HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

Munk Sándor
Zrínyi Miklós Nemzetvédelmi Egyetem
munk.sandor@zmne.hu

KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁKHOZ KAPCSOLÓDÓ, SAJÁTOS KATONAI (VÉDELMI SZFÉRABELI) KÉPESSÉGEKET IGÉNYLŐ FELADATOK

Absztrakt

Az információs szolgáltatásokat nyújtó és más, hagyományos infrastruktúráknak is hátteréül szolgáló információs infrastruktúrák biztonságának szerepe napjainkban folyamatosan növekszik. A kritikus információs infrastruktúrák védelme a kritikus infrastruktúra védelem egyik alapvető összetevőjévé vált. Mivel a kritikus infrastruktúrák biztonsága a nemzeti biztonság egyik alapvető összetevője, a katonai, illetve védelmi szféra – saját kritikus infrastruktúrái védelmén túl – sajátos képességeire támaszkodva bővebb feladatokkal is rendelkezik. Jelen publikáció elemzi a sajátos képességek iránti igény okait és rendszerezi, meghatározza a kritikus információs infrastruktúrák védelméhez szükséges sajátos katonai (védelmi szférabeli) képességeket.

Role of the security of information infrastructures providing information services, and support for other kinds of traditional infrastructures, in our days continuously grows. Protection of critical information infrastructures became one of the basic components of critical infrastructure protection. Since security of critical infrastructures is a basic component of national security, military, and defense sphere – beyond their duties regarding protection of their own critical infrastructures – based on their special capabilities, have additional tasks, and responsibilities. This publication analyses the roots of the demands for special capabilities, and describes special military (defense) capabilities, necessary for critical information infrastructure protection.

***Kulcsszavak**: kritikus információs infrastruktúra védelem, katonai/védelmi képességek, informatikai felderítés, informatikai ellentevékenység, informatikai bűnügyi eljárások ~ critical information infrastructure protection, military/defence capabilities, cyber intelligence, cyber counteractivities, cyber forensics.*

BEVEZETÉS

A távközlés és az Internet forradalma az emberek előtt az együttműködés, az összekapcsolódás és a különböző szolgáltatások igénybevételének rendkívüli távlatait nyitotta meg. A világ társadalmai ma már egyre növekvő mértékben függnek a tágabb értelemben vett informatika eszközeitől és szolgáltatásaitól, az információs technológiáktól. Ez a növekvő függőség ok-okozati módon vonta maga után az információs szolgáltatásokat nyújtó és más, hagyományos infrastruktúráknak is hátteréül szolgáló információs infrastruktúrák biztonságának megnövekvő szerepét. A kritikus információs infrastruktúrák védelme a kritikus infrastruktúra védelem egyik alapvető összetevőjévé vált.

A kritikus infrastruktúra általános értelemben mindazon infrastruktúrák (működtető személyzet, folyamatok, rendszerek, szolgáltatások, létesítmények, és eszközök összessége), melyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létére, lét- és működési feltételeire jelentős negatív hatással jár. A kritikus információs infrastruktúra pedig információs tevékenységeket támogató rendszerek, eszközök olyan összessége, amely önmagában kritikus infrastruktúra, vagy lényeges szerepet játszik más kritikus infrastruktúrák működésében. A kritikus információs infrastruktúra fogalma értelmezhető nemzeti, védelmi, illetve regionális és szervezeti keretek között is.

A nemzeti kritikus infrastruktúrák és ezen belül a kritikus információs infrastruktúrák védelme jellemzően többszereplős feladatrendszer. Napjainkban a kritikus információs infrastruktúrák jelentős része – piacgazdaságra épülő államokban mintegy 80-90%-uk – az adott államtól teljes egészében, vagy részben független magánvállalkozások kezelésében van. Így a védelem megvalósításában egyaránt érintettek a kormányzati szervek és intézmények, az egyes infrastruktúrák tulajdonosai és üzemeltetői, sőt az informatikai ipar szereplői, bizonyos vonatkozásokban pedig még az információs szolgáltatásokat igénybevevő felhasználók is.

Bár az ezzel kapcsolatos vélemények esetenként eltérőek, véleményem szerint a fogalom alapvető elemeiből kiindulva a nemzeti kritikus információs infrastruktúrának mindenképpen részét képezi az adott állam védelmi és ezen belül katonai kritikus információs infrastruktúrája is. Ennek megfelelően a katonai, illetve a védelmi szféra szervezetei saját infrastruktúrájuk védelméhez kapcsolódóan szerepet játszanak a nemzeti kritikus információs infrastruktúrák védelmében.

Néhány megállapításra alapozva – mint azt egy korábbi publikációmban [1] már összegeztem – előzetes hipotézisként az is megfogalmazható, hogy a katonai, illetve védelmi szféra az előzőekben megfogalmazottnál bővebb feladatokkal rendelkezik, jelentősebb szerepet játszik a kritikus információs infrastruktúra védelemben. Az első megállapítás azt hangsúlyozza, hogy a kritikus infrastruktúrák biztonsága a nemzeti biztonság egyik alapvető összetevője, így megvalósításában érintett (lehet) a katonai, a rendvédelmi, a katasztrófavédelmi és nemzetbiztonsági szakterület is. A második – nemzetközi tapasztalatokra épülő – megállapítás szerint a kritikus infrastruktúrákhoz hasonló, összetett rendszerek informatikai védelmében leginkább a többnemzeti műveletekben résztvevő katonai erőknek vannak tapasztalatai. Végül a harmadik megállapítás szerint a kritikus infrastruktúrák elleni információs támadásokat végrehajtók felderítése, a támadók elleni fellépés, de legalábbis e feladatok nagyobb része és egészének koordinációja a védelmi szféra feladata.

Mindezek alapján jelen publikáció alapvető célja a kritikus – elsősorban nemzeti – információs infrastruktúrák védelme sajátos katonai, illetve más védelmi szférabeli képességeket igénylő feladatainak feltárása, elemzése. Ennek érdekében:

- elemzi a sajátos képességek iránti igények alapvető típusait;

- rendszerezi, meghatározza a kritikus információs infrastruktúrák védelméhez szükséges sajátos katonai képességeket és az ezekkel szemben támasztott követelményeket;
- rendszerezi, meghatározza a kritikus információs infrastruktúrák védelméhez szükséges sajátos más, védelmi szférabeli képességeket és az ezekkel szemben támasztott követelményeket.

SAJÁTOS KÉPESSÉGEK IRÁNTI IGÉNYEK OKAI

A **kritikus infrastruktúra védelem feladatrendszere** a szakirodalomban, a vonatkozó szabályozókban és dokumentumokban különbözőféleképpen jelenik meg. A feladatrendszer leírására általában a feladatok jellegére épülő, jellemzően a biztonságot megsértő eseményhez viszonyított időrendet is tükröző osztályozást használnak. Az egyes feladatcsoportok – a kritikus infrastruktúra védelem lényegéből következően – jelentős hasonlóságokat mutatnak a válságkezelés, szükséghelyzet-kezelés, incidens-kezelés, illetve kockázatkezelés feladatrendszereinek összetevőivel.

Egy ITU kutatási anyag [2, 1-4.o.] a kritikus információs infrastruktúra védelem lényegi feladatait a következő négy csoportba sorolja: megelőzés és korai figyelmeztetés, észlelés, reagálás és válságkezelés . Ezeket az anyag a kritikus információs infrastruktúra védelem négy "tartóoszlopának" nevezi. Az első feladatcsoport alapvető rendeltetése, hogy a védekezésben érintettek fel legyenek készülve a bekövetkező incidensekre, megkapják az időbeni figyelmeztetést a várható fenyegetésekről. A második csoport lényege az új fenyegetések minél gyorsabb felfedezése. Ebbe az új technikai fenyegetési formák mellett bele kell érteni az általános kockázati helyzet változásait is (pld. új bűnözői, vagy terrorista csoportok). A reagálás magában foglalja a működés, szolgáltatás megszakadása okainak azonosítását és megszüntetését. Az incidensre adott válasz szintén nem csak technikai, létfontosságú része lehet a támadók megbüntetése. Ebbe a csoportba tartozik az incidens elemzése és a tapasztalatok közreadása is. Végül a válságkezelés feladatcsoportba az incidens bekövetkezését követő döntéshozatali, irányítási és koordinációs feladatok tartoznak.

Az Európai Kritikus Infrastruktúra Védelmi Program a védelem feladataira vonatkozó elképzeléseket a fogalomjegyzékben körvonalazza. [3, 19-23.o.] A kritikus infrastruktúra védelem feladatai a fogalom leírásában öt csoportot alkotnak: felkészülés, védekezés, mérséklés, reagálás és helyreállítás. Külön meghatározás írja le a megelőzés, a reagálás tartalmát. A megelőzés rendeltetése a veszélyeztetésnek kitettség, a veszélyeztetés bekövetkezési valószínűsége, illetve a bekövetkezés esetén fellépő károk csökkentése. A reagálás fogalma a dokumentum szerint a biztonságot megsértő esemény rövidtávú közvetlen hatásaihoz kapcsolódik.

Az Egyesült Államok Védelmi Minisztériuma első kritikus infrastruktúra védelmi tervében [4] a tevékenységeket hat fázisba csoportosítja: elemzés és értékelés, javítás/kiküszöbölés, figyelés és tájékoztatás, mérséklés, reagálás és helyreállítás/újraszervezés. A dokumentum következő változata [5] már nem tartalmaz ilyen felsorolást, de az egyes összetevők ebben is megjelennek. A javítás/kiküszöbölés a felismert sebezhetőségek (gyengeségek, hiányosságok) megszüntetésére irányuló tevékenységeket foglalja magában. A figyelés és tájékoztatás a felderítéstől származó figyelmeztetések összegyűjtése, szintetizálása és elosztása. A mérséklés a figyelmeztetések, vagy az incidens bekövetkezése után a potenciális káros hatások csökkentésére irányuló tevékenységek összessége. A dokumentum a kritikus infrastruktúra védelmet összekapcsolja a műveletbiztonság olyan más területeivel, mint: az erők megóvása; terrorizmus elleni harc; információvédelem; műveletfolytonosság; vegyi, biológiai, radiológiai, nukleáris és nagy erejű robbanás elleni védelem.

Összességében tehát megállapítható, hogy a kritikus információs infrastruktúra védelem főbb feladatcsoportjai közé a következőket sorolhatjuk: elemzés és értékelés (fenyegetések és

sebezhetőségek); kiküszöbölés (sebezhetőségek); felkészülés és felkészítés; figyelés, észlelés és tájékoztatás; mérséklés; reagálás; és helyreállítás.

A **kritikus információs infrastruktúra védelem szereplői** széleskörű áttekintését adja a 2002 óta kétévente megjelenő Nemzetközi Kritikus Információs Infrastruktúra Védelmi Kézikönyv. A kézikönyv 2006-os kiadása [6] már 20 ország és 6 nemzetközi szervezet kritikus információs infrastruktúra védelmi politikáját és megvalósításának helyzetét összegzi. A következőkben a kézikönyv országonkénti 'Szervezeti áttekintés' pontjaiban foglaltak alapján tekintjük át röviden és rendszerezzük a védelemben érintett szereplőket.

A kézikönyvben megfogalmazott összegzés [6, Vol I. 394-398.o.] alapján megállapítható, hogy a különböző országokban a kritikus információs infrastruktúra védelem feladatai megvalósításának szervezetrendszere rendkívül heterogén, számos szervezetet, intézményt, hatóságot foglal magában. A kormányzati szereplők között vannak minisztériumok, ágazatközi szervezetek, minisztériumokon belüli szervezeti egységek (hivatalok, bizottságok) és minisztériumok alárendeltségébe tartozó szervezetek. Az érintett szereplők között szinte minden országban találkozunk a köz- és magánszféra partnerségére épülő szervezetekkel is. Az érintett szereplők körét, helyét és feladatrendszerét különböző tényezők befolyásolják: hagyományok, történelmi tapasztalatok, az erőforrások elosztása, valamint az aktuális fenyegetésekkel kapcsolatos politikai elképzelések.

A különböző országoknál a tágabb értelemben vett védelmi szféra szervezetei közül találkozhatunk katonai (honvédelmi), rendvédelmi, katasztrófavédelmi és nemzetbiztonsági szereplőkkel. Ezek köre és jelentősége alapvetően az információs infrastruktúra szerepére vonatkozó elképzelésektől függ.

A kritikus információs infrastruktúra védelemmel kapcsolatos alapvető megközelítések négy csoportba sorolhatóak. [6. Vol II. 60-62.o.] Az első szerint ez egy technikai szintű, információ-, illetve informatikai biztonsági kérdés kiemelt tekintettel az Internet-biztonságra. A második megközelítés lényege az e-gazdasághoz kapcsolódó működésfolytonossági (üzletmenet-folytonossági) szemlélet. A harmadik a rendvédelmi megközelítés, amely az informatikai bűnözés elleni tevékenységre összpontosít. Végül a negyedik a kritikus információs infrastruktúra védelmet nemzetbiztonsági megközelítésben, annak lényeges összetevőjeként szemléli.

Az első két elképzelést valló országok esetében az információs infrastruktúra alapvetően az információs társadalom, az információgazdaság, az információs szolgáltatások bázisa, így a kritikus információs infrastruktúra védelem alapvető felelősei az e-kormányzatért, valamint az informatikáért és távközlésért felelős szervezetek, illetve a katasztrófavédelmi (veszélyhelyzet-kezelési) szervezetek. Többségében ezen országok esetében is megemlítésre kerül a rendőrség, mint az informatikai bűnözés elleni harc megvalósítója, azonban ez erőteljesebben a harmadik megközelítés esetében jelenik meg. Az informatikai bűnözésnek azonban minden esetben csak egy elemét alkotják a kritikus információs infrastruktúrák elleni támadások.

A védelmi szféra szervezeteinek jelentősebb szerep azon országokban jut, amelyek megfogalmazzák az információs infrastruktúrák nemzetbiztonsági jelentőségét és ehhez kapcsolódóan reális veszélynek tartják a terrorfenyegetettséget, sőt egyes esetekben már az államilag támogatott/megvalósított információs támadásokat. Ezen országokban így kiemelt szerepet kapnak katonai szervezetek és a nemzetbiztonsági szolgálatok is.

A **sajátos – adott szereplőhöz kötött – képességek iránti igények** mögött általános értelemben több különböző indok is állhat, amelyeket jelen publikációban két nagy csoportba sorolunk. Az első csoportot azok az esetek alkotják, amelyekben a kritikus információs infrastruktúra védelemhez szükséges, vagy ahhoz nagymértékben hasonló képességek sajátos eszköz- és eljárásrendszere, valamint az ezek alkalmazására való felkészültség egy adott

szereplőhöz kapcsolódik. A második csoportba pedig azok az esetek tartoznak, amikor egy adott tevékenység végrehajtását, illetve végrehajtóját jogszabályok írják elő, korlátozzák.

A feladatvégrehajtáshoz szükséges sajátos eszköz- és eljárásrendszer, illetve alkalmazási képesség önmagában nem feltétlenül jelenti azt, hogy az ezekkel rendelkező – például katonai, vagy védelmi szférabeli – szereplő mellett ugyanilyen képesség más, új szereplőknél nem építhető ki, de ez utóbbi legalábbis az erőforrások gazdaságos felhasználása szempontjából mindenképpen megfontolásra érdemes. Egy új képesség kialakítása az állami – és benne a katonai, védelmi – szférában alapvetően központi akarat alapján történik, a civil szférában pedig a törvények határai között különböző (gazdasági, stb.) szempontok alapján szabadon. A sajátos katonai, védelmi képességek nagyobb csoportjának egy alcsoportját alkotják azok a képességek is, amelyek hasonló – esetünkben civil (állami és magán-) – képességek szükséghelyzetben történő kiegészítésére/megerősítésére, kiváltására, ideiglenes helyettesítésére irányulnak.

A jogszabályok által korlátozott ('állami monopóliumként' kezelt) tevékenységekre irányuló képességek esetében nincs mód ezek más forrásokból történő helyettesítésére, sőt ezen tevékenységek más szereplők által történő megvalósítása egyenesen illegális. Ebbe a csoportba számos – például nemzetbiztonsági, bűnüldözési, stb. – tevékenység tartozik. Az ebbe a csoportba sorolható általános feladatköröknek a kritikus információs infrastruktúrák védelme során szükséges sajátos, a tömegkommunikációban informatikai, számítógépes, vagy hálózati minősítő jelzőkkel ellátott változatai (például 'számítógépes törvényszéki szakértés) napjainkban is még csak kialakulóban vannak.

A kritikus információs infrastruktúrák védelme az információs társadalom kiépülésével, az információs szolgáltatások széleskörű elterjedésével és a tágabb értelemben vett informatika eszközrendszerének egyre kiterjedtebb alkalmazásával párhuzamosan egyre nagyobb jelentőségre tesz szert. Ezzel egyidőben fokozatosan bővülő mértékben fognak jelentkezni a különböző sajátos védelmi képességekkel szembeni igények, követelmények is. Mindez minden bizonnyal vonatkozni fog a sajátos katonai és más védelmi szférabeli képességekre is, amelynek egyes jeleivel már ma is találkozhatunk.

A következőkben sorra vesszük a kritikus információs infrastruktúra védelem főbb feladatcsoportjait és külön-külön megvizsgáljuk, hogy ezek közül melyekben van (lehet) szükség speciális katonai, illetve tágabb értelemben vett védelmi szférabeli képességekre.

SAJÁTOS VÉDELMI KÉPESSÉGEKET IGÉNYLŐ FELADATOK

Egy állam haderejének a kritikus infrastruktúra védelemmel és ezen belül a kritikus információs infrastruktúra védelemmel kapcsolatos feladatai, valamint a feladatok végrehajtásához szükséges képességek általános értelemben három nagy csoportba sorolhatóak. Az első csoportot a haderő saját kezelésében lévő kritikus (információs) infrastruktúrák védelmére irányuló feladatok alkotják. A második – az előzővel szoros kapcsolatban álló – csoportba a haderő számára közvetlenül, vagy a saját kritikus infrastruktúráján keresztül kritikus szolgáltatást nyújtó, más szereplők, szervezetek kezelésében álló infrastruktúra összetevőkkel kapcsolatos tevékenységek tartoznak. Végül a harmadik csoport az adott állam más kritikus infrastruktúrái védelmére irányuló, támogató feladatokat foglalja magában. Jelen publikációban a továbbiakban alapvetően ez utóbbi csoport feladataira összpontosítunk.

A **kritikus információs infrastruktúrákat fenyegető támadások** általános értelemben lehetnek anyagi (fizikai), információs, vagy szellemi jellegűek. Az első csoportba többek között a következőek tartoznak: fizikai behatás; elektromágneses, vagy radioaktív besugárzás; illetve anyagi (fizikai) jellemzők megfigyelése, érzékelése, lehallgatása. A második csoportba pedig azokat a fenyegetéseket sorolhatjuk, amelyek az adott rendszer által értelmezhető,

feldolgozható információt juttatnak be, vagy a rendszer által kezelt információt, megvalósított információs tevékenységet módosítanak, törölnek, vagy szereznek, figyelnek meg az adott (hagyományos információfeldolgozási, vagy informatikai) rendszer saját folyamatai, résztevékenységei útján. Végül a harmadik – a továbbiakban részletesebben nem tárgyalt – csoportot az emberi tudatban érvényesülő szellemi kölcsönhatások (pld. megtévesztő propaganda, pánik-, vagy félelemkeltés, stb.) alkotják.

A kritikus információs infrastruktúrákat érintő veszélyek csoportosíthatóak forrásaik, kiváltóik szerint is: megkülönböztethetünk tudatos szereplőkhöz köthető fenyegetéseket, valamint gondatlanságból származó és természeti, vagy ipari eredetű veszélyeztetéseket. A katonai és rendvédelmi szervezeteknek mindenekelőtt az első csoport esetében lehetnek feladatai, a megelőzés a második csoport esetében alapvetően a katasztrófavédelem feladata.

A **kritikus információs infrastruktúrák biztonságát szándékosan fenyegető szereplők**, egyben az adott állam (esetleg együttműködő államok szervezete) biztonságát is fenyegetik. Ezek között napjaink megváltozott biztonságpolitikai környezetében a hagyományos nemzetállami szereplők mellett egyre nagyobb szerephez jutnak az úgynevezett nem állami szereplők: államon belüli, az adott állammal szemben álló szereplők (pld. nemzeti, etnikai, vallási, vagy törzsi alapon szerveződő politikai-katonai szervezetek, vagy bűnszervezetek); valamint terrorista szervezetek, csoportok és nemzetközi bűnszövetkezetek. [7]

A biztonságpolitikai szereplők körében bekövetkezett változásoknál is jelentősebb a biztonsági kockázatok körének a biztonság átfogó értelmezéséhez kapcsolódó kibővülése. Az új típusú – köztük pld. információs jellegű – veszélyek, kockázatok és fenyegetések elméleti szinten számos dokumentumban megfogalmazásra kerültek, azonban az államok túlnyomó többségében teljeskörűen még ma sem érvényesül az újszerű biztonságfelfogás és nem alakult ki az ehhez kapcsolódó rendszerszemléletű felelősségi rend és cselekvési programok.

A Magyar Köztársaság esetében Szenes Zoltán megállapítása szerint is "a külső biztonság kezelése többé-kevésbé a helyén van (Külügyminisztérium, Honvédelmi Minisztérium, Miniszterelnöki Hivatal), a belső biztonság komplex értelmezése és gyakorlata kezd kialakulni (Belügyminisztérium[1]), a biztonság 'puha' aspektusai (gazdasági biztonság, információs biztonság stb.) teljesen esetlegesen jelennek meg az elméleti és gyakorlati szférában." [7]

Egy adott szervezet esetében az informatikai védelem tevékenységrendszere mintegy a szervezet 'határain belül' valósul meg. Egy szervezetnek ugyanis általában jogszerűen nincs lehetősége és többnyire nincs is megfelelő képessége közvetlen (pld. képességcsökkentést eredményező, elrettentő) ráhatást gyakorolni a fenyegetést megvalósító szereplőkre és korlátozottak a fenyegető szereplőkről történő információszerzésre irányuló lehetőségek is. Ezzel szemben a kritikus infrastruktúrák védelme egy adott állam biztonsága megőrzésének része, így megvalósítása során felhasználhatóak, sőt felhasználandóak az állam jogilag és materiálisan rendelkezésre álló képességei, lehetőségei.

Jelenleg jellemzően nincs egységesen elfogadott elgondolás az új típusú fenyegetésekhez kapcsolódó egyes feladatok különböző szervezetekhez rendelésére. **A védelmi szféra különböző szervezeteinek hagyományos rendeltetése** szerinti feladatmegosztás az információs színtéren nem minden esetben és általában csak kiegészítő értelmezésekkel, megfontolásokkal valósítható meg. Tekintsük át először kivonatosan a védelmi szféra főbb összetevői feladatainak jelenleg érvényben lévő törvényi szabályozását.

A katonai erő feladata az adott állam függetlenségének, területének, légterének, lakosságának és anyagi javainak külső támadással szembeni fegyveres védelme [8, 70.§. a)]. A rendőrség feladata a közbiztonság és a közrend védelme, valamint az államhatár őrzése, a határforgalom ellenőrzése és az államhatár rendjének fenntartása [9, 1.§. (1)]. A

[1] Napjainkban már Igazságügyi és Rendészeti Minisztérium.

nemzetbiztonsági szolgálatok feladata pedig a külföldre vonatkozó, illetve külföldi eredetű, a nemzet biztonsága érdekében hasznosítható információk megszerzése [10, 4.§ a) és 6.§ a)], valamint a Magyar Köztársaság szuverenitását, érdekeit veszélyeztető tevékenységek felderítése és elhárítása [10, 5.§ a)-d) és 7.§ a)-d)].

A katonai erő esetében a rendeltetés megfogalmazásának lényegi elemei közé a 'külső' és a 'fegyveres' jelzők tartoznak. Az előbbi értelmezése viszonylag egyértelmű, az utóbbié viszont ma már egyre kevésbé. Fegyver alatt általánosságban támadás vagy védekezés megvalósítására, vagy ezek hatásfokának, hatótávolságának megnövelésére alkalmas eszközt értünk. Átvitt értelemben minden, ami képes másban (tárgyban, élőlényben) kárt tenni, fegyvernek tekinthető. A hagyományos fegyverek mellett így jelentek meg a haderők haditechnikai arzenáljában az elektronikai hadviselés eszközei.

A kritikus infrastruktúra védelem feladatai közül a **sajátos katonai/védelmi képességek** vonatkozásában első lépésben kizárhatóak az olyan általános jellegű feladatok, mint a fenyegetések és sebezhetőségek elemzése és értékelése, a felkészülés és felkészítés, valamint a felismert sebezhetőségek megszüntetésére, illetve a szükségtelen kockázatok elkerülésére irányuló tevékenységek túlnyomó többsége.

A fennmaradó feladatok, illetve az ehhez szükséges sajátos képességek célszerűen időrendi csoportosításban vizsgálhatóak, amelynek alapvető határpontjait a kritikus információs infrastruktúrák biztonságát fenyegető esemény bekövetkezése, a veszélyeztető hatások megszüntetése/megszűnése, illetve az eredeti állapot helyreállása képezheti. A következőkben sorra vesszük az egyes időszakok fő feladatait és az ezek során felhasználható sajátos képességeket.

A **biztonságot fenyegető esemény bekövetkezése előtti időszak** fő feladata a fenyegetés bekövetkezésének megelőzése, illetve a biztonság megsértésének folyamatos figyelése, észlelése és a bekövetkezés esetén a szükséges riasztások, tájékoztatások megtétele.

A kritikus információs infrastruktúrák biztonságát tudatosan fenyegető (támadó) szereplőkhöz kapcsolódó megelőzési feladatok – más, ellenséges környezetben zajló tevékenység-rendszerekhez hasonlóan – magukban foglalják a potenciális támadók körének naprakész meghatározását; tevékenységük folyamatos figyelemmel kísérését; a fenyegetés megvalósítására irányuló képességeik csökkentését; a támadás végrehajtásától történő elrettentésüket; valamint a potenciális fenyegetéseik elleni védelmi képességek kialakítását. Ezek között az információs színtéren két nagyobb, a védelmi szférához kapcsolódó feladatcsoport azonosítható. Az első a 'passzív' felderítés/hírszerzés, a második pedig az 'aktív' ellentevékenység (zavarás, lefogás, pusztítás). Ezek részletesebb elemzésére a továbbiakban kerül majd sor.

A kritikus információs infrastruktúrák biztonságát fenyegető események figyelése és észlelése, a szükséges riasztások, tájékoztatások megtétele egy összetett szervezet- és eszközrendszer feladata, amelynek szervezeti összetevőit a különböző megnevezésű egységek (számítógépes vészhelyzeti reagáló csoport, számítógépes biztonsági esemény kezelő központ, számítógépes biztonsági esemény reagáló csoport, stb.[2]), speciális eszközrendszerét pedig többek között a különböző behatolás érzékelő és megelőző rendszerek[3] képezik. A biztonsági központok infrastruktúra összetevőkhöz, területi egységekhez köthetőek, fenntartásuk és működtetésük speciális katonai/védelmi képességeket tulajdonképpen nem igényel. Működésük folytonosságának biztosítása azonban szükségessé teheti védett – állami, katonai, vagy védelmi szféra – objektumokban történő elhelyezésüket.

A **biztonságot fenyegető esemény bekövetkezése utáni időszak** fő feladata a káros hatások érvényesülésének csökkentése, mérséklése, majd – amennyiben lehetséges – e

[2] Computer Emergency Response Team (CERT), Computer Security Incident Response Center (CSIRC), Computer Security Incident Response Team (CSIRT).

[3] Intrusion Detection/Prevention System (IDS/IDP).

hatások megszüntetése, végül az okozott károk elhárításának, a működés helyreállításának megkezdése. Az első feladatcsoport tevékenységei alapvetően a veszélyeztetett információs infrastruktúra védelmének általános és célorientált megerősítésére irányulnak, azonban a káros hatások csökkentésére, megszüntetésére mód van – az előzőekben már említett – a támadók ellen irányuló, a védelmi szférához kapcsolódó ellentevékenység segítségével is.

A kritikus információs infrastruktúrák esetében – egyes esetekben, megfelelő eszközrendszer birtokában – más szereplők mellett a védelmi szféra szervezetei, ezen belül is kiemelten az érintett katonai (híradó és informatikai) szervezetek átmenetileg képesek lehetnek a megtámadott infrastruktúrák kieső, vagy csökkentett szolgáltatásai pótlására, kiegészítésére. Erre telepítés után alapvetően a tábori híradó és informatikai rendszer erői és eszközei alkalmasak. Ennek megfelelően a kritikus információs infrastruktúrák védelmének keretében például célszerű meghatározni, hogy a Magyar Honvédségnek e célra milyen képességeket és kapacitásokat kell kialakítania és fenntartania.

A **veszélyeztető hatások megszüntetését/megszűnését követő időszak** fő feladata a kritikus információs infrastruktúrák teljeskörű működésének helyreállítása, az okozott károk következményeinek felszámolása, valamint a bekövetkezett támadás, veszélyeztetés elemzése, a biztonság fenntartásához szükséges védelmi intézkedések megtétele. E tevékenységek túlnyomó többsége első ránézésre nem igényel sajátos katonai, védelmi képességeket. Van azonban egy olyan szakterület, amelyik napjainkban általános értelemben is egyre növekvő jelentőséggel bír és ezen belül a kritikus információs infrastruktúrák védelmében is számottevő szerepet játszik.

Az előzőekben említett szakterület a bűnügyi (igazságügyi) nyomrögzítés, szakértés[4] az információs színtéren. Az igazságügyi nyomrögzítés, szakértés kezdetei a törvényszéki orvostanhoz köthetőek, amely speciális szakterületként a 19. század végén jelent meg, majd jelentős bővülés után alakult ki az igazságszolgáltatási rendszer számára érdekes kérdéseket megválaszoló tudományok rendszere[5]. Az információs színtéri szakértés, nyomrögzítés alapvető rendeltetése leegyszerűsítve az, hogy – más szakterületekkel együttműködésben – biztosítsa a jogellenes cselekedeteket elkövetők azonosítását és tevékenységük bizonyítását. A kritikus információs infrastruktúrák védelme esetében ez pedig hozzájárulhat a biztonságot szándékosan fenyegető szereplők elrettentéséhez, illetve felfedésükhöz és megbüntetésükhöz.

A következőkben sorra vesszük az előzőekben említett, katonai (védelmi) szférához köthető, speciális képességeket igénylő feladatokat, tevékenységeket.

Felderítés/hírszerzés az információs színtéren

Az információs színtérnek a kritikus információs infrastruktúrák biztonságát szándékosan fenyegető szereplőivel kapcsolatos információk megszerzése – a potenciális támadók körének naprakész meghatározása, tevékenységük figyelemmel kísérése – céljában, funkcióiban és feladataiban lényegében nem különbözik a nemzetbiztonsági szolgálatok, a katonai és a rendvédelmi szervezetek hírszerző, felderítő tevékenységétől, annak integráns részét képezi. Ebből – valamint a kapcsolódó törvényi szabályozásból – kifolyólag e tevékenység, illetve az ehhez szükséges képességek kiépítése és felhasználása szinte kizárólagosan a védelmi szféra feladata.

A kritikus információs infrastruktúrák biztonságát fenyegető szereplőkre vonatkozó információk megszerzése több szempontból is szorosan kapcsolódik a felderítés/hírszerzés 'hagyományos' területeihez. Egyrészt a potenciális veszélyt jelentő szereplők nem feltétlenül csak információs infrastruktúrákat fenyegetnek, hanem más, biztonsági szempontból lényeges célpontokat, másrészt az információs infrastruktúrákat nem feltétlenül [csak] információs támadásokkal, hanem hagyományos (pld. fizikai) módon is veszélyeztetik, így a rájuk

[4] Cyber forensics.
[5] Forensic sciences (forensics) = bírósági, bűnügyi tudományok.

vonatkozó egyes információk 'hagyományos' felderítési forrásokból, eszközökkel is – esetenként csak onnan – beszerezhetőek és ezeket más területek is felhasználhatják.

A kritikus információs infrastruktúrák védelméhez, egyben az informatikai biztonsághoz kapcsolódó felderítés/hírszerzés kialakulóban lévő speciális szakterülete az informatikai eszközökben megtalálható és az informatikai hálózatokon áramló információk megszerzése, összegyűjtése, elemzése és értékelése. E terület megnevezésére az angol nyelvű szakirodalomban különböző kifejezésekkel találkozhatunk: 'computer network exploitation', 'cyber intelligence', 'cyber surveillance'.

Az Egyesült Államok haderejében a számítógép-hálózati hadviselés[6] kifejezés az információs műveletek legújabb, ötödik területeként jelent meg [11, II-4 – II-5.o.]. A számítógép-hálózati hadviselés három összetevőjét a számítógép-hálózati támadás, a számítógép-hálózati védelem és a számítógép-hálózati felderítés képezi.[7] A **számítógép-hálózati felderítés** – szószerinti fordításban inkább számítógép-hálózati 'kihasználás' – "számítógépes hálózatok segítségével végrehajtott támogató műveletek és felderítési információszerző képességek, amelyek rendeltetése adatgyűjtés célpontot képező, vagy szembenálló felekhez tartozó informatikai rendszerekből és hálózatokból" [11, Glossary GL-6.o.] Ugyanezen kifejezés NATO értelmezése már közvetlenül nem tartalmaz a felderítésre utaló összetevőt, közelebb áll a 'kihasználás' tartalmához: "számítógép, vagy számítógép-hálózat, illetve a bennük rendelkezésre álló információk felhasználása előny megszerzése céljából" [12, 2-C-12.o.]

A számítógép-hálózati hadviselés hármas tagolása és ezen belül a számítógép-hálózati felderítés helye, szerepe tulajdonképpen az elektronikai hadviselés hármas felosztását – elektronikai ellentevékenység, elektronikai védelem és elektronikai támogató tevékenység – követi, ami egyben átvezet a rádióelektronikai felderítés szakterületéhez: "az elektronikai támogató tevékenységnek gyakorlatilag azonosak a feladatai a jelfelderítéssel (Signal Intelligence, SIGINT), de …" [13, 3.o.].

A **rádióelektronikai** (másnéven jel-) **felderítés**[8] a felderítés egyik információszerzési eljárása (módja), amely "passzív eszközökkel az elektromágneses kisugárzások gyűjtéséből, értékeléséből, analizálásából, feldolgozásából szerzi információit" [14, 37.o.]. A rádióelektronikai felderítés eljárásainak további osztályozására a szakirodalomban nem alakult ki közmegegyezés, a SIGINT technológiák köre a technológiai fejlődéssel együtt bővült, változott (kommunikációs felderítés, rádiótechnikai felderítés, stb.[9]). A NATO értelmezés szerint a rádióelektronikai felderítés a kommunikációs és rádiótechnikai felderítést összefoglaló fogalom. [12, 2-S-7.o.]

A rádió-, fax-, telex-, vagy radareszközök közötti kommunikáció lehallgatása a kommunikációs hálózatok struktúrájának, forgalmi viszonyainak, az egyes csomópontok szerepének felderítése mellett – az esetleges rejtjelfejtés után – többnyire a továbbított információk (üzenetek) megismerését is biztosította. Mindez azonban jelentősen megváltozott a számítógépek közötti csomagkapcsolt információcsere megjelenésével. Napjainkban – a 'minden IP felett' korszakában – már egyre kevésbé kerülhető meg az IP-alapú kommunikáció lehallgatása, elemzése és az ebből származó felderítési információk előállítása.

Az új felderítési információszerzési eljárás, amelynek megnevezésére egyes szakirodalmakban megjelent a '**számítógépek közötti jelfelderítés**'[10] kifejezés, még csak kialakulóban lévő technológia, azonban szerepe és jelentősége már elvitathatatlan. A

[6] Computer Network Operations (CNO).
[7] Computer Network Attack (CNA), Computer Network Defense (CND) és Computer Network Exploitation (CNE).
[8] Signals Intelligence (SIGINT).
[9] Communications Intelligence (COMINT), Electronic Intelligence (ELINT).
[10] Computer-to-computer SIGINT (C2C SIGINT).

szakterület számára "a következő időszak legfontosabb technológiai kihívása a számítógép-hálózatok felderítése, elemzése, illetve az adatforgalom lehallgatása, vagyis a C2C-SIGINT" [15, 160. o.] "A hír-szerző közösség évtizedes elutasítása után a korszerű technológiák megváltoztatják a hálózatok megfigyelésének régi megoldásait. Számos új technológia biztosítja a számítógépek között (C2C) áramló adatok elfogását, elemzését és hasznosítását ellenséges környezetben." [16, *.o.]

A számítógépek, illetve tágabb értelemben az információs tevékenységeket megvalósító informatikai eszközökre, valamint a bennük tárolt és köztük – adatok formájában – áramló információk megszerzésére irányuló **újszerű felderítési eljárások és módszerek** alapját az elsődleges adatszerzés képezi. Az informatikai eszközökben feldolgozott, tárolt információkhoz hozzá lehet jutni az eszközök, vagy adathordozóik fizikai megszerzésével; az eszközök működés közbeni elektronikus lehallgatásával; valamint rosszindulatú programok bejuttatásával. Az informatikai eszközöket összekapcsoló hálózatokon áramló információk megszerezhetőek a hálózati útvonalak fizikai megcsapolásával, vagy elektronikus lehallgatásával; valamint a hálózati kapcsolóelemekből (központok, kapcsolók, átjárók, útvonalválasztók, stb.).

A felsoroltak közül a fizikai és az elektronikus felderítési módszerek gyakorlatilag napjainkban is rendelkezésre állnak, bár a korszerű kommunikációs eljárások (pld. frekvenciaugratásos, vagy szórt spektrumú módszerek) megnehezítik a felderítést és az adatszerzést. Az újszerű megoldások közé így a rosszindulatú programokra (tulajdonképpen informatikai támadásokra) épülő, illetve a hálózati kapcsolóelemekhez kapcsolódó adatszerzés tartoznak. Az előbbivel, a 'passzív támadásokkal' más vonatkozásokban részletesebben a következő alpont foglalkozik majd, amelynek alapvető megállapításai érvényesek a kritikus információs infrastruktúrákat fenyegetők felderítésére is.

A hálózati kapcsolóelemekből történő információszerzés vizsgálatához már meg kell különböztetnünk a **belső ('hazai') és** a **külső ('külföldi') szereplők**, pontosabban az államon belüli és az azon kívüli informatikai infrastruktúrához kapcsolódó szereplők körét. Ettől függnek ugyanis az alkalmazható eljárások és módszerek és ettől függ, hogy kihez – melyik szervezethez – célszerű telepíteni az adott (felderítő) képességet.

Egy adott államon belül – megfelelő felhatalmazás birtokában – általában törvények biztosítják a nemzetbiztonsági és rendvédelmi szervek számára, hogy információkat szerezzenek be és megfigyeljék, lehallgassák a kommunikációs és/vagy informatikai hálózatokon zajló információcserét. Ez utóbbi technikai feltételeit az adott államon belül az érintett szolgáltatók (távközlési, internet, stb.) kötelesek biztosítani, így az arra felhatalmazott szervek az adott államon belül kiterjedt felderítési lehetőségekkel rendelkeznek.

Az információs színtér 'határok felettiségéből' következően a kritikus információs infrastruktúrákat fenyegető szereplők a világon szinte bárhol lehetnek, bárhonnan elérhetik, veszélyeztethetik a védendő infrastruktúrákat. Egy adott államnak a saját területén kívül két lehetősége van az információkhoz, információforgalomhoz, vagy ezek egy részéhez hozzáférni: együttműködés (uniós, szövetségi, vagy kétoldalú) révén, vagy titkos, hírszerzési információszerzési módszerekkel.

Ellentevékenység az információs színtéren

Az információs színtérnek a kritikus információs infrastruktúrák biztonságát szándékosan fenyegető szereplői ellen irányuló tevékenység rendeltetése, hogy csökkentse a fenyegetés megvalósítására irányuló képességeiket, elrettentse őket a támadás végrehajtásától. Az ellentevékenység katonai értelmezés szerint eszközök és módszerek alkalmazása az ellenséges tevékenység hatékonyságának csökkentésére [17, 129.o.]. Ennek megfelelően az ellentevékenység irányulhat a fenyegetést kiváltó szereplőre, az általa felhasznált eszközre, a védendő objektumot érő fenyegető hatásra, valamint épülhet a megtévesztésre is. Az

ellentevékenység módszereinek és eszközeinek többsége lényegét tekintve csak kevésbé, de céljaiban, esetleg mértékében különbözik a támadásoktól.

Az információs infrastruktúrák védelmét szolgáló ellentevékenység jellegét tekintve lehet adminisztratív (jogi), fizikai és információs. Az első csoportba tartozik például a joghátránnyal fenyegetés, illetve annak megvalósítása (büntető intézkedések), amelynek végrehajtói a törvényhozás, az igazságszolgáltatás és a rendvédelem szereplői. A második csoportot meghatározott feltételek fennállása esetén a fizikai megsemmisítés, pusztítás, rombolás alkotják és végrehajtói a katonai erők. A továbbiakban azonban részletesen csak a harmadik csoportba tartozó információs jellegű ellentevékenységgel foglalkozunk.

Az Egyesült Államok haderejében már a 2000-es évek elején megfogalmazódott **a számítógép-hálózati védelem aktív összetevőinek** szükségessége. Egy légierő akadémiai tanulmány aktív védelemnek azon rendszabályok összességét tartja, amelyek meghiúsítják a folyamatban lévő támadásokat, vagy a további támadásokat megnehezítik. Ezek közé sorolja, az ellentámadást, a megelőző támadást és az aktív megtévesztést[11]. Az ellentámadás a támadó informatikai rendszerei elleni számítógép-hálózati támadás az eredeti támadás során, vagy közvetlenül azt követően. A megelőző támadás a szembenálló fél (potenciális fenyegető) informatikai rendszerei elleni támadás abból a célból, hogy megakadályozza hatékony támadás indítását a saját rendszereink ellen. Végül az aktív megtévesztés a támadás eltérítése a saját rendszerekről azok virtuális helyettesítőire, ezzel abban a hitben hagyva a támadót, hogy sikerrel járt, de tevékenysége valójában semlegesítésre került. [18; 3-4.o.]

Az információs jellegű **megelőző támadás és ellentámadás** gyakorlatilag információs támadás a potenciális, vagy aktuális támadó ellen. Ennek eszköze lehet bármilyen támadó eszköz vagy módszer: a támadó fél rendszerébe bejuttatott rosszindulatú program, túlterheléses támadás, vagy megtévesztő üzenet. Mivel az ellentevékenység célja lehet a fenyegető szándékról történő lemondatás is, a megelőző, vagy ellentámadás lehet akár aszimetrikus is. Vagyis a fenyegetést közvetlenül megvalósító rendszer helyett irányulhat a fenyegetést kiváltó szereplő más rendszereire, eszközeire, vagy értékeire.

A kritikus információs infrastruktúrák védelmét, mint az adott állam biztonságának fenntartását szolgáló megelőző és ellentámadások megvalósítása funkcionális szempontból – mivel túlnyomó többségében a biztonságot kívülről fenyegető szereplők ellen irányul – a katonai erők feladata. Erre a megállapításra jut például egy 2008-ban kibocsátott tanulmány is. [19]

A **megfelelő képességgel rendelkező katonai szervezetek** kialakítása a nagyobb haderőkben már a 2000-es évek elején megkezdődött. A szakirodalomban ezek közé sorolják mindenekelőtt az Egyesült Államokat, Oroszországot és Kínát, de egy 2007-es McAfee jelentés szerint már körülbelül 120 állam használja az Internetet politikai, katonai, vagy gazdasági kémkedésre és támadásokra, épít ki informatikai támadási képességeket. [20, 12.o.]

Napjaink informatikai támadásainak egyik sajátos eszköze a rosszindulatú programok segítségével saját ellenőrzés alá vont számítógépek– akár több milliós – összessége (botnetek). Ennek megfelelően merült fel az Egyesült Államok hadseregében az informatikai megelőző és ellentámadások egyik eszközeként a **katonai botnetek** alkalmazása. A katonai botnet nem rosszindulatú programok segítségével, szándékuk ellenére felhasznált zombi gépek segítségével, hanem a végrehajtó kód saját eszközökre történő telepítésével lehetne kialakítható. A szerző elgondolása szerint bázisául felhasználhatók lennének például behatolás ellenőrző eszközök, a nem minősített hálózathoz csatlakozó számítógépek, sőt az elavulásuk miatt leváltásra kerülő eszközök is. [21]

Az informatikai megelőző és ellentámadások legnagyobb problémái közé a **'célmegjelölés'**, a **hatások célzottsága** és a **jogi kérdések** tartoznak. Számos szakmai anyag,

[11] Counterattack, preemptive attack, active deception.

publikáció foglalkozik ezekkel a kérdésekkel, amelyek között az első lényegét az képezi, hogy az információs színtéren – nagyrészt az Internet sajátosságai következtében – nem könnyen azonosítható a fenyegetést közvetlenül megvalósító informatikai rendszer, vagy eszköz és a mögötte álló szereplő. Közismert tény, hogy az azonosítás alapját képező IP cím egyrészt könnyen hamisítható[12], másrészt a fenyegetés kiváltható más, gyanútlan szereplő informatikai eszközének felügyelet alá vonásával és felhasználásával. Emellett ma már szolgáltatásként állnak rendelkezésre olyan 'anonimizáló' hálózatok, amelyek segítségével a hálózaton áramló információk (ezzel együtt műveletek) forrása visszakövethetetlenné tehető.[13]

Problémát jelent az informatikai támadások célzottsága is, ugyanis napjaink alapvetően csomagkapcsolt technológiára épülő hálózatai esetében egy adott, a fenyegetés megvalósításában résztvevő eszköz, vagy összetevő (végberendezés, hálózati csatolóelem, hálózati vonalszakasz, hálózati szegmens, stb.) támadása általában nem csak a megcélzott szereplőre, hanem számos más, vétlen szereplőre is hatással lehet.

Végül az informatikai megelőző és ellentámadások – tekintettel arra, hogy a jelenleg kialakulóban lévő gyakorlat szerint ezek a haderők feladatai között jelennek meg – jelentős jogi problémákat is felvetnek. Ezek közül az első, hogy a nemzetközi hadijog, vagy a humanitárius jog milyen módon vonatkozik az informatikai támadásokra. A kérdés megválaszolása többek között attól függ, hogy az informatikai támadások fegyveres konfliktust jelentenek-e; alkalmazásuk mennyiben okoz sebesülést, sérülést, halált, stb.; vagy hogy mennyiben különböztethetőek meg a katonai és civil célpontok. Ezt elemzi például részletesen [22] is.

További jogi problémát jelenthet a katonai erő hazai alkalmazásának viszonylag általánosan alkalmazott korlátozása, ugyanis az információs színtéren nem mindig különíthető el könnyen a hazai és a nem hazai jelleg. Ez utóbbira nincs még igazán kialakult jogi gyakorlat, vagyis hogy mi dönt: a fenyegető szereplő, a felhasznált eszközök, vagy például a közreműködő szolgáltatók honossága. Ez szintén az informatikai megelőző, vagy ellentámadások elrendelése során jelent problémát.

A bemutatott problémák könnyen belátható módon megnehezítik a védelmi célú, informatikai megelőző, vagy ellentámadások eredményes megvalósítását, sőt már a végrehajtásukkal kapcsolatos vezetői döntések meghozatalát is.

Az **aktív megtévesztés** tulajdonképpen átmeneti formának is tekinthető a támadás és a védelem között, hiszen nem közvetlen ráhatás a támadó félre és nem közvetlenül irányul a fenyegetett rendszer(ek) védelmére. Míg a passzív megtévesztés célja a valós szándékok és képességek elrejtése, addig az aktív megtévesztés nem valós szándékokat és képességeket hitet el a szembenálló féllel, beavatkozva ezzel – mintegy támadva – annak döntéshozatali folyamatait.

Az aktív megtévesztésnek a védelem passzív formáival szemben nem a támadó kizárása a célja a megvédendő rendszerből, hálózatból, hanem a támadás átirányítása egy nem valós rendszerbe, hálózatba, amely ugyanolyan, pontosabban hasonló erőforrásokkal és adatokkal van felszerelve, mint a valós rendszer. Mindez elősegíti a támadó megtévesztését céljai elérését illetően; erőforrásainak szétforgácsolását; valamint nem utolsósorban tevékenységének, alkalmazott módszereinek és eljárásainak megfigyelését. [18, 21-22.o.]

Az informatikai aktív megtévesztés alapvető eszköze a **'mézesbödön'** (honeypot), egy csapda az informatikai rendszerek elleni támadások, jogosulatlan hozzáférések detektálására, eltérítésére és bizonyos mértékben ellenrendszabályok végrehajtására. A 'mézesbödön' általában egy speciális informatikai eszköz, amelynek nincs valós felhasználói szolgáltatása.

[12] IP megtévesztés = IP address spoofing.

[13] Napjaink egyik alapvető anonimizáló hálózat (TOR, The Onion Router) kialakítását egyébként eredetileg az Egyesült Államok Haditengerészetének Kutató Intézete (US Naval Research Laboratory) támogatta.

Így normál körülmények között nem is vesz részt az információcserében: nem küld és nem vár információkat. Amennyiben ezek mégis bekövetkeznek, az a támadás, jogosulatlan hozzáférés egyértelmű jele. Egy hálózatba kapcsolódó, egymással együttműködő 'mézesbödönök' 'mézesbödön hálózatot' (honeynet) alkotnak. A 'mézesbödönök' alkalmazásának szükségességét már 2000-ben felvetette Winn Schwartau, az információs műveletek egyik élenjáró kutatója. [23]

Az aktív megtévesztés alkalmazása közel áll, szorosan kapcsolódik a behatolás ellenőrző eszközök alkalmazásához, így általános esetben részét képezheti egy adott szervezet informatikai védelmi szakemberei, szervezeti egysége feladatrendszerének. A kritikus információs infrastruktúrák esetében azonban egy nemzeti szintű aktív megtévesztési rendszer kialakítása, telepítése, összehangolt működtetése a felderítéssel és ellentevékenységgel megbízott szervezetben – a katonai erőn belül – célszerű. Mindezt indokolja, hogy a katonai műveleteknek régóta egyik összetevője a napjainkban már az információs műveletek közé sorolt megtévesztés. [11, I-1.o.; 12, 2-D-2; 24, 95-100.o.]

Bűnügyi eljárások az információs színtéren

A krimináltechnika, vagy más néven természettudományos kriminalisztika a tárgyi bizonyítékok létrejöttének, felkutatásának és rögzítésének a törvényszerűségeit valamint azokat a vizsgálati technikákat és módszereket tanulmányozza, amelyek alkalmasak a tárgyi bizonyítási eszközökön meglévő bizonyítékok feltárására és bizonyító erejük hiteles igazolására. A kontinentális krimináltechnika fogalmi megfelelője az angolszász jogrendszerekben a bűnügyi (igazságügyi) tudomány.

A **bűnügyi (igazságügyi) tudomány** (Forensic science, gyakran rövidítve forensics) a különböző tudományok széles körének alkalmazása a jogrendszer kérdéseinek megválaszolására. Más megfogalmazásban: a tárgyi bizonyítékok felkutatására, vizsgálatára, értékelésére alkalmazott tudományos ismeretanyag. [25, 41.o.] A hagyományos szakterületek közé tartozott többek között a törvényszéki orvostan, a daktiloszkópia, vagy a fegyvertan. Az új típusú bűncselekmények megjelenése és a tudományos, technikai fejlődés szükségessé és egyben lehetségessé is tette új bűnügyi szakértői, vizsgálati módszerek, szakterületek megjelenését. Az információs színtérhez, az informatikai rendszerekhez, eszközökhöz és hálózatokhoz kapcsolódóan az idők során számos fogalom megjelent.

Az **informatikai bűnügyi eljárások** összetevői időben egymást követően jelentek meg. Elsőként a számítástechnikai bűnügyi eljárások (computer forensics) jelent meg, mint a számítógépekben és a digitális adathordozókon megtalálható bűnügyi (igazságügyi) bizonyítékokhoz kapcsolódó szakterület. Egy FBI ügynök már az 1990-es évek közepén egy konferencia előadásban definiálja a 'computer forensics' fogalmát és elemzi, hogyan biztosítható a digitális információhordozóknak a hagyományos papíralapú bizonyítékokhoz hasonló elfogadhatósága. [26]

Az információtechnológia fejlődésével az információs tevékenységeket támogató különböző szakterületek (információszerzés, továbbítás, megjelenítés) eszközei egyre inkább azonos összetevőkre (processzorokra, tárakra, memória-elemekre, megjelenítő elemekre) épültek, így a szakterület a számítástechnikai jelző ellenére kiterjedt a mobiltelefonokra, digitális kamerákra, más technikai eszközökbe beágyazott informatikai részegységekre. Részben ehhez kapcsolódóan, részben ettől függetlenül találkozhatunk a 'digital forensics', vagy napjaink divatos jelzőjéhez kapcsolódóan a 'cyber forensics' kifejezéssel is.

Viszonylag önálló szakterületként jelent meg a hálózati, vagy Internet bűnügyi eljárások (network forensics, Internet forensics). A hálózati bűnügyi eljárások lényege a hálózaton továbbított adatok elfogása, rögzítése és elemzése a hálózati események azonosítása, a hálózatokon keresztül megvalósított veszélyeztetések felderítése és bizonyítása. A megvalósítás két alapvető módszere: mindent rögzíteni, majd később elemezni; vagy figyelni,

szűrni, így csak a 'gyanús' adatokat, eseményeket rögzíteni. Ez a technológia nem új, bizonyos értelemben előzményének tekinthetőek a telefonlehallgatások, az ECHELON rendszer, illetve az FBI elsősorban e-mail-ek megfigyelését szolgáló Carnivore programja. Míg a számítástechnikai bűnügyi eljárások megfogható tárgyakkal (számítógépek, technikai eszközök, adathordozók, stb.) dolgozik, addig a hálózati bűnügyi eljárások tárgya nem tartós: ha nem ismeri fel, vagy nem rögzíti, nem tud felhasználható eredményt szolgáltatni. [27]

Az előzőekben vázlatosan bemutatott módszerek és az ezeket támogató eszközök a napjainkban általánosan elfogadott értelmezés szerint mindenekelőtt a rendvédelem alkalmazási területéhez kapcsolódnak. Könnyen belátható módon szorosan kapcsolódnak a kritikus információs infrastruktúrák biztonságának megőrzéséhez is, amelyben rendvédelmi szempontból szerepük a biztonsági fenyegetések (bűncselekmények) felfedése, megelőzése, bekövetkezésük esetén pedig a cselekmények és elkövetőik azonosítása és ennek jogi erejű bizonyítása. Magyarország esetében e szakterület alkalmazásának jogosult szereplői a Nemzeti Nyomozó Iroda, valamint a szakterületen működő igazságügyi szakértők.

Az állampolgárok által birtokolt, vagy továbbított információk jogosulatlan megismerés elleni védelmét az államok többségében jogszabályok biztosítják. A különböző távközlési, informatikai és más hálózatokon áramló információkhoz történő hozzáférés jogát általában szintén törvények szabályozzák, Magyarországon pld. az elektronikus hírközlésről szóló törvény kötelezi a szolgáltatókat, hogy bizonyos adatokat folyamatosan naplózzanak, meghatározott ideig őrizzenek és azokat a nyomozó hatóságoknak meghatározott feltételek fennállása esetén adják át. [28]

A hálózatokon áramló információk rendvédelmi célú megfigyelésének eszköze az úgynevezett **jogszerű megfigyelés** (Lawful Interception). A hálózati adatforgalom valós időben történő jogszerű megfigyelésének lehetősége a hagyományos – alapvetően vonalkapcsolt – kommunikációs hálózatokban biztosított volt, mindezt a hozzáférési hálózatokban nemzetközi szabványok szabályozták. Ilyen szabványosításra a csomagkapcsolt, ezen belül az IP-alapú hálózatok esetében nem került sor és maga a csomagkapcsolt üzemmód is megnehezíti egy adott félhez köthető információcsere megfigyelését. Mindebből következően az Internet 'lehallgatása' egyrészt számos nehézségbe ütközik, másrészt az alkalmazható technikák az arra nem jogosultak számára is rendelkezésre állnak.[14]

A rendvédelmi alkalmazás mellett az **informatikai bűnügyi eljárások a katonai alkalmazásban** is meg kell jelenjenek, mint az egy információs hadviselési szakértő tanulmányában már 2002-ben megfogalmazta. Definíciója szerint az informatikai bűnügyi eljárások katonai értelemben "tudományosan igazolt módszerek felkutatása és alkalmazása digitális bizonyítékok gyűjtésére, feldolgozására, értelmezésére és felhasználására, annak érdekében, hogy:

- bizonyító erejű leírást nyújtson az összes támadó jellegű információs tevékenységről a szervezeti és kritikus infrastruktúra támadást követő teljeskörű helyreállításához;
- vesse össze, értelmezze és jelezze előre a szembenálló fél tevékenységeit, valamint azok hatásait a tervezett katonai műveletekre;
- tegye a digitális adatokat alkalmassá és meggyőzővé egy bűnügyi vizsgálati folyamatban történő felhasználásra." [29, 3.o.]

Az Egyesült Államok Védelmi Minisztériumában 2002-ben felállításra került egy Informatikai Bűnüldözési Központ (Cyber Crime Center), amely meghatározza a szakterület eljárási szabályait, módszereit és eszközeit; segítséget nyújt a katonai nyomozó hatóságok bűnügyi, kémelhárító, terrorizmus elleni és csalásokkal szembeni tevékenységéhez. A központ az 1998-ban létrehozott Számítástechnikai Bűnügyi Laboratórium (DoD Computer Forensics Laboratory) bázisán került kialakításra. A központ tevékenységének három pillére:

[14] Lásd például a 2008 nyarán felfedett, a Border Gateway Protocol hibájára épülő 'lehallgatási' lehetőséget.

a laboratórium, egy oktatási intézmény és egy kutatóintézet. Rendeltetése, hogy hozzájáruljon a Védelmi Minisztérium katonai igazságügyi, katonai biztonsági tevékenységének továbbfejlesztéséhez és az információs színtéri fölény megteremtéséhez.

Az informatikai bűnügyi eljárások megkerülhetetlen részét fogják képezni a NATO által Észtországban 2008 végéig felállítandó Informatikai Védelmi Központ[15] feladatrendszerének. A központ felállítása közvetlenül kapcsolódik a kritikus információs infrastruktúrák védelméhez, mivel indokát az Észtország – ezen belül kritikus infrastruktúrái – ellen 2007 májusában indított kiterjedt támadás képezte. A támadás egy NATO tagállamot ért, azonban az informatikai támadások hadijogi tisztázatlansága miatt, illetve a támadó fél bizonyítható azonosításának hiányában a NATO nem tudta (akarta) érvénybe léptetni az 5. cikkely szerinti reagálást, így a válaszlépés szakértők kiküldésére korlátozódott.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Egy nemzeti kritikus információs infrastruktúrának mindenképpen részét képezi az adott állam védelmi és ezen belül katonai kritikus információs infrastruktúrája is. Ennek megfelelően a katonai, illetve a védelmi szféra szervezetei saját infrastruktúrájuk védelméhez kapcsolódóan szerepet játszanak a nemzeti kritikus információs infrastruktúrák védelmében. A katonai, illetve védelmi szféra az előzőekben megfogalmazottnál bővebb feladatokkal rendelkezik, jelentősebb szerepet játszik a kritikus információs infrastruktúra védelemben.

A kritikus infrastruktúrák biztonsága a nemzeti biztonság egyik alapvető összetevője, így megvalósításában érintett a katonai, a rendvédelmi, a katasztrófavédelmi és nemzetbiztonsági szakterület is. A kritikus infrastruktúrákhoz hasonló, összetett rendszerek informatikai védelmében leginkább a többnemzeti műveletekben résztvevő katonai erőknek vannak tapasztalatai. Végül a kritikus infrastruktúrák elleni információs támadásokat végrehajtók felderítése, a támadók elleni fellépés, de legalábbis e feladatok nagyobb része és egészének koordinációja a védelmi szféra feladata.

A kritikus információs infrastruktúra védelemmel kapcsolatos nemzeti megközelítések négy csoportba sorolhatóak:

- technikai szintű, információ-, illetve informatikai biztonsági megközelítés, kiemelt tekintettel az Internet-biztonságra;
- e-gazdasághoz kapcsolódó működésfolytonossági (üzletmenet-folytonossági) szemlélet;
- rendvédelmi megközelítés, amely az informatikai bűnözés elleni tevékenységre összpontosít;
- nemzetbiztonsági megközelítés, amely a kritikus információs infrastruktúra védelmet annak lényeges összetevőjeként szemléli.

A védelmi szférához kapcsolódó sajátos képességek iránti igények mögött állhat az, hogy a kritikus információs infrastruktúra védelemhez szükséges, vagy ahhoz nagymértékben hasonló képességek sajátos eszköz- és eljárásrendszere, valamint az ezek alkalmazására való felkészültség a védelmi szféra valamely szereplőjéhez kapcsolódik, vagy az adott tevékenység végrehajtását, illetve végrehajtóját jogszabályok írják elő, korlátozzák.

A katonai és rendvédelmi szervezeteknek mindenekelőtt a kritikus információs infrastruktúrákat tudatosan fenyegető szereplők esetében vannak (lehetnek) feladatai, a gondatlanságból származó és természeti, vagy ipari eredetű veszélyeztetések alapvetően a katasztrófavédelem feladatkörébe tartoznak. A katonai (védelmi) szféra feladatai elsősorban a következő területekhez kapcsolódhatnak: a 'passzív' felderítés/hírszerzés és az 'aktív' ellentevékenység (zavarás, lefogás, pusztítás) az információs színtéren; a megtámadott infrastruktúrák kieső, vagy csökkentett szolgáltatásai pótlása, kiegészítése; végül a bűnügyi eljárások (nyomrögzítés, szakértés) az információs színtéren.

[15] Cooperative Cyber Defense Center of Excellence.

A kritikus információs infrastruktúrák biztonságát szándékosan fenyegető szereplőkkel kapcsolatos információk megszerzése – a potenciális támadók körének naprakész meghatározása, tevékenységük figyelemmel kísérése – céljában, funkcióiban és feladataiban lényegében nem különbözik a nemzetbiztonsági szolgálatok, a katonai és a rendvédelmi szervezetek hírszerző, felderítő tevékenységétől, annak integráns részét képezi, így az ehhez szükséges képességek kiépítése és felhasználása szinte kizárólagosan a védelmi szféra feladata. Napjainkban kialakulóban van a felderítés/hírszerzés egy speciális szakterülete: az informatikai eszközökben megtalálható és az informatikai hálózatokon áramló információk megszerzése, összegyűjtése, elemzése és értékelése.

Az információs infrastruktúrák védelmét szolgáló ellentevékenység jellegét tekintve lehet adminisztratív (jogi), fizikai és információs. Az információs jellegű ellentevékenység típusai: az ellentámadás, a megelőző támadás és az aktív megtévesztés. A megelőző támadás és ellentámadás gyakorlatilag információs támadás a potenciális, vagy aktuális támadó ellen. Ennek eszköze lehet bármilyen támadó eszköz vagy módszer. A kritikus információs infrastruktúrák védelmét szolgáló megelőző és ellentámadások megvalósítása a katonai erők feladata. A megfelelő képességgel rendelkező katonai szervezetek kialakítása a nagyobb haderőkben már a 2000-es évek elején megkezdődött. Az informatikai megelőző és ellentámadások legnagyobb problémái közé a 'célmegjelölés', a hatások célzottsága és a jogi kérdések tartoznak. Az aktív megtévesztés célja a támadás átirányítása egy nem valós rendszerbe, hálózatba, ami elősegíti: a támadó megtévesztését céljai elérését illetően; erőforrásainak szétforgácsolását; valamint tevékenységének, alkalmazott módszereinek és eljárásainak megfigyelését. A kritikus információs infrastruktúrák esetében egy nemzeti szintű aktív megtévesztési rendszer kialakítása, telepítése, összehangolt működtetése a felderítéssel és ellentevékenységgel megbízott szervezetben – a katonai erőn belül – célszerű.

A kritikus információs infrastruktúrák biztonságának megőrzését is szolgáló informatikai bűnügyi eljárások mindenekelőtt a rendvédelem alkalmazási területéhez kapcsolódnak. Ezen belül a hálózatokon áramló információk rendvédelmi célú megfigyelésének eszköze az úgynevezett jogszerű megfigyelés. Az informatikai bűnügyi eljárásoknak a rendvédelmi alkalmazás mellett a katonai alkalmazásban is egyre növekvő szerepük van, amelyet számos katonai szervezet, intézmény felállítása is bizonyít.

Összességében megfogalmazható, hogy a katonai (védelmi) szféra számos sajátos képességgel vesz részt, vagy kell részt vegyen a kritikus információs infrastruktúrák védelmében. Ezen képességek, illetve kialakításuk és működtetésük részletesebb vizsgálata további kutatásokat igényel.

FELHASZNÁLT IRODALOM

[1] MUNK Sándor: A kritikus infrastruktúrák védelme információs támadások ellen. – *Hadtudomány*, 2008/1-2. (95-106.o.)

[2] SUTER, Manuel: *A Generic National Framework for Critical Information Infrastructure Protection (CIIP)*. – Center for Security Studies, ETH, Zurich, August 2007.

[3] *COM(2005) 576, Green Paper on a European Programme for Critical Infrastructure Protection.* – Comission of the European Communities, Brussels, 17 November 2005.

[4] *The Department of Defense Critical Infrastructure Protection (CIP) Plan.* – US Department of Defense, 18 November 1998.
[http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm, 2008.04.10.]

[5] *DoD Directive 3020.40, Defense Critical Infrastructure Program (DCIP).* – US Department of Defense, 19 August 2005.

[6] ABELE-WIGGERT, Isabelle-DUNN, Miriam: *International CIIP Handbook 2006. Vol. I., Vol. II.* – Center for Security Studies, ETH, Zurich, 2006.

[7] SZENES Zoltán: Válaszúton a magyar biztonságpolitika. – *Új Honvédségi Szemle*, 2005/12. (62-79.o.)
[8] *2004. évi CV. törvény a honvédelemről és a Magyar Honvédségről.*
[9] *1994. évi XXXIV. törvény a Rendőrségről.*
[10] *1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.*
[11] *Joint Publication 3-13, Information Operations.* – US Joint Chiefs of Staff, 13 February 2006.
[12] *AAP-6(2007) NATO Glossary of Terms and Definitions (English and French).* – NATO Standardization Agency (NSA), Brussels, 2007.
[13] HAIG Zsolt-VASS Sándor-VÁNYA László: *Elektronikai hadviselés (kézirat).* – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2008.
[14] HAIG Zsolt: Az információs műveletek, a SIGINT és az elektronikai hadviselés kapcsolatrendszere. – 'A SIGINT a XXI. század kihívásainak tükrében' tudományos szakmai konferencia, Budapest, 2006. november 15., *Felderítő Szemle különszám*, 2007 február (27-48.o.)
[15] MAGYAR László: A SIGINT szerepe az aszimmetrikus fenyegetések elleni küzdelemben. – 'A SIGINT a XXI. század kihívásainak tükrében' tudományos szakmai konferencia, Budapest, 2006. november 15., *Felderítő Szemle különszám*, 2007 február (158-162.o.)
[16] PETERSON, David E.: Surveillance Slips Into Cyberspace. – *Signal* 2005/6 (61-66.o.)
[17] *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.* – Joint Chiefs of Staff, 12 April 2001 (As Amended Through 31 August 2005)
[18] HOLDAWAY, Eric J.: *Active Computer Network Defense: An Assessment.* – Air Command and Staff College, Air University, Maxwell Air Force Base, April 2001.
[19] ANDERSON, Levon: Countering State-Sponsored Cyber Attacks: Who should Lead? – In. Groh et. al. (szerk.) *Information as Power, Volume Two*. U.S. Army War College, Carlisle Barracks, 2007 (105-122.o.)
[20] *Virtual Criminology Report - Cybercrime: The Next Wave.* – McAfee Inc., November 2007.
[21] WILLIAMSON, Charles W.: Carpet bombing in cyberspace. Why America needs a military botnet? – *Armed Forces Journal*, May 2008 (20-25.o.)
[22] SCHMITT, Michael N.: Wired warfare – Computer network attack and *jus in bello*. – *International Relations Research Center Review*, June 2002 (365-399.o.)
[23] SCHWARTAU, Winn: Honeypots wreek sweet revenge against cyber intruders. – *Network World Fusion*, 2000. december 14.
[http://www.networkworld.com/columnists/2000/00173866.html 2008.08.31.]
[24] *A Magyar Honvédség Összhaderőnemi Doktrínája (Tervezet).* – HM HVK Hadműveleti Csoportfőnökség, 2002 október.
[25] KATONA Géza: *A kriminalisztika és a bűnügyi tudományok.* – BM Kiadó, Budapest, 2002.
[26] POLLITT, M.: Computer Forensics: an approach to evidence in cyberspace. – In. *Proceedings of the National Information Systems Security Conference*, Baltimore, 1995 (Volume II., 487-491.o.)
[27] BERGHEL, Hal: The Discipline of Internet Forensics. – *Communications of the ACM*, 2003/8. (15-20.o.)
[28] *2003. évi C. törvény az elektronikus hírközlésről.*
[29] GIORDANO, Joseph-MACIAG, Chester: Cyber Forensics: A Military Operations Perspective. – *International Journal of Digital Evidence*, 2002/2 (1-12.o.)