HADMÉRNÖK

VII. Évfolyam 4. szám - 2012. december

**Krasznay Csaba**
krasznay.csaba@uni-nke.hu

# A POLGÁROK VÉDELME EGY KIBERKONFLIKTUSBAN

***Absztrakt***

*A kiberhadviselés fogalmával, eszköztárával, célpontjaival mélyrehatóan foglalkozik a nemzetközi szakirodalom, de az ilyen konfliktusok állampolgárokra gyakorolt hatásának elemzésével egyelőre csak elvétve lehet találkozni. Jelen tanulmányban gondolatkísérlet szinten áttekintésre kerül egy tisztán informatikai eszközökkel végrehajtott komplex támadás állampolgárokat érintő hatásmechanizmusa, azok a kérdések, melyek bizonyosan felmerülnének egy ilyen szituációban, valamint az állami és ipari felelősségvállalás néhány javasolt iránya.*

*The definition, toolset and goals of cyber warfare is a widely examined question in the international literature, but it is hard to find any reference that deals with the effects to the citizens of such conflicts. This study is a thought experiment, which reviews the mechanism of a complex cyber-attack related to the citizens, emerging questions in this situation, and the proposed directions of public-private responsibilities.*

***Kulcsszavak:*** *kibervédelem, kiberhadviselés, katasztrófavédelem, polgári védelem ~ cyber defense, cyber warfare, disaster management, civil protection*

## BEVEZETÉS

A világ számos országában fontos nemzetbiztonsági fenyegetésnek tartják a kritikus információs infrastruktúrákat érintő támadásokat. Nincs ez máshogy Magyarországon sem, ahol a Nemzeti Biztonsági Stratégia így fogalmaz: [1]

„Az állam és a társadalom működése – a gazdaság, a közigazgatás, vagy a védelmi szféra mellettszámos más területen is – mind meghatározóbb módon a számítástechnikára épül. Egyre sürgetőbb és összetettebbkihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatok, valamint a kapcsolódó kritikusinfrastruktúra fizikai és virtuális terében. Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szintemindenki számára elérhetővé vált eredményeit egyes államok, vagy nem-állami – akár terrorista – csoportok arrahasználhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatokrendeltetésszerű működését. E támadások eredetét és motivációját gyakran nehéz felderíteni. A kibertérbenvilágszerte növekvő mértékben jelentkező nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmivonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelemfeladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kellállnia."

A konkrét feladatok között azonban nem jelentkezik a katasztrófa- és polgári védelmi vetület, holott egy összetett kibertámadás hatásai elsősorban az állampolgárokat érintik. A nemzetközi szakirodalom áttanulmányozása sem segít abban, hogyan kell (ha kell egyáltalán) a lakosságot felkészíteni az informatikai támadások hatásaira. A civileket érintő kérdések általában három területre korlátozódnak. Egyrészt élénk vita folyik arról, hogy a piaci szakembereket milyen módon lehet bevonni egy ország kibervédelmébe. Másodszor fontosnak tartják kiemelni, hogy a lakosság számára információbiztonsági tudatosság-képzéseket kell tartani, ahol megismerhetik a biztonságos internetezés alapjait. Harmadrészt feladatként jelenik meg az, hogy a közép- és felsőoktatásban minél több védelmi szakembert képezzenek ki, akik később állami szolgálatba állva segítik a támadások elhárítását. A katasztrófa- és polgári védelmi feladatok tehát nem egyértelműek, mélységük és szükségességük vita tárgya lehet! Jelen tanulmányban éppen ezért lehetséges irányok kerülnek felvázolásra, melyek helyességét és életképességét a következő évek gyakorlata igazolhatja!

## KOMPLEX KIBERTÁMADÁSOK

A kibertámadások hatásaival kapcsolatos első kérdés az, hogy vajon megtörténhetnek-e? Ugyanis annak ellenére, hogy sokat foglalkozik a lehetőséggel a szakma, tisztán informatikai eszközökkel elkövetett komplex, komolynak nevezhető támadást még nem tapasztaltunk meg. Ismerjük az elektronikus információs rendszereinktől való függésünket, van elképzelésünk arról, milyen hatással járna ezek támadása, de ezeket a hatásokat eddig csak elszigetelten és legtöbbször nem szándékos incidens kapcsán tapasztalhattuk meg. Szakmai körökben ismert a Digitális Mohács forgatókönyv, mely egy elképzelt kibertámadás lefolyását mutatja be Magyarország ellen. [2] Az ott leírtak jó kiindulópontot jelentenek, de 2009-es publikációja óta olyan események történtek, melyek segítenek az ebben leírt lépéseket pontosítani.

Napjainkban jól elkülöníthető a kiberfenyegetések négy fajtája. Ezek a kiberbűnözés, a hacktivizmus és kiberterrorizmus, a kiberkémkedés és a kiberhadviselés. A kiberbűnözés célja az informatikai eszközökön keresztüli haszonszerzés, elsősorban a hagyományos szervezett bűnözői csoportokhoz köthető. A hacktivizmus és a kiberterrorizmus ugyan fogalmilag különálló cselekmény, de közös bennük, hogy elsősorban kisebb, decentralizált csoportok hajtják végre azokat az informatikai bűncselekményeket, melyek célja az, hogy minél

szélesebb tömegek lássák a csoport által képviselt ideológiai véleményt. Hatásuk elenyésző, ugyanis azt a fajta szervezettséget nem tudják felmutatni, mely egy hatékony kibertámadáshoz szükséges lenne. A médiahatásuk azonban igen komoly. A kiberkémkedés az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést jelenti. A kiberhadviselés az államok közötti konfliktusokban jelenik meg, melynek során a felek informatikai eszközöket vetnek be egymás elektronikus információs rendszereinek befolyásolásának céljából.

Ezek közül a kiberterrorizmusnak és a kiberhadviselésnek lehet olyan vetülete, mely szükségessé teszi az összehangolt lakossági védelem megszervezését. Egy kiberterrorista esemény bekövetkezése azonban felettébb valószínűtlen, hiszen azok a csoportosulások, melyeknek érdekében állhat egy ilyen cselekmény végrehajtása, eddig nem mutatták jelét annak, hogy a szükséges képességek birtokában lennének. A Stuxnet kártékony kód megismerése óta tudjuk, hogy a lehetőség adott egy informatikai eszközökkel végrehajtott támadáshoz, de ezek kivitelezése olyan szellemi, anyagi és titkosszolgálati kapacitást igényel, melyet még egy államilag támogatott terroristacsoport sem tud felmutatni. Itt elsősorban az emberi erőforrás hiányát kell kiemelni, hiszen még napjainkban is kevés olyan szakember van a világon, akiknek programozói tudása elégséges lenne olyan kódok megírására, mely alkalmas egy sikeres kibertámadás véghezvitelére.

A kiberhadviselés azonban komoly, egyre növekvő lehetőség, mellyel a hagyományos, fegyveres konfliktusok kísérőjeként már napjainkban is számolni kell. Az intelligens fegyverek kiterjedt használata szükségszerűen magával hozza az ezeket irányító informatikai rendszerek ellehetetlenítésének igényét. Ha ezt a képességet egy ország kifejleszti, automatikusan készen áll a polgári célpontok támadására is, hiszen a fegyverzeteket irányító szoftverrendszerek nem sokban vagy egyáltalán nem különböznek a polgári kritikus információs infrastruktúráktól. Ennek a fejlődésnek az egyik lehetséges végeredménye a „kölcsönös kiberelrettentés” kialakulása, mely hasonlóan a nukleáris fegyverek területéhez azt fogja eredményezni, hogy bár az országok képesek egymás elektronikus információs rendszereire pusztító hatású csapást mérni, de mivel ismerik saját sérülékenységüket és a potenciális ellenfelek képességeit, ezzel a fegyverrel inkább nem élnek. Ennek példája lehet a Kína és Japán között kitört konfliktus a Szenkaku-szigetek miatt. [6] Annak ellenére, hogy mindkét ország képes komoly informatikai csapást intézni a másik felé, eddig elszigetelt esetektől eltekintve ódzkodtak élni ezzel a fegyverrel.

A kölcsönös kiberelrettentés különlegessége az is, hogy gyakorlatilag az összes ország ki tudja fejleszteni a kibertámadási kapacitását, hiszen az közel sem igényel akkora befektetést, mint bármely más fegyverzeté, ráadásul a nemzetközi jogi státusza sem alakult még ki teljesen. Egy komplex, összetett kibertámadás lehetőségével éppen ezért komolyan kell számolni, hiszen nehezebben kontrollálható, mint bármely más fegyverzet, a támadó kiléte nehezen bizonyítható, hatásai pedig jóval kiterjedtebbek, mint egy fegyveres csapásé amellett, hogy a halálos áldozatokkal nem, vagy csak nagyon kismértékben, járulékos formában kell számolni.

A rendelkezésre álló tapasztalatok szerint egy kibertámadás akkor jelent igazán komoly tehertételt egy országnak, ha koordinált, hullámokban jövő, multiszektoriális, hírszerzési információkkal támogatott és elsődlegesen károkozási célú. Koordinált, azaz olyan katonai irányítás áll mögötte, mely rendelkezik valamilyen stratégiai céllal, és annak rendeli alá az egyes műveleti tevékenységeket. Hullámokban jövő, ami azt jelenti, hogy a védelemért felelős szervek számára a támadások elhárítása rendkívül nehézzé válik, mivel a támadások típusai és célpontjai változatosak, előre kiszámíthatatlanok és egymást követők. Ennek ráadásul komoly demoralizáló hatása is van. Multiszektoriális, tehát több iparágat érintő, ami szintén megnehezíti a védelmet, hiszen a védelmi koordináció általában csak kevés iparágat ölel fel, a legtöbb stratégiai területen nincsen kialakult információbiztonsági együttműködés.

Hírszerzési információkkal támogatott, azaz az informatikai támadásokhoz szükséges információk nem csak nyílt forrásból származnak, hanem titkosszolgálati adatgyűjtés és információelemzés is segíti azokat, valamint egyes informatikai támadások végrehajtásához emberi erőforrást is igénybe vesznek az ún. social engineering módszer keretében. Elsődlegesen károkozási célú, ami elválasztja a kiberkémkedéstől a kibertámadásokat, ugyanis ebben az esetben az a cél, hogy az állam és polgárai érezzék a támadást, azaz látványosnak kell lennie a beavatkozásoknak.

Jó példa minderre Irán esete. A már említett Stuxnet kártékony kód felhasználását egyértelműen a kiberhadviselés egyik eszközének tekinthetjük, de sajtóértesülések szerint Barack Obama elnök széles körben engedélyezte az informatikai eszközök használatát az iráni konfliktus megoldása érdekében. [7] Ezek közé tartozik az USA virtuális iráni nagykövetségének megnyitása, mely egy angol és perzsa nyelvű honlap, amin keresztül többek között az iráni állampolgárok amerikai szemszögű tájékoztatása is megvalósítható. De az ENSZ által elrendelt gazdasági szankciók kikényszerítése is kivitelezhetetlen lenne informatikai eszközök nélkül. [8] És ezek csak azok a legálisan használható elemek, melyekről jelenleg tudomásunk van. Az iráni hatóságok folyamatosan gyanúsítják az amerikai és izraeli kormányokat informatikai beavatkozásokkal, amikre válaszul az amerikai hatóságok Iránt gyanúsítják az országban található célpontok elleni támadásokkal. [9], [10] Irán tehát az első kiberháborús zóna, ahol jogilag megalapozott és nemzetközileg nem kellően szabályozott, de legalábbis nem bizonyítható forrásból érkező informatikai támadások vegyesen fordulnak elő.

Egy komplex, kiterjedt kibertámadás az iráni példa alapján szinte biztosan célba veszi az ország közigazgatási rendszereit, nagyvállalatait, médiáját és alapvető közműveit is. Ennek célja kettős. Egyrészt a célpont ország gazdasági működésének ellehetetlenítése, másrészt az uralkodó politikai osztállyal szembeni bizalmatlanság erősítése. A modern gazdaság elképzelhetetlen elektronikus információs rendszerek nélkül, így ezek támadása segíti az első cél elérését. Az alapvető ellátási láncok megbontása pedig az egész országban olyan elégedetlenséget válthat ki, ami a politikai vezetés ellen hat, hiszen nehezen magyarázható és még nehezebben bizonyítható a tömegeknek, hogy egy áramszünetet vagy az ivóvíz szennyezését külső informatikai támadó váltotta ki. Így a támadók részéről ez a megoldás lényegesen egyszerűbb, biztonságosabb és olcsóbb, mint egy hagyományos fegyveres beavatkozás.

## TÁRSADALMI HATÁSOK

Egy kiberkonfliktus társadalmi hatása kiszámíthatatlan. Arra vannak hazai és nemzetközi példák is, hogyan reagál a közvélemény egy kritikus informatikai rendszer véletlen leállására, de arra vonatkozóan nincsen semmilyen tapasztaltunk, hogy egy komplex kibertámadás milyen reakciókat váltana ki. Ami bizonyos, hogy az internetes kommunikáció leállása közvetve és közvetlenül is káoszt okozna, ahogy azt a 2012-es new yorki Sandy hurrikán alatt is érezni lehetett. [11] Ekkor a távközlési szolgáltatások mellett a korunk alapvető információforrásaiként szolgáló hírportálok jó része is elérhetetlenné vált a válságterületen élő polgárok számára.

Ha nincsen internet és távközlés, akkor az elektronikus fizetési megoldások is ellehetetlenednek. Márpedig minél fejlettebb egy ország, annál kevesebb készpénzt használnak és a különböző elektronikus megoldások uralják a piacot. Ez érezhetően befolyásolja az emberek hétköznapjait, akadályozza a kereskedelmet, de ami még ennél is rosszabb, komoly hatással van a gazdaság egészére. Ráadásul az internet hiánya nem csak a banki műveleteket veti vissza, hanem más szektorokban is megmutatkozik a hatása. Jó példa erre Egyiptom esete, ahol az arab tavasz idején a kormányzat lekapcsolta az országból kimenő

internetes forgalmat. Ez az OECD becslése szerint legalább 90 millió dollár kárt okozott az országnak és komoly fennakadást jelentett az egész gazdaságnak. [12] Ha egy kiterjedt támadással kell szembenézni, az mérhető károkat okoz egy ország gazdasági teljesítményében.

Az iráni kiberháború komolyan felveti azt a lehetőséget is, hogy a támadó az ország alapvető közműveinek működését próbálja befolyásolni. A Stuxnet bebizonyította, hogy van lehetőség az ún. ipari termelésirányító rendszerek (SCADA –Supervisory Control and Data Acquisition) működésének befolyásolására. Az olyan közművek, mint a víz, gáz, áram szolgáltatások mind alapvetően függnek az ilyen rendszerektől. Eddig nem történt olyan informatikai incidens, mely széles körben érintette volna az állampolgárok közművekhez való hozzáférését, de ezzel a lehetőséggel mindenképpen számolnia kell a kibervédelem felelőseinek.

Ahogy azzal is, hogy bonyolult, informatikafüggő ellátási láncok alakultak ki, melyek nélkül az alapellátás más elemei sem működőképesek. Az élelmiszerellátás például függ a gyártói, logisztikai, közlekedési és kereskedelmi elektronikus információs rendszerektől, ha ezek bármelyike működésképtelen, akkor az alapvetően fontos árucikkek nem, vagy csak jelentős késéssel tudnak eljutni az állampolgárokhoz. Eddig ilyen támadás sem került napvilágra, de a támadás kivitelezése egyszerűbbnek tűnik, mint a közművek esetén, hiszen kevésbé védett, széles körben elterjedt információs rendszerekkel dolgoznak ezekben a szektorokban.

A kiterjedt informatikai támadások nem várt halálesetekhez is vezethetnek az összeomló informatikai rendszerek közvetett hatásaként. Itt elsősorban a mentésirányító rendszerekre kell gondolni, melyeket Magyarországon ezekben az években kívánnak modernizálni és teljesen számítógépes alapokra építeni. Amennyiben ezek nem megfelelően működnek, könnyen előfordulhat olyan káosz, mint 1992-ben a londoni irányítási rendszer esetében, ahol a nem megfelelően működő számítógépes rendszer egyes becslések szerint 20-30 megelőzhető halálesetet eredményezett, mivel a mentők nem értek időben a helyszínekre. [13]

Nem véletlen, hogy Magyarország, hasonlóan a fejlett ipari országokhoz, kiemelten kezeli a kiberfenyegetéseket. A politikai döntéshozók is felismerték kitettségünket és stratégiai kérdésként kezelik a területet. De hasonlóan a világ számos országához, a kibervédelem megfelelő szervezése hosszú folyamat, melynek csak az elején járunk. A komoly informatikai hagyományokkal rendelkező országok is elsősorban az elrettentés stratégiáját használják, hiszen a hatékony védelem sok éves fejlesztést igényel. A Magyarországhoz hasonló méretű országoknak viszont az elrettentés lehetősége nem áll rendelkezésre, így az országban található anyagi és emberi erőforrások hatékony kihasználásával kell a megfelelő eljárásokat kialakítaniuk és állampolgáraikat megvédeniük. Ahogy országunk Nemzeti Katonai Stratégiája fogalmaz, „a nem fegyverrel elkövetett, halálos áldozatot közvetlenül nem követelő, de hatalmas anyagi károkat és káoszt előidézni képes újfajta, aszimmetrikus kihívások miatt bővült a háború és a támadás fogalmainak jelentése. A károkozás mértékétől függően egy nem fegyveres támadás – megítélését tekintve – akár egy fegyveres támadással is egyenértékű lehet. Ilyen fenyegetést jelent elsősorban a kiberhadviselés, amely anyagi kár okozásában és a közrend megzavarásában potenciálját tekintve egyre kevésbé marad el a hagyományos fegyverektől.” [14]

## KATASZRÓFA- ÉS POLGÁRI VÉDELMI FELADATOK

A katasztrófavédelemről szóló törvény szerint a katasztrófa „a veszélyhelyzet kihirdetésére alkalmas, illetve e helyzet kihirdetését el nem érő mértékű olyan állapot vagy helyzet, amely emberek életét, egészségét, anyagi értékeiket, a lakosság alapvető ellátását, a természeti környezetet, a természeti értékeket olyan módon vagy mértékben veszélyezteti, károsítja, hogy a kár megelőzése, elhárítása vagy a következmények felszámolása meghaladja az erre rendelt szervezetek előírt együttműködési rendben történő védekezési lehetőségeit, és különleges intézkedések bevezetését, valamint az önkormányzatok és az állami szervek folyamatos és szigorúan összehangolt együttműködését, illetve nemzetközi segítség igénybevételét igényli.” [15] Az előző fejezetekben vázolt komplex informatikai támadások eredményezhetik ezt az állapotot, bár le kell szögezni, hogy erre eddig nem volt példa világunkban. A következőkben tehát abból a feltételezésből kell kiindulni, hogy az informatikai katasztrófahelyzet reálisan bekövetkezhet, és hatása megfelel a törvényben foglalt definíciónak.

A törvény részletesen szól az állami és civil szereplők katasztrófahelyzetekben történő szerepvállalásáról. A kiberkatasztrófák esetében azonban több feladat és felelős nem egyértelműen meghatározott. Szükséges tehát ezeket a hiányosságokat pótolni! Először is tudatosítani kell, hogy a hagyományos katasztrófák könnyen lehetnek informatikai támadások következményei, azaz „egyenjogúsítani” kell a kiberkatasztrófákat más eseményekkel! Ezután gondoskodni kell arról, hogy az informatikai katasztrófák is kezelhetők legyenek a katasztrófavédelmi törvény keretében!

A Kormány feladatai többek között a következőket tartalmazzák:

- meghatározza a Kormány tagjainak és a védekezésben érintett állami szerveknek a katasztrófavédelemmel kapcsolatos feladatait,
- összehangolja a katasztrófavédelemmel összefüggő oktatási, képzési, tudományos kutatási és műszaki fejlesztési tevékenységet,
- létrehozza az országos katasztrófavédelmi információs rendszert.

Jelenleg a kibervédelem számos szerv feladata között megtalálható, nem lehet egységes, központi koordinációról beszélni. Fontos feladat az ország kibervédelmi stratégiájának elfogadása, ebben az érintett szervek feladatainak meghatározása és a szükséges erőforrások biztosítása. Amíg ez a stratégia nem készül el, az elektronikus információbiztonságról szóló törvény elfogadása is jelentős előrelépést jelentene, hiszen ez már tartalmazza a szervezett kibervédelem létrehozásához szükséges alapelveket. Szintén ez a törvény tenné lehetővé azt is, hogy az országos katasztrófavédelmi információs rendszer az informatikai incidensekről is naprakész információkat kapjon.

A kibervédelemben élen járó országok mintájára és a törvény szellemében meg kell teremteni az oktatási és kutatás-fejlesztési kapacitásokat erre a területre is! A Nemzeti Közszolgálati Egyetemen komoly hagyománya van mind a kibervédelmi, mind a katasztrófavédelmi oktatásnak, ez jó bázist biztosíthatna egy komoly, európai léptékben is jelentős oktatói-kutatói bázis létrehozására és fenntartására. Ennek keretében végrehajtható lenne a kritikus információs infrastruktúrák felmérésének feladata is, melyek védelme a katasztrófák elleni védekezésért felelős miniszter feladatai között szerepel.

A központi államigazgatási szerv vezetőjének feladati között a következők szerepelnek:

- a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszterrel egyeztetve végrehajtja a katasztrófavédelmi célú távközlési, informatikai, valamint ágazati mérő- és ellenőrző rendszerek egységes irányítási rendszerbe illeszkedő kialakítását és működtetését,

– kijelöli az ágazat katasztrófavédelemben részt vevő szerveit és a katasztrófavédelembe bevonható gazdálkodó, valamint az önkéntesen jelentkező civil szervezetek közül az állandó együttműködésre alkalmas és a helyi részvételnél átfogóbb tevékenységre is képes szervezeteket, meghatározza a katasztrófavédelemmel kapcsolatos feladataikat, jogszabály alapján intézkedik felkészítésükre és a működési feltételeik megteremtésére.

Komplex kibertámadások esetén a korábbi fejezetben írtak szerint a távközlési és informatikai hálózatok is célpontok lehetnek. Mindenképpen érdemes tehát végiggondolni azt a helyzetet, hogy ezek a rendszerek nem megfelelően működnek! Különösen azért, mert a közelmúltban az Egységes Digitális Rádiótávközlő Rendszer (EDR) leállásáról számolt be a sajtó, így nem elképzelhetetlen, hogy a védelemért felelős szerveknek az EDR működésképtelensége mellett kell dolgoznia. [16]

A kibervédelem területén működnek olyan civil szervezetek, melyek katasztrófahelyzetben bevethetők lennének, de ezek pontos feladatai egy ilyen szituációban nem egyértelműek. Az Önkéntes Kibervédelmi Összefogás (KIBEV) céljai között például a következő tétel is szerepel: „a KIBEV felajánlja az állam számára tagjainak szaktudását és tettrekészségét abból a célból, hogy a haza kiberterének védelmét szolgálja”. Az ilyen civil szervezeteket hatékonyan lehet bevonni a katasztrófa- és polgári védelem különböző területeire.

A megyei, fővárosi és helyi védelmi bizottság „szervezi a lakosság és a védekezésben érintett szervezetek riasztásának és tájékoztatásának előkészítését és végrehajtását”, a megyei, fővárosi védelmi bizottság elnöke pedig „felelős a riasztás, tájékoztatás előkészítéséért és végrehajtásáért, gondoskodik a lakosság és a gazdálkodó szervezetek riasztásához, tájékoztatásához szükséges eszközök működtetéséről”. A digitális világban azonban ez nem egyszerű feladat. Egy összehangolt kibertámadás ugyanis a médiafelületeket is érintheti, így nem könnyű eljuttatni a hiteles tájékoztatást a lakosság felé. A lakosság számára napjainkban a hírek elsődleges forrása az internet és az elektronikus hírközlő médiumok. Élve a feltételezéssel, hogy a legolvasottabb internetes honlapok is támadás áldozatai lesznek, azaz nem érhetők el, vagy feltörésük után hamis információkat közölnek, ezek nem megfelelő források. Ide kell érteni a Magyar Távirati Irodát is, mely szintén e-mailek és a weboldala segítségével juttatja el a szükséges információt a médiumoknak. A tévék és rádiók alapvetően ezekből a forrásokból táplálkoznak, így ide sem könnyű eljuttatni a megfelelő híreket. Ráadásul szinte minden helyen tisztán informatikai eszközökkel készítik a műsorfolyamot, ami szintén egy kiváló lehetőség a külső beavatkozásra. A digitális átállás pedig előbb-utóbb magával hozza azt is, hogy a műsorszórás is elképzelhetetlen lesz informatikai eszközök nélkül.

Több ország a helyi hírközlők kiesése miatt a Facebook és Twitter oldalakat választotta vészhelyzeti közlésekre. Így tett a Budapesti Közlekedési Központ is, mely a 2013. január eleji havazás idején az elérhetetlen saját weboldala helyett a Facebookot választotta elsődleges közlési felületnek. Viszont ha nincsen megfelelő internet-elérés, akkor ezek a csatornák is elérhetetlenné válnak. Mindenképpen végig kell tehát gondolni, hogyan biztosítható napjainkban a tömegtájékoztatás feladata megfelelő internetes és informatikai eszközök nélkül!

A megyei, fővárosi védelmi bizottság elnöke „folyamatosan értékeli a kialakult helyzetet, a védekezés helyzetét, minderről jelentést tesz a … miniszteri biztosnak és tájékoztatja a kormányzati koordinációs szervet”. Ez feltételezi, hogy az incidens mértékéről és jellegéről megfelelő információk állnak rendelkezésre helyi és országos szinten is, azaz a védekezésért felelős szerveknél megvalósul a szituációs tudatosság (situational awareness). Ehhez viszont szükség van a támadások célpontjaitól, elsősorban a kritikus információs infrastruktúrák üzemeltetőitől származó információkra, méghozzá közel valós időben. Ez egyfajta központi

információs rendszert feltételez, melybe előre meghatározott rend szerint érkeznek az információk. Természetesen előzetesen definiálni kell azt, hogy milyen incidenseket kell jelenteni, milyen részletezettséggel, hogyan lehet az üzleti titkokat védeni és hogyan lehet az információk hitelességét biztosítani. Foglalkozni kell továbbá a lakossági bejelentések fogadásával is, hiszen nem elképzelhetetlen, hogy a káosz fokozása érdekében a támadó egy, a lakosságot széles körben érintő, kártékony kódokat felhasználó támadást is indít.

A polgármester „részt vesz a feladatainak ellátása érdekében, a hivatásos katasztrófavédelmi szervek által szervezett felkészítéseken", valamint „kijelöli a katasztrófák elleni védekezéssel összefüggő feladataiban közreműködő közbiztonsági referenst", aki a „polgármester katasztrófák elleni védekezésre való felkészülési, védekezési, helyreállítási szakmai feladataiban, továbbá rendvédelmi és honvédelmi feladataiban közreműködő, köztisztviselői jogviszonyban álló, e feladat ellátására a polgármester által kijelölt, e törvény végrehajtási rendeletében meghatározott végzettséggel rendelkező személy". Az egyértelmű, hogy egy kiberkatasztrófa esetén a katasztrofális hatást nem az informatikai rendszer hiánya, hanem az abból következő események jelentik. Azonban nagyon fontos, hogy a törvény szerint a polgármester és az általa kinevezett közbiztonsági referens legalább a kiberbiztonság alapvető fogalmával tisztában legyen, hogy jobban megérthessék egy kiberkatasztrófa mibenlétét. A szervezett oktatásokon tehát, ha röviden is, de érdemes kitérni arra, hogy mit jelentenek napjainkban az informatikai rendszerek, és milyen hatással lehetnek ezek kimaradásai. Hasznos lehet olyan katasztrófavédelmi gyakorlatok szervezése, melynek során akár kiváltó okként, akár egy elemként megjelenik a kibertámadás. Az elektronikus információbiztonságról szóló törvény tervezete foglalkozik az oktatás kérdésével, ennek keretében a katasztrófavédelemért felelős személyek rövid képzése is megvalósítható lenne!

Mivel a tanulmányban felvázolt kibertámadási forgatókönyv elsősorban a kritikus információs infrastruktúrákat célozná, elsődleges felelőssége van az azokat működtető gazdasági társaságnak az elhárításban. A törvény többek között az alábbi feladatok rója az ilyen szervezetekre:

- hatósági határozatban megjelölt, polgári védelmi kötelezettségen alapuló települési és munkahelyi polgári védelmi szervezetet hoz létre, kijelöli a munkahelyi polgári védelmi szervezet tagjait, és beosztásuk esetén gondoskodik a felkészítésükről, valamint a szervezet működtetéséről,
- szervezi és irányítja az alkalmazottak katasztrófavédelmi felkészítését.

Informatikai támadások esetében az elsődleges elhárítás egyébként is a szervezetre hárul, ahol általában egy helyi IT biztonsági koordinátor felelős az informatikai védelemért. Feladata hármas: koordinálnia kell a belső védelmet, kapcsolatot kell tartania a külső felekkel és részt kell vennie az alkalmazottak felkészítésében is. A katasztrófavédelmi tudás azonban speciális ismereteket igényel, így hasonlóan a polgármester és a közbiztonsági referensek oktatásához, a kritikus információs infrastruktúrák vezetőit és biztonsági felelőseit is megfelelő képzésben kell részesíteni az elektronikus információbiztonsági törvény tervezetének elvei alapján.

Ki kell még emelni az alkalmazottak felkészítésének fontosságát. Amennyiben az alkalmazottak hiteles, pontos és szakszerű felkészítést kapnak, és rajtuk keresztül ez az információ családtagjaikhoz, ismerőseikhez is eljut, egy kiberkatasztrófa miatt bekövetkező társadalmi pánik nagysága csökkenthető, jobban kézben tartható. A nagyvállalatok többségében jellemzően tartanak olyan információbiztonsági tudatossági oktatásokat, melyeknek keretében a kiberkatasztrófákról is szót lehet ejteni, így előzetesen is fel lehet készíteni a lakosság egy részét arra a tényre, hogy az informatikai rendszerek sérülése és annak továbbgyűrűző hatása reális lehetőség.

Szóba kerültek már azok a civil szervezetek, önkéntesek, akik hatékonyan tudnak eljárni egy kiberkatasztrófa elhárításában. A törvény szerint „az önkéntesen segítséget nyújtó személyek az adott feladat végrehajtásáért felelős személy irányításával látják el a számukra meghatározott feladatot”. Az információbiztonság területén olyan szakmai szervezetek és kapcsolatrendszer áll rendelkezésre, melyen keresztül hatékonyan lehet mozgósítani 1000-2000 szakembert. Ezeket az együttműködéseket azonban ki kell dolgozni és meg kell találni hatékony alkalmazásuk lehetőségeit!

Ki kell még térni a polgári védelem lehetőségeire is! A polgári védelem „olyan össztársadalmi feladat-, eszköz- és intézkedési rendszer, amelynek célja katasztrófa, illetve fegyveres összeütközés esetén a lakosság életének megóvása, az életben maradás feltételeinek biztosítása, valamint a lakosság felkészítése azok hatásainak leküzdése és a túlélés feltételeinek megteremtése érdekében”. Bár nehezen elképzelhető egy olyan összetett támadás, amely olyan szinten terjed ki, hogy polgári védelmi aktivitásra lenne szükség, de például egy olyan támadás, mely magyar állampolgárok informatikai eszközeit (számítógépeit, okostelefonjait) tömegesen támadja, és ezekről indulnak a kritikus információs infrastruktúrákat érintő támadások, indokolttá teheti azt, hogy élni lehessen a polgári védelmi kötelezettség élesítésével. A hagyományos katasztrófa-elhárítás mellett érdemes megemlíteni, hogy Magyarországon több tízezer informatikával hivatásszerűen foglalkozó állampolgár él, akik adott esetben részt tudnak venni a lakosságot érintő informatikai incidensek elhárításában, ezzel hozzá tudnak járulni a közvetett katasztrófaesemények kivédésében.

## ÖSSZEFOGLALÁS

Ma még megjósolhatatlan, hogy valaha is szembesülni fogunk-e olyan kibertámadással, mely érezhető hatással lesz az állampolgárok tömegei számára, illetve közvetett hatásain keresztül életek kerülnek veszélybe. El kell azonban fogadni azt, hogy mindaz, amit a tanulmány megfogalmaz, a valóságban is bekövetkezhet, hiszen egyes elemei mind megtörténtek – szerencsére eddig nem pusztító szándékkal. A politikai vezetés a kockázatot felismerte, annak hatékony kezelése azonban egyelőre kezdeti stádiumban van.

A katasztrófavédelmi törvény egyes lépései analóg módon átültethetők a kiberkatasztrófákra is, így csekély anyagi ráfordítással hatékonyan lehet felkészülni a kibertámadások kezelésére is. Jelen gondolatkísérlet több javaslatot tartalmaz a törvény kibervédelmi felhasználására, de legfontosabb feladatként az elektronikus információbiztonságról szóló jogszabály elfogadását jelöli meg. Még nem késő elkezdeni a felkészülést, a döntést viszont minél előbb meg kell hozni arról, hogy a legfejlettebb országokhoz hasonlóan létfontosságúnak tartjuk-e információs rendszereinket!

### Felhasznált irodalom


[1] Magyar Kormány: A Kormány 1035/2012. (II. 21.) Korm. határozataMagyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 19. (2012) 1383.

[2] Kovács, L., Krasznay, Cs.: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság III., 1. (2010) 44-56.

[3] Krasznay, Cs.: A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai. Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola, 2011.

[4] Kovács, L., Sipos, M.: A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. Hadmérnök V., 4. (2010) 163-172.

[5] Tang, L., Zhang X.: Can Cyber Deterrence Work? In: A. Nagorski (Eds.),*Global Cyber Deterrence – Views from China, the U.S., Russia, India, and Norway*. EastWest Institute, 2010.

[6] Kyodo, J.: Japanese websites come under attack as Senkaku squabble continues. The Japan Times Online, (2012. szeptember 20.). Forrás: http://www.japantimes.co.jp/text/nn20120920b7.html, letöltve: 2013. január 15.

[7] Sanger, D. E.: Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times (2012. június 1.). Forrás: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html, letöltve: 2013. január 15.

[8] Cordesman, A. H., Bosserman, B., Khazai, S., Gold, B.: U.S. and Iran Strategic Competition – Sanctions, Energy, Arms Control, and Regime Change. Center for Strategic and International Studies, 2012.

[9] Gladstone, R.: Iran Suggests Attacks on Computer Systems Came From the U.S. and Israel. The New York Times (2012. december 25.). Forrás: http://www.nytimes.com/2012/12/26/world/middleeast/iran-says-hackers-targeted-power-plant-and-culture-ministry.html, letöltve: 2013. január 15.

[10] Leyden, J.: US gov blames Iran for cyberattacks on American banks. The Register Online (2013. január 9.). Forrás: http://www.theregister.co.uk/2013/01/09/us_banks_ddos_blamed_on_iran/, letöltve: 2013. január 15.

[11] Kolbert, A.: Az internet örök, nem az, ami fut rajta. Index, (2012. november 13.). Forrás: http://index.hu/tech/2012/11/13/az_internet_orok_csak_ami_van_rajta_az_nem/, letöltve: 2013. január 15.

[12] Organisation for Economic Co-operation and Development (OECD): The economic impact of shutting down Internet and mobile phone services in Egypt. OECD (2011. február 4.). Forrás: http://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm, letöltve: 2013. január 15.

[13] Adamu, M., Alkazmi, A., Alsufyani, A., Al Shaigy, B., Chapman, D., Chappell, J.: London Ambulance Service Software Failure. University of Kent, 2010.

[14] Magyar Kormány: 1656/2012. (XII. 20.) Korm. határozat. Magyarország Nemzeti Katonai stratégiájának elfogadásáról. Magyar Közlöny, 175. (2012) 29710.

[15] Magyar Kormány: 2011. évi CXXVIII. törvénya katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról. Magyar Közlöny, 113. (2011) 28842-28891

[16] Magyar Távirati Iroda: Rejtély, mi okozta mentő-rendőr-tűzoltó rádiós rendszer leállását. HVG Online (2013. január 7.). Forrás: http://hvg.hu/itthon/20130107_Rejtely_mi_okozta_mentorendortuzolto_ra, letöltve: 2013. január 15.

[17] HVG.hu: Leállt a BKK honlapja, a Facebookot használják. HVG Online (2013. január 14.). Forrás: http://hvg.hu/itthon/20130114_Leallt_a_BKK_honlapja, letöltve: 2013. január 15.