Sipos Zoltán hadnagy:

A KIBERTÉR BIZTONSÁGÁVAL KAPCSOLATOS ALAPVETŐ KÉRDÉSEK ÁTTEKINTÉSE

ÖSSZEFOGLALÓ: *Rohamosan fejlődő világunkban megfelelő hangsúlyt kell fektetni az interneten keresztül történő támadások kivédésére. A tanulmányban bemutatott példákon jól látható, hogy egy bárkit érintő globális jelenségről van szó, amely szorosan kapcsolódik a 21. századhoz, és a téma figyelmen kívül hagyása a későbbiekben súlyos problémák és károk forrása lehet.*

KULCSSZAVAK: *kiberbiztonság, kibertér, kibertámadás*

BEVEZETÉS

Mi is az a kiberbiztonság? Az ITU-T X 1205-ben közreadott megfogalmazás szerint „a kiberbiztonság eszközök, irányelvek, biztonsági koncepciók, biztonsági garanciák, kockázatelemzési módszerek, akciók, képzések, gyakorlatok gyűjteménye, melyek védelemre használhatóak, hogy megvédjék a kiberteret, szervezeteket és a felhasználókat. Szervezetek és felhasználók közé tartoznak a számítástechnikai eszközök, személyek, infrastruktúrák, alkalmazások, szolgáltatások, távközlési rendszerek, valamint a küldött és fogadott, vagy tárolt információk a számítógépes környezetben."[1]

Magyar vonatkozásban a kibertér definícióját Magyarország Nemzeti Kiberbiztonsági Stratégiájában találhatjuk: *„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint e rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."*[2]

A tendencia azt mutatja, hogy egyre növekszik a kibertéren keresztül érkező fenyegetések száma. Jelenleg a sajtóban csak kisebb mértékű eseményekről hallhatunk, mint például az Óbudai Egyetem honlapjának feltörése és tartalmának megváltoztatása. Későbbiekben viszont súlyosabb károk is bekövetkezhetnek. Józan mérlegelés szerint időben kell kijelölni a határokat és felkészülni a komolyabb fenyegetésekre, hogy esetleges bekövetkezésükkor konkrét forgatókönyv álljon rendelkezésre a lehetséges negatív következmények kivédésére, elhárítására. Minden esetben a megelőzés a helyes módszer.

2012-es adatok szerint Magyarországon a 15–69 év közötti korosztály 63%-a használ internetet, és az internetezők 75%-a próbálkozott már az online vásárlással.[3] A felhasználók

[1] Overview of cybersecurity. http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (Letöltés időpontja: 2015. 08. 03.)

[2] „A Kormány 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról." http://www.mysec.hu/download/MK2013_47_M_N_Kiberbiztonsagi_Stratagiaja.pdf (Letöltés időpontja: 2015. 08. 06.)

[3] Máté Zoltán: Tendenciák és irányok az internethasználatban a világon és Magyarországon az FMCG piacon. http://tudomany.szolnok-mtesz.hu/kulonszamok/2014/2014-18-09-Mate_Zoltan.pdf (Letöltés időpontja: 2015. 08. 12.)

arra törekszenek, hogy ügyeiket gyorsan és biztonságosan intézzék, ugyanakkor megszaporodtak az internetes lopások és a hitelkártya-visszaélések. Ez arra vezethető vissza, hogy az emberek nem fordítanak elég figyelmet az internet használatából adódó veszélyekre. A felhasználók gyanútlanul használják a világháló által biztosított közösségi felületeket (pl. Facebook, Twitter, Instagram stb.). Az internethasználat elterjedésével egyre gyakoribbá váltak a személyazonossággal való visszaélések is. Fontos komolyan venni a kibertámadásokat, hiszen az elmúlt évek során több olyan eset is történt, mely nemcsak egyéneket, hanem országokat is fenyegetett. Minden olyan esemény kibertámadásnak minősül, mely aláaknázza a számítógépes hálózat funkcióit bármely célból, legyen az politikai vagy nemzetbiztonsági indíttatású, vagy egyszerűen bűnözői szándék.[4]

AZ ELMÚLT ÉVEK KIBERESEMÉNYEINEK ÁTTEKINTÉSE

A kibertérben történő támadások egyre nagyobb kockázatot jelentenek a társadalomnak, és lassan egyfajta sajátos háborús szintet érnek el.

Az 1999-es Jugoszlávia elleni NATO-bombázást[5] kísérő események jó példát szolgáltatnak a korai kibertámadások bemutatására. A bombázást követően DDoS-támadások[6] indultak a NATO weboldalai ellen. A Jugoszláv Néphadsereg elektronikus úton összegyűjtött adatok segítségével értesítette a csapatokat a várható légicsapásokról. Titkos információkhoz nem sikerült hozzáférniük, de számos kormányzati oldalon helyezték el politikai üzeneteiket.

2007 áprilisában zavargások törtek ki Tallinnban egy második világháborús szovjet emlékmű eltávolítása során.[7] Ezt követően az észt államigazgatást az interneten keresztül rendszeres támadások érték, melyek főként arra irányultak, hogy az átlagos felhasználók ne érhessék el a kormányzati honlapokat. Az ország internetes forgalmát irányító központok többször kényszerültek leállásra a szokásoshoz képest közel ezerszeres adatforgalom miatt. A rendszerek nem bírták kezelni ezt az óriási túlterhelést, így a banki és a pénzügyi szolgáltatások megbénultak, illetve bizonytalanul működtek.[8] Észtország második legnagyobb bankjának, a SEB Eesti Uhisbanknak fel kellett függesztenie a külföldi banki rendszerekbe való belépést biztosító szolgáltatásait a folyamatos internetes támadások miatt. Egy másik észt bank, a Hansabank több mint egymillió dolláros forgalomkiesést szenvedett el.[9]

Az észt események hatására a NATO bejelentette, hogy kivizsgálja a helyzetet, de nem minősítette azt katonai akciónak. Korábban az észt külügyminiszter, Urmas Paet Oroszországot vádolta azzal, hogy pszichológiailag és fizikailag is támadja Észtországot.[10]

---

[4] Oona A. Hathaway: The law of cyber-attack. http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf (Letöltés időpontja: 2015. 08. 12.)

[5] Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése. http://uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf (Letöltés időpontja: 2015. 08. 01.)

[6] Distributed Denial of Service (DDoS) – túlterheléses támadás.

[7] Bányász Péter – Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. http://mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Banyasz_Peter_Orbok_Akos.pdf (Letöltés időpontja: 2015. 08. 07.)

[8] Muha Lajos: Kiberháború az orosz–észt viszony kapcsán. https://hacktivity.com/hu/letoltesek/archivum/17 (Letöltés időpontja: 2015. 08. 07.)

[9] Prof. Dr. Kovács László mk. ezredes: Biztonságpolitika. http://eiv.uni-nke.hu/uploads/media_items/biztonsagpolitika.original.pdf (Letöltés időpontja: 2015. 08. 07.)

[10] Muha Lajos: Kiberháború az orosz–észt viszony kapcsán – Hacktivity. https://www.youtube.com/watch?v=lkuBtq_jCeo (Letöltés időpontja: 2015. 08. 07.)

Az orosz–grúz háború megindítását is kibertámadással készítették elő, amely során nemcsak katonai, hanem civil „célpontokat" (áramszolgáltató egységeket, bankokat stb.) is támadtak az orosz nemzetiségűnek beazonosított hackercsoportok.[11]

Az elmúlt időszakban Ukrajnának is számos súlyos politikai, társadalmi és katonai kihívással kellett szembenéznie. A jelenkori Ukrajnában határváltozások, zavargások és nem ritkán vérontások teszik próbára az állam szervezettségét és a társadalom tűrőképességét. Mindezek mellett egy új jelenség, a kiberhadviselés is megjelent, amely lövések leadása nélkül is kemény hatással van a társadalomra. A DDoS-támadások során kommunikációs bénultság és félretájékoztatás zavarta össze az országot.[12]

A BAE Systems közlése[13] szerint 2014-ben 22 számítógépes támadás érte az ukrán rendszereket. Ezeket az akciókat igazi profik hajtották végre. A BAE nem határozta meg, hogy pontosan ki áll a támadások mögött, de utalt arra, hogy orosz érdekeltség lehet az ügy hátterében. Erre abból lehet következtetni, hogy a vírus kódolása orosz nyelvű volt, és egy olyan logót hagytak a hackerek, ami visszavezethető az amerikai bázisok ellen 2008-ban elkövetett támadások során használt szimbólumra.

Fontos megemlíteni egy 2008-as, a Baku–Tbiliszi–Ceyhan[14] kőolajvezetéket érintő esetet, mely megközelítőleg egymilliárd dollárnyi exportbevétel kiesését okozta. A robbanást megelőzően a rendszer nem adott vészjelzést, és a kamerák sem rögzítettek semmit a tűz lángra kapásáról. A katasztrófa során 30 ezer hordó olaj ömlött ki, károsítva ezzel a természetet. Feltételezések szerint hackercsoport tört be a rendszerbe, melynek tagjai lekapcsolták a kőolajvezetékek vészjelzőit, elvágták a kommunikációs vonalakat, majd növelték a nyomást a vezetékben, így – az ott dolgozókat megtévesztve – fel tudták robbantani a vezetéket. Bár a kamerákat sikeresen leállították a robbantás előtt és 60 órányi anyagot eltávolítottak, egy másik rendszerre kötött infravörös kamera felvételeiből jól látható, hogy az incidens előtt két fekete, katonai jellegű ruházatot viselő ember laptopokkal járkált a vezeték mellett.

Iránban a Stuxnet nevezetű vírus okozott óriási gondokat a búsehri erőmű egyik rendszerén. „A Stuxnet egy olyan különleges számítógépes féreg, amely a Microsoft Windows operációs rendszert futtató gépeket fertőzi, és azokon terjed, de hatását végső soron ipari folyamatirányító rendszereken keresztül fejti ki. Támadja a folyamatok felügyeleti irányítását és adatgyűjtését, és nemcsak kémkedik a célzott ipari rendszer után, hanem át is programozza azt."[15] A vírus magára az erőműre lényegében nem jelentett fenyegetést, mert az urándúsító berendezések voltak a célpontjai. A vírus kódja az 1979. május 9-ei hivatkozást tartalmazta, és ez a dátum pontosan egybeesik azzal a nappal, amikor kivégezték Habib Elghanian zsidó üzletembert Iránban Izrael részére történt kémkedés vádjával. A sikeres vírustámadás eredménye az lett, hogy Irán 2010. november 16-án több hónapra kénytelen volt leállítani az urándúsítást, mert a Stuxnet tevékenységének eredményeképpen a centrifugák több mint 20%-a megsérült.

---

[11] Besenyő János: Újfajta háború? Internetes hadviselés Grúziában. Seregszemle, VI. évfolyam, 3. szám, 2008. december, 61–63.

[12] Cyber war in Ukraine: How NATO is helping the country defend itself against digital threats. http://www.zdnet.com/article/ukraines-cyber-warfare-how-nato-helps-the-country-defend-itself-against-digital-threats/ (Letöltés időpontja: 2015. 08. 08.)

[13] http://www.baesystems.com/home (Letöltés időpontja: 2015. 08. 08.)

[14] Jordan Robertson – Michael Riley: Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar. http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar (Letöltés időpontja: 2015. 08. 11.)

[15] Cserháti András: A Stuxnet vírus és az iráni atomprogram. Fizikai Szemle, 2011/5, 150–155. http://fizikaiszemle.hu/fsz1105/cserhati1105.html (Letöltés időpontja: 2015. 07. 26.)

2014-es adatok szerint Izrael a kiberhadviselés egyik vezető szerepet játszó állama. Az állami szektor figyelme fokozatosan fókuszál az internetes tevékenységek védelmének fontosságára. Egyre több állam követi a kibervédelem kiépítésének izraeli példáját, mert a közel-keleti ország szakemberei lenyűgöző tehetséggel és technikával védik meg, illetve használják szoftvereiket és szolgáltatásaikat.[16] Izraeli szakértők tárták fel azokat a hiányosságokat is, melyek az Alibaba[17] internetes vásárlófelületet érintették.[18] Ez a biztonsági rés lehetővé tette volna külső támadók részére, hogy „eltérítsék" a vásárlásokat, megváltoztassák a küldemények adatait, és akár le is állítsák a vásárlás folyamatát. Ezt követően egy kínai kiskereskedelmi cég is bejelentette, hogy befektet az izraeli kiberbiztonsági kezdeményezésekbe, hogy megvédje magát a hackerektől.

Mivel ma már a katonaság és az informatika szoros kapcsolatban állnak egymással, így Tel-Aviv fontosnak tartotta, hogy megfelelő állami kiberbiztonsági lépéseket tegyen, ezért a hírszerzés szervezetén belül létrehozták a kiberhadviseléssel foglalkozó 8200-as kódnevű szervezetet. Bár Izrael informatikai rendszerei fejlettek, nemcsak támadó félként, de sokszor megtámadottként is részt vesz a kiberhadviselésben. Nagy port vert fel, amikor pár évvel ezelőtt az Anonymous hackercsoport intézett állítólagos hackertámadást Izrael két kormányzati weblapja ellen. Izrael cáfolta a történéseket, és arra hivatkozott, hogy szerverek meghibásodása miatt történt a leállás. Két kormányzati honlap, a Moszad és az Israel Defense Forces (IDF) is leállt. A Moszad oldalán karbantartási felirat szerepelt, az IDF pedig nem volt elérhető.

Az Anonymous hackercsoport egy a YouTube-ra feltett videóval[19] válaszolt Izraelnek, miszerint azért történtek meg részükről ezek a lépések, mert az izraeli erők nemzetközi vizeken tartóztattak fel egy kanadai és egy ír hajót, ráadásul át is szálltak azok fedélzetére. A hackercsoport illegálisnak nevezte a gázai tengeri blokádot, és folyamatos hackertámadásokat helyezett kilátásba, amíg nem történik változás a blokáddal kapcsolatban. A csoport azóta is folyamatosan igyekszik támadni a különböző izraeli érdekeltségeket.

2002 óta számos internetes behatolás elkövetése írható Kína számlájára.[20] Kínában folyamatos a gazdasági növekedés, mely a gyengébb időszakokban is 7–8%-os volt. Kína növekvő aktivitása számos kihívás elé állítja az országokat. A kínai kibertevékenységet mi sem bizonyíthatná jobban, mint hogy egyes országokból kínai termékeket tiltottak ki ipari kémkedés vádjával. Ennek az volt az oka, hogy a kínai gyártók néhány – az egyes gyártmányaikon futó – szoftverrel és azok funkcióival nem tudtak elszámolni. Kína és az Amerikai Egyesült Államok megállapodott abban, hogy létrehoznak egy olyan közös csoportot, mely képes lesz felszámolni a kiberbiztonság területén felmerülő problémákat, és egyúttal megelőzi a hackertámadásokat, amelyek a pénzügyi szektorra, a bankokra és az élet bármely egyéb területére jelentenek fenyegetést. Fontosnak tartják, hogy minden országnak meg kell védeni polgárait, azok jogait és az ország infrastruktúráját a váratlan támadásokkal szemben.

---

[16] Gil Baram: The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case. http://www.inss.org.il/uploadImages/systemFiles/MASA5-1Eng4_Baram.pdf (Letöltés időpontja: 2015. 08. 12.)

[17] A www.alibaba.com Kína legnagyobb online kiskereskedelmi honlapja.

[18] Alibaba invests in Israeli cyber-security. http://www.israel21c.org/alibaba-invests-in-israeli-cyber-security/ (Letöltés időpontja: 2015. 08. 10.)

[19] https://www.youtube.com/watch?v=q760tsz1Z7M (Letöltés időpontja: 2015. 08. 07.)

[20] Prof. dr. Kovács László mk. ezredes: Biztonságpolitika. http://eiv.uni-nke.hu/uploads/media_items/biztonsagpolitika.original.pdf (Letöltés időpontja: 2015. 08. 07.)

Észak-Korea kiberműveleteiért a 121-es egység felelős. Komoly tevékenységről van szó, mert az eredetileg 1000 fős egység létszámát mára 17 000 fősre emelték. Amennyiben úgy adódna, akkor egy város működését is képesek lennének megbénítani, mert a legbonyolultabb számítógépes rendszerekbe is képesek behatolni. A Sony Pictures[21] tervezett egy vígjátékot, melynek lényege az észak-koreai vezető elleni fiktív merénylet volt. Nem sokkal ez után a Sony számítógépes hálózatát feltörték, melynek során bizalmas vezetői e-mailek szivárogtak ki.[22]

A fent említett példák jól demonstrálják, hogy vannak országok, melyek váratlan támadások elszenvedőiként élik meg a kibereseményeket. Ugyanakkor egyes országoknál felkészültek a támadások elhárítására, megfelelő erőt és pénzt csoportosítanak az informatikai szektorra annak biztonsága és fenntarthatósága érdekében, illetve képesek aktív, vagyis támadó tevékenységre is.

AZ ÁLLAMI ÉS ÖNKORMÁNYZATI SZERVEK ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGÁRÓL SZÓLÓ 2013. ÉVI L. TÖRVÉNY

A törvény létrejöttének oka a „társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.

Az elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell az elektronikus információs rendszerben kezelt adatok és információk bizalmasságát, rendelkezésre állását és sértetlenségét, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét."[23]

KITEKINTÉS AZ INFORMÁCIÓVÉDELEMMEL KAPCSOLATOS FELSŐ SZINTŰ MEGÁLLAPÍTÁSOKRA

„A magyar kormány 2012-ben fogadta el Magyarország új Nemzeti Biztonsági Stratégiáját, amely több szempontból is különbözik az eddigi stratégiai dokumentumoktól. A 2002-ben, illetve 2004-ben elfogadott stratégiákkal összehasonlítva a nyugati, azon belül is az Egyesült Államok stratégiaalkotásához közelítő tendencia figyelhető meg a dokumentum szerkezetében és tartalmában."[24]

[21] Sony hack: North Korea back online after internet outage. http://www.bbc.com/news/world-asia-30584093 (Letöltés időpontja: 2015. 07. 27.)

[22] Jordan Wilson: China's Position on the Sony Attack: Implications for the U.S. Response. http://origin.www.uscc.gov/sites/default/files/Research/China's%20Position%20on%20the%20Sony%20Attack_0.pdf (Letöltés időpontja: 2015. 08. 12.)

[23] 2013. évi L. törvény az állam és önkormányzati szervek elektronikus információbiztonságáról. http://www.complex.hu/kzldat/t1300050.htm/t1300050.htm (Letöltés időpontja: 2015. 09. 09.)

[24] Kiss Petra: A magyar stratégiai gondolkodás változása a nemzeti biztonsági stratégiák tükrében. http://www.mhtt.eu/hadtudomany/2012/3_4/HT_2012_3-4_Kiss_Petra.pdf (Letöltés időpontja: 2015. 08. 13.)

A biztonsági stratégiai nem más, mint az állam – illetve a szövetségi rendszer – politikájának megtervezett és összehangolt, központilag irányított megfogalmazása és a megvalósítás érdekében tett intézkedések összessége.[25]

MAGYAR STRATÉGIAI SZINTŰ KÖVETELMÉNYEK

„A globális biztonsági környezetben zajló rendkívüli dinamikájú és méretű változások kiszámíthatatlanságot okoznak. Ebben a globalizált világban a modern technológia alkalmazása és az erősödő gazdasági kapcsolatok következtében az egyes államok és térségek növekvő mértékben függenek egymástól, a biztonság külső és belső tényezői összekapcsolódnak. A biztonság összetett, és elemei szorosan összefüggenek egymással, ezért a honvédelem ügyét nem lehet a biztonság más területeitől elválasztva, önmagában értelmezni – a biztonsági kihívások kezelése összehangolt kormányzati működést kíván meg."[26]

Új kihívást és potenciális veszélyforrást jelent a kibertér hozzáférhetősége, használata, s ebből is kiemelkedik a számítógépes hálózatok elleni támadások növekvő száma és károkozási potenciálja. Az „1035/2012. sz. Kormányhatározat Magyarország Nemzeti Biztonsági Stratégiájáról" címmel 2012 márciusában hatályba lépett aktuális biztonsági stratégia megállapítja, hogy a rendszerek sebezhetősége olyan kockázati tényező, amelynek jellegzetessége, hogy a felkészült rosszindulatú támadó minimális erő összpontosításával nagy távolságokból is rendkívüli mértékű károkat képes okozni. A korszerű, biztonságos informatikai infrastruktúra kialakítása és a kormányzati rendszerek védelme ezen okból kifolyólag nélkülözhetetlen szemponttá vált, hiszen a kormányzati információs rendszert fel kell készíteni a támadások elleni védekezésre. A kiberfenyegetéseknek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát.

„Az információs társadalom kialakulásának hatása a nemzeti és nemzetközi biztonság valamennyi területén érezhető. A folyamat számos pozitív hatása mellett természetesen megjelentek e fejlődés negatív vonatkozásai is. Az egyes állami és nem állami szereplők által alkalmazott modern infokommunikációs eszközök biztonsági kockázat előidézéséhez járulhatnak hozzá."[27]

„A Magyar Honvédség egyik célja a hálózatalapú hadviselés feltételeinek megteremtése. Ennek részeként erősíteni kell a Magyar Honvédség kibervédelmét, amihez koncepcionálisan megalapozott rendszabályok kidolgozása, modern eszközök beszerzése, valamint az állomány megfelelő felkészítése és kiképzése szükséges."[28]

A Magyar Információs Társadalom Stratégia (továbbiakban: MITS) Informatikai Biztonsági Részstratégiája az információs társadalom biztonságossá tételének hosszú távú célját megvalósító út első lépése. Ahogy írják: „A stratégia céljainak megvalósításához a biztonsági elvárások teljesítményét kormányzati szinten támogatni és koordinálni kell, továbbá

[25] Jávor Endre: A biztonsági stratégia kidolgozása során érvényesítendő elvek és módszerek. http://www.zmne.hu/kulso/mhtt/hadtudomany/2000/2_3.html (Letöltés időpontja: 2015. 09. 01.)

[26] Magyarország Nemzeti Katonai Stratégiája, 2012. http://www.kormany.hu/download/a/40/00000/nemzeti_katonai_strategia.pdf (Letöltés időpontja: 2015. 08. 13.)

[27] Magyarország Nemzeti Katonai Stratégiája, 2012.

[28] Magyarország Nemzeti Katonai Stratégiája, 2012, 82. pont.

szükség van az informatikai rendszerek fejlesztőinek, felhasználóinak, üzemeltetőinek aktív közreműködésére is."[29]

A MITS fő céljai között szerepel az információbiztonsági tudatosság és az ismeretek fejlesztése, mely célok megvalósításához az alábbi főbb feladatok esetében komoly előrelépésre van szükség (a teljesség igénye nélkül):

- „a jogszabályi és intézményi környezet biztosítása,
- a biztonsági követelmények kidolgozása, nemzetközi szabványok honosítása,
- a biztonságos információs rendszerek kialakításának és fenntartásának támogatása,
- a biztonsági szempontok érvényesítése a fejlesztés, tervezés és üzemeltetés során,
- az informatikai biztonsági szempontok érvényesítéséhez szükséges források megteremtése."

KÜLFÖLDI SZEREPVÁLLALÁS

Fontosnak tartom a NATO követelményrendszerének bemutatását az információs vonatkozások szempontjából, mert annak a Magyar Honvédségben a fejlesztések alapját kell képeznie.

Napjaink új hadviselési formája a hálózatközpontú hadviselés, mely hozzájárul a vezetés felgyorsulásához. A gyorsabb vezetés alapja pedig nem más, mint „az információs fölény, az erők sebességben, precizitásban és reagálóképességben megnyilvánuló hatásalapú alkalmazása",[30] mely lehetővé teszi a technológiai, helyzeti vagy mennyiségi hátrányok ellensúlyozását.

A NATO hálózat által biztosított képességének (NATO Network Enabled Capability) a célja olyan környezet felépítése, ahol az adatgyűjtő elemek, a döntéshozók és a szükséges hatásokat kiváltó erők egy alhálózatokból álló hálózatba integrálódnak, bármely helyszínről megfelelő formában és időben biztosítva a felhasználók számára a szükséges adatokat.[31]

A NATO komolyan vette az egyre gyakoribbá váló kibertámadásokat, és 2008. május 14-én létrehozta a NATO Kibervédelmi Kiválósági Központot[32] (NATO Cooperative Cyber Defence Centre of Excellence – NATO CCD COE), melynek Magyarország is tagja. A központ célja, hogy összegyűjtsön minden olyan információt, amely kapcsolatban áll a kibertérrel, és amely a 21. századi kiberbiztonság fenntartásához szükséges. A központ székhelye Észtország fővárosában, Tallinnban található, és 2008. október 28-tól jogilag is nemzetközi katonai szervezetnek minősül.

Finanszírozási szempontból nem szövetségi támogatású, működését a benne szerepet vállaló szponzorállamok biztosítják. Észtország a szükséges infrastruktúrával és az adminisztratív költségekkel járul hozzá a működéséhez, a szakemberek és kutatók fizetését pedig a támogató országok, azaz Lengyelország, Lettország, Litvánia, Magyarország, Németország, Olaszország, Spanyolország, Szlovákia és az Amerikai Egyesült Államok biztosítják. A központ minden év júniusában konferenciát szervez, melynek középpontjában az aktuális kiberbiztonsági kérdések állnak.

---

[29] Magyar Információs Társadalom Stratégia, 2013. http://itf.njszt.hu/23r4r23r/uploads/2013/08/MITS-magyar.pdf (Letöltés időpontja: 2015. 08. 13.)

[30] Arthur K. Cebrowski – John J. Garstka: Network-Centric Warfare: Its Origin and Future. 1998. http://www.kinection.com/ncoic/ncw_origin_future.pdf (Letöltés időpontja: 2015. 09. 03.)

[31] Information Superiority and NATO Network-Enabled Capability. www.act.nato.int (Letöltés időpontja: 2015. 09. 08.)

[32] A NATO Kibervédelmi Kiválósági Központja. http://old.biztonsagpolitika.hu/?id=16&aid=1148&title=a-nato-kibervedelmi-kivalosagi-kozpontja (Letöltés időpontja: 2015. 07. 26.)

A felhasználókkal szembeni problémák akár 80%-át meg lehetne előzni azzal, ha körültekintőbben használnánk az információs teret. A kormányok közötti bizalmatlanság azt eredményezi, hogy a tapasztalatmegosztás csekély, vagy teljes mértékben elmarad – miközben a támadók köreiben jellemző a szoros együttműködés –, így azok egy lépéssel mindenben előrébb járnak. Akik próbálják kiküszöbölni a kibertámadásokat, sokszor jogi akadályokba ütköznek, melyek lassítják, illetve gátolják munkájukat, az illegálisan tevékenykedők azonban, akik kárt akarnak okozni, minden probléma nélkül képesek azt megtenni. Nem elég a kormányszintű összefogás, fontos lenne bevonni a magánszférát is, főképpen a nagyobb vállalatokat, mert a gazdasági szféra is nagyszámú támadással szembesül, melyeket szakemberek, illetve forrás hiányában nem minden esetben képesek elhárítani.

A közelmúltban hazánkban is történtek lépések az internetbiztonság kihívásainak való megfelelés érdekében. 2015. október 1-jén megalakult az állami és önkormányzati szervek elektronikus információs rendszerei védelmét támogató Nemzeti Kibervédelmi Intézet, az NKI. Az intézet az újragondolt szervezeti rendszerben, a kérdéskörrel foglalkozó szervezeteket, feladatokat és szolgáltatásokat fogja össze, koordinálja és végzi.[33]

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A kiberbiztonság kérdésköre napjainkban dinamikus fejlődés előtt áll, s korunk egyértelműen megköveteli a Magyar Honvédségtől is, hogy lépést tartson ezzel. Azért választottam írásom témájául a kibertér biztonságával kapcsolatos alapvető kérdések bemutatását, hogy az olvasó lássa, mennyire komoly fenyegetéssel kell szembenéznünk.

Az információs társadalmat érő fenyegetések miatt kiemelten fontos a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.

Nem elég csak a kormányoknak és az országoknak összefogniuk, a magánszemélyekre is súlyos felelősség hárul. Az interneten keresztül érkező fenyegetések mellett az egyéni hibákat sem zárhatjuk ki. Az egyének által elkövetett hibák, legyenek azok akár szándékosak vagy nem szándékosak, a végeredmény szempontjából hasonló pusztító hatást képesek kifejteni. Elég egy otthoni vírusos gépbe csatlakoztatott külső adathordozó, ami a munkahelyi számítógépbe helyezve máris fertőzi az értékes adatokat tároló hálózatot.

Az újfajta fenyegetések tárháza és lehetősége óriási, akár kis költésvetésből is kivitelezhető, bármiféle katonai beavatkozás nélkül. Egy karosszékből a Föld bármely pontján lévő célpontokat meg lehet semmisíteni egy gomb vagy billentyű megnyomásával. Az újfajta fenyegetés elleni felkészülést és védelmet igen fontos komolyan venni.

A legnagyobb probléma az, hogy a bonyolult, összetett és eltérő jogszabályi háttér, az eltérő struktúrák, technológiai és gazdasági érdekek, valamint a partnerségi bizonytalanság miatt nem egyszerű az országok közötti együttműködés. Ugyanakkor a támadó felek úgy tudnak együttműködni, hogy fizikailag nem is kell egymáshoz közel lenniük, akár a világ más-más pontján is tevékenykedhetnek. Azért nehéz a kibervédelmet összpontosítani, mert a kibertámadások kiszámíthatatlanok és nehezen nyomon követhetőek.

Több ország felismerte annak fontosságát, hogy az új típusú támadás jellemzően alacsonyabb anyagi ráfordítást igényel, mint a hagyományos támadások, és viszonylag egyszerű

[33] http://www.honvedelem.hu/cikk/53822_megalakult_a_nemzeti_kibervedelmi_intezet (Letöltés időpontja: 2015. 10. 29.)

az informatikai szférára pénzt fordítani ahelyett, hogy hosszú éveken át képeznének ki katonákat. A híreket követve egyre több kibereseménnyel találkozhatunk, és a nagy kérdés az, hogy a világ felkészült-e ezekre a támadásokra. A digitalizált világban számítógépek egyik pillanatról a másikra vehetik át épületek vagy akár egész városok irányítását. A megfelelő biztonsági lépések megtétele nélkül védtelenek leszünk a támadásokkal szemben, melyek óriási pusztítással is járhatnak. A tét igen nagy, és a biztonság létfontosságú mindenki számára. A fő célnak az esetleges incidensek és konfliktusok megelőzését kell tekinteni.

FELHASZNÁLT IRODALOM

2013. évi L. törvény az állam és önkormányzati szervek elektronikus információbiztonságáról. http://www.complex.hu/kzldat/t1300050.htm/t1300050.htm

A Kormány 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. http://www.mysec.hu/download/MK2013_47_M_N_Kiberbiztonsagi_Stratagiaja.pdf

A NATO Kibervédelmi Kiválósági Központja. http://old.biztonsagpolitika.hu/?id=16&aid=1148&title=a-nato-kibervedelmi-kivalosagi-kozpontja Alibaba invests in Israeli cyber-security. http://www.israel21c.org/alibaba-invests-in-israeli-cyber-security/

Anonymous #OpIsrael https://www.youtube.com/watch?v=q760tsz1Z7M

http://www.baesystems.com/home

Baram, Gil: *The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case*. http://www.inss.org.il/uploadImages/systemFiles/MASA5-1Eng4_Baram.pdf

Bányász Péter – Orbók Ákos: *A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében*. http://mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Banyasz_Peter_Orbok_Akos.pdf

Besenyő János: *Újfajta háború? Internetes hadviselés Grúziában*. Seregszemle, VI. évfolyam, 3. szám, 2008. december.

Cebrowski, Arthur K.: *Network-Centric Warfare: Its Origin and Future*. 1998. http://www.kinection.com/ncoic/ncw_origin_future.pdf

Cyber war in Ukraine: How NATO is helping the country defend itself against digital threats. http://www.zdnet.com/article/ukraines-cyber-warfare-how-nato-helps-the-country-defend-itself-against-digital-threats/

Cserháti András: *A Stuxnet vírus és az iráni atomprogram*. Fizikai Szemle, 2011/5. http://fizikaiszemle.hu/fsz1105/cserhati1105.html

Hathaway, Oona A.: *The law of cyber-attack*. http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf

http://www.honvedelem.hu/cikk/53822_megalakult_a_nemzeti_kibervedelmi_intezet

Information Superiority and NATO Network-Enabled Capability. www.act.nato.int

Jávor Endre: *A biztonsági stratégia kidolgozása során érvényesítendő elvek és módszerek*. http://www.zmne.hu/kulso/mhtt/hadtudomany/2000/2_3.html

Kassai Károly: *Kiberveszély és a Magyar Honvédség.* Hadmérnök, VII. évfolyam, 4. szám, 2012. december. http://hadmernok.hu/2012_4_kassai.pdf

Kiss Petra: *A magyar stratégiai gondolkodás változása a nemzeti biztonsági stratégiák tükrében*. http://www.mhtt.eu/hadtudomany/2012/3_4/HT_2012_3-4_Kiss_Petra.pdf

Prof. dr. Kovács László: *Biztonságpolitika*. http://eiv.uni-nke.hu/uploads/media_items/biztonsagpolitika.original.pdf

Magyar Információs Társadalom Stratégia, 2013. http://itf.njszt.hu/23r4r23r/uploads/2013/08/MITS-magyar.pdf

Magyarország Nemzeti Katonai Stratégiája, 2012. http://www.kormany.hu/download/a/40/00000/nemzeti_katonai_strategia.pdf

Máté Zoltán: *Tendenciák és irányok az internethasználatban a világon és Magyarországon az FMCG piacon*. http://tudomany.szolnok-mtesz.hu/kulonszamok/2014/2014-18-09-Mate_Zoltan.pdf

Muha Lajos: *Kiberháború az orosz–észt viszony kapcsán*. (Hacktivity.) https://www.youtube.com/watch?v=lkuBtq_jCeo, https://hacktivity.com/hu/letoltesek/archivum/17

Overview of cybersecurity. http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Robertson, Jordan–Riley, Michael: *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*. http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

Sony hack: North Korea back online after internet outage. http://www.bbc.com/news/world-asia-30584093

Szentgáli Gergely: *A NATO kibervédelmi politikájának fejlődése*. http://uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf

Wilson, Jordan: *China's Position on the Sony Attack: Implications for the U.S. Response*. http://origin.www.uscc.gov/sites/default/files/Research/China's%20Position%20on%20the%20Sony%20Attack_0.pdf