggel Kínából intéztek támadásokat. Ennek, a későbbi nyomozások során az amerikaiak a Titan Rain (Titáneső) kódnevet adták.

A fentiek szerint információs hadviselési támadás végrehajtásához nem kell nagy felkészültségű ezermilliárd dolláros évi hadi költségvetésű államnak lennie a támadónak. Sőt, gyakorlatilag nem is kell államnak lennie, az ilyen támadások legtöbb fajtáját megfelelő felkészültséggel, viszonylag olcsón bármilyen érdekcsoport kivitelezni tud. Ezeknek a hadviselési formáknak ezért már új nevük is van, „állam nélküli" (stateless) vagy aszimmetrikus hadviselésnek hívják őket, mivel a szemben álló felek nem szükségszerűen nemzetál-

lamok, hanem érdekcsoportok. Természetesen lehet nemzetállam is, de pl. egy nemzetállam lehet az egyik fél, míg a másik fél lehet szervezett bűnözői csoport, terrorista csoport, ipari kémek csoportja, multinacionális vállalat, vagy akár nemzetközösség is. Különböző ismérvek alapján a katonai irodalom mindezt az ún. negyedik generációs hadviseléshez sorolja, amelynek fő jellemzői a fentieken kívül a hagyományos hadviselési formák és a hátország eltűnése, a békeidő és a háborús idő összemosódása, nincs katonai vagy polgári célpont megkülönböztetés, valamint az információs hadviselés, ezen belül is leginkább az ún. kibernetikai hadviselés (cyberwarfare).

Az információs hadviselési támadások legveszélyesebb formája az, amikor az a már fentebb említett un. kritikus infrastruktúra, vagy annak elemei ellen irányul. A kritikus infrastruktúra definíciója egyértelműbb, mint az információs hadviselésé, mégis világszerte több definíció létezik belőle. A készülőben lévő magyar szabályozás egyik alapdokumentuma, a 2080/2008 (VI. 30.) Korm. határozat[6] (Zöld Könyv) az Európai Unió kritikusinfrastruktúra-védelmi programjára (European Programme for Critical Infrastructure Protection – EPCIP), valamint az ahhoz kapcsolódó irányelv javaslatra[7] támaszkodik, amikor a következőképpen határozza meg a kritikus infrastruktúrát:

> *„Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra-elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában."*

A hivatkozott kormányhatározat a továbbiakban a következőt írja arról, hogy mi is tekintendő kritikus infrastruktúrának:

> *„Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotórészei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszú távon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére."*

Bár mind az EU programja, mind a magyar Zöld Könyv infrastruktúráról beszél, ez kissé félrevezető lehet a szó hagyományos értelmezésekor, ha nem tartjuk szem előtt a definíciót. A kritikus infrastruktúra értelmezése ugyanis nem a szigorúan vett infrastruktúrát jelenti, hanem, ahogy a fenti definíció is jelzi, az ahhoz kapcsolódó szolgáltatásokat mint alapszolgáltatásokat is. Csak az adott szolgáltatásokkal együtt érdemes beszélni arról ugyanis, hogy egy adott társadalom, gazdaság működőképessége fennmarad, vagy éppenséggel sérül. Éppen ezért az USA is hasonlóan definiálja a kritikus infrastruktúrát:

> *„Az infrastruktúrák olyan egymástól függő hálózatok és rendszerek összessége, amelyek meghatározott ipari létesítményeket, intézményeket (beleértve a szakembereket és eljárásokat, illetve elosztó képességeket) tartalmaznak. Mindezek biztosítják a termékek megbízható áramlását az Egyesült Államok védelmi és gazdasági biztonságának fenntartása, valamint a minden szinten zavartalan kormányzati munka és a társadalom egésze érdekében."*[8]

A világon bárhol, ahol a kritikus infrastruktúrák védelmével foglalkoznak, több olyan területet jelölnek ki, ahol ez értelmezhető. A már hivatkozott EPCIP mintegy tizenegy fő területet jelöl ki az energetikai ipartól a közlekedésen át az egészségügyig. A magyar Zöld Könyv is hasonlóan tesz, amikor tízféle szektorban határoz meg kritikusinfrastruktúra-elemeket.

Mindezen területek között azonban van egy, amely mindent áthat, mindegyikre hatással van, de önálló területként is megjelenik. Ez pedig az az infokommunikáció, infokommunikációs infrastruktúra, amely jelen dolgozat középpontjában áll. Az infokommunikáció kiemelt jelentőségét hangsúlyozza az is, hogy külön elnevezése is van a kritikusinfrastruktúra-védelem területén, a kritikus információs infrastruktúra (KII, vagy angolul Critical Information Infrastructure – CII).

A kritikus információs infrastruktúra védelme két szempontból is kiemelt jelentőségű minden egyes kritikusinfrastruktúra-szektor védelmének tárgyalásakor. Az egyik az, hogy ahogy jeleztük, minden más kritikusinfrastruktúra-területre hatással van. Ki tudna ugyanis elképzelni a mai információs társadalomban pl. bármilyen energetikai vagy közlekedési területet informatikai rendszerekre alapuló vezérlés nélkül? De ugyanígy a pénzügy, a kormányzat vagy a közbiztonság sem lehet meg kommunikáció és informatikai rendszerekre épülő nyilvántartások nélkül. S ha a fenti területeket kritikusként definiáljuk, akkor az azok támogatásához, működtetéséhez, felügyeletéhez használt infokommunikációs infrast-

ruktúrának is értelemszerűen a kritikus tartományba kell esnie. Ez tehát az egyik szempont, ami kiemeli a többi közül a kritikus információs infrastruktúrákat.

A másik szempont, amiért a kritikus információs infrastruktúrák kiemelten kezelendők, az az, hogy elsősorban ezek a célpontjai az információs hadviselési támadásoknak. Azoknak a támadásoknak tehát, amelyek viszonylag könnyen és olcsón igen nagy károkat tudnak okozni, veszélyeztetve egy társadalom, egy kultúra fennmaradását, egy gazdaság működését.

Ebből a szempontból tehát a védelem megszervezésének kiemelt jelentősége van. Ezt ismerték fel a magukat fejlettnek tartó államok, államszövetségek, amikor programokat fogalmaztak meg, állami szerveket hoztak létre a kritikus infrastruktúra, ezen belül a kritikus információs infrastruktúra védelmére.

Ami azonban elsőre nem tűnik triviálisnak, az az, hogy a kritikus infrastruktúra védelme elsősorban állami feladat. Pedig, ha belegondolunk, alapvetően állami feladatnak kell lennie, több szempontból is. Ha a teljes kritikusinfrastruktúra-spektrumot tekintjük, nyilvánvaló, hogy már kiválasztásuk is állami feladat, hiszen az állam, a kormányzás az, amely összetartja a társadalmat, így rálátása van azon elemekre, amelyek feltétlenül szükségesek egy társadalom, egy gazdaság működtetéséhez.

Másrészt a mai, modernnek nevezett társadalmakban a kritikusinfrastruktúra-elemek többsége nem állami, hanem magánkézben (esetleg más állam kezében) van. Nyilvánvaló, hogy az egyéni érdekek mást diktálnak, mint a közérdek, aminek védelmére maga az állam is létrejött. Éppen ezért, ha egy vállalatvezetőt megkérdezünk, neki egészen biztos más érdekei lesznek vállalatával kapcsolatosan, mint ha ugyanezt a vállalatot mint kritikusinfrastruktúra-elemet tekintjük. A vállalatvezető a tulajdonosi érdekeket szolgálja, amikor a profitérdekeket helyezi előtérbe, amely nyilvánvalóan az egyéni érdekeket szolgálja. A közérdek azonban nyilván mást diktál, hiszen egy kritikusinfrastruktúra-elemet akkor is működőképesen kell tartani egy társadalom fennmaradása érdekében, ha annak működtetése veszteséges, sőt ez esetben profitérdekekről még csak szó sem eshet. Ezúton is látszik tehát az, hogy az egyéni érdekek összessége nem szükségszerűen jelenti a közérdeket, sőt ellene hat. Ezért a kritikusinfrastruktúra-védelemnek, ha nem is tejes egészében, de szervezésében, stratégiájában, szabályozásában mindenképpen állami feladatnak kell lennie.

Ha kiemelten kezeljük a kritikus információs infrastruktúrát, akkor még több érv is amellett szól, hogy ennek védelme elsősorban állami feladat. Itt ugyanis korlátozottan igaz az, hogy ezek magánkézben vannak. Ugyanis az állam saját szolgáltatásainak jó részét infokommunikációs rendszerek felhasználásával támogatja, illetve végzi. Jóformán nem található olyan államilag ellátott terület, amely ne venne igénybe infokommunikációt saját működéséhez. Természetesen ezek nem mindegyike tekintendő kritikus információs infrastruktúrának, azonban belátható, hogy az állam működésében különösen sok olyan terület van, amely kritikus és infokommunikációra támaszkodik. Például kritikus, információs infrastruktúra-elemek segítségével tartja nyilván állampolgárai adatait az állam, ezek nélkül nem lenne adófizetés, nem lenne költségvetés, nem lenne egészségügy, szociális ellátás, oktatás stb. Gyakorlatilag ezek igénybevételével működik a teljes közigazgatás, és ezek segítségével nyújt az állam szolgáltatásokat, amelyek közül egyre több szolgáltatás már közvetlenül is elektronikus formában vehető igénybe az állampolgárok által, mint e-kormányzati szolgáltatás. Ha pedig nincsenek állami szolgáltatások, akkor a társadalom szétesik, a gazdaság működőképessége megbénul, végső soron a kultúra megsemmisül. Az állam maga is ezekre az infrastruktúrákra támaszkodik, egy ilyen kritikusinfrastruktúra-elem bármilyen okból történő kiesése gyakorlatilag káoszba, anarchiába tudja sodorni az adott nemzetállamot.

A kritikus infrastruktúra, ezen belül a kritikus információs infrastruktúra védelme tehát jórészt állami – nemcsak központi közigazgatási, hanem önkormányzati hatáskörbe is tartozó – feladat, a védelem megszervezése pedig kifejezetten az. Nyilvánvalóan nem várható az államtól, hogy minden egyes kritikusinfrastruktúra- elemet saját forrásból finanszírozottan védjen (ne feledjük el, hogy mindig védeni kell ezen elemeket, nincs külön békeidő és háborús idő).

Azonban elvárhatók az államtól a következők:

– Elvárható az államtól, hogy vezesse a védelmet és kidolgozza a védelem stratégiáját. Ezt Magyarországon az előző kormányzati ciklus alatt tradicionális okokból az akkori Nemzeti Gazdasági és Fejlesztési Minisztérium (NFGM) vezetésével végezték az EU-előírásoknak megfelelően, habár inkább helye lett volna a Közlekedési, Hírközlési és Energiaügyi Minisztériumban (KHEM), mivel ez utóbbihoz tartozik az infrastruktúra nagyobb része. A jelen kormányzati ciklusban a védelempolitika pedig a minisztériumok átalakítása folytán a Nemzetgazdasági Minisztériumnál (NGM) maradt, bár a területtel ma az infrastruktúráért is felelős Nemzeti Fejlesztési Minisztérium (NFM), valamint a Bel-

ügyminisztérium (BM), azon belül is az Országos Katasztrófavédelmi Főigazgatóság (OKF) is foglalkozik. Mindemellett több más szervnek is feladata van ezzel kapcsolatban, többek között a Kormányzati Koordinációs Bizottságnak (KKB) is. A védelemszervezés már csak azért is az állam feladata, mivel amellett, hogy az állam a fentiekben leírtak szerint a közérdeket képviseli, átlátása van arról, hogy egy-egy infrastrukturális elem kiesése milyen tovagyűrűző hatásokkal jár a társadalmat és a gazdaságot tekintve. Szintén az államnak van átlátása arról is, hogy az adott kritikusinfrastruktúra-elem milyen egyéb kritikusinfrastruktúra-elemekkel van olyan kölcsönhatásban (interdependencia), amely esetleg egy vagy több más kritikusinfrastruktúra-elem kiesését eredményezi.

– Elvárható az államtól, hogy kijelölje[9] a nemzeti kritikusinfrastruktúra- (National Critical Infrastructure – NCI) elemeket, valamint az európai kritikusinfrastruktúra (European Critical Infrastructure – ECI) elemeket (ez utóbbiba az EPCIP szerint azok tartoznak, amelyek legalább két országot érintenek), valamint ezeket a kijelöléseket folyamatosan felülvizsgálja.
– Elvárható az államtól, hogy kijelölje a feladatokat, megalkossa a megfelelő szabályozást a területen, amelyben minden adott központi kormányzati szervnek részt kell vennie (csakúgy, mint a kijelölésben). Ez a tevékenység Magyarországon még az előző kormányzati ciklusban szintén beindult[10], ennek eredménye többek között a már említett kormányhatározat is. Sajnos azonban még a kormányváltást megelőzően – egyes források szerint a válságnak is köszönhetően – alábbhagyott a lendület, más prioritások kerültek előtérbe, így a jelenlegi kormányzatnak újra kell gondolnia a további teendőket.
– Elvárható az államtól az egyes területeken szükséges anyagi finanszírozás is, természetesen az adott területen lévő kritikusinfrastruktúra-elem tulajdonosainak saját finanszírozásával együttesen. Magyarországon ezen a téren további lépések szükségesek, meg kell ugyanis határozni, hogy milyen területen, mely kijelölt elemnél, milyen időszakban, milyen típusú beruházási, illetve üzemeltetési jellegű állami, és esetlegesen EU-s finanszírozás szükséges. Ez esetben egyéb szervek mellett külön szerepe lehetne a Nemzeti Fejlesztési Ügynökségnek (NFÜ) is.
– Elvárható az államtól a közreműködés, a gazdasági és civil szereplőkkel való kooperáció, a felügyelet és az ellenőrzés. Ezeken a területeken Magyarországon még nem kiforrott az állami szerepvállalás, nem kiforrott a megfelelő intézményrendszer[11] megalkotása, átstrukturálása.
– Végül elvárható az államtól, hogy a folyamatos védelem érdekében mindig szervezze a fentieket, mint egy körfolyamatot. Ha ugyanis pl. egyfajta fenyegetettség valószínűsége megnő, azaz magasabb lesz ennek a kockázata, úgy nagy valószínűséggel adaptív módon igazítani kell hozzá a stratégiát, és minden további tevékenységet.

Reméljük, mindezen tevékenységek elindulnak, az államnak időben sikerül koncentrálnia a feladatok pontos végrehajtására, a védelem kiépítésére és folyamatos fenntartására mielőtt az első komolyabb információs hadviselési támadás az országot eléri.

Lábjegyzet

[1] Toffler, A. (2001): A harmadik hullám, Információs társadalom A-tól Z-ig sorozat 2. kötet, Budapest
[2] Libicki, M. (1995): What is Information Warfare? Center for Advanced Concepts and Technology Institute for National Strategic Studies, National Defense University
[3] Department of Defense Dictionary of Military and Associated Terms – Joint Publication (JP) 1–02., 2001
[4] Information Operations – Joint Publication (JP) 3–13, 2006
[5] Az információs hadviselés alapjai, Egyetemi jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2000
[6] Zöld Könyv a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
[7] COM(2006)786 – A Bizottság közleménye – A létfontosságú infrastruktúrák védelmére vonatkozó európai programról, Brüsszel, 2006
[8] Critical Foundations Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructures Protection; Washington, 1997
[9] COM(2006)0787 – Javaslat A Tanács irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről, Brüsszel, 2006
[10] 2080/2008 (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.
[11] Suter, M. (2007): A Generic National Framework For Critical Information Infrastructure Protection (CIIP), August