ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel


# BIZTONSÁGPOLITIKA

Prof. Dr. Kovács László mk. ezredes

Nemzeti Közszolgálati Egyetem

**Budapest, 2014**

# Tartalomjegyzék

# Bevezetés

Az elmúlt néhány évtizedben a biztonság abszolút módon értékelődött fel a minket körülvevő világban. A bekövetkezett nemzetközi, politikai, gazdasági, illetve technikai és technológiai változások együttesen okozzák azt, hogy mára a biztonság vált minden ország és minden nemzetek közötti szövetség számára az egyik legfontosabb tényezővé.

Ugyanakkor a 21. század elejére a biztonság egyik meghatározó tényezője az információ, valamint az információ megszerzésében, összegyűjtésében, rendszerezésében, feldolgozásában és elosztásában kulcsszerepet játszó információs infrastruktúrák.

Minden ország számára ezeknek az infrastruktúráknak a biztonságos üzemeltetése (kialakítása, fenntartása, fejlesztése) az egyik legnagyobb kihívás, és amely egyre inkább a legfontosabb biztonsági összetevő is. Nagyon sok esetben nemzetbiztonsági kihívást is jelentenek azok a veszélyforrások, amelyek ezeket a kritikus, avagy más terminológiával élve létfontosságú infrastruktúrákat fenyegetik. Ezek a rendszerek azonban nem mindig működnek látványosan, hiszen paradox módon nagyon sokszor csak akkor vesszük észre őket, amikor már nem működnek, annyira a mindennapjaink részévé váltak. Ezek az információra alapozott infrastruktúrák a mindennapi közműszolgáltatásoktól kezdődően, a gazdasági életen át a közigazgatásig, vagy akár a mindennapjaink legapróbb részletéig mindenhol ott vannak, mára olya annyira fontossá váltak, hogy egyre inkább valóban ezek védelme a legfontosabb nemzetbiztonsági kérdés.

Ennek megfelelően ez a terület kiemelten jelenik meg a biztonságpolitikában is. Az európai országok korábban nemzeti szinten próbáltak választ adni erre a kérdésre. Számos ország az információs társadalom építése és fejlesztése, más országok az információs infrastruktúrák oldaláról közelítették, illetve közelítik meg még ma is ezt a problémakört. Utóbbi megoldási mód esetében az információs infrastruktúrák több országra, régióra vagy akár több kontinensre is kiterjedő interdependenciája (azaz összefüggése, egymásra utaltsága) azt is feltételezi, hogy ez a nemzeti szinten végzett és megvalósított védelem koordinált és az érintett felek (országok) között egyeztetett módon történik. Ez már magában hordozza annak a szükségességét, hogy közös, tehát országhatárokon átívelő elgondolás – közös európai, vagy akár globális biztonságpolitikai irányelvek – szülessenek ezen a téren is.

Ennek megfelelően jegyzetünk jelen fejezetében nagyon röviden megvizsgáljuk, hogy napjainkban melyek azok a legfontosabb tényezők, elvek, intézmények, amelyek a biztonságpolitikában elengedhetetlen szerepet játszanak. Majd ezt követően az információbiztonság szerepét és jelentőségét, az erre irányuló, és az ezzel összefüggésben lévő kibertéri biztonságot tekintjük át.

Mindez azzal is jár, hogy a biztonságpolitikát nem teljes vertikumában mutatjuk be, hanem annak csak egy szűk, ám annál fontosabb szegmense – az információ oldaláról – vázoljuk és értékeljük mindezt. Ugyanakkor a fejezet végén az *Irodalom* című részben felsoroljuk mindazokat a forrásokat, amelyek jelen fejezet elkészítésekor egyrészt hivatkozási forrásként szolgáltak, másrészt pedig mintegy ajánlott irodalomként eligazodást nyújthatnak a biztonságpolitika bővebb megismeréséhez, illetve más részeinek és területeinek tanulmányozásához.

# A biztonságpolitikáról röviden

## 1. A biztonságpolitika fogalma és tárgya

A biztonság felértékelődésével együtt jár a biztonság fogalmi meghatározásának igénye. Ugyanakkor azonban azt láthatjuk, hogy a biztonságnak még ma sem létezik olyan általános értelemben elfogadott definíciója, amely minden korszakban és minden történelmi kontextusban megfelelő lenne. Ez annak ellenére van így, hogy az emberiség kialakulásától napjainkig a fennmaradásunkhoz és a társadalmak fejlődéséhez a történelem során – bár eltérő jelleggel és tartalommal –, mindig kiemelt jelentőséggel bírt a biztonság kérdése.

A biztonság megfogalmazható a fenyegetés, vagy a fenyegetettség hiányaként, vagy a fenyegetés elhárításának képességeként. (Gazdag, 2011) A Hadtudományi Lexikon a következő definícióval él a biztonság meghatározására: „*egyéneknek, csoportoknak, országoknak, régióknak (szövetségi rendszereknek) a maguk reális képességein és más hatalmak, nemzetközi szervezetek hatékony garanciáin nyugvó olyan állapota, helyzete (és annak tudati tükröződése), amelyben kizárható v. megbízhatóan kezelhető a bekövetkező veszély, ill. adottak az ellene való eredményes védekezés feltételei.*” (Szabó J., 1995)

Az elmúlt évtizedekben a biztonság fogalmi meghatározása mellett a biztonsággal foglalkozó tanulmány(ok) tudományterületi besorolása is komoly szerepet kapott. Mindezek egyfajta meghatározás szerint biztonsági tanulmányokat jelentenek, amelyek definíciója a következőket foglalja magába: „*a biztonsági tanulmányok területe a szervezett emberi közösségek (államok), valamint az államok által létrehozott nemzetközi rendszerek vizsgálata.*” (Gazdag, 2011)

A biztonsági tanulmányok, illetve azok interdiszciplináris jellege a következő tudományterületekkel mutat kapcsolatot: (Gazdag, 2011)

- történelemtudomány;
- állam- és jogtudomány;
- politika tudomány;
- nemzetközi tanulmányok;
- közgazdaság tudomány;
- hadtudomány.

A biztonságpolitika, mint szakpolitika a következő két szakpolitikai területtel határos:

- védelempolitika;
- külpolitika.

Mindezek után egyfajta megfogalmazás szerint a biztonságpolitika: „*az általános politika része, a kormányok tevékenységének központi területe. Célja, az adott közösség békéjének megőrzése, a veszélyek csökkentése, illetve elhárítása, a kihívások kezelhető szinten tartása.*" (Gazdag, 2011)

A biztonság különböző területeinek vizsgálata, valamint a biztonság fogalmának az adott korhoz való igazítása természetszerűleg minden korszak velejárója. A 20. század végén, illetve a 21. század elején az átalakuló világ, az új biztonsági kihívások, illetve az azokra adható minél adekvátabb válaszok megtalálása érdekében a biztonság fogalmának kiterjesztését javasolta számos kutató. Közülük kiemelkedik Barry Buzan, aki Ole Weaverrel és Jaap de Wildével közösen a biztonság fogalmát öt szektorra osztotta: katonai, politikai, gazdasági, társadalmi és környezeti biztonsági szektorra. (Gazdag, 2011) Ugyanakkor a 21. század – amennyiben követjük a buzani gondolkodás analógiáját – még egy további biztonsági szektort is magával hozott, ez pedig az információbiztonság.

Az információbiztonság, mint biztonsági szektor megjelenését az indokolja, hogy az információ vált az egyik meghatározó erőforrássá a 20. század végére, illetve a 21. század elejére. Ez azzal is jár, hogy az információ, mint erőforrás birtoklása hatalmi kérdés.

Ugyanakkor az információhoz való hozzáférés, az információ feldolgozása (szűrése, átalakítása, kezelése, tárolása, stb.), valamint annak elosztása az egyre növekvő, és egyre nagyobb mennyiségű adat és információ mennyisége miatt igen komoly problémák egész sorának forrása. Mindezeknek számos oka lehet, kezdve a nem, vagy nem megfelelően biztonságos információs rendszerektől, egészen addig, hogy ehhez az információ tömeghez való hozzáférés magában foglalja a kémkedést, a hírszerzést, vagy akár az olyan tevékenységeket, mint pl. a pénzmosás, vagy illegális üzleti tevékenységek is.

Amennyiben elfogadjuk az információbiztonság, mint biztonsági szektor fontosságát, akkor azt is a biztonságpolitikai vizsgálatunk tárgyává kell tenni, hogy az információk milyen rendszereken keresztül jutnak el a felhasználókig, illetve ezeken a rendszerek belül milyen utakat jár be egy-egy adott információ. Mindezeknek megfelelően az információs infrastruktúrák vizsgálata is elengedhetetlen, mert ezek a rendszerek olyan alapvető funkciókat látnak el, mint pl. a nélkülözhetetlen javak előállítása, szállítása és a létfontosságú

szolgáltatások folyamatos elérhetőségének biztosítása. Ezek a rendszerek megteremtik az összeköttetést és az együttműködés képességét, valamint hozzájárulnak a közbiztonság és az ország külső biztonságának fenntartásához.

# 2. Biztonságpolitika Magyarországon

Mielőtt hazánk biztonságpolitikáját, illetve annak legfontosabb tényezőit, valamint annak alapvető dokumentumait áttekintenénk, szükséges a biztonsággal kapcsolatos nemzeti szintű biztonságot meghatározó intézményekről[1] szót ejteni.

Az állam az egyetlen olyan intézménye társadalmunknak, amely monopolhatalommal rendelkezik az erőszakszervezetek (hadsereg, rendfenntartó erők, stb.) tekintetében. Ez a monopolhatalom azonban sokszor nagyon kényes egyensúlyra épül, amelyet az államhatalmi ágak valósítanak meg. Az államhatalmi ágak a következők:

- törvényhozói hatalom;
- végrehajtói hatalom;
- bírói hatalom.

Számos országhoz hasonlóan hazánkban is a kormány játsza a legfőbb szerepet a biztonság területén. Ugyanakkor az is elmondható, hogy napjainkban számos ország, így hazánk is egy úgynevezett nemzeti biztonsági stratégiában fogalmazza meg, hogy az ország hogyan kívánja nemzeti céljainak elérése érdekében a politikai, gazdasági, diplomáciai és katonai eszközeit felhasználni.

Hazánk jelenleg érvényben lévő nemzeti biztonsági stratégiája 2012-ben jelent meg a 1035/2012. (II.21.) Korm. határozata formájában Magyarország Nemzeti Biztonsági Stratégiájáról címmel. A stratégia rendeltetése, „*hogy az értékek és érdekek számbavétele, valamint a biztonsági környezet elemzése alapján meghatározza azokat a nemzeti célokat, feladatokat és átfogó kormányzati eszközöket, amelyekkel Magyarország a nemzetközi politikai, biztonsági rendszerben érvényesíteni tudja nemzeti biztonsági érdekeit*.” (Nemzeti Biztonsági Stratégia, 2012)

[1] Itt hangsúlyozni kell, hogy Magyarországról beszélünk, mert a biztonságpolitika intézményrendszere, valamint azok megvalósulási formái országonként eltérőek lehetnek.

A stratégia a következő fő részekből áll:

- Magyarország biztonságpolitikai környezete;
- Magyarország helye és biztonságpolitikai érdekei a világban;
- a Magyarországot érintő biztonsági fenyegetések, kihívások és azok kezelése;[2]
- a Nemzeti Biztonsági Stratégia végrehajtásának eszközrendszere.

A stratégia a biztonság fogalmát a következő összefüggésben tárgyalja: „*A biztonság fogalma egyre átfogóbb értelmezést nyer. A folyamatosan változó biztonsági környezetben a kihívások, kockázati tényezők és fenyegetések ma már több síkon – az egyének, közösségek, államok és régiók szintjén, valamint globális szinten – jelennek meg, és az egyének, kormányzati és nem kormányzati szervezetek, valamint transznacionális szereplők széles körét érintik. Mára elengedhetetlenné vált a biztonság politikai, katonai, gazdasági és pénzügyi, társadalmi, ezen belül emberi és kisebbségi jogi, valamint környezeti dimenziójának együttes kezelése. Ugyanakkor a 21. században a biztonság katonai szegmense is új hangsúlyokkal jelenik meg. Egyre inkább előtérbe kerülnek azok a biztonságpolitikai kihívások, amelyek kezeléséhez átfogó és összehangolt politikai, gazdasági és – szükség esetén – katonai fellépésre van szükség.”* (Nemzeti Biztonsági Stratégia, 2012)

A nemzeti biztonsági stratégiából kiindulva készítik el a különböző ágazati stratégiákat, pl. nemzetbiztonsági, energetikai, külügyi vagy külkapcsolati, gazdasági-pénzügyi, illetve katonai stratégia.

Jelen fejezetben ezekből csak a katonai stratégiát emeljük ki. Hazánk jelenleg érvényben lévő nemzeti katonai stratégiája a Kormány 1656/2012. (XII. 20.) Korm. határozata Magyarország Nemzeti Katonai Stratégiájának elfogadásáról címmel 2012-ben született meg. E stratégia fő célja, „*hogy Magyarország Alaptörvényével, a védelmi szféra tevékenységét meghatározó jogszabályokkal, az Észak-atlanti Szerződés Szervezetének ... Stratégiai Koncepciójával, valamint az Európai Biztonsági Stratégiával összhangban, továbbá a Nemzeti Biztonsági Stratégiában lefektetett elvek alapján kijelölje azokat a stratégiai szintű célkitűzéseket, irányokat, eszközöket és forrásokat, amelyek révén a Magyar Honvédség teljesítheti küldetését.”* (Nemzeti Katonai Stratégia, 2012)

[2] Itt megjelenik a kiberbiztonság kérdése, amelyet az utolsó fejezetünkben külön mutatunk be.

# 3. Biztonság és biztonságpolitika a kibertérben

Korábban már megállapítottuk, hogy a 21. században a biztonságpolitika egy új szegmenssel bővült, ez pedig az információbiztonság területe.

Az információ különböző információs rendszereken keresztül jut el hozzánk, amely információs rendszerek pedig a kiberteret hozzák létre. Amikor először halljuk azt a kifejezést, hogy kibertér, akkor nagy valószínűséggel az internet jut eszünkbe. Ugyanakkor, ahogy ez fejlődik és terjeszkedik, és ahogy a mindennapok egyre inkább elengedhetetlen részévé válik, úgy lesz egyre több információs rendszer és szolgáltatás is a kibertér része, amelyek azonban nem feltétlenül mindig a hagyományos internet részei.

A katonai terminológiában azt a teret, ahol a különböző információs folyamatok megvalósulnak, azaz, ahol például elektronikus eszközökkel szereznek információt, ahol ezeket feldolgozzák, majd a produktumot eljuttatják a felhasználókhoz információs hadszíntérnek nevezik. Ezen a hadszíntéren mindezek mellett az elektronikai rendszerek ellen számos tevékenység is zajlik, hiszen a szembenálló fél mindig igyekszik megakadályozni a másik fél – jelen esetben információs és elektronikai – rendszereinek használatát.

Ez az információs hadszíntér azonban jóval többet jelent, mint a számítógép-hálózatok által megvalósított kibertér. Ennek oka az, hogy az elektromágneses spektrumot is a kibertér részének kell tekintenünk (pl. a vezeték nélküli rádió-kommunikáció e tartomány segítségével valósul meg), valamint ki kell egészítenünk e teret más frekvencia tartományokkal, mint pl. a mechanikus rezgések és a részecskesugárzások fizikai tartománya.

A kibertér katonai értelmezése tehát kiterjeszti a megszokott és általánosan elterjedt nézetet, azaz az internettel való azonosítást. A kibertér katonai értelmezése e dimenzió kiterjesztésével már nemcsak a számítógép-hálózatok működési környezetét sorolja ebbe a megfogalmazásba. Napjainkban a hadseregek a harctéren elektronikai eszközökből (pl. rádiók, radarok, navigációs eszközök, harctéri azonosító berendezések stb.) és számítógépekből olyan hálózatokat hoznak létre, ahol igen nehéz különválasztani egymástól a rendszert alkotó komponenseket. Amennyiben ezek elleni tevékenységről és a saját oldalon ezek védelméről beszélünk, akkor mindenképpen egy komplex rendszerként kell azokat értelmezni, melyeknek közös működési környezetük van.

Katonai értelemben tehát a kibertér a hadviselésnek a hagyományos dimenziókkal, azaz a földi-, légi-, tengeri- és kozmikus színterekkel hasonlatos, azzal egyenértékű tartománya. (Haig, Várhegyi, 2008)

Biztonsági oldalról megvizsgálva a kiberteret számos olyan tevékenységet kell számba vennünk, amelyek ebben a térben zajlanak. Az egyik ilyen a kiberbűnözés.

A kiberbűnözés 15-20 évvel ezelőtt még csak a jól vagy kevésbé jól megírt rosszindulatú szoftverekről, valamint az azokkal elkövetett támadásokról szólt. Ugyanakkor napjainkra ez a helyzet gyökeresen megváltozott. A hagyományos bűnözés (is) felfedezte az új dimenziót, azaz a kiberteret. A kibertérben bekövetkező támadások jelentős része ma anyagi haszonszerzés céljából következik be. Ezeknek a támadásoknak a jelentős részét a korábban hagyományos bűnelkövetéssel foglalkozó bűnözői csoportok követik el úgy, hogy megvásárolják azt az informatikai és technológiai tudást (szakembereket), amelyekkel egy-egy ilyen akció elkövethető. A változás egyik másik igen markáns jele, hogy ma az egyéni felhasználók a támadások célpontjai, hiszen a jól védett, nagy rendszerek támadása sokszor igen erőforrás igényes, és nem is mindig hozza meg az elvárt eredményt. Természetszerűleg az egyéni felhasználókat ért támadások mellett, vagy éppen azokon keresztül a különböző bankokat, illetve pénzintézeteket is támadják. Mindezek mellett olyan új kiberbűnözési formák is robbanásszerűen terjedtek el, mint pl. a számítógépes csalás, amelyek célpontjai elsősorban szintén az egyéni felhasználók.

A kiberbűnözést a következő kategóriákra lehet felosztani:

- számítógép segítségével elkövetett bűncselekmény: olyan bűncselekmény, amelyben az elkövetés ténye a bűncselekmény, a számítógép „csak” eszköz;
- számítógépek és/vagy számítógép-hálózatok ellen elkövetett bűncselekmény: ilyen lehet pl. az adatokhoz való illetéktelen hozzáférés, az adatok vagy információk módosítása, manipulálása, törlése, megsemmisítése, ellopása, a számítógép vagy hálózat működésének akadályozása, stb.

A kiberbűnözés elleni fellépés egyik igen fontos jogi, a biztonságot is befolyásoló lépése az Európa Tanács 2001. november 23-án, Budapesten elfogadott Számítástechnikai bűnözésről szóló egyezménye. Az egyezményt azóta nagyon gyakran Budapest Convention, azaz Budapest Konvenció névvel is illetik. Az egyezményt első körben az aláíró 12 ország közül csak 5 ratifikálta, köztük hazánk 2004. július 1-jén. Ezt követően 2011. október 1-ig az

Európa Tanács 31 tagja és az Egyesült Államok ratifikálta az egyezményt.[3] (Convention on Cybercrime, 2001)

Az egyezmény különösen fontos, mert az Európai Unió, illetve az egyezményt aláíró országok felismerték, hogy egy olyan közös büntetőjogi politika kialakítása szükséges, amely alapján megfelelő, közösen megalkotott, elfogadott és alkalmazott elvek mentén lehet csak nemzeti jogszabályokat hozni a kiberbűnözéssel szemben. (Convention on Cybercrime, 2001)

Ugyanakkor az olyan nagyobb volumenű kibertámadásokkal kapcsolatosan, amelyek célja és motivációja nem gazdasági indíttatású, illetve nem anyagi haszonszerzés, és amelyek mögött nem egy gazdasági érdekcsoport, hanem adott esetben egy ország áll, nagyon sokáig a biztonságpolitika nem számolt. Elsőként a 2007-ben bekövetkezett, Észtország elleni kibertámadások[4] világítottak rá, hogy ez a terület is végképp a biztonságról való gondolkodás elengedhetetlen része kell, hogy legyen. Ugyanakkor, a kibertámadásokra, illetve magára a kiberháborúra nemzetközi jogi szabályozás jelenleg sem létezik.

2013-ban tették közzé az ún. Tallinn Manual-t, amely eredeti angol címe *Tallinn Manual on the International Law Applicable to Cyber Warfare*, azaz a Kiberhadviselésre alkalmazható nemzetközi jog Tallinni Kézikönyve. Ez az első olyan dokumentum, amely ugyan egy tudományos elemzés és ajánlás gyűjtemény, de mégis átfogó módon a kiberhadviselés nemzetközi szabályozásának lehetőségeit és kérdéseit vizsgálja. A Tallinn Manual-t egy közel 20 fős nemzetközi csoport készítette a tallinni NATO Cooperative Cyber Defence Centre of Excellence (NATO Kibervédelmi Kiválósági Központ) felkérésére és annak közreműködésével. A tanulmány, bár nem egy kötelező érvényű hivatalos NATO dokumentum, mégis a nemzetközi jog és a nemzetközi humanitárius jog alkalmazhatóságát vizsgálja a kiberhadviselésben, és számos előremutató új javaslatot fogalmaz meg a területre. (Schmitt, 2013)

[3] Az egyezmény magyarul a következő linken érhető el: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS%20185%20Hungarian.pdf

[4] A 2007. áprilisában és májusában Észtországot ért kibertámadásokkal jelen fejezet egyik későbbi alfejezete bővebben foglalkozik.

# A biztonságpolitika változása

## 1. Megváltozott környezet

A II. Világháború végéig a biztonság fenntartásának egyik alapvető eszköze a katonai erő volt. A háború után azonban a társadalom biztonsága, illetve annak megteremtése és fenntartása került előtérbe, de a hidegháború időszakában javarészt még mindig a katonai erő, mint biztonsági tényező dominált.

Az 1990-es évek elején bekövetkezett világméretű politikai változások alapvető kérdésekben késztették a biztonságpolitika különböző iskoláit addigi elveik átértékelésére. A Szovjetunió felbomlása, a Varsói Szerződés megszűnése véget vetett egy korszaknak. Újra kellett értékelni mindazokat a veszélyeket és kihívásokat, amelyekkel a nagy katonai szövetségként egyedül maradó NATO, illetve a fejlett nyugati államok néztek szembe.

A NATO 1991. november 7-8-án, Rómában megtartott csúcsértekezlete az új helyzetben való kiútkeresést, valamint a megváltozott kockázatokat és kihívásokat elemezte. (NATO, 1991) A biztonsági kockázatok és kihívások elemzésekor elvetették egy nagy, hagyományos – tömeghadseregekre alapozott – agresszió kialakulásának közvetlen veszélyét, de új kihívásként jelentek meg olyan tényezők, mint a nemzetközi terrorizmus, a regionális-, etnikai konfliktusok, vagy mint például a fegyvergyártási technológia nem ellenőrzött elterjedése. Mindezek alapján a szövetség újragondolt koncepciójában fontos szerepet kapott a nemzetközi békefenntartás, vagy például a nem háborús műveletekhez (Military Operation Other than War – MOOTW) kapcsolódó katonai tevékenységek alapvető stratégiai alapjainak meghatározása.[5]

Az új kihívásoknak megfelelően megkezdődött a nagy, tömeghadseregek átalakítása és felkészítése az új feladatokra. A kisebb, de jobban felszerelt hadseregek kialakítása felé indultak el a fejlesztések, amelyekben a fő hangsúlyt a profizmus és a mozgékonyság kapta,

[5] A római csúcs utáni időszakban bekövetkezett változások a nem háborús katonai műveletek értelmezésében is változást hozott. Ma már válságreagáló műveletekről (Crisis Response Operations – CRO) beszélhetünk, amely a nem háborús műveletek átfogó meghatározása, és mint ilyen, ebbe a fogalomkörbe tartoznak például a béketámogató műveletek is.

valamint ezekkel összhangban az új kor technikai vívmányainak maximális kihasználása a jellemző.

A NATO 1999. április 23-24-én, Washingtonban lezajlott csúcsértekezlete a római csúcs óta eltelt időszak változásait értékelte. (NATO, 1999) Ebben újból elvégezték a biztonsági kockázatok és kihívások elemzését, amelyek szintén kiemelt szerepet tulajdonítottak a terrorizmus veszélyének, illetve a regionális és a helyi konfliktusok kialakulásának.

A 2002 novemberében megtartott prágai csúcs – a 2001. szeptember 11-i Egyesült Államokat ért terrortámadások miatt – alapvetően megváltozott világpolitikai helyzetben zajlott le. Bebizonyosodott, hogy a korábbi, a veszélyeket és kihívásokat vizsgáló elemzések helyesek voltak, és az egyik legnagyobb veszélyforrás a terrorizmus, illetve ennek nemzetközi megnyilvánulási formái lettek. A csúcsértekezlet többek között a megváltozott helyzetnek megfelelően döntött a Szövetség katonai struktúrájának átalakításáról, és kiadta az úgynevezett Prágai Képesség Ajánlás (Prague Capabilities Commitment) csomagot, amely az új kihívásoknak való megfeleléshez olyan képességek kialakítását tűzi ki célul, amelyek nagymértékben a tagországok önálló – immár növelni és fejleszteni kívánt – képességeire épült. (NATO, 2002)

A NATO 2010-es lisszaboni csúcstalálkozója után a Szövetség új stratégiai koncepciót dolgozott ki, amely meghatározza a NATO fejlődésének következő szakaszát. Az új koncepcióban a jelenlegi és a jövőben felmerülő biztonsági kihívásokra is válaszolni tudó, hatékony, új képességekkel felruházott és új partnerekkel együttműködő szövetség képe rajzolódott ki. (NATO, 2010)

A 2001. szeptember 11-i amerikai terrortámadások egyrészt igazolták a veszélyek korábbi helyes elemzését, amelyek a terrorizmust jelölték meg a veszélyforrások közül az egyik legfontosabbnak, másrészt komoly hiányosságokra mutattak rá. Beigazolódott, hogy az egyik legfontosabb tényező korunkban az információ. Az információ megszerzése, összegyűjtése, feldolgozása, elemzése, értékelése azonban óriási feladat. Különösen nehéz ez abban az esetben, ha nagyon sok szervezet – esetenként több nemzet, más-más rendeltetésű és feladatú szervezetei – végzik ezt a feladatot. A szeptember 11-i események hátterének elemzése és értékelése is azt mutatta, hogy bár nagyon sok – az információszerzéssel és feldolgozással foglalkozó szervezet és intézmény rendelkezett részinformációkkal, ezekből mégsem állt össze az a teljes kép, amely figyelmeztető jelként jelent volna meg a legmagasabb szinten, és

amely alapján elkerülhetőek lettek volna a terrorista-támadások. Megállapítható, hogy nem volt meg a megfelelő információáramlás a rész-információkkal rendelkezők között, nem volt megfelelő az információfeldolgozás rendje.[6] (Kovács, 2003)

# 2. Az információtechnológia biztonságpolitikára és hadügyre gyakorolt hatása

A biztonságpolitika változásait elemezve gyakran felmerül a kérdés az információs technikai és technológiai forradalom vívmányainak felhasználásával kapcsolatban: vajon nem túl sérülékenyek-e a rendszereink? Nem hordozzák-e önmagukban a támadhatóság lehetőségét? A kérdésre adandó lehetséges válasz összetett. Természetesen ezek a számítógépekre és digitális technikákra alapuló rendszerek megnövekedett kockázatot, és mindezekkel együtt nagyobb sérülékenységet is magukban hordoznak. Ezekre azonban fel lehet készülni, és ki lehet dolgozni a sérülékeny pontok vagy eljárások védelmére szolgáló technikai, szervezésbeli védő mechanizmusokat.

Ugyanakkor egyet biztosan ki lehet jelenteni biztonságpolitikai szempontból: nevezetesen azt, hogy az információs rendszerek sérülékenységei, illetve az ezeket a sérülékenységeket fenyegető támadások minden ország számára olyan biztonsági kockázatot jelentenek, amelyeket ma már nem lehet figyelmen kívül hagyni. Ennek megfelelően tehát teljesen jogos az információbiztonság, mint biztonsági szektor megjelenése a biztonságpolitika korábban tárgyalt fő szektorai – katonai, politikai, gazdasági, társadalmi és környezeti biztonsági szektorok – mellett.

Mindezek alapján az egyik legnagyobb biztonságpolitikai kihívásnak a katonai és az információbiztonsági szektorok egymásra hatását, azaz a kiberhadviselést tekinthetjük. Ezért a hadseregek és a hadviselés átalakulását is meg kell vizsgálnunk, hiszen egyrészt az információs kihívások a hadseregekben alkalmazott információs rendszerek esetben is fennállnak. Itt is a kérdésként merül fel az értékelemzés, azaz ezen eszközök használata és

[6] Ez annak ellenére következett be, hogy már 1997-ben, az Amerikai Egyesült Államok elnökének előterjesztettek egy javaslat csomagot, amely az amerikai nemzeti infrastruktúrák védelmének kérdéskörében folytatott vizsgálat eredményeit és a védelemmel kapcsolatos kormányzati tevékenységeket tárgyalja. Ebben konkrét javaslatok szerepelnek többek között arra vonatkozóan, hogy a különböző információszerzéssel foglalkozó szervezetek milyen módon koordinálják, és hogyan valósítsák meg az adatok és információk konkrét cseréjét. (Critical Foundations, 1997)

alkalmazása jár-e akkora előnnyel, hoz-e akkora hasznot, hogy megérje vállalni az ezekben esetlegesen megbúvó veszélyeket. A válasz határozott igen, mert akkora előnyre tehet szert az ilyen fajta rendszerek és eszközök alkalmazója, amely elengedhetetlen a siker – a győzelem – eléréséhez.

De nem minden ország, és nem minden érdekeit érvényesíteni kívánó csoport, vagy szervezet engedheti meg magának a modern, a kor technikai színvonalát elérő eszközök és rendszerek használatát. Ez elsősorban gazdasági és anyagi kérdés, hiszen a legújabb technikai és technológia kutatás-fejlesztése, illetve adott esetben egyszerű megvásárlása is meghaladhatja nagyon sok ország vagy fegyveres csoport anyagi lehetőségeit. Ezért ezen országok, vagy csoportok vélt vagy valós érdekeik érvényesítéséhez egyéb eszközöket keresnek. Akkor, tehát ha egy fejlett ország információs technikát alkalmazó hadseregével szemben egy méreteiben, technikai színvonalában, felszerelésében, eszközeiben és eljárásaiban jelentősen eltérő (kisebb) erő áll, aszimmetrikus hadviselésről[7] beszélünk. Ez ma jórészt a terrorizmusban ölt testet. Ezek az erők céljaik eléréséhez, amelyek megnyilvánulhatnak a konkrét pusztításban, vagy egyszerűen csak a figyelemfelkeltést szolgálják, használhatnak hagyományos eszközöket, de kihasználhatják az információs technika és technológia előnyeit is. Azt azonban nem szabad figyelmen kívül hagyni, hogy a hagyományos eszközökkel elkövetett terrorista támadásokéval összehasonlítható, vagy akár az azokkal okozható károkat nagyságrendekkel meghaladó pusztítás végezhető egy, az információs technikát felhasználó, úgynevezett információs támadással. Mai fejlett társadalmaink ugyanis oly mértékben függővé váltak az információs infrastruktúráktól, információs szolgáltatásoktól, illetve mindezek mindennapjainkba olyan szinten beleintegrálódtak, hogy ezek támadása komoly veszélytényezővé vált. Ezek támadásával, amelyhez nem szükséges komoly, fejlett technikát felsorakoztató hadsereg, óriási károk okozhatók. Az ilyen és ehhez hasonló aszimmetrikus támadások kivédése egyrészt megelőzéssel érhető el, azaz ezeket a rendszereket védetté kell tenni az ismert lehetséges támadásokkal szemben (ez azonban rendkívül pénz és időigényes), másrészt folyamatos információszerzéssel, és ezen információk értékelésével, illetve az eredmények folyamatos – a különböző országok, szervezetek, ügynökségek közötti – kicserélésével, vagy kölcsönös átadásával lehet. (Kovács, 2003)

A 21. század hajnalán a hadügy területén is számos új elvet kellett megismernünk, illetve nagyon sok már meglévő elvet, eljárást kellett és kell folyamatosan a változásoknak

[7] Az aszimmetrikus hadviselés ennél természetesen jóval összetettebb fogalom, mégis gyakran a technikai és technológiai fölény kapcsán hangzik el e kifejezés.

megfelelően újragondolni és újrafogalmazni. Olyan fogalmak és ezzel együtt új hadviselési formák jelentek meg, mint például az információs műveletek (Information Operation), információs hadviselés (Information Warfare), hálózat központú hadviselés (Network Centric Warfare), hatás alapú műveletek (Effect Based Operation). Az új fogalmak, hadviselési formák új tartalommal és filozófiával gyarapítják a hadügyi gondolkodást.

A háborúk és a fegyveres konfliktusok napjainkban is a szárazföldi, tengeri, légi és kozmikus térségekben – háborús terekben – zajlanak, amelyekbe minden olyan polgári, katonai, szövetséges vagy koalíciós terület és erőforrás beletartozik, amely valamilyen formában az adott háborúban vagy fegyveres konfliktusban részt vesz. Azonban akkor, amikor megjelentek azok az információs infrastruktúrák, amelyek már nem csak regionális, hanem globális méretűvé is váltak, alapvető változásokat okoztak a háborús tér tartalmi megjelenését és megítélését illetően. A háborúk addigi dimenziói – a szárazföldi, légi, tengeri, kozmikus (űr) – tovább bővültek és kiegészültek az információs dimenzióval. Ennek következtében a klasszikus háborús tér átalakul egy komplex, az információs technikára alapozott, információs, digitális háborús térré. Természetesen a valódi háborúkat továbbra is a fizikai dimenziókban vívják, de ezek mellett, ezekkel párhuzamosan – mivel az információ döntő tényező a háború kimenetelében – folyik az információ megszerzéséért, megtartásáért, hatékony felhasználásáért folyó küzdelem, amelyet az információs hadszíntéren folytatnak a szembenálló felek. „*Azt a sokdimenziós működési teret (szférát), ahol a katonai tevékenységek – azon belül a katonai információs tevékenységek (műveletek) – zajlanak, információs hadszíntérnek nevezzük.*” (Haig, Várhegyi, 2005)

A hagyományos háborús terekben folyó katonai tevékenységek mellett, azokkal párhuzamosan, egyrészt azok támogatására, az információs hadszíntéren információs tevékenységek – információs műveletek – zajlanak. Minden olyan tevékenységet információs műveletnek nevezhetünk, amelyek a szembenálló fél információs rendszereire, végső soron információira gyakorolnak olyan hatást, amelyekkel a döntéshozók a politikai és gazdasági célkitűzések elérése érdekében támogathatók, illetve a saját információs rendszerekben rejlő képességek maximális kihasználását és megvédését teszik lehetővé.

Az információs műveletek különböző elkülönülten is létező információs tevékenységek közötti koordinációt jelentenek, melyeknek szükségességét az információs tevékenységek nagyságrendekkel növelhető hatékonysága adja.

Az információs műveletek fogalma mellett gyakran elhangzó és gyakran hallható kifejezés az információs hadviselés is. A két fogalom közötti különbség egyrészt a terminológiai értelmezésben, másrészt a fogalmat definiálók körében keresendő. Más megfogalmazást használnak a katonák és más megfogalmazást azok, akik civil szemmel kutatják és gondolkodnak az információs hadviselésről. Részben az eltérések és különbségek ezekből származtathatók.

Az információs technika és technológia alkalmazása a katonai vezetésben azt eredményezte, hogy a korszerű hadseregek vezetése és irányítása egyre inkább számítógépes információs rendszerekre épül. Az információs műveletekkel párhuzamosan, azokkal egy időben megjelent egy új hadviselési mód, amelyet a katonai terminológia Hálózat Központú Hadviselésnek (Network Centric Warfare – NCW) nevez. Ez azonban inkább egy újfajta – az információs kor követelményeihez és megnövekedett fizikai lehetőségeihez alkalmazkodó – gondolkodási mód, sem mint a „hadviselés" szószerinti értelmezése. „*Az NCW egy újfajta gondolkodásmódra – a hálózatos gondolkodásra – alapul. Az NCW arra a harci erőre fókuszál, amely a harcban résztvevő összes szereplő hatékony és gyors kapcsolatából generálódik.*" (Alberts, Gartska, Stein, 1999)

A hálózat központú hadviselést elemezve láthatjuk, hogy annak egyik rendkívüli előnye abban rejlik, hogy a szenzortól kezdve a döntéshozón át a végrehajtóig egységes – bár komplex és strukturált – hálózatba rendezett elemek összessége között az információáramlás rendkívüli módon felgyorsult, tehát az információk egyik pontból a másik pontig történő eljutása jóval kevesebb időt igényel, mint korábban. Eddig a végrehajtó csak azokra az információkra tudott támaszkodni, amelyeket a saját szenzorjai által nyert adatokból elő tudott állítani, de e filozófia mentén felépített rendszerben a feladat végrehajtása érdekében olyan információkhoz is hozzájuthat, amelyek más felderítési forrásból származnak, és amelyek világosabbá teszik a helyzetet, ezáltal megalapozottabb döntéseket tud hozni. (Kovács, 2004)

Szintén nagyon új elem a hadviselés területén a hatás alapú műveletek (Effect Based Operations – EBO) elmélete. A hatás alapú műveletek az egyidejűleg folytatott párhuzamos műveleteken alapszanak. Napjainkig megszoktuk, hogy a különböző műveletek egymás után sorozatban, lineárisan követik egymást. Például az első öbölháborúban (1991) a hosszantartó légicsapások befejeztével következett a szárazföldi tűzelőkészítés, és csak ezt követően történt meg a konkrét szárazföldi támadás. A hatás alapú műveletek a végletekig lepontosított, időben és térben koordinált, szinkronizált műveleteket jelentenek. A precíziós fegyverekkel

végrehajtott csapások és sebészi pontosságú tevékenységek egymás fizikai és az ellenségre gyakorolt pszichikai hatásait – azokat mintegy meghatványozva – használják ki. A hatás alapú műveletek ma még elsősorban a légierő fogalomtárában kapnak nagy szerepet, de mint ahogy azt a második öbölháború (2003) is bizonyította, hamarosan a harc többi dimenzióiban is meghatározó szerepe lehet. (Kovács, 2003)

Mindezeket összegezve elmondhatjuk, hogy a hadviselésben és a hadseregek mindennapi életében is egyre fontosabbá válik az információ, illetve azok az információs rendszerek, amelyeken keresztül az információ megszerzése, feldolgozása, elemzése és értékelése, valamint annak felhasználókhoz való eljuttatása megtörténik. Ugyanakkor ezek a rendszerek, csakúgy, mint maga az információ lesznek az elsődleges célpontok egy háborúban. A célpontok között pedig egy fegyveres konfliktussal párhuzamosan a civil információs rendszerek is – legyenek azok közigazgatási, pénzügyi, ellátó, vagy egyéb információs infrastruktúrák – ugyanúgy szerepelni fognak, mint a korábban említett katonai rendszerek.

# 3. Kiberhadviselés

Napjaink egyik legnagyobb biztonsági fenyegetését az államilag támogatott kibertámadások jelentik. Így azok nagyobb veszélyt és kihívást jelentenek, mint azt korábban gondoltuk.

A kiberhadviselés azonban nem ma kezdődött, számos közvetett előzményét ismerjük. Elektronikai hadviselésről például azóta beszélhetünk, amióta a rádió megjelent a háborúk történetében.

Nem kell katonai szakértőnek lenni ahhoz, hogy lássuk, mindenki készül a potenciális ellenfelek elleni fegyveres konfliktusra informatikai eszközökkel is. Ennek első és legalapvetőbb szakasza az információszerzés a kibertérben. Ez lehet a közvetlen elődje vagy előfutára a kiberhadviselésnek. Ma a hadseregek is nagyon sok civil rendszert használnak, amelyek jellemzői nem titkosak, de hogy hogyan és mire használják ezeket, azt az országok nagyon szeretnék tudni egymásról. Az, hogy ki lett a győztes a II. Világháborúban, még azon múlt, hogy melyik ország tudta az ellenség ipari kapacitásait a legnagyobb hatásfokkal csökkenteni, valamint ezzel párhuzamosan a sajátját a maximálisan teljesítményre sarkallni. Ma viszont az győz, aki a szemben álló fél információs infrastruktúráját képes tönkre tenni vagy legalább annak működését akadályozni tudja, miközben a sajátját képes megvédeni.

Sok ország doktrínája azonban nem csak (kiber)védekezést tartalmaz, hanem fenntartja a jogot a megelőző csapások indítására is. A kiberhadviselés során maga a támadás néhány másodperc, de az információgyűjtés, és a támadáshoz szükséges rendszerek megszervezése sokáig tart, de ennek mindig vannak áruló jellemzői. Vannak országok, ilyen az Egyesült Államok, Kína, Európában pedig például Franciaország, amelynek a katonai doktrínájában a megelőző csapás lehetősége már szerepel, és ezt kiterjesztik az kibertérre is.

Ugyanakkor a kiberhadviselés területén az ország-ország elleni kiberháborúval szemben, vagy akár azzal párhuzamosan az egyéni vagy kis csoportban elkövetett informatikai támadások lesznek a jellemzőek. Ma már egy egyén is rendelkezhet olyan felkészültséggel, hogy sikeres támadást mérjen egy régióra egy jól megszervezett és előkészített támadással. Egy terrorista is hatalmas károkat tud okozni, ha pedig már tucatnyian vannak, akkor még komolyabb hatásuk, miközben jól el tudnak bújni, nehéz őket nyomon követni, a motivációjukat kitalálni. Ilyen csoportok nemzeti szinten nem okoznak nagy kárt, de az a szervezet, amelynek, vagy akinek kárt okoznak, esetenként hatalmas veszteségeket lesz kénytelen elkönyvelni.

A hadtudomány jelenlegi állásából azt a következtetést tudjuk levonni, hogy a közeljövőben még minden konfliktus velejárója lesz a fizikai támadás, a fizikai pusztító tevékenység, amelyek a hadviselés négy klasszikus – hagyományos – dimenzióiban, a korábban már említett szárazföldön, levegőben, vízen (és víz alatt), valamint a világűrben fognak megtörténni. Ugyanakkor egyre aktívabb és egyre hevesebb tevékenység várható az információs dimenzióban, azaz a kibertérben is.

Ha a közeljövőben teljesen legyőzni nem is lehet majd egy országot kibertérben, de az információs rendszerek már említett összefüggése és egymásra utaltsága miatt hatalmas károk okozhatók. Ezek a károk pedig közvetett módon – pl. a vezetés és irányítás, a koordináció, a bizalom, stb. megbomlása vagy elvesztése miatt – kihathat a fizikai dimenzióban zajló küzdelmekre is. Egy, a fizikai támadásokkal párhuzamosan megvalósított kibertámadás következtében megbénulhat a közigazgatás, az energiaszolgáltatás rendszerirányítása, a pénzügyi rendszer vagy a gazdasági életben is nélkülözhetetlen kommunikáció.

Egy esetleges kiberháború esetén azonban mindenképpen meg kell vizsgálni a felek lehetséges motivációját is. Az talán nyugodtan kijelenthető, hogy Európában valószínűleg nem fogja megtámadni egyik ország sem a másikat informatikai eszközökkel. Lehetséges azonban, hogy más földrészen, például Ázsiában vagy Afrikában olyan konfliktus alakul ki,

amelynek megoldása az Európai Unió vagy a NATO érdeke is, de itt megint nem egy ország áll majd szemben egy másikkal, hanem egy szövetség egy politikai rezsimmel. A politikai rendszerrel szimpatizálók pedig intézhetnek támadásokat a szövetség tagországai ellen, de ez inkább terrorizmus, bűnözés vagy hacktivizmus, semmint a klasszikus háború. Ezek valószínűleg elszigetelt cselekmények lesznek, amelyeket várhatóan jól tudnak majd kezelni az országok szervezetei. Általánosságban elmondható, hogy egy nagyobb volumenű kiberháborúnak kicsi a valószínűsége. A globális gazdasági élet meghatározó szereplői nem fognak totális kiberháborút indítani, mert ezzel maguknak okoznának gazdasági veszteséget. Ez igaz Kínára is. Kína jelenlegi tudásunk szerint szintén nem fog totális kiberháborút indítani, hiszen az igen nagyban az exportra építő gazdasága nagyban függ attól, hogy az Egyesült Államok vagy az Európai Unió mennyi árut vásárol tőle. Az persze egy más kérdés, hogy Kína használ-e különböző kiber „trükköket" (információszerzés, beépített malwarek) a saját gazdasági érdekeinek az érvényesítésére vagy elősegítésére.

A kiberhadviseléssel kapcsolatban nagyon gyakran felmerül a kérdés, hogy vajon ebben a hadviselésben milyen fegyverekről lehet beszélni? Ennek megértéséhez a kibertámadások anatómiáját, azaz a kibertámadások felépítését kell segítségül hívnunk.

Önmagában a kibertérben folyó bármilyen katonai tevékenység nagy vonalakban és alap filozófiájában hasonló a hagyományos, fizikai dimenzióban történő katonai eseményekhez. Ahogy egy hagyományos katonai támadás sem, úgy egy kibertámadás sem előzmények nélküli. Egy-egy ilyen támadást – legyen szó akár egyéni, egy csoport, vagy állami támogatással elkövetett akcióról – minden esetben megelőzi az adat- és információszerzés. Ez az a klasszikus felderítés, amely esetünkben a kibertér részét képező információs rendszerek és a számítógép-hálózatok sérülékenységeit, gyenge pontjait, azok felépítését és főbb funkcióit, valamint az ezeket kezelő szakszemélyzet tevékenységét, szokásait, stb. térképezi fel. Teszi mindezt azért, hogy egy viszonylag tiszta és világos képet kapjon a támadások mögött álló erő arról, hogy hol és milyen mértékű kell, hogy legyen a tervezett akció ahhoz, hogy a kitűzött célokat elérje.

Az információszerzést az információ feldolgozása és értékelése követi. Ekkor lehet a (kiber) célpontokat is megjelölni, függően a támadás céljaitól. Ez a tevékenység azonban jóval több időt vesz igénybe, mint a támadás, hiszen a kibertérben a támadások általában nagyon-nagyon rövid idő alatt lezajlanak (kivétel ez alól nyilvánvalóan a túlterheléses támadásokat, amelyek akár órákon, vagy napokon keresztül is tarthatnak). A felkészüléshez tehát idő kell, és amely

felkészülés nem csak a kibertérben, hanem a fizikai dimenzióban is meg kell, hogy történjen. Ennek oka lehet pl. a social engineering alkalmazása, hiszen nagyon sokszor csak ezzel a módszerrel lehet kielégítő információkat szerezni a támadni kívánt félről.

Ezt követheti a kiberfegyverek alkalmazása. Kiberfegyverként felfogható minden olyan eszköz, amely a különböző informatikai vagy információs sérülékenységeket ki tudja használni. Ez azt is jelenti, hogy az egyébként is széles körben, naponta akár több ezres, vagy több tízezres nagyságrendben születő rosszindulatú programoktól kezdve egészen a túlterheléses támadásokig minden szóba jöhet, mint lehetséges kiberfegyver. Ez ugyanakkor egy hatalmas üzlet is, hiszen például a nulladik napi sérülékenységek ma óriási értékkel bírnak, legyen szó akár a (kiber) feketepiacról, akár egy állam hadserege által történő fejlesztésről.

Az első kiberfegyver alkalmazására 2010-ben láthattunk először példát. 2010 őszén immár nem csak a szakmai sajtó, hanem a nemzetközi hírügynökségek is egyre több hírt közöltek egy olyan rosszindulatú program gyors terjedéséről, amely már nem az egyszerű otthoni felhasználókat vette célba, hanem az elvileg jól őrzött és komoly, nagy biztonsági rendszerekkel rendelkező ipari létesítményeket. Az elsődleges célpontok Irán különböző atomlétesítményei, illetve azok ipari irányítási rendszerei voltak. A Stuxnet névre keresztelt féregvírus megdöbbentette a szakmát is, hiszen – mind felépítésében és működésében, mind célját tekintve – rendkívül újszerű számítógépes kártevőről volt szó.

A rosszindulatú programok több évtizedes történetében ez volt az első olyan szoftver, amely nagy tömegben ipari létesítmények vezérlő szoftverei működését támadta. A találgatások politikai felhangoktól sem voltak mentesek, hiszen a féreg előfordulási gyakorisága és észlelése Iránban volt a legmagasabb. Ez rögtön szemet szúrt a különböző médiumoknak, és rögtön hírül is adták: a féreg célpontja az iráni atomlétesítmények, konkrétan azok működésének leállítása. Ezeket a találgatásokat az informatikai biztonsági cégek elemzései alátámasztották, hiszen nagyon gyorsan kiderült, hogy valóban olyan ipari vezérlő szoftverek ellen készült a Stuxnet, amelyeket Irán is használ pl. a bushehri atomerőműben, vagy a natanzi centrifugáinál. (Kovács, Sipos, 2010)

A Stuxnet esetből számos messzire vezető következtetést is levonhatunk. Az egyik és talán legfontosabb: megjelennek az államilag támogatott kibertámadások, és ezzel összefüggésben az államilag szponzorált kiberfegyverek fejlesztései is. Egy másik következtetés: ha ipari

létesítmények ellen be lehet vetni ilyen fegyvereket, akkor a jóval kevésbé védett, és így jóval sebezhetőbb egyéb polgári információs rendszerek ellen is bizonyára készíthető ilyen, vagy ehhez hasonló kiberfegyver.

A Stuxnetettel fémjelzett támadások előtt azonban már 2007-ben láthattunk példát egy egész ország elleni kibertámadásra, illetve támadás sorozatra. 2007 áprilisában, Észtország fővárosában a „Tallinn felszabadítóinak szovjet emlékműve" áthelyezése miatt hatalmas zavargások és utcai megmozdulások kezdődtek. Az utcai megmozdulásokkal párhuzamosan rendszeres internetes támadások is bekövetkeztek főként Észtországon kívülről, amelyek kezdetben elsősorban az észt államigazgatás hivatalos kommunikációs vonalainak és weboldalainak blokkolására irányultak. Mindezek mellett az interneten és mobiltelefon-üzeneteken keresztül folytatódtak az intenzív propaganda-támadások, amelyek fegyveres ellenállásra és további erőszakra szólítottak fel.

A kibertámadások megkezdésétől számított harmadik héten – 2007 májusában – Észtország internetes hálózata már szinte teljesen megbénult.

Az összeomlást minden elemző szerint külső túlterheléses támadások kényszerítették ki. Az első forgalombénító DDoS-támadások május elején kezdődtek, célpontjaik a parlament, a kormányhivatalok, sőt a bankok és az észt média számítógépes központjai voltak. Az észt hálózaton az adatforgalom sokszor órákon át a normális ezerszerese volt. Az ország internetes forgalmát irányító központok napjában többször leálltak, az állami szervek hálózatait le kellett választani az internetről. A banki rendszerek megbénultak, a pénzügyi megbízások rendszeresen akadoztak. A támadások azért is érintették érzékenyen a balti államot, mert már akkor is kiugróan fejlett volt az ország internetes kultúrája.

Május közepén tetőzött a támadási hullám, de utána még több alkalommal, bár kisebb intenzitással továbbra is nagy volt a terhelés, számos hálózati rendszer még hetekig csökkentett üzemmódban volt csak képes dolgozni. Május 15-én például az ország második bankja, a SEB Eesti Uhisbank a tömeges internetes támadások miatt kénytelen volt felfüggeszteni a külföldről való banki rendszerekbe való belépést biztosító szolgáltatását. Egy észt bank, a Hansabank nyilvánosságra hozta a támadások miatti veszteségét, a jelentés szerint 2007. május 10-én több mint egymillió dolláros forgalomkiesést szenvedtek el.

Az elemzők szerint az akciók túlságosan jók és összehangoltak voltak ahhoz, hogy mindössze néhány rosszindulatú programozó indítsa őket. Néhány támadást sikerült orosz szerverekig

visszanyomozni, sőt az Európai Parlament állásfoglalásában leszögezte, hogy e támadások az orosz közigazgatás IP címeiről érkeztek, de az alkalmazott támadási technikák miatt rendkívül nehéz volt a forrásokat pontosan meghatározni.

Az Európai Parlament 2007. május 24-én állásfoglalást adott ki ez ügyben. A NATO május közepén szakértőt küldött Észtországba, hogy kivizsgálja a történteket, és segítsen kivédeni a további támadásokat.

Az online beavatkozást sem az észtek, sem az EU, sem a NATO nem minősítette katonai akciónak. A NATO nyilvánosan nem foglalt állást abban a kérdésben, hogy kik voltak a támadók, kinek az irányításával történt, támadásnak minősíti-e egyáltalán az eseményeket. A NATO hivatalosan bejelentette, hogy a Szövetség vizsgálja, milyen hatásai lehetnek ezeknek az akcióknak, és folyamatos kapcsolatban állt az észt szervekkel.

Az incidenseket követően a NATO komoly lépéseket tett annak érdekében, hogy ezt, illetve a jövőben bekövetkező hasonló helyzeteket kezelje. 2008-ban létrejött egy kibervédelmi kiválósági központ Tallinnban, amely egy kutató- és koordináló intézet, és amely számos jogi és technikai ajánlást tesz. E kiválósági központnak Magyarország is teljes jogú tagja 2010 óta.

2012 vége óta teljes kapacitással működik egy NATO-szintű CERT, amely a védelmi szféra informatikai rendszereinek incidenskezelését végzi. Ennek értelemszerűen sok kapcsolódási pontja van a nemzeti CERT-ekkel, amelyek a helyi technikai védekezést illetve incidenskezelést végzik.

# 4. Kína, mint globális (kiber) biztonságpolitikai tényező

Az elmúlt években Kína nagyiramú gazdasági fejlődése már-már általánossá és megszokottá vált. A világméretű gazdasági válság természetesen Kínát sem kerülte el, de a gazdaság növekedése, amely a leggyengébb években is 7-8 % volt, és amely bár kínai szemmel ugyan nem túl jó eredmény, még mindig jóval magasabb, mint ami a világ többi részének gazdasági fejlődése.

Másfél évtizede még nem keltett nagy feltűnést a volt amerikai nemzetbiztonsági főtanácsadó Zbigniew Brzezinski figyelmeztetése, amely szerint az Egyesült Államok legnagyobb vetélytársa Kína lesz, mégpedig belátható időn belül. (Brzezinski, 1999) Ugyanakkor

Brzezinski jóslata ma már nem csak gazdasági téren látszik beigazolódni, hanem a katonai potenciál különböző szegmenseiben is. Ennek igen szembetűnő jelét adják azok a kínai törekvések, amelyek az információs technológia polgári felhasználása mellett azok egyre több katonai alkalmazásában figyelhetők meg. Mindezek alapján ma már kijelenthető, hogy Kína a kiberhadviselésben különösen gyorsan fejlődik, így meghatározó és megkerülhetetlen szereplővé vált ezen a területen is.

Kína azonban már több mint egy évtizede markáns szereplője e területnek, hiszen 2002-től kezdődően amerikai számítógépes biztonsággal foglalkozó hatóságok számos Kínának tulajdonítható informatikai behatolás sorozatot észleltek – elsősorban nem titkos – amerikai katonai, kormányzati és a kormánnyal szerződésben lévő közepes- és nagyvállalatok számítógépes rendszereibe és hálózataiba. A később Titan Rain-nek (Titán Esőnek) elkeresztelt, igen szisztematikus és jól felépített támadások alatt a kínai hackerek hozzávetőleg 10-20 Terabájtnyi adatot töltöttek le a megtámadott számítógépekről. Csak összehasonlításképpen: a Kongresszusi Könyvtár (nem mellesleg a világ legnagyobb könyvtára) összes könyve kb. 10 Terabájtnyi adatot képvisel. (Report to Congress, 2008)

Ezt követően hatalmas visszhangot váltott ki a német sajtóban, majd később a német politikai életben is, hogy Németországban több kormányzati számítógépen is kínai kémprogramokat találtak. Az ügy annak fényében vált különösen izgalmassá, hogy mindez néhány nappal Angela Merkel német kancellár hivatalos kínai útja előtt robbant ki 2007 augusztusában. (Kovács, 2009)

Az információbiztonsági szakemberek számára egyáltalán nem voltak meglepőek a kínai kémprogramok, hiszen nem első alkalommal fordult elő ilyen eset. 2005-ben hasonló programokat találtak többek között elektronikai eszközöket gyártó vállalatok számítógépein. Ezzel kapcsolatosan fontos hangsúlyozni, hogy a kis és közepes vállalatok sokkal nagyobb veszélynek vannak kitéve ezen a téren, mint a nagyvállalatok, hiszen az esetükben nincs még meg az a teljes körű és átfogó informatikai védelmi rendszer, amely teljesen ki tudná védeni a hasonló támadásokat. (Spiegel, 2005) Az elektronikai ipar mellett a gyógyszergyárak, az autóalkatrész gyártók, de akár az élelmiszeripar különböző cégeit is fenyegeti ez a veszély. Ez elsősorban az ipari kémkedés, illetve a know-how eltulajdonításában jelentkezik. Ezektől a cégektől a hackerek által ellopott információk, illetve ezek későbbi felhasználása csak Németország esetében több milliárd dollár kárt okoznak évente. (Spiegel 2, 2005)

Ahogy Németország esetében úgy az Egyesült Államok esetében sem szokatlan és egyáltalán nem meglepő a kínaiak kibertevékenysége. A már említett Titan Rain támadás sorozat 2002-ben kezdődött, de szakértők még 2005-ben is találtak arra utaló nyomokat, hogy elsősorban kínai területről érkeztek illegális számítógépes behatolások olyan nagyvállalatok és kutatóintézetek rendszereibe, mint például a SANS Institute, a Lockheed Martin, a Sandia National Laboratories, a Redstone Arsenal, vagy a NASA. Természetesen a Pentagon különböző rendszereit is érintették a támadások. Ugyanakkor itt is megfigyelhető volt, hogy elsősorban a nem titkos rendszerekből töltöttek le adatokat a hackerek.

2008 áprilisában kínai hackerek összehangolt támadást terveztek a CNN televíziós hírcsatorna ellen. A támadás azokat a kritikus hangvételű riportokat lett volna hivatott megbosszulni, amelyek az olimpiai láng és a körülötte kialakult tiltakozó megmozdulások hivatalos kínai kezelését mutatták. A CNN közleményében számolt be róla, hogy a csatorna weboldalának érezhető lassabba vált az elérése, amely nagy valószínűséggel egy támadás következménye, így egy forgalomszűrőt volt kénytelen alkalmazni. Az összehangolt, nagy – vélhetően DDoS – támadás terve azonban elég gyorsan napvilágra került, és ennek következményeként, mivel a meglepetés ereje már elmúlt, csak kisebb támadások következtek be, nemcsak a CNN, hanem egyéb amerikai online médiumok ellen.

2009 áprilisában kínai (és orosz) hackerek behatoltak az Egyesült Államok villamosenergia rendszerébe. A támadások nem egy pontot vagy rendszerelemet értek, azokat az egész országban számos helyen észlelték. A támadók nem okoztak kárt, de nyilvánvaló, hogy sok gyenge vagy sebezhető pontot feltérképeztek. Nem ez volt ez első ilyen – az energia rendszert érintő – támadás, hiszen 2001-ban a kaliforniai elektromos rendszerbe hatoltak be hackerek. Akkor egyértelműen bizonyítható volt, hogy a támadás kínai kommunikációs hálózatról érkezett. Persze ebben az esetben is nagyon nehéz megmondani, és ami még nehezebb bizonyítani, hogy valójában ki is követte el a támadásokat.

Ezekből a támadásokból levonható az a következtetés, hogy a külföldre irányuló kínai cyber tevékenységek elsődleges célja nem a legszigorúbban őrzött titkok ellopása vagy megszerzése. Ezeknél sokkal fontosabb, hogy a támadók akcióik során olyan tapasztalatokra tesznek szert, amelyek a különböző rendszerek gyenge pontjaira derítenek fényt. Mindezek alapján egyelőre az egyes infrastruktúrák, akár a kritikus információs infrastruktúrák elemzése és analizálása tűnik a fő célnak. Az, hogy ezeket az információkat maga a kínai állam, vagy egyes hacker csoportok fogják-e használni, az ma még kérdéses.

Mindamellett, hogy Kínában megközelítőleg 250 olyan hacker csoport van, amelyek „államilag megtűrtek”, egyes hírek szerint a kínai hadsereg is komoly erővel rendelkező számítógép-hálózati műveletekre[8] alkalmas egységet tart fent. (Report to Congress, 2008) Az egység létezéséről természetesen szintén nincs hivatalos információ, de gyaníthatóan sok olyan hackert fog össze illetve alkalmaz, akik magasan képzettek, hatalmas informatikai tudással és tapasztalattal rendelkeznek, amelyek egy részét kínai katonai akadémiákon szerezték.

Az amerikai hadsereg is megkülönböztetett figyelmet szentel ezeknek a csoportoknak és „szakértőknek”. Egyrészt az amerikai infrastruktúra – kiemelten az információs infrastruktúra – védelme, másrészt az olyan sérülékeny katonai információs rendszerek védelme a fő feladat, mint amilyen a NIPRNet[9] (Nonsecure Internet Protocol Router Network). Ez a hálózat jelenleg elengedhetetlen a nem titkos, de szenzitív harctámogatási információk szétosztására az amerikai hadseregben mind békében, mind háborús műveletekben. A rendszer különösen sérülékeny, mert a publikus internethez kapcsolódik. Elemzők szerint e létfontosságú rendszer gyenge pontjait a kínaiak már feltérképezték, és fennáll a veszélye, hogy adott körülmények között képesek komoly károkat is okozni, amely a működőképességet is veszélyezteti. (Report to Congress, 2008)

Mindazonáltal a 2007-es Észtországot ért kibertámadások is jól bizonyítják, hogy egy fejlett információs infrastruktúrával rendelkező ország különösen sebezhető abban az esetben, ha a támadások azok a kulcsfontosságú rendszerek vagy rendszerelemek ellen irányulnak, amelyek feltérképezése pont a fent említett támadásokkal viszonylag egyszerűen megvalósítható.

Kína külföld felé irányuló kibertevékenysége mellett érdemes megvizsgálni azokat a lépéseket, amelyeket elsősorban a saját állampolgárai ellenőrzése érdekében tesz kínai területen.

A kínai internet felhasználók száma az elmúlt években dinamikusan – a világ más területeihez mérve sokkal gyorsabban – növekedett. 2008-ban 42 %-al nőtt a felhasználók száma, amely

[8] Számítógép-hálózati műveletek (Computer Network Operations – CNO): a korábban már bemutatott információs műveletek körébe tartozó tevékenység a szembenálló fél információs rendszereibe történő beavatkozást jelent, amely során egyrészt információt szerez azok felépítéséről, támadható gyenge pontjairól, másrészt csökkenti azok képességeit, vagy megakadályozza azok működését, miközben a saját számítógép-hálózatok működőképességét védi.

[9] A NIPRNet-el párhuzamosan működik a SIPRNet (Secret Internet Protocol Router Network), amely fő feladata elsősorban a minősített információk szétosztása teljesen különválasztott titkosított hálózaton.

2009-ben elérte a 298 milliót, 2012-ben pedig már közel 540 millió fő használta naponta az internetet.[10]

Ugyanakkor ez a ma már közel 600 millió internetező óriási problémákat is jelent a kínai állami vezetésnek. Az állam a gyorsan növekvő felhasználói kör ellenére (vagy éppen emiatt) megpróbálja kordában tartani azokat az információkat, amelyek elérhetőek az egyszerű internet felhasználó számára. Kína a webes cenzúra biztosítására egy, a nyugati országokban csak Kínai Nagy Tűzfalnak nevezett saját rendszert fejlesztett ki, amelyet a 2003-as indulástól folyamatosan használ. A hivatalos nevén Aranypajzsnak (Jindun gongcheng) hívott hardver és szoftver rendszert a Közbiztonsági Minisztérium tartja fent. Egyes szakértői vélemények szerint a sokmillió felhasználót 50 ezer „net rendőr" ellenőrzi folyamatosan, azaz ennyi ember működik közre a Kínai Nagy Tűzfal üzemeltetésében. (Kovács, 2009)

A rendszer által a leggyakrabban cenzúrázott tartalmak közé tartoznak az olyan betiltott csoportok, mint a Falun Gong; az olyan hírforrások, amelyek például az 1989-es Tiananmen téri eseményekkel foglalkoznak; a tajvani kormány hivatalos oldalai; a pornográf internet oldalak; vagy például a Tibet függetlenségéhez kapcsolódó weboldalak. Az internetes tartalmak cenzúrázására számos kifinomult informatikai technikát alkalmaznak. Ezek közé tartozik például az IP cím blokkolás. Gyanús, vagy nem kívánatos IP címek esetében blokkolják a HTTP, az FTP, és akár a POP3 protokollokat is. Több website-ot kiszolgáló szerver esetében, amennyiben azok akár egyikén is van olyan tartalom, amely tiltott, akkor egyik hosztolt site sem érhető el. További technika a DNS-szűrés és átirányítás. Olyan tartományneveket, amelyeken tiltott tartalom van, a DNS szerver egyáltalán nem oldja fel, vagy hibás IP címet küld vissza a felhasználónak. Gyakran alkalmazott szűrési megoldás a kulcsszavak alapján történő csomagszűrés, amely már természetesen URL esetében is működik. Ez azt jelenti, hogy az előre meghatározott szavakra vagy fogalmakra történő keresés esetén a rendszer blokkolja a kapcsolatot. Ez már kereső programok esetében is működik, azaz ha egy kereső program olyan oldalakat ad fel találatként, amelyeken tiltott szavak találhatók, akkor a rendszer blokkolja ezeket az oldalakat is. Ha valamilyen szűrőmechanizmus bontja a TCP kapcsolatot, a rendszer egy bizonyos ideig (általában 1-30 percig) a további kapcsolódási kísérleteket is blokkolja, azaz bünteti a felhasználót, amiért rossz helyen és rossz tartalmat keresett. (Kovács, 2009)

[10] Az európai internetfelhasználók száma 2012-ben 505 millió.

Mindezek mellett Kína a szofisztikált cenzúrázási megoldásoknál sokkal drasztikusabb eszközöktől sem riad vissza, amennyiben érdekei vagy a helyzet úgy kívánja. A 2009. június végén a Hszincsiang tartomány fővárosában, Urumcsiben kitört ujgur zavargások kapcsán egyszerűen korlátozták a területen az internet hozzáférést, valamint a nemzetközi telefonvonalakat lekapcsolták. Ennek oka nagy valószínűséggel az volt, hogy a szeparatista Ujgur Világkongresszus szervezet vezetője – a jelenleg az Egyesült Államokban élő Rebija Kadír – az internet segítségével szervezte és irányította a tüntetéseket.

Hasonló lépéseket tett a kormány a tienanmen téri tüntetések huszadik évfordulója alkalmával is. Több olyan közösségi weboldalt is letiltottak, köztük a kínai fiatalok között is legnépszerűbb Twittert, ahova a megemlékezéssel kapcsolatos beszámolók kerültek fel. De ezen kívül ideiglenesen a Hotmail levelező rendszert is blokkolták. A „hagyományos" média képviselőit azon kívül, hogy meglehetősen érdekes módszerekkel akadályozták a téren történő forgatásokban (pl. esernyővel takarták el civil ruhás rendőrök a kamerák elől a riportereket), zavarták a BBC, a CNN és a francia TV 5 Monde kínai adásait is.

# 5. Terrorizmus, mint biztonságpolitikai kihívás a kibertérben

## *Hagyományos terrorizmus*

A hagyományos terrorizmus (öngyilkos merénylők, nemzetközi terrorszervezetek, illetve az általuk végrehajtott terrortámadások) kutatása és vizsgálata évtizedek óta komoly témát szolgáltat a biztonságpolitikának.

Amennyiben a hagyományos terrorizmus és a kibertérből érkező terrorizmus egymásra talál, és párhuzamosan elkövetett, egymást mintegy kiegészítő akciókat hajtanak végre, akkor hatványozottan nagyobb károkat okozhatnak, mint a külön külön-külön elkövetett hagyományos-, illetőleg kiberterror-támadások.

Mindezeknek megfelelően szükséges a terrorizmus főbb fogalmainak, szereplőinek és mozgatórugóinak az áttekintése, mivel számos azonosság tételezhető fel a hagyományos és a kiberterrorizmus különböző formái között. Mindezeken túl, amennyiben sikerül felvázolni

néhány jelentős tényezőt – pl. az okokat, a szereplőket, az indítékokat és a célokat, vagy akár a végrehajtás módszereit – a hagyományos terrorizmus kapcsán, akkor talán sikerül a kiberterrorizmus néhány hasonló jellemzőjét – az erre a tevékenységre, illetve az ebben szereplők esetében – megvizsgálni.

A mai értelemben vett hagyományos terrorizmus az 1970-es években történt számos terrorakció kapcsán került ismét a figyelem középpontjába. Talán még sokak emlékezetében élénken él az olyan terrorcsoportok neve, mint például a Fekete Szeptember[11]; IRA[12]; Baader-Meinhof Csoport[13] vagy Vörös Brigádok[14], amelyek abban az időben a napi hírek meghatározói voltak a különböző akcióikkal. (Kovács, 2006)

2001. szeptember 11. azonban újra a mindennapok részéve tette a terrorizmust. A Pentagon és a Világkereskedelmi Központ elleni merényletek rádöbbentették a világot arra, hogy a hidegháború elmúltával már nem a nagyhatalmi szembenállás a legfőbb veszélyforrás, hanem a terrorizmus, illetve ennek egyik legveszélyesebb formája: a nemzetközi terrorizmus. Szeptember 11-ét követően írások, elemzések és szakértői magyarázatok tucatjai születtek a terrorizmust, mint a 21. század új és egyik meghatározó veszélyforrását elemezve.

[11] 1972. augusztus 26. és szeptember 11. között Münchenben rendezték meg a XX. nyári olimpiát. September 5-én a Fekete Szeptember nevű terrorista csoport nyolc tagja az olimpiai faluban behatolt az izraeli csapat szálláshelyére, ahol két izraeli sportolót megöltek és kilencet túszul ejtettek. Miután az izraeli kormány megtagadta a követelt 200 palesztin fogoly szabadon bocsátását, a terroristák a német kormánytól repülőgépet követeltek a túszok elszállítására. A terroristákat és a kilenc túszt két helikopteren átszállították a fürstenfeldbrucki katonai repülőtérre, ahol egy Boing repülőgép már várakozott, hogy elszállítsa őket valamelyik arab országba. A repülőtéren a német rendőrség túszmentési akciót kezdeményezett, amely olyan szerencsétlenül végződött, hogy a terroristák megölték túszaikat, illetve a tűzharcban öt terrorista és egy rendőr is meghalt. A három további terroristát elfogták.

[12] 1972. január 30-án – amit azóta „véres vasárnapként" emlegetnek – a brit katonák az internálás ellen tüntető tömegbe lőttek, és 13 embert megöltek. Egyes vélemények szerint ez az esemény járult a leginkább hozzá ahhoz, hogy az IRA terrorista szervezetté váljon. Az IRA 1972 februárjában kezdte meg terrorhadjáratát a protestáns és a brit célpontok ellen. Az erőszak megfékezésére a brit kormány felfüggesztette az észak-ír parlamentet és átvette az országrész irányítását, ahol már tizenötezer brit katona állomásozott. Az IRA bombamerényletekkel és gyilkosságokkal válaszolt erre a lépésre.

[13] Andreas Baader és Ulrike Meinhof vezette csoport nevéhez számos – az 1970-es évek elején elkövetett – merénylet és gyilkosság fűződik. Csoportjukat később átnevezték a RAF–Rote Armee Fraktion, azaz a Vörös Hadsereg Frakció névre.

[14] Vörös Brigádok – Brigate Rosse, olasz terroristacsoport, amely a 60-as évek végén Renato Curcio vezetésével szerveződött a Trentói Egyetem szélsőbaloldali köreiben. Tagjai lelkesedtek a forradalom eszméjéért, a parlamentáris demokráciát csak álarcnak tartották, amely mögött zavartalanul folyik a kizsákmányolás és az elnyomás. Céljuk az állam meggyengítése és a proletárforradalom kirobbantása volt. Ezt gyújtogatások, robbantások, emberrablások, gyilkosságok útján akarták elérni. Aldo Moro volt olasz miniszterelnök, a baloldallal történelmi kiegyezést kereső kereszténydemokrata politikus 1978. március 16-i elrablásával, majd megölésével politikai válságot idéztek elő. Ők a felelősek a bolognai pályaudvar felrobbantásáért is. Bár a csoport tagjait már a 70-es évek közepétől kezdték letartóztatni és elítélni, aktivitásuk a 80-as évek végéig tartott. A megszűntnek hitt szervezet 2003 őszén ismét hallatott magáról. Az olasz rendőrség ekkor tartóztatott le hat embert, akit Massimo D'Antona kormányzati tisztviselő négy évvel azelőtti, és Marco Biagi tanácsadó 2002-es megölésével vádoltak. (Magyar Virtuális Enciklopédia)

A terrorizmus fogalmának meghatározása meglehetősen nehéz feladat, hiszen egyrészt nem létezik egységesen elfogadott definíciója, másrészt pedig akárhány megfogalmazást is nézünk azok számos ponton eltérnek egymástól. Ennek oka elsősorban talán abban keresendő, hogy a fogalom megalkotói más és más szemszögből vizsgálják a kérdést, és így természetszerűleg más és más álláspontot is képviselnek. Mindezek ellenére – vagy talán éppen az előbb említett okok miatt –, álljon itt egyetlen megfogalmazás a terrorizmus leírására, amelyet a Magyar Hadtudományi Társaság határozott meg a Hadtudományi Lexikonban: „*Terror, megkülönböztetés nélküli támadás: minden olyan erőszakos cselekmény, vagy azzal való fenyegetés, amelynek elsődleges célja, hogy rettegést keltsen a polgári lakosság körében.*" (Szabó J., 1995)

Amióta az emberiség háborúkat vív egymással, azóta minden háború természetszerűleg erőszakos cselekményeket tartalmaz és félelmet kelt az emberekben. Amiben a háború mégis különbözik a terrorizmustól az az, hogy itt nem elsődleges cél a terrorizálás, a félelemkeltés, hanem az csak egy járulékos tény, hiszen Clausewitzcel élve a háború nem más, mint a politika folytatása erőszakos eszközökkel; két élőerő nyílt összeütközése. Egy másik meghatározó különbség a háború és a terrorizmus között az lehet, hogy a háborúkat alapvetően államok vívják, míg a terrorizmus az állammal (vagy több állammal) szembenálló nem állami csoportok, szervezetek jelenítik meg. Ehhez még az a jellemző is hozzájárul, hogy „*a terrorizmus lényege egyértelműen a nyílt ütközet tagadása*." (Townshend, 2001)

Természetesen a történelemben nagyon sok példát láthatunk arra, hogy az állam, vagy az állami hatalmat gyakorlók lépnek fel a terror eszközeivel az ország állampolgáraival szemben. Ez a fajta terror azonban inkább elnyomó, sokszor brutálisan totális befolyása miatt érdemli ki ezt a jelzőt, ellentétben az általunk tárgyalt hagyományos terrorizmus figyelemfelkeltő, demonstráló jellegével.

A terrorizmus lehetséges motivációinak kutatása összetett. Megvizsgálva számos terrorakciót az azonban közös tényként értékelhető, hogy minden terrorakció egyik kulcseleme a nyilvánosság. Ez az egyik, nagyon sok esetben – eltekintve a hasonló kivitelezési módoktól –, az egyetlen közös a különböző terrorakciók között. Függetlenül az indítéktól minden terrorszervezet számára létfontosságú a nyilvánosság különböző fokú biztosítása, hiszen csak ezen keresztül lehetséges, hogy a társadalom szélesebb rétegei is kapjanak információt magáról az akcióról, illetve a szervezet céljairól. A terrorszervezet csak így tudja biztosítana, hogy az erőszakos eszközökkel elkövetett akciók a megfélemlítésen, a bizonytalanságon

keresztül befolyásolják a közvéleményt, illetve a kormányzatot. Így tehát a terrorakciók a nyilvánosság számára és a nyilvánosság befolyásolására születnek. Ennek hiányában a terrorizmus értelmetlen és céltalan. (Kovács, 2006)

## *Terrorizmus és az információtechnológia*

A különböző terrorista szervezetek és csoportok is ugyanúgy használják, és kihasználják a csúcstechnika nyújtotta lehetőségeket, mint a hétköznapok többi szereplője. Az internet segítségével kommunikálhatnak, szervezhetik akcióikat. Az internetről letölthető és viszonylag könnyen kezelhető titkosító programok segítségével még annak a veszélye is igen kicsi, hogy kommunikációs, kapcsolattartó tevékenységüket „lehallgassák".[15] A titkos üzenetváltás egy másik módszere lehet az úgynevezett szteganográfia.[16] Ez azt jelenti, hogy látszólag érdektelen és ártalmatlan hordozókba építenek be a kívülállók számára láthatatlan módon információkat. Ilyenek hordózók lehetnek például különböző formátumú képek, ahol a kép digitális jelei közé vannak elrejtve az információk, vagy ilyen lehet akár egy hang fájl is, amely esetében a háttérzaj tartalmazhatja az információt.

Új tagok verbuválása, toborzása terén szintén hatalmas lehetőségeket nyújt az internet a hagyományos terrorista szervezetek számára. A különböző terrorista szervezetek által fenntartott weboldalakon nyíltan is történik új tagok toborzása. Ezeken az oldalakon a potenciális új tagok meggyőzésére számos megoldás kínálkozik. A webes technikának köszönhetően egy weboldalon lehetőség van felhívni az érdeklődők figyelmét az „ügyre" különböző írásokkal, publikációkkal, a szervezet történetének és vezetőinek bemutatásával, az eddigi akciókról készített videók, pedig sokszor le is tölthetők.

A terrorista szervezetek számára is adott a lehetőség, hogy a számukra szükséges információkat megkeressék az internet segítségével. A különböző akciók elkövetéséhez számos leírást találhatnak. Így pl. „házkészítésű bomba" (homemade bomb) szavakat begépelve az egyik legismertebb internetes keresőbe 0,31 másodperc alatt közel 300 millió találatot kapunk. Ezeknek a találatoknak a jelentős része természetesen esetünkben (a

[15] Meg kell azonban jegyezni, hogy gyakran hangoztatott szakértői vélemények szerint a kódolt adatcsomagok megfejtése, és ezáltal az információtartalom visszanyerése az esetek jelentős részében az elektronikus felderítésre szakosodott NSA-nek (National Sacurity Agency) nem jelent különösebb gondot.

[16] A szteganográfia nem a 21. század találmánya. Már az ókorban is használtak olyan eszközöket és eljárásokat, amelyek segítségével titkos üzeneteket lehetett küldeni valamely nyílt üzenetbe rejtve. Ilyen volt például a „láthatatlan" tinta, amely alkalmazásával az üzenet csak akkor vált láthatóvá, ha megfelelő hőmérsékletűre melegítették. Napjainkban a szteganográfia a digitális technika alkalmazásával újra fénykorát éli.

terroristák esetében) irreleváns. De a sokmilliónyi találat között van olyan, amely kész recepttel szolgál az otthon, akár a kereskedelemben szabadon megvásárolható alapanyagokból való bombák előállításához („konyhakész bomba"). A találatok között nagyon sokáig keresnünk sem kell, hogy akár kész videofilmeket is találjunk a témában. Ugyanakkor természetszerűleg a célpontokról is számos információ állhat rendelkezésre a terrorista szervezetek, vagy a terroristák számára, amely abszolút módon könnyíti meg az akciók végrehajtását.

## *Kiberterrorizmus*

2001. szeptember 11-e után közvetlenül megjelentek azok az elemzések, amelyek a kibertérben bekövetkező terrortámadások lehetőségét vizsgálták. Ezek alapján megszületett a kiberterrorizmus első meghatározása, amely Dorothy Denning professzor asszonytól származik: „*a kiberterrorizmus számítógép alapú támadást vagy fenyegetést jelent, amelynek célja, hogy megfélemlítsék, vagy kikényszerítsék a kormányok vagy a társadalmak részéről az adott terror szervezet politikai, vallási, vagy ideológiai céljainak elérését*." (Denning, 2001)

Később a kiberterrorizmusra vonatkozó későbbi elemzéseket követően az FBI kiber részlegének vezetője – Keith Lourdeau – a következő megfogalmazást adta: „*A kiberterrorizmus olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs lehetőségekkel úgy hajtanak végre, hogy azok rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében.*" (Testimony of Keith Lourdeau, 2004)

A meghatározásokból is kitűnik, hogy a terrorista csoportok két, egymástól elkülöníthető célból használják az információtechnológiát. Az első csoportba, azok a terrorista szervezetek tartoznak, amelyek a már említett célokra – propaganda, toborzás, adatszerzés – használják e rendszereket. Gyakran e tevékenységet soft, azaz puha típusú kiberterrorizmus névvel is illetik. A másik – hatványozottan veszélyesebb – csoportba azok a terroristák tartoznak, akik nemcsak ilyen úgynevezett soft tevékenységre kívánják használni a rendszereket, hanem azt, illetve azon keresztül rombolni vagy egyéb erőszakos, hard cselekményeket is végre akarnak hajtani. Célpontjaik között nemcsak az internet szerepel, hanem minden olyan kritikus információs infrastruktúra is, amelyek információtechnológiai eszközökkel, vagy fizikai támadásokkal pusztíthatók. (Haig, Kovács, Ványa, 2011)

Ilyenek lehetnek az energiaellátó rendszerek rendszerirányító számítógép-hálózatai, a kommunikációs hálózatok, a pénzügyi-gazdasági rendszer számítógép-hálózatai, a védelmi szféra riasztási, távközlési, számítógép-hálózatai, a közigazgatás információs rendszerei. (Haig, Kovács, Ványa, 2008)

A terrorista célú kibertámadások során alkalmazható eszközök és módszerek nagy hasonlóságot mutatnak a más célú (pl. kiberbűnözés során alkalmazott) támadásokéval. A kiberterrorista ugyanúgy használhat rosszindulatú programokat (férgeket, kémprogramokat, backdoor programokat, keyloggereket), valamint változatos informatikai támadási módszereket (például DoS, DdoS, man-in-the-middle attack, cross site scripting).

A kiberterrorizmus és általában az informatikai támadások vonatkozásában különösen nagy veszélyt jelent a fentiekben bemutatott Stuxnet és annak következményei, hiszen a Stuxnet okozta pánikot követően számos hír látott arról napvilágot, hogy a Stuxnet, illetve az abban megjelenő új informatikai támadási módszerek terrorszervezetek kezébe kerültek. (Haig, Kovács, Ványa, 2011)

Mindezeket összefoglalva marad tehát a kérdés: a kiberterrorizmus valódi veszélyt jelent számunkra, vagy csak a média illetve a politika által túlerőltetett fogalom, amelynek ma már nem sok realitása van? Hiszen ilyenkor mindig feltesszük a következő kérdést: kinek is állna érdekében terrorcselekményeket végrehajtani és rendszereinket támadni?

Erre a kérdésre a korántsem megnyugtató válasz: 2001. szeptember 11-e a példa a motivációra és az akaratra, amelyet korábban az átlagember elképzelni sem tudott volna.

A kérdéseinkre egy másik nézőpontból is születhet válasz. Ez pedig a már korábban is felvetett tényező: fordítsuk meg a kérdést: mennyire biztonságosak a rendszereink? Vannak-e sérülékenységek rendszereinkben? Ha ezekre a válasz igen lesz, akkor már nem lehetünk nagyon magabiztosak, és nem zárhatjuk ki egy bármilyen célú vagy indíttatású – akár politikai, gazdasági, vallási, vagy akár ideológiai – támadás bekövetkezését.

Mindezeknek megfelelően a kiberterrorizmus jelentette fenyegetés valós (természetesen a realitásokat figyelembe véve kell felmérni ezt a veszélyt), hiszen egy-egy ilyen támadás következménye nem csak technikai és anyagi értelemben lenne hatalmas, hanem bizony akár emberéletekben is beláthatatlan károkat okozna. Ezt a – talán nagyon is markáns – megállapítást az is alátámasztja, hogy ma egyre többen rendelkeznek azzal a tudással,

amelyek egy-egy ilyen támadás elkövetéséhez szükséges lehet. Az akciók megtervezéséhez pedig számos forrás áll rendelkezésére bárkinek, aki az infokommunikációs eszközöket csak egy kicsit is tudja használni.

# Védelem és biztonság a kibertérben

# 1. Az Európai Unió és a NATO kibervédelmi stratégiája

## *Kibervédelmi stratégia a NATO-ban*

A NATO a 2007-es észt incidens óta kiemelt területként kezeli a kibertérben zajló eseményeket. Az nagyon gyorsan kiderült és világossá vált, majd számos NATO hivatalnok hangsúlyozta is, hogy a kibertér védelme érdekében központi koordináció és központi irányítói szerep szükséges.

Szintén többször kinyilatkoztatott tény a NATO-ban, hogy az eltérő technikai fejlettségű országok, vagy akár az egyes országokon belüli eltérő fejlettségű régiók, eltérő módon kezelik a biztonságot is, így a kiberbiztonságot is, amely hatalmas kockázatot jelent a Szövetség számára. Az úgynevezett digitális szakadék, amely az eltérő technikai és társadalmi (oktatási, gazdasági, stb.) fejlettségből eredeztethető az egyik legfontosabb megoldandó problémaként jelenik meg.

A NATO 2010-es lisszaboni csúcstalálkozója után a Szövetség Stratégiai Koncepciójában is szerepelteti, hogy az egyre kifinomultabb számítógépes támadások miatt a Szövetség információs és kommunikációs rendszerek védelme az egyik legsürgősebb feladat: „*A kibertámadások egyre gyakoribbá, szervezettebbé és a kormányok, vállalkozások, gazdaságok és potenciálisan a közlekedési és ellátási hálózatok valamint más kritikus infrastruktúrák számára is egyre nagyobb károkat okozóvá válnak. Elérhetik azt a küszöböt, ami már a nemzeti és euro-atlanti prosperitást, biztonságot és stabilitást veszélyezteti. Külföldi haderők és titkosszolgálatok, szervezett bűnözők, terrorista és/vagy szélsőséges csoportok egyaránt lehetnek egy ilyen támadás végrehajtói.„*(NATO, 2010)

2011. június 8-án a NATO védelmi miniszterek jóváhagyták a NATO újradefiniált kibervédelmi politikáját. E politika világos jövőképet határoz meg a kibervédelem területén az egész szövetség vonatkozásában, valamint egy kapcsolódó cselekvési terv végrehajtásáról is rendelkezik. 2011 októberében a miniszterek elfogadták e cselekvési terv részleteit is.

2012 februárjában, egy 58 millió eurós szerződés került megkötésre, amely a NATO kiberincidens kezelési képesség (NATO Cyber Incident Response Capability - NCIRC) teljes kiépítését tette lehetővé. Mindezekkel párhuzamosan a Szövetség egy úgynevezett kiberfenyegetés előrejelző központot (Cyber Threat Awareness Cell) is létrehozott annak érdekében, hogy fokozza a hírszerzési információk megosztását valamint a reális helyzetismeretet. (NATO, 2012)

Mindezekkel összhangban van a 2012-es chicagói csúcs után kiadott hivatalos állásfoglalás szerint: „*A számítógépes támadások továbbra is jelentősen növekedni fognak mind azok számát, mind azok kifinomultság és a komplexitását tekintve. Megerősítjük a lisszaboni csúcstalálkozón tett számítógépes védelmi kötelezettségvállalásainkat. Lisszabon után tavaly a NATO elfogadta a Cyber Védelmi Koncepció című politikát és cselekvési tervet, amely most kerül végrehajtásra. Építve a NATO meglévő képességeire, a NATO Számítógép Vészhelyzeti Incidenskezelő Képesség (NATO Computer Incident Response Capability -NCIRC) Teljes Műveleti Képessége (Full Operational Capability - FOC), beleértve a legtöbb helyszínt és a felhasználót, kialakításra kerül 2012 végéig. Vállaljuk, hogy biztosítjuk a forrásokat és véghezvisszük a szükséges reformokat ahhoz, hogy minden NATO alá tartozó szerv központosított számítógépes védelemben részesüljön, annak érdekében, hogy a fokozott számítógépes védelmi képességekkel megvédjük a kollektív NATO értékeket.*

*Tovább integráljuk a számítógépes védelmi intézkedéseket a Szövetség struktúrájában és folyamataiban, valamint minden egyes tagországában, és továbbra is elkötelezettek vagyunk mindazon nemzeti kibervédelmi képességek ügyében, amelyek erősítik az együttműködést és a kölcsönös átjárhatóságot a Szövetségen belül, többek között a NATO védelmi tervezési folyamatokban. Továbbra is fejleszteni fogjuk azokat a képességeinket, amelyekkel képesek vagyunk a megelőzésére, a felderítésére, a védelemre, és a számítógépes támadások következményeinek felszámolására. Arra törekszünk, hogy párbeszédet folytassunk a partner nemzetekkel, a nemzetközi szervezetekkel, többek között az EU-val, az Európa Tanáccsal, az ENSZ-el és az EBESZ-el, abból a célból, hogy a számítógépes biztonsági fenyegetésekkel kapcsolatban javítani lehessen a közös biztonságot és a konkrét együttműködést. Teljes mértékben kihasználjuk az észtországi Kibervédelmi Kiválósági Központ (Cooperative Cyber Defence Centre of Excellence – CCDCOE) által kínált szakértelmet.*" (NATO Chicago, 2012)

Ugyanezen csúcsértekezlet után került kiadásra a Védelmi Képességek: A NATO Erők 2020-ban (Summit Declaration on Defence Capabilities: Toward NATO Forces 2020)

dokumentum, amely a kiberbiztonságot szintén előtérbe helyezi. (Toward NATO Forces 2020)

## *Kibervédelmi stratégia az Európai Unióban*

Az Európai Unió, hasonlatosan az egyes országokhoz először a kritikus infrastruktúrák oldaláról közelítette meg a védelem kérdését. Ugyanakkor az uniós jogi és intézményi rendszer legtöbb elemével szemben, itt nem lehet tagállami gyakorlatokra és tapasztalatokra alapozni az európai lépéseket, és a kezdeti döntéseket úgy kellett meghozni, hogy erre sem az alapszerződésben, sem a másodlagos jogszabályokban nem volt utalás erre a területre.

A 2004 nyarán kezdődött meg az Európai Unió Bizottsága és Tanácsa felkérésére egy átfogó stratégia kidolgozása a létfontosságú infrastruktúrák védelmére. A Bizottság 2004 októberében közleményt fogadott el A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben címmel, amelyben javaslatokat tett arra vonatkozóan, hogyan lehetne az európai megelőzést, felkészültséget és a válaszadást javítani a létfontosságú infrastruktúrákat érintő terrortámadások tekintetében. (EC Commission, 2004. 1.) Ebben a közleményben a Bizottság meghatározást adott a kritikus infrastruktúra fogalmára, valamint meghatározta azokat az ágazatokat, melyek ide tartozhatnak.[17] (EC Comission, 2004. 2.)

Az Európai Bizottság 2005 novemberében tette közzé az úgynevezett Zöld Könyvét. (EC Commission, Zöld Könyv, 2005). A dokumentum 11 szektorra, és 37 termékre/szolgáltatásra osztotta az európai kritikus infrastruktúrákat. A Zöld Könyv nyomán lefolytatott konzultáció alapján 2006. december 12-én irányelv-javaslatot terjesztettek a Miniszterek Tanácsa elé Az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. (EC Commission, 2006)

Ezt követően folyamatos az elmozdulás a kritikus infrastruktúrák irányából a kiberbiztonság megteremtése és fokozása felé. 2010-ben megjelent a Digitális Menetrend 2010 dokumentum, amely az Európa 2020 Stratégia része, majd ezután az EU egyik – a kibertér védelmében talán legfontosabb – szervezetének az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) megerősítésére és modernizálására vonatkozóan közleményt adták ki. 2011

[17] A Miniszterek Tanácsa ezt követően két dokumentumot fogadott el a terrortámadások megelőzése, felkészültség és válaszadás területeken, majd a terrorfenyegetések- és támadások következményeivel kapcsolatos EU szolidaritási programot, amelyek alapján a 2004. december 16–17-i brüsszeli állam- és kormányfői csúcstalálkozó felszólította az Európai Bizottságot, hogy dolgozzon ki javaslatot egy Kritikus Infrastruktúra Védelmi Európai Programra.

márciusában tették közzé az Európai Bizottság közleményét a kritikus informatikai infrastruktúrák védelméről: „Eredmények és következő lépések: a globális kiberbiztonság felé” címmel (COM(2011) 163 final).

2013 év elején jelent meg az EU külügyi és biztonságpolitikai főképviselője és az Európai Bizottság által közösen kidolgozott új EU-s kiberbiztonsági stratégia. Ez az első olyan átfogó dokumentum, amelyet az Európai Unió a kiberbiztonság területén megalkotott. A stratégia nagyon egyértelmű célokat és prioritásokat tűz ki az EU nemzetközi kibertér-politikája terén, amelyek között a szabadság és nyitottság, a jogkövetés, a kiberbiztonsági kapacitások kiépítése, valamint a kibertérrel kapcsolatos nemzetközi együttműködés ösztönzése is megjelenik. (EC Cybersecurity Strategy, 2013)

# 2. Nemzeti kibervédelmi stratégiák

Az európai országok nemzeti szinten próbálnak választ adni arra a problémára, amely a kibertér egyre kiterjedtebb fontosságából és az ezzel összefüggő veszélyekből ered. Az európai országok kiberbiztonsági stratégiáinak elemzésekor láthatjuk, hogy számos ország az információs társadalom és annak biztonsági vetületei, más országok pedig a kritikus információs infrastruktúrák és azok biztonsági kérdései felől közelítik meg a kérdést.

A nemzeti, illetve kormányzati szintű kiberbiztonsági stratégiák – a korábban kifejtett okok miatt, országonként eltérő módon – a biztonságot, az információs társadalom fejlődését illetve zavartalan működését, illetve a kritikus információs infrastruktúrák védelmét külön-külön, vagy akár egyszerre is tárgyalják, illetve ezeket célozzák meg. Az ismertetésre kerülő nemzeti szintű kiberstratégiák alapvetően az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA – European Network and Security Agency)[18] ország értékeléseinek felhasználásával készültek.

[18] Az ENISA fő tevékenysége arra koncentrál, hogy az EU-ban a hálózat- és információbiztonság megfelelően magas szintű legyen. Ennek érdekében az ügynökség szaktanácsokkal segíti a tagállamok különböző hatóságait, valamint az uniós intézményeket a hálózat- és információbiztonság különböző kérdéseiben. Az ENISA fórumot biztosít ahhoz, hogy az érintettek megoszthassák egymással bevált módszereiket, továbbá elősegíti a kapcsolatépítést az uniós intézmények, a tagállami hatóságok és a vállalkozások között.

## *Magyarország*

Hazánkban az ezredforduló környékén alapvetően az információs társadalom építése, majd ennek fejlesztése volt az a stratégiai irány, amelyet az adott kormány fő célkitűzésnek tekintett a kibertér tekintetében. 2001-ben került kiadásra a Nemzeti Információs Társadalom Stratégia, amely alapvetően hét részben – Infrastruktúra-fejlesztési Program, Gazdaságpolitikai Program, Kultúra Program, Oktatási Program, Társadalompolitikai Program, Elektronikus Kormányzati Program, Önkormányzati Program – határozta meg azokat az alapvető célkitűzéseket, amelyek hazánkban az információs társadalom építéséhez elengedhetetlenek. (NITS, 2001)

Ezt a dokumentumot 2003-ban – újabb stratégia követte, amely a Magyar Információs Társadalom Stratégia néven került kiadásra. E stratégia célja volt, hogy Magyarországon tudásalapú gazdaságot létrehozva, az információs társadalom fejlesztésével az egyén és a közösség életminőségének és életkörülményének javítását lehessen elérni. (MITS, 2003)

2010-ben jelent meg a harmadik olyan hazai stratégia, amely az információs társadalom kialakítását, építését és fejlesztését célozta meg. A Digitális megújulás cselekvési terv 2010-2014 címet viselő dokumentum összhangban van az Európai Unió célkitűzéseivel és annak infokommunikációs programjaival. A stratégia alcíme Az infokommunikációs ágazat cselekvési terve a társadalom és a gazdaság megújulásáért, amely tükrözi az információs társadalom építésének és fejlesztésének érdekében szükséges kormányzati, gazdasági és össztársadalmi feladatokat. (DMCST, 2010)

Természetesen hazánkban is született a technikai oldal, azaz a kritikus infrastruktúrák védelmére irányuló kormányzati elgondolás. Ez a 2080/2008. (VI.30.) Korm. határozat A Kritikus Infrastruktúra Védelem Nemzeti Programról címet viseli. Ebben határozatban célozta meg a magyar kormány a teendőket és a felkészülés alapvető teendőit a kritikus infrastruktúrák védelmének területén. Ez a dokumentum, illetve kormányhatározat már tartalmaz utalásokat és némi kategorizálást a kritikus információs infrastruktúrák vonatkozásában, ugyanakkor a fogalom meghatározása, azaz, hogy mit tekintünk kritikus információs infrastruktúrának, annak részletes felsorolása, osztályozása, valamint a védelem konkrét feladatainak leírása azonban nem történt meg.

2012 áttörő változást hozott Magyarországon azzal, hogy a Nemzeti Biztonsági Stratégiába[19] kiemelt helyen került be, mint veszélyforrás a kiberkihívások jelentette veszély. Az új Nemzeti Biztonsági Stratégia, bár néhány helyen meglehetős trivialitásokat is tartalmaz – pl. bekerült a szövegbe a következő: „Az állam és a társadalom működése – a gazdaság, a közigazgatás, vagy a védelmi szféra mellett számos más területen is – mind meghatározóbb módon a számítástechnikára épül" (Nemzeti Biztonsági Stratégia, 2012) – mégis előremutató, hiszen államilag elfogadott, a nemzet biztonságát meghatározó stratégiai elvek először tartalmazzák e terület fontosságát és védelmének szükségességét. A stratégia természetszerűleg felméri a terület veszélyforrásait: „*Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem-állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését*." (Nemzeti Biztonsági Stratégia, 2012)

A stratégia ezt követően hangsúlyozza a nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmi vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására a koordinált védelem kialakítását, valamint az ezeken a területeken történő védelmi célú felkészülést.

Mindezek megvalósítására elsődleges feladatként a stratégia megjelöli a kibertérben jelentkező meglévő vagy potenciális fenyegetések és kockázatok rendszeres felmérését és priorizálását, a kormányzati koordináció erősítését, a társadalmi tudatosság fokozását, valamint a nemzetközi együttműködési lehetőségek kiaknázását.

2012 év végére elkészült a röviden csak Kritikus infrastruktúrákról szóló törvény,[20] amely a terület egyik legjobban várt jogszabálya volt, és amely számos utalást tartalmaz a kibertér különböző – nyilvánvalóan a kritikus infrastruktúrák vonatkozású – területein megteendő védelmi és a védekezésre felkészülést jelentő lépéssel kapcsolatosan.

2013 év elején a Kormány elfogadta a Nemzeti Kiberbiztonsági Stratégiát,[21] majd erre építve fogadta el a Parlament az úgynevezett Információbiztonsági törvényt.[22] Ez a törvény szintén

[19] 1035/2012. (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

[20] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[21] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

egy nagyon nagy űrt pótol hazánk kibervédelmében, mert végre törvényi alapokon szabályozott a kibervédelem területén szerepet kapó szervezetek mintegy 75-80 %-ának feladata, jog- és hatásköre.

## *Lengyelország*

Lengyelországban 2010-ben kezdődött meg a Kormányzati számítógépes biztonság 2011-2016 cselekvési terv[23] kidolgozása.

Az RPOC meghatározza a nemzeti információbiztonságban szerepet játszó minden szereplő feladatait és felelősségi körét, valamint az elérendő célokat a 2011 és 2016 közötti időszakban.

Lengyelországban a CERT közösség kulcsfontosságú szerepet játszik a kialakítandó kiberstratégia megalkotásában. A CERT GOV.PL csapat működési keretein belül létrehozott Belső Biztonsági Ügynökség (ABW) aktív szerepet tölt be a kormányzati CERT feladatainak megvalósulása során. Együttműködve a CERT Polskával, amely a legrégebbi nemzeti CERT, state-of-the-art korai előrejelző rendszert, az ARAKIS-GOV-ot működtetik annak érdekében, hogy valamennyi kormányzati hálózat vonatkozásában a malware-ekkel és más új biztonsági fenyegetésekkel szemben a védelmet biztosítani tudják.

A legnagyobb távközlési szolgáltatók Lengyelországban együttműködnek a kormánnyal különböző fórumok fenntartásában, amely fórumok a visszaélésekről, a közös kezdeményezésekről adnak számot, valamint együttműködési felülete biztosítanak a közös incidenskezeléshez.

2007-ben kezdődött meg a Lengyelország információs társadalom fejlesztési stratégia 2013-ig dokumentum kidolgozása. Ez a stratégiai dokumentum előirányozza egy olyan társadalom kialakítását, ahol az állampolgárok és a vállalkozások tudatosan használják az ICT nyújtotta lehetőségeket a gazdasági, társadalmi és kulturális fejlődés érdekében. Ennek hatékony támogatásával egy korszerű és felhasználóbarát közigazgatás létrehozása a cél.

[22] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[23] Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016, RPOC

Lengyelország információs társadalom stratégiája választ kíván adni a sajátos lengyel kihívásokra, ugyanakkor összhangba kívánja hozni mindezt az európai kezdeményezésre létrejött Európai digitális menetrenddel.

A stratégia számos elvet határoz meg Lengyelország információs társadalmának kialakításához, úgymint hozzáférhetőség, biztonság bizalom: hozzáférés biztosítása a megbízható információkhoz vagy biztonságos szolgáltatásokhoz, amelyek elengedhetetlenek a polgárok és a vállalkozások számára, a nyitottság és a sokszínűség: nincs preferencia az információhoz való hozzáférés, különösen a lakosság tájékoztatásának kérdésében, egyetemesség és elfogadhatóság: erőfeszítéseket kell tenni annak biztosítása érdekében, hogy aktívan részt vegyen minél több szereplő az információs társadalom kiépítésében, amely alapján az a lehető legnagyobb mértékben megvalósítható, és az információs társadalom termékei és szolgáltatásai minél szélesebb körben hozzáférhetővé váljanak, kommunikáció és interoperabilitás: az információ keresésére és hozzáférése a biztonságos, gyors és egyszerű legyen. (Enisa, Poland, 2009)

## *Cseh Köztársaság*

A Cseh Köztársaság új nemzeti biztonsági kutatási stratégiáját, amelyet a Belügyminisztérium dolgozott ki 2008-ban hagyta jóvá a cseh kormány. A stratégia középpontjában olyan prioritások felállítása került, amely a kiválóságot, a legjobb gyakorlatok elterjesztését és alkalmazását, valamint a beruházások racionalizálását célozta meg. Három fő területen határozott meg prioritásokat: a polgárok biztonsága (beleértve a terrorizmus elleni tevékenységet, a szervezett bűnözést, a polgári védelmet, a környezeti biztonságot, stb.), a létfontosságú infrastruktúrákat (beleértve az energia-, víz-, élelmiszer-, a közlekedés, banki és pénzügyi, az IKT szektorokat, stb.), valamint a válságkezelés (beleértve a korai figyelmeztetést és a felkészülést).

A stratégia meghatározott horizontális prioritásokat is, amelyek közül kiemelkedik az incidens előrejelzés és speciális forgatókönyvek kidolgozása, a készenlét (tudatosítása), az innováció, a felhasználók és eszközök azonosítása, valamint mindezek mellett a koordináció az EU-val.

Mindezeken túl 2011 januárjában elfogadásra került a Digitális Cseh Köztársaság stratégiai dokumentum, amely alapvetően a nagy sebességű hálózati hozzáférés fejlesztését volt hivatott

rendezni. E dokumentumban a fő prioritásként és fő célként jelenik meg a Cseh Köztársaság polgárainak és a vállalatainak nagy sebességű internet kapcsolatának kialakítása, valamint az, hogy mindenkinek legyen lehetősége az elektronikus kommunikációs technológiák használatára. A folyamat és a stratégia végrehajtásának, valamint a nyílt platformok cseréjének, és a legjobb gyakorlatok regionális és helyi szinten történő bevezetése és végrehajtása ellenőrzésére az Ipari és Kereskedelmi Minisztérium elindította a www.digitalnicesko.cz információs portált. Ezen a portálon közzéteszik a legfontosabb híreket, jogszabályokat, valamint az ajánlott technológiai megoldásokat. A stratégia előirányozza a pénzügyi források hatékony felhasználását pl. az Európai Beruházási Bank, a Vidékfejlesztési Alap és a strukturális alapok vonatkozásában.

2011-ben készült el és került kiadásra a Cseh Köztársaság Kiberbiztonsági stratégiája a 2011-2015 közötti időszakra, amely alapvetően a Cseh Köztársaság Nemzetbiztonsági Stratégiájára alapul. A stratégia fő célja, hogy a Cseh Köztársaság területén a számítógépes biztonság megszilárduljon, és létrejöjjön egy hiteles információs társadalom szilárd jogi alapokon. A dokumentum elkötelezett a biztonságos információtovábbítás és feldolgozás felé, valamint annak – az élet valamennyi területén történő –, szabad és biztonságos megosztása mellett. A dokumentumban nagyon fontos stratégiai célok kerültek megfogalmazásra, úgymint a területet meghatározó jogszabályi háttér kidolgozása, a közigazgatás és a kritikus infrastruktúrák kiberbiztonságának erősítése, nemzeti CERT ügynökség megalapítása, a nemzetközi együttműködés fokozása, együttműködés erősítése az állam, a magánszektor és az akadémiai szektorok között, illetve a kiberbiztonság tudatosságának növelése. (Enisa, Czech republic, 2009)

## *Szlovák Köztársaság*

2009 októberében a szlovák kormány elfogadta az új Információs Társadalom Stratégia 2009-2013 című dokumentumot. E stratégiai dokumentum – címének megfelelően – a Szlovák Köztársaság aktualizált információs társadalom stratégiáját rögzíti.

Az új stratégia felváltotta az eredeti Információs Társadalom Stratégiát és cselekvési tervet. Ennek oka elsősorban az volt, hogy az előző stratégia megjelenése (2004) óta eltelt időben olyan új kihívások és trendek jelentek meg, amelyekre már a régi stratégia nem tudott megfelelő és adekvát válaszokat adni. Ez a stratégia lefedi az addig rész-stratégiák által

kezelt területeket, ugyanakkor a korábban a rész-stratégiák által meghatározott területeket nem szabályozza részletesen.

Az átdolgozott stratégia meghatározza azokat a legfontosabb fejlesztési területeket és prioritásokat, amelyek a Szlovák Köztársaság információs társadalmának építése során elengedhetetlenek. Ilyenek például a szélessávú hozzáférés növelése, az információbiztonsági szabványok kidolgozása, az e-kormányzat és e-egészségügy fejlesztése, a digitális írástudás fejlesztése, az e-oktatás kialakítása, valamint az energiafogyasztás csökkentése és az energia hatékonyság növelése.

Meg kell még említeni Szlovákia Nemzeti Informatikai Biztonsági stratégiáját, amelyet a szlovák kormány 2008 augusztusában fogadott el. Ez a dokumentum három szintet tartalmaz. Az első szint leírja a hosszú távú információbiztonsági stratégiai célokat Szlovákia számára. A második szint a stratégiai prioritásokra összpontosít, a harmadik szint pedig feltárja a legfontosabb problémákat, valamint meghatározza az ezek kezelésével kapcsolatos feladatokat. A dokumentum nagyon világosan szétválasztja a hatásköröket, meghatározza a prioritásokat és a megteendő intézkedéseket. A dokumentum a nem minősített információk védelméhez szükséges feladatokat is meghatározza, azaz ajánlásokat tesz az információszivárgás, a jogosulatlan információ felhasználás és az adatok integritásának megsértése elkerülése érdekében.

2010-ben történt meg a Kiberbiztonsági Törvény előkészítése, amelyet a Szlovák Pénzügyminisztérium jegyzett, és amely törvény alapvetően a közigazgatás különböző ágazataiban használt információs rendszerek működését hivatott szabályozni. (Enisa, Slovakia, 2009)

# Irodalom


1035/2012. (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról

2008 Report to Congress of the U.S.-China Economic and Security Review Commission One Hundred Tenth Congress Second Session. U.S. Government Printing Office, Washington, November 2008.

Alberts, D. S., Gartska J. J., Stein, F. P. (1999): *Network Centric Warfare. Developing and Leveraging Information Superiority. 2nd edition (Revised).* (Library of Congress, Washington)

A NATO 2010-es új stratégiai koncepciója: Aktív Szerepvállalás, Modern Védelem Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról.

Az Európai Közösségek Bizottsága: A Tanács irányelve az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. Brüsszel, 12.12.2006 COM(2006) 787 végleges

Broad, W. J., Markoff, J., Sanger, D. E. (2011): *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*. In: New York Times, 2011. január 15. (http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&scp=2&sq=stuxnet&st=cse)

Brzezinski, Z. (1999): *A nagy sakktábla.* (Európa, Budapest)

Commission of the European Communities: Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the fight against terrorism, Brussels, 20.10.2004 COM(2004) 702 final (http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf)



Commission of the European Communities: Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the fight against terrorism, Brussels, 20.10.2004 COM(2004) 702 final (http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf)



Convention on Cybercrime, 2001. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp

Critical Foundations – Protecting America's Infrastructures. (Washington, 1997)

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (http://ec.europa.eu/information_society/newsroom/cf/document.cfm?doc_id=1667)

Denning, D. E. (2001): *Is Cyber Terror Next?* (http://essays.ssrc.org/sept11/essays/denning.htm)

Digitális Megújulás Cselekvési Terv 2010-2014. Nemzeti Fejlesztési Minisztérium, 2010.

Enisa country reports – Czech Republic. http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/CzechRepublic.pdf

Enisa country reports – Slovakia. http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Slovakia.pdf

Enisa country reports – Poland. http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Poland.pdf

Európai Bizottság, Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról , COM(2005) 576, 2005. november 17. (Commission of the European Communities: Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005 COM(2005) 576 final)

Gazdag Ferenc (szerk.) (2011): *Biztonsági tanulmányok – Biztonságpolitika*. (ZMNE, Budapest)

Haig Zs., Kovács L., Ványa L. (2006): *Információs hadviselés – információs terrorizmus – kiber-terrorizmus* (Verlag Dashöfer Szakkiadó, Budapest)

Haig Zs., Várhegyi I. (2005): *Hadviselés az információs hadszíntéren.* (Zrínyi, Budapest)

Haig Zs., Várhegyi I. (2008): *A cybertér és a cyberhadviselés értelmezése*. in: Hadtudomány, 2008. e. (http://www.zmne.hu/kulso/mhtt/hadtudomany/2008_e_2.pdf)

Haig Zs., Kovács L., Ványa L. (2008): *Kritikus információs infrastruktúrák támadása, védelme*. in: Dunaújvárosi Főiskola Közleményei, XXIX/1.

Haig Zs., Kovács L., Ványa L. (2011): *Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata.* in: Felderítő Szemle X./1-2.

Kovács L. (2003): *Az elektronikai felderítés korszerű eszközei, rendszerei és azok alkalmazhatósága a Magyar Honvédségben*. Doktori (PhD) értekezés (ZMNE, Budapest)

Kovács L. Sipos M. (2010): *A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala.* in: Hadmérnök 5/4. (http://www.hadmernok.hu/2010_4_kovacs_sipos.pdf)

Magyar Információs Társadalom Stratégia, 2003.

Magyar Virtuális Enciklopédia - Vörös Brigádok
http://www.enc.hu/1enciklopedia/fogalmi/poltud/vor_brig.htm

Muha L. (2007): *A Magyar Köztársaság információs infrastruktúráinak védelme.* Doktori (PhD) értekezés (ZMNE, Budapest)

NATO and cyber defense.
http://www.nato.int/cps/en/natolive/topics_78170.htm

NATO Chicago Summit Declaration.
http://www.nato.int/cps/en/SID-D95FAE1D-99C8ECE1/natolive/official_texts_87593.htm

NATO Summit Declaration on Defence Capabilities: Toward NATO Forces 2020
http://www.nato.int/cps/en/natolive/official_texts_87594.htm

Nemzeti Információs Társadalom Stratégia, 2001.

Prague Summit Declaration
http://www.nato.int/docu/pr/2002/p02-127e.htm

Schmitt, M. N. (edit.) (2013): *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, Cambridge)

Spiegel Online - Infizierte Regierungscomputer: Innenministerium bestreitet Schäden durch Hackerangriffe
http://www.spiegel.de/netzwelt/tech/0,1518,502008,00.html

Spiegel Online - Plagiate-Industrie: Chinesische Hacker spionieren deutschen Mittelstand aus
http://www.spiegel.de/wirtschaft/0,1518,465041,00.html

Szabó József (szerk.) (1995): Hadtudományi Lexikon. (MHTT, Budapest)

Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004.
(http://www.fbi.gov/congress/congress04/lourdeau022404.htm)

The Alliance's New Strategic Concept, NATO on-line library, Ministerial Communiqués,
http://www.nato.int/docu/comm/49-95/c911107a.htm

The Alliance's Strategic Concept
http://www.nato.int/docu/pr/1999/p99-065e.htm

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.
(http:// www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf)

Townshend, C. (2001): *A terrorizmus.* (Magyar Világ kiadó, Budapest)

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.