Bányász Péter−Orbók Ákos

A NATO KIBERVÉDELMI POLITIKÁJA ÉS KRITIKUS INFRASTRUKTÚRA VÉDELME A KÖZÖSSÉGI MÉDIA TÜKRÉBEN[1]

Rezümé:
Századunkra egyfajta paradigmaváltás figyelhető meg az információs hadviselés terén. Az informatika terén végbemenő változások új kihívások elé állítják a nemzetek biztonságát. Jelen tanulmány azokat a veszélyeket kívánja bemutatni, melyeket egy kibertámadás jelenthet egy ország kritikus infrastruktúrájára. A támadók csupán számítógép-hálózatok felhasználásával, anélkül, hogy konvencionális hadviselést alkalmaznánk, a „digitális kőkorszakba"bombázhatják vissza a megtámadott országot. A szerzők arra tesznek kísérletet, hogy bemutassák azokat az új eszközöket, amelyekkel kivitelezhető egy ilyen támadás.
***Kulcsszavak**:*
kritikus infrastruktúra, kibervédelem, információbiztonság, közösségi média, NATO

Bányász, Péter – Orbók, Ákos

NATO'S CYBER DEFENCE POLICY, FURTHERMORE CRITICAL INFRASTRUCTURE PROTECTION IN THE LIGHT OF SOCIAL MEDIA

Abstract:
To our century it can be observed a kind of paradigm change in the field of information warfare. Changes in the information technology are generated new challanges in the security of nations. This study demonstrates the danger of a possible cyber attack at a country's CI. The attackers use only computer networks, without applying the conventional warfare, they could put the attacked country back into the "Digital Stone Age". The authors make an attempt at to show the new tools, whereby can be carried out the above mentioned attack.
Keywords:
critical infrastructure, cyber security, information security, social media, NATO

Új kor virradt 2012. július 19-én. Barack Obama, az Amerikai Egyesül Államok elnöke benyújtja a Szenátus elé a Kibervédelmi törvénytervezetet, amely világosan jelzi, megváltozott világunkban az információs műveletek alapjaiban rendezték át a hadviselés fogalmát, módozatait. [1] A dátum azért meghatározó, mert az egyre többször megfogalmazott igényt, mi szerint megfelelő választ kell adni napjaink egyik

[1] A Magyar Hadtudományi Társaság 2012. évi pályázatán I. helyezést elért tanulmány a Kritikus Infrastruktúra Védelmi Kutatások TÁMOP-4.2.1. B-11/2/KMR/001 Civil-katonai partnerség alprogram Közlekedési kritikus infrastruktúra védelem kiemelt kutatási terület támogatásával készült el.

legnagyobb kihívására, a kibertámadásokra, a legmagasabb szinten kezdték prioritásként kezelni.

De nem csak az USA ismerte fel az ezzel kapcsolatos veszélyeket. Az Europol igazgatóhelyettese, Troels Oerting arra hívta fel a figyelmet a hamarosan beinduló új kiberbűnözésre szakosodott központ elindítása kapcsán, hogy az európai kormányoknak fel kell készülnie a több milliárd eurós károkat okozó támadások elhárítására. [2] A veszélyt mi sem példázza jobban, minthogy 2011-hez képest 400%-al növekedett a kibertámadások száma. [3] Felmérések szerint Kína – amellett, hogy őt vádolják a legnagyobb számú kibertámadás végrehajtásával – szenvedi el a legtöbb online támadást. [4] A nyugati országok mellett a keletiek is egyre nagyobb figyelmet fordítanak erre a területre. Kína mellett India is védelmi prioritásként jelölte meg kibervédelmi képességeinek erősítését. A döntés hátterében azon félelem áll, hogy a Stuxnet-szerű támadásokkal az indiai nemzeti kritikus infrastruktúrák működési feltételeit ronthatják. Ennek érdekében Manmohan Singh miniszterelnök, aki egyben a Nemzetbiztonsági Tanács vezetője is, felhatalmazást adott Defence Intelligence Agency-nek és a National Technical Research Organisation-nek, hogy szükség esetén nem részletezett támadó műveleteket hajtson végre. [5]

A kibertér lényegéből fakadóan mégis egy olyan terület, ahol nem lehet azt a fajta hadviselést alkalmazni, ami az elmúlt évezredekben bevett gyakorlatnak számított. Ez a fejlődés nagyban elősegíti az aszimmetrikus hadviselés vívását, ami a terroristáknak adhat plusz előnyöket. (Horváth, 2006) Míg az elmúlt időszakban a kibervédelem elsősorban az ipari kémkedés, adatlopások elleni védelemre összpontosult, fokozatosan alakult át a külföldi kormányok – főként Kína hatására – által alkalmazott hálózatok ellen végrehajtott támadások kezelésére. Ez a folyamat indította el a hadseregek támadó képességének fejlesztését, amellyel képessé válhatnak az ellenséges államok kritikus infrastruktúrájának megsemmisítésére. [6]

Az elmúlt években számos eset hívta fel a figyelmet megváltozott környezetre. Tanulmányunkban a megítélésünk szerint legfontosabb eseményeket kívánjuk bemutatni, amelyek mintegy mérföldkőként szolgáltak a jelenleg is formálódó kibervédelmi politikák meghatározásakor. Bármennyire is szeretnénk, munkánkban nem tárunk a nagyközönség elé forradalmi újításokat, hanem a mások által korábban megfogalmazott igényeket kívánjuk újból hangsúlyossá tenni.

A biztonság- és védelempolitikával foglalkozók számára a kibertámadások jelentette veszélyek nem hatnak nóvumként, azonban a széles közvélemény, illetve a döntéshozók nem rendelkeznek megfelelő ismeretekkel a kérdéskör kapcsán.

Több szerző hívta fel a figyelmet a kibertérből érkező fenyegetések kezelésében tapasztalható hiányosságokra. Ezek közé tartozik Horváth Attila *Hogyan értessük meg a kritikus infrastruktúra komplex értelmezésének szükségességét és védelmének fontosságát* (2010), illetve Kovács László és Krasznay Csaba *Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen* (2010) című munkái. Ahogy a szerzők is bemutatják, rengeteg hiányosság tapasztalható jelenleg ezeken a területeken. Tanulmányunk célja az említett írásokra reflektálva, hogy ráirányítsuk a döntéshozók figyelmét gyenge kibervédelmi képességünk fejlesztésének sürgető mivoltára. Ez azonban több területre érvényes stratégiai koncepciót kíván meg:

- megfelelő törvényi szabályozás kidolgozását;
- az oktatás kiterjesztését, amelynek irányulnia kell egyrészt az állampolgárok tudatos felhasználókká történő nevelésére, másrészt pedig egy esetleges, a kritikus infrastruktúrát ért támadás következményeire való felkészítésére;

- a kutatóhelyekkel való szoros együttműködés megteremtését;
- a költségvetési források növelését.

Tanulmányunk négy kérdéskört tárgyal. Először bemutatjuk a kritikus infrastruktúrákat ért kibertámadásokat, amelyeknek megvizsgálunk mind a jogi környezetét, mind a technikai hátterét. Ezt követően korunk egyik legdinamikusabb, ám egyúttal legnagyobb veszélyforrásait jelentő eszközét, a közösségi médiát vesszük górcső alá, elemezve azokat az aspektusait, amelyek a kritikus infrastruktúrák megtámadásához használhatóak. Fontos azonban már itt leszögeznünk, nem csak a közösségi média jelentett fenyegetésekkel foglalkozunk, hanem javaslatot teszünk azon területeken történő alkalmazásához, amelyek esetében felhasználhatjuk a kritikus infrastruktúra védelmére. Ahogy Magyarország Nemzeti Biztonsági Stratégiája fogalmaz, az ország védelmét a szövetségi kereteken belül kívánjuk megvalósítani. Ebből adódóan nem hanyagolhatjuk el az Észak- Atlanti Szövetség kibervédelmi politikájának bemutatását. Végezetül a megítélésünk szerint legnagyobb hatású - az iráni urándúsító ellen végrehajtott - kibertámadás leírását végezzük el, melynek szükségességét a Stuxnet vírus támasztja alá, ami megítélésünk szerint a hadviselés az eddigiekben ismert és alkalmazott módszereit alapjaiban változtatta meg, mintegy kinyitva Pandora szelencéjét.

Tanulmányunkban, az informatikai hadviseléssel foglalkozó szakirodalom mellett számos eseményleírást dolgoztunk fel.

A KRITIKUS INFRASTRUKTÚRA VÉDELME

A Kritikus infrastruktúra alatt a 2080/2008. (VI. 30.) Korm. határozat fogalmi meghatározása alapján olyan, „… *egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában. Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.”*

A kritikus infrastruktúrák meghibásodása, sérülése bekövetkezhet az embertől független körülmények hatására, mint pl. természeti katasztrófák esetén, de nem zárhatóak ki a szándékos rongálás, terrorizmus,[2] katonai támadás esetei. Témánk

[2] A terrorszervezetek mára rendszeresen használnak számítógépet, internetes kommunikációra, propagandára, kibertámadások előkészítésére. Ahogy Horváth Attila (2009) fogalmaz: „*Az al-Kaida terrorhálózat szervezésében a legkorszerűbb szervezési elvek érhetők tetten, a működésükhöz széles körben használják a modern kommunikáció minden eszközét és módszerét. Az illegális tevékenység és a hálózat elleni nemzetközi fellépés, hajsza miatt az egyes csoportok egymástól elszigetelve, sajnálatos módon hatékonyan tudnak a világ különböző területein terrorakciókat megszervezni és végrehajtani.”*

szempontjából kizárólag ezen utóbbi aspektussal foglalkozunk, ezen belül a számítógéppel a kritikus infrastruktúra elemnek ellen végrehajtott támadásokkal. Ennek érdekében szükségesnek ítéljük a 2007-ben bekövetkezett, Észtországot ért támadás, illetve a 2008-ban kirobbant orosz−grúz háború eseményeinek felelevenítését. Ezt követően bemutatjuk a kibertámadások jogi környezetét, illetve a technikai lehetőségeit.

Az orosz−észt kiberháború

2007 áprilisában zavargások törtek ki a NATO tagállam Észtország fővárosában, Tallinban a második világháborús szovjet emlékmű eltávolítása okán. A rendőrök és tüntetők összecsapásán, Oroszország kereskedelmi bojkottal való fenyegetésén és a két ország diplomáciai kapcsolatainak megromlásán túl egy olyan folyamat indult meg, amely alapjaiban változtatta meg a hadviseléssel kapcsolatos kereteket és elméleteket. Bár a NATO-t korábban is érte kibertámadás,[3] azonban ez az esemény volt, amelyik teljes egészében mutatta meg, milyen típusú kihívást jelent az információs hadviselés.

A támadások április 27-én kezdődtek, és május közepéig tartottak különböző intenzitással, amelynek során a bankokat, közintézményeket másodpercenként 100 megabájtos forgalmat generáló támadások érték 178 országból. Az Arbor Networks nevű, online biztonságtechnikai cég elemezte az Észtországot ért támadásokat, amin belül 128 esetben regisztráltak túlterhelést. Ezek az esetek nagy részében egy órán át tartottak, de 15 alkalommal öt óránál is hosszabb ideig tartottak.[4] A támadók célja az ország gazdasági és telekommunikációs hálózatának a megbénítása volt, melynek hatására az alábbi sikereket könyvelhették el:

- fennakadások voltak tapasztalhatóak az online pénzátutalások rendszerében, illetve a webes kereskedelem folyamatosságában;
- az állami intézmények honlapjai nagyobb részt elérhetetlenné váltak;
- az online adatforgalmat irányító, kulcsfontosságú szerverek naponta omlottak össze;
- számos állami intézményt ideiglenesen le kellett választani a hálózatról.

Ahhoz, hogy egy ilyen támadássorozat képes legyen megbénítani egy országot, természetesen fejlett informatikai hálózat megléte szükséges. Észtország ilyen téren az élvonalba sorolható, ugyanis a pénzintézetek az interneten bonyolítják a tranzakciókat, az e-kormányzat szinte teljes egészében kiváltja a hagyományos közigazgatást, oly annyira, hogy még a parlamenti választásokat is az interneten keresztül bonyolítják le. Ez pedig mindennél jobban világítja meg a támadás sikerességét, amiért az észt védelmi minisztérium szóvivője a szeptember 11-ei eseményekhez hasonlította a történteket: a támadások idején a hálózatok túlterhelése következtében a döntéshozók, a parlamenti képviselők nem fértek hozzá e-mailjeikhez, hálózatra kötött eszközeikhez, csupán telefonon, faxon voltak képesek reagálni az eseményekre.

Ahogy korábban említettük, a tüntetések kezdetekor Oroszország kereskedelmi bojkottal fenyegette meg Észtországot, ami vélhetően nem okozott

[3] Először 1999-ben, a Szerbia elleni katonai beavatkozás során szerbiai, majd később orosz és kínai hackerek indítottak támadást a NATO és különböző államok honlapjai ellen. A betörések során a támadók nem szereztek meg titkos adatokat.

[4] A leghosszabb támadás több mint tíz órán át tartott, míg sikerült a szerverek összeomlását elérni.

volna akkora gazdasági károkat, mint amekkorát a kritikus infrastruktúráját ért támadás jelentett. Ennek szemléltetésére csak egy kiragadott példát alkalmaznánk: Észtország legnagyobb pénzintézete, a Hansabank a május 10-ei támadások során több mint egymillió dolláros kárt szenvedett el. [7]

2009-ben Konsztantyin Goloszokov egy, a Kreml által támogatott ifjúsági mozgalom, a Nási egyik vezetője bevallotta, hogy szervezetük állt az észt támadás végrehajtása mögött. Bár a kezdetektől Oroszországot nevezték meg az észtek felelősnek, erre nem volt semmilyen bizonyíték.[5] Goloszokov a Financial Timesnak azt nyilatkozta, hogy a támadást nem támogatták a kormány részéről, ők maguk szervezték meg, de a céljuk nem kibertámadás volt, hanem az észt kormány figyelmének ráirányítása, hogy az emlékmű eltávolítása törvénytelen. [8] Érdemes azonban kritikával kezelnünk a nyilatkozatot, ugyanis a Nási bizonyítottan Vlagyiszlav Szurkov kezdeményezésére jött létre, aki egy, a Kremlhez köthető ideológus. [9]

Az egy évvel később lezajlott orosz−grúz háború szintén ráirányította a figyelmet az információs hadműveletek szerepének felerősödésére. A NATO kibervédelmi politikájának kialakulásával a későbbiekben foglalkozunk, most azonban tekintsük át a 2008-as orosz−grúz háború témánk szempontjából releváns vonatkozásait.

Az orosz−grúz háború

Nem célunk a konfliktus teljes körű bemutatása, a szembenálló felek katonai potenciáljának, a háború kirobbanásának hátterének ismertetése. Ezekről kiváló értekezések születtek többek között Lattmann Tamás,[6] Rácz András[7] vagy Tálas Péter[8] által. Jelen fejezetben arra szándékozunk rávilágítani, hogy napjainkban a konvencionális hadviselés mellett elengedhetetlen a kibertéri műveletek párhuzamosan való megvívása, amely egyrészt a kritikus infrastruktúrák elérhetetlenné tételét foglalja magában, másrészt a harcoló katonák kognitív műveletekkel történő kiegészítését kell, hogy jelentse.

A Dél-Oszétia ügyében kirobbant konfliktus az első olyan háború, amelyben a katonai műveletekkel összhangban kiberhadvisielést is folytattak, elsősorban kormányzati szerverek elérhetetlenné tételével, honlapok megjelenésének megváltoztatásával. A konfliktus kirobbanása előtt már történtek informatikai támadások grúz célpontok ellen, azonban a legkomolyabb akciókat közvetlenül a katonai támadások előtt hajtották végre, amely az orosz kormány idő és térbeli koordinációjára utal. Ezt erősíti meg egy 2009-ben nyilvánosságra hozott jelentés, amelyben a grúz kiberháború vizsgálatára összeállt csoport, a Project Grey Groos az orosz katonai elhárítást[9] és a szövetségi biztonsági szolgálatot nevezte meg a grúz rendszerek ellen irányuló támadások szervezőinek.[10] [10]

[5] Több esetben sikerült kimutatni, hogy orosz kormányzati gépekről indult a támadás, de mivel 178 ország fertőzött gépeiről hajtották végre a rendszerek túlterhelését, így nem lehetett bizonyítani, hogy valóban az orosz kormány kezdeményezte volna.

[6] Lattmann Tamás: Grúz-orosz konfliktus- az erő alkalmazása és a nemzetközi jog, Nemzet és biztonság, 2008. szeptember

[7] Rácz András: Az ötnapos háború − a grúziai konfliktus, Nemzet és biztonság, 2008. szeptember

[8] Tálas Péter: A grúz−orosz háború geopolitikai értelmezése, Nemzet és biztonság, 2008. szeptember

[9] Glavnoye Razvedyvatel'noye Upravleniye − GRU

[10] The Federal Security Service of the Russian Federation − FSB

Mielőtt rátérnénk a kiberháború technikai hátterének ismertetésére, vizsgáljuk meg a mögötte húzódó jogi környezetet.

A kibertámadások értelmezése a nemzetközi és hazai jogban

Az Észtországot ért kibertámadásnak, az ország kritikus infrastruktúráját ért támadásán túl egy nagyon fontos következménnyel járt: nevezetesen, tisztázatlan az ilyen események jogi szabályozása. Esetünkben egy NATO tagállamot ért támadás a szövetség 5. cikkelyének, azaz a kollektív védelem passzusának értelmében az egész szervezetet ért támadásnak feleltethető meg. [11] Nem véletlen tehát, hogy a támadások megindulásakor a NATO szakértők nem katonai támadásként értelmezték az észt kritikus infrastruktúra megbénítását, de hamar világosság vált, hogy a NATO-nak fel kell készülnie a kibertérből érkező kihívások kezelésére. Ez az attitűd azonban ráirányítja a figyelmet egy napjainkig tisztázatlan területre: a kibertámadások kezelésére, helyére a nemzetközi jogban. Jelenleg is vita folyik az államok között, hogy milyen normákkal szabályozzák a kibertérben folyó hadviselést.

Harold Koh, az amerikai Külügyminisztérium jogtanácsosa szerint a kibertámadások fegyveres támadásnak minősülnek és kiválthatják az önvédelemhez való jogot, amennyiben halálos áldozatokat, sérülteket vagy komoly károkat okoznak.[11] Indoklása szerint az ezeket kiváló események a nemzetközi jog megsértését jelentik és erőszak alkalmazását vonja maga után. [12] De nem Koh az egyetlen, aki casus belliként értelmezi a kibertámadásokat. Tony Blair korábbi nemzetbiztonsági főtanácsadója, Sir Richard Mottram is háború cselekménynek tekinti a kibertámadásokat. [13]

2012 nyarára elindult az a folyamat, amely az államok kiberhadviselés szabályozására tett törekvéseinek kezdetét jelentheti. Egyelőre Kína és az USA kezdett kétoldalú, informális tárgyalásokba a China Institute of Contemporary International Relations és a Center for Strategic and International Studies szervezésében. A tárgyalások főbb céljainak az online támadások korlátozását, a jobb kommunikációt és a harmadik fél által jelentett kockázatok csökkentésének módjait tűzték ki. A kormányzati tisztviselőkből, illetve tanácsadó szervezetek tagjaiból álló delegációknak azonban nincs felhatalmazásuk a kibertámadások korlátozásáról szóló egyezmény megalkotására. [14]

Szerencsére elmondhatjuk, hogy Magyarországon is foglalkoznak a döntéshozók az információs rendszerek védelmével. Ahogy a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012 (II.21.) kormányhatározat 31. pontja fogalmaz a kibervédelemről: „*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. Egyre sürgetőbb és összetettebb kihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatok, valamint a kapcsolódó kritikus infrastruktúra fizikai és virtuális terében. 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. E támadások eredetét és motivációját gyakran nehéz felderíteni. A*

[11] Ilyen eset lehet például az atomerőművek elleni támadás, sűrűn lakott területek fölött megnyitott gát, légi irányítás ellen elkövetett támadásból származó repülőgép szerencsétlenség.

kibertérben világszerte növekvő mértékben jelentkező 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 Magyarországnak is készen kell állnia.

a) Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérése és priorizálása, a kormányzati koordináció erősítése, a társadalmi tudatosság fokozása, valamint a nemzetközi együttműködési lehetőségek kiaknázása.

b) A nemzeti kritikus információs infrastruktúra védelmének erősítése mellett szövetségeseinkkel és EU-partnereinkkel együtt arra törekszünk, hogy az információs rendszerek biztonsága erősödjön, valamint részt vegyünk a megfelelő szintű kibervédelem kialakításában." [15]

Ennek keretében került kidolgozásra Magyarország kibervédelmi stratégiájának részeként az információbiztonsági törvénytervezet. [16] A dokumentum alapvető jogokat és kötelezettségeket állapít meg, személyi hatálya szerint a kormányzati adatokat kezelő szervezetek, a nemzeti adatvagyont kezelő szervezetek és a létfontossági információs infrastruktúrák védelmére, a tárgyi hatálya az elektronikus információs rendszerek védelmére terjed ki. A tervezet leghangsúlyosabb eleme azon törekvés, mely szerint az egyes elektronikus információs rendszerek biztonsági osztályokba szükséges sorolni, és ezekhez a követelményekben meghatározott intézkedések párosítását irányozza elő. A javaslat másik fontos eleme, hogy megállapítja az egyes szervezetek biztonsági szintjét, melyek a biztonsági problémák megoldására, kezelésére való felkészültségét, érettségét fogalmazza meg. Kiemelendő, hogy a javaslat az oktatás, az információbiztonsági tudatosság növelésének fontosságát hangsúlyozza.

A kiberháború eszközei

Az jogi háttér, illetve a két releváns eset ismertetését követően térjünk rá, hogyan, milyen technikai feltételekkel lehet megvívni egy, a kritikus infrastruktúrák ellen végrehajtott támadást. Ennek érdekében szükség mutatkozik különböző fogalmak tisztázására.

Az információs hadviselés fogalma jelentős átalakuláson ment keresztül az elmúlt évtizedekben. Kezdetekben az információ megszerzését, valamint az ebből fakadó előnyök gazdasági és politikai eredményekké való felhasználását jelentette. Mára a katonai terminológia elsősorban − Kovács László (2009) fogalmi meghatározását kölcsönözve − „… *olyan összehangolt és koordinált tevékenységeket takarnak, amelyek a műveleti biztonság, a katonai megtévesztés, a pszichológiai műveletek, az elektronikai hadviselés és a számítógép-hálózati műveletek különböző akcióival támogatják a harc sikeres megvívását*" érti.

Annak érdekében, hogy a támadók sikerrel tudják végrehajtani az egyes kritikus infrastruktúra elemeket blokkolását, megfelelő információkkal kell rendelkezzenek a kiválasztott célpont felépítéséről, sebezhetőségéről, képes kell legyen a támadás megindításakor ezen rendszerek képességeinek optimális esetben teljes körű szüneteltetésére, adott esetben csökkentett funkciójú

üzemelésének elérésére, miközben a saját számítógépes rendszerének működését biztosítja. Céljuk eléréséért ún. számítógép-hálózati műveleteket alkalmaznak.[12]

Ha a támadók rendelkeznek a szükséges információkkal, egy zombi-hálózat segítségével képessé válhatnak a kiválasztott célpontok túlterheléssel történő összeomlását elérni. Zombi-gépek alatt azokat az eszközöket értjük, amelyek egy rosszindulatú program segítségével átveszik a felhasználó tudta nélkül a számítógép feletti irányítást.[13] A felhasználó sok esetben ebből nem érzékel semmit, hiszen az adott szoftver egy egyébként hasznos funkciót lát el a számítógépen, de emellett olyan programrészeket telepít, amely nem kívánt műveleteket is végrehajthat. Ilyen művelet lehet adathalászat a számítógépen tárolt fájlokhoz való hozzájutással[14] vagy a felhasználó által lenyomott billentyűinek sorrendjének megjegyzésével és egy távoli szerverre való átküldésével;[15] netán a tárolt adatállomány módosítása, törlése; de utat nyithat a következő támadás végrehajtása előtt. Ennek okán nevezik ezeket a programokat legelterjedtebb fajtájukról „trójai" programoknak.

A már megfertőzött zombi-gépeket egy ún. zombi-szerver koordinálja. A zombi-szervernek képesnek kell lennie akár több millió számítógép irányítására is. [17] A már korábban említett orosz−grúz konfliktus során többek között spamküldésre[16] használt zombi-hálózatokat is felhasználtak.[17] Egy ilyen felhasznált hálózat mögött a szentpétervári illetékességű szervezett bűnözői kör, a Russian Buisness Network állhatott, amely a spamküldéstől kezdve az identitáslopáson át a gyermekpornóig bezárólag minden internetes bűnözési formában képviselteti magát. [18]

Egy ilyen botnet létrehozásához nem csupán a felhasználói felelőtlenséghez kapcsolódhat. Tanulmányunk írásának időpontjában került napvilágra a Microsoft bejelentése, amely egy kínai botnet hálózat felszámolását adta hírül. Az eset érdekességét az adja, hogy az újonnan vásárolt készülékekben gyárilag be voltak építve a megfigyelő programok. [19]

A fentebb tárgyalt, Észtországot érintő esetben ún. szolgáltatás-megtagadással járó támadással (Denial of Service − DoS) bénították meg az adott kritikus infrastruktúrát. A DoS támadás jellegéből fakadóan az egyik legnehezebben kivédhető internetes támadás, ugyanis a támadók a válaszadó rendszert hamis kérésekkel bombázza, melynek hatására a rendszer képtelen kiválasztani a valós, illetve hamis kéréseket.[18] Láthatjuk, a DoS támadás célja a hálózat normál működésének megakadályozása, melyet egy automatizált hálózat felhasználásával, túlterheléssel valósít meg.

A DoS támadásokat két csoportba sorolhatjuk. Az ún. protokolltámadások az adott alkalmazás vagy protokoll hiányosságait használják fel, míg az ún. elárasztásos támadások a megtámadott hálózat erőforrásai nem képesek kiszolgálni a kliensek által küldött óriási adatmennyiséget.

[12] Computer Network Operations − CNO
[13] malicious software – mailware
[14] Ezt a folyamatot nevezik phishingnek, ami kivitelezhető sniffinggel (szaglászással) vagy sniferrel (lehallgatással). Sniffing esetén a hálózaton zajló információk állandó követésére, a hálózat felderítésére nyílik módunk, sniffer esetén pedig az üzenetküldésre alkalmas hálózatokból az információ kinyerésére biztosít lehetőséget.
[15] Ezt nevezi a szakirodalom keyloggingnak.
[16] Spam alatt a kéretlen reklámküldeményeket értjük.
[17] Más néven botnet
[18] Már pedig annak eldöntése, hogy melyik felkérés valós, melyik hamis, lehetetlen.

A DoS támadások egyik válfaja az ún. elosztott-támadás (Distributed DoS-DDoS), amely alkalmazásakor több támadó együttesen kívánja elérni a rendszer összeomlását.

A kibertámadások jogi, technikai ismertetése, illetve a két relevánsabb eset feldolgozása után elérkeztünk a témánk kulcsrészéhez: hogyan hajtható végre egy kritikus infrastruktúrát érintő támadás a közösségi média felhasználásával.

A KÖZÖSSÉGI MÉDIA

A közösségi média (social media) „*internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom*”.[19] (Andreas Kaplan−Michael Haenlein, 2010). A közösségi média eszközei alatt tehát azokat az eszközöket értjük, amelyen a tartalmat a felhasználók állítják elő, osztják meg egymás közt, amihez a felületet egy adott szolgáltató biztosítja. Ezen tartalom lehet írott, képi, videó, zene formátum. A közösségi média eszközei ez által a közösségi oldalak, kép- és videó megosztó oldalak, illetve a blogok, mikroblogok.

Napjainkra a különböző eszközök használata olyan mértékűvé vált, hogy nem becsülhetjük le a hadtudományokban betöltött szerepét. Annál is inkább, hiszen az egyes közösségi média eszközök felhasználhatóak a hadsereg népszerűsítésére, válságkommunikáció menedzselésére, a harcoló katonák családtagjaikkal való kommunikációjának biztosítására, de kiváló terepet nyújt a nyílt forrású hírszerzésre, akár szélsőséges esetben egyes államok belpolitikai eseményeinek érdekeinknek megfelelő befolyásolására,[20] vagy a témánk szempontjából relevanciával bíró, a kritikus infrastruktúrák elleni támadás előkészítésére. A továbbiakban azt vizsgáljuk, hogyan béníthatóak meg a közösségi eszközök felhasználásával a kritikus infrastruktúrák.

Témánk szempontjából négy területtel kívánunk foglalkozni: a nyílt forrású hírszerzéssel, az egyéni felelősség kérdésével, a hadsereg pozitív percepcionálásának megteremtésével, amelynek többek között megfogalmazott célja a hackerek kritikus információs infrastruktúra védelmébe történő bevonása, illetve a kríziskommunikációban betöltött szerepéről.

A nyílt forrású hírszerzés

Nyílt forrású hírszerzés (Open Source Intelligence − OSINT) alatt olyan információgyűjtési eljárást értünk, amely során a felhasználható információkat kizárólag nyílt forrásból gyűjtjük, majd elemezzük. Ilyen nyílt források lehetnek a

[19] A web 2.0 (vagy „webkettő”) kifejezés olyan internetes szolgáltatások gyűjtőneve, amelyek elsősorban a közösségre épülnek, azaz a felhasználók közösen készítik a tartalmat vagy megosztják egymás információit. Ellentétben a korábbi szolgáltatásokkal, amelyeknél a tartalmat a szolgáltatást nyújtó fél biztosította (például a portáloknál), webkettes szolgáltatásoknál a szerver gazdája csak a keretrendszert biztosítja, a tartalmat maguk a felhasználók töltik fel, hozzák létre, osztják meg vagy véleményezik. A felhasználók jellemzően kommunikálnak egymással, és kapcsolatokat alakítanak ki egymás között.

[20] Talán nem véletlen, hogy az iráni vezetés úgy döntött, lekapcsolja országot az internetről és saját hálózatot fejleszt ki. Legújabb lépésként letiltotta a Google szolgáltatásait (hivatalos indoklás szerint a Mohamedet gúnyoló videóra válaszul), de a valóság az lehet, hogy félnek egy „arab tavasz” jellegű esemény bekövetkezésétől [20].

hagyományos- és elektromos médiumok, az internet, könyvtárak, szakértők tanulmányai stb. Az információ szabadon hozzáférhető voltából következik, hogy természetesen nem helyettesítheti a minősített információkból származó tudást, de az olyan információkat nyerhetünk ki belőle, amely segít tájékozódni a minősített információk között. Az OSINT nagy előnye, hogy szabadon, bárki által hozzáférhető adatokhoz juthatunk hozzá valós időben, viszonylag kis költségek mellett. Hátránya a rendelkezésre álló adatok nagy száma, illetve egyes anyagok pontatlanságokat tartalmaznak vagy dezinformációs céllal állították elő.

Vizsgáljuk meg közelebbről, milyen adatokhoz férhetünk hozzá nyílt forrású hírszerzést a közösségi média elemeire alkalmazva. Első körben kiválasztjuk a célpontunkat, melynek székhelyéről, telephelyeiről a célpont hivatalos honlapján tájékozódhatunk. Hogy ez a célpont közüzem, tömegközlekedést ellátó vállalat vagy egyéb, a kritikus infrastruktúra működtetését ellátó intézmény, jelen esetben irreleváns.

Ezt követően számos ingyenes szolgáltatás áll rendelkezésünkre, amellyel a megtámadni kívánt területről műhold képet és egyéb, akár 3D-s térképet tölthetünk le.

Sok esetben a videó megosztó oldalak is segíthetik a támadókat a célpont felderítésében, hiszen amatőrök rengeteg videót töltenek fel ezekre az oldalakra, amely célzott keresés esetén hiánypótoló információkat szolgáltathat. Azonban fontos egy másik aspektust is kiemelnünk. Az átlagnál valamivel nagyobb konspirációs érzékkel- már pedig egy, a kritikus infrastruktúrát megtámadni szándékozó csoport esetén nem túlzás feltételezni meglétét- könnyű szerrel használhatjuk az információk a csoport egyes tagjai közti megosztására, anélkül, hogy gyanút keltene bárkiben. Gondoljunk csak bele, egy okostelefonnal, amellyel mára HD[21] minőségű felvételeket készíthetünk, milyen, számunkra fontos felvételeket készíthetünk a célpont környékén, ha ezt valamilyen legendával álcázzuk. Ezt követően csak pár perc egy videó megosztó oldalra való feltöltés, amelyből a beavatott szemek kiemelik a lényeget, míg a véletlenül oda tévedő látogatók csak egy újabb érdektelen videót látnak.

A nyílt forrású hírszerzés egy másik részét biztosíthatják a különböző közösségi oldalak és mobil platformok, amelynek azonban részletes vizsgálatát a következő alfejezetben hajtjuk végre.

Az egyén felelőssége

Általánosságban elmondhatjuk, a felhasználók jelentős nem foglalkozik személyes adatainak védelmével, vagy az általa használt informatikai eszközök megfelelő biztonsági garanciák betartásával. Ezt a fajta nemtörődömséget használják ki a kiberbűnözők. Érdemes azonban kettéválasztani a kérdéskört.

Maradva az előző alfejezet gondolatánál, nyílt forrású hírszerzéssel rengeteg információhoz juthatunk hozzá az óvatlan felhasználók nem tudatos segítségével.[22] Bár materiális értelemben a közösségi média használata sok esetben ingyenes, mégis óriási árat fizetünk a kvázi díjmentes használatért cserébe: személyes adatainkat, kapcsolati hálónkat, életünk szinte miden mozzanatát adjuk ki a

[21] High-definition, azaz nagy felbontású

[22] Nagy port kavart egy 2009-es eset, amelyben az új MI:6 igazgató felesége posztolta Facebookon az elérhetőségüket és az életük számos momentumát. [21]

cégeknek, amelyek aztán vállalatoknak adja el reklámcélra ezeket az összegyűjtött adatokat.

Egy nemrégiben az interneten publikált konferencia a mobilszolgáltatók törvényben szabályozott adatgyűjtésével foglalkozik. Malte Spitz „Your phone company is watching" című előadásából hátborzongató kép bontakozik ki. [22] EU-s, illetve tagállami szabályozás értelmében, minimum hat hónapig, maximum két évig kötelesek a mobil, valamint internetszolgáltatók tárolni az előfizetőhöz kapcsolódó adatokat, mint a beszélgetéseinek időtartalma, kikkel folytatta a beszélgetéseket, mikor, milyen szöveges üzenetet küldött, kinek, hol használta a mobiltelefonját, illetve hol tartózkodik éppen az illető. A szolgáltatótól kikért, tárolt adatokból Malte Spitz egy megdöbbenő videót készített. Ebből a térkép alapján lekövethető, hogy a vonatkozó időszakban – egyebek mellett − milyen gyakorisággal és mire használta mobiltelefonját, hol, milyen eszközzel járt. [23] Míg a szolgáltatókat törvény kötelezi az adatgyűjtésre, addig mi önként szolgáltatjuk ki adatainkat a közösségi oldalaknak. Gondoljunk csak a Facebookra, amely az európai adatvédelmi panaszokra reagálva ideiglenesen kikapcsolja Európában az arcfelismerő szoftverét, míg az aggályoknak megfelelően nem kerül átdolgozásra. [24] Az arcfelismerő szoftvert tavaly nyáron vezetette be a közösségi oldal, amelynek lényege, hogy a feltöltött fényképekből automatikusan felismeri az oldalon regisztrált felhasználókat.

Napjainkra a közösségi eszközök egyre nagyobb mértékben költöznek át a mobil platformokra.[23] Az okostelefonokat és tableteket, jellegükből fakadóan praktikus használatukat különböző alkalmazásokkal biztosíthatjuk. Az egyes alkalmazások, legyen szó közösségi oldalról, híroldalról, videó megosztóról, térképről, különböző engedélyeket követelnek meg. A legnépszerűbb közösségi eszközök, hogy csak a legfontosabbakat említjük, az alábbi adatainkhoz kérnek hozzáférést: az összes partnerünk elérhetősége, kivel mennyi ideig, milyen rendszeresen kommunikálunk, sms-eink és e-mail-jeink olvasása, GPS-alapú helymeghatározás során tartózkodási helyünk. Ezen adatok kiszolgáltatásáról a felhasználók nagy többségének fogalma sincs. Természetesen a felsorolt biztonsági tényezőkön egyéb veszélyeket is jelentenek a mobilalkalmazások. Egy-egy vírus elrejthető a népszerű alkalmazásokba, ami által a hackerek átvehetik az uralmat a telefonunk kamerája fölött és a megszerzett információt továbbíthatják a kívánt helyre. [25]

Nem régiben jelentette be Symantec a világ egyik legnagyobb kiberbűnözést vizsgáló kutatásának, a Norton Kiberbűnözési Tanulmány legújabb eredményeit. [26] Az évente kiadott jelentés célja, hogy átfogó képet nyújtson kiberbűnözés fogyasztókra gyakorolt hatásairól, valamint az új technológiák fejlődésének és alkalmazásának biztonsági következményeiről. A 2012-es felmérés 24 ország több mint 13 000 felnőtt megkérdezésével készült. Az eredmény ijesztő: másodpercenként 18 áldozata van a kiberbűnözésnek, ami másfél millió áldozatot jelent nemzetközi szinten. Az anyagi veszteséget lebontva egyéni szintre, a felhasználóknak átlagosan 197 dollár közvetlen anyagi veszteséget jelent az online bűnözés, ami egy átlagos négytagú magyar család havi élelmiszerfogyasztásának felel meg. Az elmúlt 12 hónapban világszerte 556 millió felnőtt volt online áldozat, ami több mint ez Európai Unió teljes lakossága. Ez az adat azt jelenti, hogy az internetező felnőttek közül 46 százalék esett kiberbűnözők csapdájába az elmúlt évben, hasonlóan a 2011-es adatokhoz (45 százalék). A tanulmány kiemeli a

[23] mobiltelefonokra, táblagépekre

kiberbűnözés átalakuló trendjét, ami egyre nagyobb ütemben irányul a közösségi oldalak, valamint a mobilalkalmazások ellen:

- a közösségi oldalak felhasználóinak 15 százaléka jelentette, hogy valaki feltörte a profiljukat és az ő nevükben használta az oldalt;
- tízből egy felhasználó vallotta be, hogy dőlt már be közösségi hálózatokon terjedő átveréseknek, hamis linkeknek;
- míg 75 százalék tisztában van azzal, hogy a kiberbűnözők a közösségi hálózatok felé fordultak, kevesebb, mint felük (44 százalék) használ olyan biztonsági megoldást, amely védi őket a közösségi oldalakon felbukkanó fenyegetések ellen, és csak 49 százalék használja az adatvédelmi beállításokat, hogy beállítsa, ki láthatja a megosztott információit;
- a mobiltelefon-felhasználók közel egyharmada (31 százalék) kapott szöveges üzeneteket ismeretlen számokról, amelyek arra kérték, hogy kattintson egy linkre, vagy tárcsázzon egy ismeretlen számot egy hangposta üzenet eléréséhez.

Legyen szó bármilyen informatikai rendszer elleni támadásáról, sok esetben olyan komplex védelemmel rendelkeznek, hogy a számítógépes betöréssel egyáltalán nem, vagy csak kis mennyiségben lehet információhoz jutni. Ennek kiküszöbölésére használatos az ún. Social Engineering, melynek eszközével a felhasználók bizalmába való férkőzéssel, csalással, adott esetben erőszakkal, zsarolással férkőznek hozzá a kívánt információkhoz.[24] Az előbbiekben tárgyalt eszközöket felhasználva könnyű szerrel férhetünk hozzá az adatvédelemmel nem törődő felhasználók bizalmába, esetleg használhatjuk fel ellene a megszerzett információkat.[25]

Az egyéni felelősség másik aspektusát jelenti a közösségi média eszközeinek zombi-hálózatok létrehozására való felhasználásának lehetősége. Korábban foglalkoztunk az ún. zombi-hálózatok működésével, így most csupán arra teszünk kísérletet, hogy felvázoljuk röviden, milyen módszerrel használhatjuk a közösségi eszközöket zombi gépekké változtatásával. Ahogy fentebb már említettük, a felhasználók döntő többsége nem használ vírusirtót, nem foglalkozik az informatikai eszközök védelmének fontosságával. Általános tendencia, hogy a közösségi oldalakon unaloműzés céljából különböző szórakoztatónak szánt alkalmazást használunk. Ezek az alkalmazások sok esetben építenek az emberek gyanútlanságára, naivitására, tudatlanságára, ami által a „legenyhébb" esetben hozzáférést kérnek az összes általa megadott esetben[26] vagy vírussal fertőzik meg a felhasználó gépét.[27] Mind az adathalászat, mind a vírussal fertőzött gépek veszélyeit korábban taglaltuk, így újból nem térünk ki rá.

Elengedhetetlen azonban, hogy ezen a ponton jelezzük az állampolgárok tudatos felhasználókká történő nevelésének fontosságát. Erre szolgál kiváló példával

[24] Magyarul leginkább a pszichológiai manipuláció fogalmát feleltethetjük meg

[25] Elég csak arra gondolni, hogy egy csalfa férj mobiltelefonja folyamatosan sugározza a tartózkodására vonatkozó információkat, hozzáférhetünk levelezéseihez, üzeneteihez, ami elég jó alapot biztosít azok kezébe, akik zsarolással szeretnék megszerezni az általuk fontosnak tartott információt, mondjuk hozzáférést a belső informatikai rendszerhez.

[26] Erre kiváló példa a „Mi az indián neved?" elnevezésű alkalmazás, amit pár nap alatt 800 ezer ember használt. Később derült csak ki, hogy valójában egy ékszerbolt készítette az alkalmazást, ami által az összes felhasználó adatához hozzáfért és használhatta fel reklámkampánya céljából. [27]

[27] Ez esetben a vírusok terjesztői általában hírességekről készítenek álhíreket („nézd meg XY-t részegen/meztelenül"), melyben a botrányra/bulvárra szomjazó emberek hiszékenységét, kíváncsiságát használják ki, hogy a hivatkozásra való kattintással fertőzzék meg az eszközöket.

az US ARMY, amely 2011 februárjában kiadott egy, a közösségi médiával foglalkozó kézikönyvet, amelyben ajánlásokat fogalmaz meg többek között az elvárt biztonsági beállítások bemutatására.[28] [28]

Ez a fajta oktatás nem csupán azt hivatott szolgálni, hogy elkerüljék adataik nem kívánt – és sok esetben illegális – felhasználását, informatikai eszközeik védelmének biztosítását, hogy ez által felhasználhatóak legyenek a fent taglalt forgatókönyvekben való nem tudatos részvételben, de megítélésünk szerint legalább ilyen súllyal bír az állampolgárok felkészítése egy esetleges kritikus infrastruktúrát ért támadás/meghibásodás esetére. [30]

A közösségi média, mint a hadsereg pozitív percepcionálásának eszköze

A közösségi média jelentette veszélyek, kockázatok ismertetése után térjünk rá az eszköz által nyújtott pozitív lehetőségeinek taglalására. A korábban már citált Digitális Mohács című tanulmány *Védelmi lehetőségek* című alfejezetében a szerzők azt a megállapítást teszik, hogy a védelmi tervezés szempontjából elengedhetetlen a hackerek bevonása a kritikus infrastruktúrák védelmébe. Ehhez azonban egy olyan stratégiai gondolkodás szükséges, amely megteremti a hadsereg pozitív percepcionálásának lehetőségét. Ennek egyik eszköze lehet a közösségi média felhasználása. Ne feledjük, a híres-hírhedt Anonymous csoport a 4chan nevű fórum tagjaiból szerveződött. [31] Ez az évek során rengeteg támadást indított különböző államok belpolitikai döntéshozatalának befolyásolása céljából, nem egy esetben sikerrel járva.[29] Ahhoz, hogy elérhetőek legyenek ezek a hackerek, egy olyan stratégia kidolgozása szükséges, amely a hadsereg népszerűsítését a web 2.0 eszközeinek való megfeleltetését is magában foglalja, hiszen ezek azok a területek, ahol igazán esély kínálkozik a hackerek és a „digitális bennszülöttek" megszólítására.[30]

Kríziskommunikáció

Napjainkban az információt egyre nagyobb mértékben fogyasztjuk a közösségi oldalakon. A közösségi szolgáltatások felismerték ennek jelentőségét, és hogy még jobban bevonják a felhasználókat, egy olyan módszertant dolgoztak ki, melynek során azon ismerőseink preferenciáját tárják elénk, akikkel leggyakrabban tartjuk az oldalon a kapcsolatot. Egy algoritmus értelmezni próbálja az érdeklődési körünket (megjegyezve, milyen hírekre, videókra kattintunk a leggyakrabban), és ennek megfelelően „kitalálja", milyen hírek érdekelnek bennünket, majd átrendezve az oldal

[28] Az ebben rejlő kockázatok illusztrálásként egy 2007-es eset szolgál. Egy iraki bázisra új helikopterek érkeztek, melyeket az ott szolgálatot teljesítő katonák mobiltelefonjukkal fényképeket készítettek és feltöltötték közösségi oldalakra. Nem számoltak azonban azzal, hogy a telefon rögzíti a geolokációs pontokat, amely felkelők kezébe került, akik négy AH-64-es Apache-t semmisítettek meg egy aknavetős támadás során. [29]

[29] Lásd pl. az amerikai törvényhozás elé benyújtott Stop the Online Piracy Act visszavonásának kikényszerítését. [32]

[30] A digitális bennszülött terminológiáját Marc Prensky (Digitális bennszülöttek, digitális bevándorlók, 2001) alkotta. A fogalom egy olyan generációt takar, akik „anyanyelvi" szinten beszéli a számítógépek, internet digitális nyelvét, aminek következtében eltérő módon dolgozzák fel a környezetükből kinyert információkat, más agyi struktúrák alakultak ki esetükben.

tartalmát, ezeket a tartalmakat emeli ki. Ennek megvan az a veszélye, hogy beszűkülté teszi a valóságértelmezést, meghagyva természetesen a tévedés lehetőségét, hiszen az algoritmus matematikai összefüggések alapján állítja össze a tartalmat.

Ennek ellenére a felhasználók médiafogyasztása a közösségi oldalak prioritásának elvén történik, és a felhasználók megosztásaiból kerülnek át a híroldalakra. Arról nem is beszélve, hogy a történéseket, legyenek bármilyen banálisan, rendszeresen megosztják ismerőseikkel („esik a hó"). Természetesen ez az attitűd jellemző a nagyobb volumenű eseményeknél is. A szerző emlékszik olyan esetre, amikor 2010 őszén a Richter-skála szerinti 1,8−2,0 körüli földrengés volt érzékelhető lakóhelyén, amivel szinte egy időben a helyi ismerősei nagy számban osztották meg a földrengés tényét. Ezt a felhasználói magatartást állíthatjuk a kríziskommunikáció szolgálatába. A már említett, az US Army által kiadott Közösségi Média Kézikönyv külön fejezetben foglalkozik a válságkommunikációval, amely a hazai példákkal ellentétben azt fogalmazza meg, hogy a lehető legtöbb információt osszuk meg a közösségi oldalakon, bevonva a segélyszervezeteket és az egyéb, érintett állami intézményeket. A közösségi média előnye, hogy a tájékoztatás valós időben történhet.

Reményeink szerint, az eddigiekkel sikerült alátámasztani a bevezetőben megfogalmazott állításunkat, mi szerint a kibertámadások olyan veszélyforrást jelentenek, amik alapjaiban változtatják meg a hadviselés szerepét. A továbbiakban bemutatjuk, az Észak-Atlanti Szövetség formálódó kibervédelmi politikáját, valamint a történelem eddigi legjelentősebb kibertámadását, ami véleményünk szerint visszafordíthatatlan hatásokkal bír az információs műveletekre.

A NATO ÚJ STRATÉGIÁJA

Az új alapelvek

Az előző stratégia elfogadása (1999) óta a NATO több új típusú kihívással szembesült. Gondoljuk csak 2001. szeptember 11-ei terrortámadásra, az iraki háborúra vagy az első ízben végrehajtott nagyszabású kibertámadásra Észtország ellen, ami a NATO tagállam kritikus infrastruktúráját bénította meg hosszú időn keresztül. Az évtized közepétől kezdve többen szorgalmazták egy új stratégia kidolgozását, de csak 2009-ben került sor egy tervezet elkészítésére. Az új stratégiát 2010-ben fogadták el, amit egy fél éves nyilvános nemzetközi vita előzött meg, aminek tanulságit egy tanácsadói csoport foglalta össze, és tett javaslatokat, majd egy másik csoport kidolgozta a szövegtervezetet. Az állam és kormányfők végül a harmadik módosított változatot fogadták el, amely az *Aktív szerepvállalás és modern védelem* címet kapta. A végül elfogadott koncepció három fő jeligét fogalmazott meg: a kooperatív biztonságot, a válságkezelést és a kollektív védelmet, utóbbira „… *szilárd kötelező érvényű kötelezettségként utal, ráadásul kiterjeszti azokra az új biztonsági kihívásokra is amely a szövetség egyes tagjainak vagy a szövetség egészének biztonságát fenyegetik. Ez a megerősítés főleg a kelet európai tagállamok számára voltak fontosak".* [33] (Varga, 2010). A koncepció mellet egy új kooperatív hálózatot kíván létrehozni a meglévő struktúrák mellé, amellyel szintén a biztonságot kívánja erősíteni. Az új hálózat minden releváns biztonsági szervezettel és nemzettel együtt kíván működni, így például Oroszországgal is, amelyre formális keretekben a korábban létrejött Oroszország−NATO Tanács szolgál.

A találkozón egy katonai intézkedés csomagot is elfogadtak. Ebben olyan fontos témák szerepeltek mind az új parancsnoksági rendszer véglegesítése, rakétavédelmi akcióterv, a hagyományos és nukleáris képességek áttekintése, valamint az új információs hadviselési stratégia. 2010. augusztus 1-jén létrejött egy új típusú biztonsági kihívásokkal foglalkozó divízió, amelynek vezetője Iklódi Gábor. A divízió olyan területekkel foglakozik, mint a Tudomány a Békéért Program, a tömegpusztító fegyverek, a terrorizmus elleni küzdelem, nukleáris politika, energiabiztonság, valamint a kiberbiztonság. Ennek a divíziónak a keretén belül létrehoztak egy előrejelző stratégiai elemző-értékelő egységet is, amely civil és katonai szakértőkből áll.

A lisszaboni döntés előtt a koncepció kidolgozásának fontos momentuma volt a Madeleine Albright által vezetett szakértői csoport, amelynek a megállapításai a következők a jövőre: *„A NATO a jövőben is a transzatlanti kapcsolatok megvalósítója. A tagállamok az 5. cikkely garanciáit mind elméletben, mind gyakorlatban erősíteni kívánják. A tagállamok ellen irányuló hagyományos támadás valószínűsége csekély, de nem kizárható. Legvalószínűbb fenyegetés lehet a ballisztikus rakétákkal elkövetett támadás, a terrorcselekmények és a számítógépes rendszerek elleni támadás."* A jelentésnek köszönhetően a tagállamok egy háromnapos gyakorlatot tartottak *Cyber Coalition 2010* néven, amelyben a résztvevők szakemberei a számítógépes rendszerek elleni támadások elhárításával foglalkoztak. [34] A helyzetgyakorlat abból állt, hogy több tagállam és a főparancsnokság számítógépes rendszerei ellen indítottak külső támadást. A cél az volt, hogy a lehető leggyorsabban és legpontosabban határozzák meg az elkövetőket vagy a támadás eredetét. Az ilyen gyakorlatok minden estben hozzájárulnak a NATO elhárító képességének javulásához, és nem utolsó sorban az elrettentés erősítéséhez.

Anders Fogh Rasmussen, a NATO főtitkára 2010 októberében kijelentette, hogy a stratégia fontos része lesz a szövetség feladatainak meghatározása és újragondolása. Ennek fontos részét képezi a kiépítendő rakéta védelmi rendszer és a „kiberterrorizmus" elleni védelem. A kibertér globális jellégét és az ebből adódó veszélyeket felismerve a NATO és szövetségesei együtt kívánnak működni a, a nemzetközi szervezetekkel és a magán szektorral, egyetemekkel, illetve a NATO-val partnerségi együttműködést kötött államokkal, olyan módon, hogy az előmozdítsa és kiegészítse egymást, elkerülve a párhuzamosságokat, és felkészüljenek a támadások elhárítására.

A NATO tehát a fő hangsúlyt a saját kommunikációs és információs rendszerének a védelmére helyezi. Továbbá, hogy védje információs rendszerinek hálózatát, a NATO-nak fokoznia kell azon képességeinek fejlesztését, amelyekkel felül tud kerekedi a számítógépes fenyegetések széles skálájával, amivel egyre inkább szembesül. 2010. július 8-án a védelmi miniszterek elfogadták a stratégiai koncepcióra épülő Kibervédelmi irányelvet, amely egységbe foglalja a tagállamok védelmi intézkedéseit ezen a területen. Az irányelv a rugalmas elhárítás képességére és a megelőzésre helyezi a hangsúlyt. Ezért minden NATO szerveztet központosított ellenőrzés és védelem alá vonnak, valamint mindenhol a legmodernebb kibervédelmi és információbiztonsági irányelvek alapján működtetik azokat. Emellett meghatározták azt is, hogy a NATO partnereivel, nemzetközi szervezetekkel, kutatóközpontokkal és a magánszektor szereplőivel milyen formában fog együttműködni a jövőben. A kibervédelmi irányelvekkel együtt a miniszterek elfogadták a végrehajtáshoz szükséges akciótervet is. [35] (Csiki 2011)

Az akcióterv összetevői

Az összetevők:

- A NATO–nak ki kell dolgoznia azokat a követelményeket, amelyeket a tagállamoknak minimálisan teljesíteniük kell ahhoz, hogy a NATO szervezeti hálózata a jövőben is működhessen.
- A NATO segíti a szövetségeseket abban, hogy a nemzeti számítógépes védelmi színvonalát a megfelelő mértékben fejleszthessék a tagok annak érdekében, hogy a nemzeti infrastruktúrát sebezhetőségét minimalizálják.
- Segítséget nyújt kibertámadás esetén a tagállamoknak.
- Meghatározásra kelül a számítógépes védelmi követelmények fontossági sorrend szerint, valamint a kibervédelmet integrálják a NATO védelmi protokolljába.
- A NATO fel fogja mérni katonai erejének védelmi képességeit, valamit egy ilyen típusú támadás hogyan befolyásolja a missziók tervezését és lefolytatását.
- A kibervédelmi képességeket kell meghatározni a NATO-val együttműködő államok számára, amelyek biztosítják az elvárt szintek minimális telesítését.
- A NATO–nak erősítnie kell azon képességeit, amelyek elősegíti a korai felismerését, a tudatos helyzetértékelést és az elemzési képességet egy ilyen jellegű támadás esetén
- A NATO-nak ki kell fejleszteni egy tudatossági programot, valamit törekednie kell a kibertérből érkező fenyegetések beemelésére az ezután következő gyakorlataiba.
- A NATO és szövetségesei támogatni fogják egy együttműködési kibervédelmi kiválósági központ felállítást Tallinban.[31] [36]

A NATO kibervédelmi törekvései az átfogó megelőzési elveken, az ellenálló képességein és a párhuzamosságok elkerülésén alapulnak. A megelőzés és az ellenálló képesség különösen fontosak mivel minden erőfeszítés ellenére a valóság az, hogy még mindig léteznek veszélyforrások, amely ellen védekeznünk kell. Az ilyen támadások ellen a legjobban úgy védekezhetünk, ha kellő képen növeljük felkészültségi szintünket és csökkentjük a kockázatát a működési zavaroknak és azok következményeiknek. A rugalmas elhárítás és a reagálás a legfontosabb, mert ez teszi lehetővé a támadás következményeinek minimalizálását és a gyors helyreállítást. Jelen cikk terjedelmi keretei nem biztosítják, hogy megvizsgáljuk, a kitűzött célok hogyan valósultak meg a valóságban, terveink szerint erre egy másik tanulmányban keresünk válaszokat.

A STUXNET

2010-ben a Natanz mellett kialakított urán dúsító telepén egy számítógépes vírus közel 1000 gázcentrifugát tett tönkre, ezzel akár több, mint két évre is hátráltatva Irán urándúsítási kísérleteit.[32] Az urándúsító magas biztonsági szintje ellenére a vírus képes volt megfertőzni az vezérlő számítógépeket, és átvenni az irányítást felettük. A kártevő több biztonsági rést kihasználva vette át az irányítást a szoftverek

[31] Coorporative Cyber Defense Center of Exelance in Tallin

[32] A gázcentrifuga az urán dúsításhoz szükséges eszköz, amely nagy sebességgel forogva a gáz halmazállapotú urán-izotópokat szétválasztja.

felett. Az újdonságot az jelenti, hogy nem egy általános parancs végrehajtása volt a feladata, ahogy az a vírusok többségére jellemző. A vírusokat leginkább a válogatás nélküli adatlopásokra vagy szoftverek rombolására készítik, valamint önmaguk másolása és továbbküldésére programozzák. Ez utóbbi a Stuxnetre is igaz, az iráni felfedezése után százezres nagyságrendű számítógépben és hálózatban találták meg a világ minden pontján. Ez egy nagyon fontos momentumra utal, mivel addig, amíg a feladatát nem végezte el nem fedezték fel, tehát a vírus kifejezetten és célzottan a Natanz-i dúsító üzem centrifugáinak irányítására tervezték, illetve minden ilyen szoftverrel működtetett centrifugára.

A vírus felépítése

Ez a vírus egy teljesen új jelenség a számítógépes vírusok között. A féregnek nevezett csoportba tartozik, de sokkal összetettebb és kifinomultabb azoknál, ezt a programot nem egy általános célra tervezték, ahogy az ebbe a csoportba tartozó elődeit.[33] Ez a kártevő kifejezetten az ipari alkalmazások megfertőzése és azok irányítása volt a célja, ezen belül a centrifugáknak a tönkretételére.

„A Stuxnet olyan különleges számítógépes féreg, amely MS Windows operációs rendszert futtató gépeket fertőz, és azokon terjed, de hatását végső soron internetre nem kapcsolt ipari folyamatirányító rendszereken keresztül fejti ki. Támadja a folyamatok felügyeleti irányítását és adatgy1jtését (SCADA2), és nem csak kémkedik a célzott ipari rendszer után, hanem át is programozza azt. Az első olyan kártevő, mely programozható logikai vezérlők (PLC)[34] rootkitje, azaz rejtett, privilegizált módon fér hozzájuk, aláaknázva rajtuk a szabványos operációs rendszer vagy más alkalmazás m1ködését. A Stuxnet kivételes képességei ezen túl egyetlen gyártó termékeire összpontosulnak: a Siemens cég – f0leg vegyipar, energiatermelés, szállítás területén használatos – eszközeire (WinCC illetve STEP7)”. [37] (Cserháti 2011)

A vírus két tulajdonságában különbözik az elődeitől: egyrészt egy kifejezett célobjektum elérésére tervezték, úgy, hogy a célba juttatásához nem csupán az internetre hagyatkoztak, azt csak közvetítő közegnek használva, amihez a korábban már tárgyalt Social Engineeringet használták fel. Ugyanis az urándúsító üzem teljesen elszigetelt, nem kapcsolódik sem az internetre, sem az ország hálózatára. Tehát a vírus csak valamilyen adathordozó segítségével juthatott be az épület rendszerébe. Másrészt az előbbiekből következően terjedése közben észrevehetetlen kellett legyen. Mivel több rétegű parancssorral rendelkezik, ezért csak komoly kutatással lehet a nyomára akadni, így a pusztító tevékenységét csak abban a számítógépben kezdi meg, ahova szánták a készítői, tehát csak akkor lehet felfedezni, ha már a működését megkezdte.

A Stuxnet eredete

Az eredetéről csak feltételezéseket ismerünk, azonban a paramétereknek ilyen szintű ismerete komoly hírszerzési potenciált igényel.[35] A fejlesztés a hírszerzés mellet nagy költségekkel is párosul, tehát a magányos vagy az Anonymous típusú

[33] Számítógépes féreg
[34] Programmable Logic Controler
[35] Ipari kémkedés, iráni ügynökök fenntartása.

hacker-csoportosulásokat kizárhatjuk a készítők feltételezett csoportjából. Tehát vagy egy bűnözői csoport vagy terror szervezet remélt hasznot az elkészítéséből, de ezek a csoportok jellemzően felfedik magukat a remélt haszon érdekében. Mivel ilyen esemény nem következett be, illetve az említett magas szintű hírszerzés ténye alapján joggal feltételezhetjük, hogy állami szereplők állnak a háttérben.

A Stuxnet hatása

Az urándúsító üzemben okozott kár Irán számára valóban nagy volt − legalább két évvel is visszavethette a sikeres hasadóanyag előállításában −, de igazi hatása abban jelentkezik, hogy megnyitotta az utat a hasonló jellegű támadások előtt. Elsősorban azért mert egy teljesen új jelenséggel álltak szembe, egy olyan számítógépes támadással, amelynek a megelőzése, kivédésére tett erőfeszítések kimenetele minimum bizonytalan. Indoklásunk szerint, maradva az iráni példánál, ennek elsődleges oka, hogy a vírus olyan biztonsági réseket használt ki, amiről a gyártókon kívül senkinek- így az iráni mérnököknek, informatikusoknak-, a támadókat leszámítva nem volt tudomása.[36] Így a támadók mindig lépéselőnyben voltak, ebből következik, hogy a védekezés csak reakció tud lenni a támadásra. Még ha szimulált támadásokkal próbálnának lépést tartani a vírusgyártókkal, az rengeteg változót jelent az elhárítók számára, amelynek az anyagi vonzata is beláthatatlan. Nem csak a vírus terjedési módja az akadálya a sikeres megelőzésnek, hanem annak működési paramétereit sem sikerült teljes egészében megfejteniük a szakembereknek. Az eredeti Stuxnet felfedezése után ma már detektáltak módosított változatokat is úgy, mint a Gauss.[37] Felmerülhet a kérdés milyen következményei lesznek a kiberbiztonságra nézve ennek az új kártevőnek? Ha a program felépítését megfejtették és tovább fejlesztve újabb támadásokhoz használható, akkor a kritikus infrastruktúrák kiberfenyegetettsége új minőséget kap a jövőben.

* * *

Tanulmányunkban a kibervédelem jelentette veszélyeket, illetve ezek egy speciális szeletét igyekeztünk bemutatni, amely napjainkra a legnagyobb fenyegetést jelentik biztonságunkra nézve: a közösségi média a kritikus infrastruktúrák ellen irányuló kibertámadásokban betöltött szerepét. A kritikus infrastruktúrák komplex értelmezésének és a kibervédelem terén tapasztalt égető hiányosságok leküzdésének fontosságára több szerző hívta fel a figyelmet, de megítélésünk szerint nem lehet elégszer hangsúlyozni e terület relevanciáját, annál is inkább, hogy a technikai fejlődés új eszközöket ad a támadók kezébe. Tanulmányunk célja −

[36] Ilyen biztonsági rés például, hogy a MS Windows az autorun.inf fájlokat automatikusan elindítja, a microsoft fejlesztő cégek számára kiadott digitális aláírásnak hozzáférhetősége, ezzel használója teljes jogosultságot szerzet a rendszerben, illetve a Win CC és a Simens PLC között működő step7 illesztő program gyenge védettsége.

[37] Böngészőkön keresztül lehallgatja a felhasználó munkamenetét valamint ellopja a jelszavakat és adatokat gyűjt a számítógép hálózati kapcsolatairól, futó folyamatokról, BIOS-ról és a CMOS RAM-ról, és a helyi-, a hálózati és a hordozható adattárolókról. valamint megfertőzi a hordozható adattárolókat ezzel terjed a gépek között.(http://tech.cert-hungary.hu/tech-blog/120810/ujabb-taggal-bovult-a-stuxnet-csalad [37](Cserháti2011)

ennek megfelelően − a döntéshozók figyelmének felhívását tűzte ki célul, hiszen a megfelelő védelemi képességek feltételeinek megteremtésében kulcsszereplők. Ennek érdekében példákon keresztül illusztráltuk a már bekövetkezett kibertámadásokat, amelyek alapjaiban rengetették meg és helyezték más paradigmába az információs műveletekről alkotott fogalmainkat.

Felvázoltuk, milyen keretek között támadható a kritikus infrastruktúra a közösségi média eszközein keresztül, hogy végül javaslatot tegyünk azon hiányosságok megszüntetésére, melyek kiküszöbölése nélkül nem lehet biztosítani a megfelelő kibervédelmet. Tanulmányunkban érintettünk három olyan területet (a hadsereg pozitív percepcionalizálásának lehetőségét, a közösségi média kríziskommunikációban való felhasználhatóságát, illetve a NATO kibervédelmi politikájának kitűzött céljai elvi deklarációjának és megvalósulásának összehasonlítását), melyek jelen cikk terjedelmi korlátaiból kifolyólag csupán rövid ismertetésére nyílt módunk, de valljuk, a bennük rejlő potenciál további kutatásokat, mélyre szántóbb bemutatást igényel, külön-külön rájuk specializált vizsgálatot követően.

IRODALOMJEGYZÉK

Tanulmányok

BABOS, Tibor: „Globális közös terek” a NATO-ban, Nemzet és Biztonság, 2011. április

CSIKI, Tamás: A NATO védelmi minisztereinek brüsszeli találkozója, 2011. július

HORVÁTH, Attila: Az élelmiszerellátási lánc kritikus infrastruktúrái, terrorfenyegetésének jellemzői, Hadmérnök, 2009., p. 441.

HORVÁTH, Attila: Hogyan értessük meg a kritikus infrastruktúra komplex értelmezésének szükségességét és védelmének fontosságát, Hadmérnök, 2010.

HORVÁTH, Attila: Terrorfenyegetettség, célpontok, nagyvárosok közlekedése, Nemzetvédelmi Egyetemi Közlemények. A Zrínyi Miklós Nemzetvédelmi Egyetem Tudományos Lapja. 10. évfolyam 3. (tematikus) szám. Budapest, 2006.p. 16

KAPLAN, Andreas- HAENLEIN, Michael: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizonts, 2010

KOVÁCS, László − KRASZNAY, Csaba: Digitális Mohács- Egy kibertámadási forgatókönyv Magyarország ellen, Nemzet és Biztonság, 2010

KOVÁCS, László: Informatikai hadviselés kínai módra, Nemzet és Biztonság, 2009. szeptember

Office of The Chief of Public Affairs: *U.S. Army Social Media Handbook*, 2011. http://fbmonitor.com/social_media_handbook.pdf

PRENSKY, Marc: Digitális bennszülöttek, digitális bevándorlók, 2001.

RÁCZ, Lajos: Informatikai hadviselés nem csak kínai módra, Nemzet és Biztonság, 2010. február

SZENES, Zoltán: Új NATO-stratégia, Nemzet és Biztonság, 2010. december

ZMNE SVKI: A lisszaboni NATO- és EU–USA csúcstalálkozó agendája és várható eredményei, 2010/17.

Internetes hivatkozások

[1] Dávid Imre: Obama: a kibertámadások komoly veszélyt jelentenek, Computer World, 2012. július 23., http://computerworld.hu/obama-a-kibertamadasok-komoly-veszelyt-jelentenek-20120723.html Letöltés ideje: 2012. október 6.

[2] Staff Writer: The EU points its guns at cyber criminals, The Information Daily, 2012. augusztus 9., http://www.egovmonitor.com/node/53238
Letöltés ideje: 2012. október 6.
[3] Cyberattacks up 400% since 2011, Info Security, 2012. augusztus 30., http://www.infosecurity-magazine.com/view/27876/cyberattacks-up-400-since-2011/
Letöltés ideje: 2012. október 6.
[4] Agencies: China world's biggest cyber attack victim, says report, Global Times, 2012. július 5., http://www.globaltimes.cn/content/719138.shtml
Letöltés ideje 2012. október 6.
[5] Phil Muncaster: India to greenlight state-sponsored cyber attacks, The Register, 2012. június 11., http://www.theregister.co.uk/2012/06/11/india_state_sponsored_attacks/?goback=.gde_3502864_member_123369450
Letöltés ideje 2012. október 6.
[6] A New Kind of Warfare, The New York Times- The Opinion Pages, 2012. szeptember 9., http://www.nytimes.com/2012/09/10/opinion/a-new-kind-of-warfare.html?_r=4&ref=opinion& Letöltés ideje: 2012. október 6.
[7] Hancu: Az oroszok visszabombázzák Észtországot az online kőkorszakba, Index, 2007. május 31., http://index.hu/tech/net/eszt290507
Letöltés ideje: 2012. október 6.
[8] Charles Clover: Kremlin- backed group behind Estonia cyber blitz, Financial Times, 2009. március 11., http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html
Letöltés ideje: 2012. október 6.
[9] Dajkó Pál: Ifjú oroszok hajtották végre az észtek elleni internetes támadást, IT Café, 2009. március 12., http://itcafe.hu/hir/kibertamadas_esztorszag_oroszorszag.html
Letöltés ideje: 2012. október 6.
[10] Project Grey Goose: Russia/Georgia Cyber War – Findings and Analysis, 2008. október 17., http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report
Letöltés ideje: 20012. októbet 2.
[11] Az Észak- Atlanti Szerződés, 1949. április 4., http://www.nato.int/cps/en/natolive/official_texts_17120.htm
Letöltés ideje: 2012. szeptember 28.
[12] Ellen Nakashima: U.S. official says cyberattacks can trigger self-defense rule, The Washington Post- National Security, 2012. szeptember 19., http://www.washingtonpost.com/world/national-security/us-official-says-cyberattacks-can-trigger-self-defense-rule/2012/09/18/c2246c1a-0202-11e2-b260-32f4a8db9b7e_story.html
Letöltés ideje: 2012. szeptember 20.
[13] Brian Wheeler: Cyber attacks 'acts of war' - Sir Richard Mottram, BBC News, 2011. február 16., http://www.bbc.co.uk/news/uk-politics-12485147
Letöltés ideje: 2012. szeptember 20.
[14] Robert Lemos: U.S., China Talks Address Cyber-Weapons, Not Cyber-Spying, eWeek, 2012. augusztus 14., http://www.eweek.com/c/a/Security/US-China-Talks-Address-CyberWeapons-not-CyberSpying-329861/
Letöltés ideje: 2012. szeptember 20.

[15] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012 (II.21.) kormányhatározat, Magyar Közlöny, 2012. évi 19. szám, http://www.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf
Letöltés ideje: 2012. október 1.
[16] Dajkó Pál: Elkészült az információbiztonsági törvény tervezete, IT Café, 2012. szeptember 26., http://itcafe.hu/hir/muha_lajos_kibertorveny_kibervedelem_tervezet.html
Letöltés ideje: 2012. október 1.
[17] Négymillió pécéből áll az elpusztíthatatlan zombihálózat, Index, 2011. június 30., http://index.hu/tech/2011/06/30/negymillio_pecebol_all_az_elpusztithatatlan_zombihalozat/ , Letöltés ideje: 2012. szeptember 25.
[18] Kiberháború zajlott a Kaukázusban, SG.hu, 2008. augusztus 14., http://www.sg.hu/cikkek/62049/kiberhaboru_zajlott_a_kaukazusban
Letöltés ideje: 2012. október 3.
[19] Nagy Balázs András: Gyársoron települő vírushálóra támad a Microsoft, MobilPort, 2012. szeptember 14., http://www.mobilport.hu/hirek/20120914/gyarsoron_telepulo_virushalora_tamad_a_microsoft/ , Letöltés ideje: 2012. október 4.
[20] Irán betiltja a Google-t és a Gmailt, Index, 2012. szeptember 24., http://index.hu/tech/2012/09/24/iran_betiltja_a_google-t_es_a_gmailt/
Letöltés ideje: 2012. október 5.
[21] Kirsty Walker: Farce of the Facebook spy: MI6 chief faces probe after wife exposes their life on Net, Daily Mail, 2009. július 6., http://www.dailymail.co.uk/news/article-1197757/New-MI6-chief-faces-probe-wife-exposes-life-Facebook.html
Letöltés ideje: 2012. október 2.
[22] Malte Spitz: Your phone company is watching, TED, 2012. június, http://www.ted.com/talks/lang/en/malte_spitz_your_phone_company_is_watching.html , Letöltés ideje: 2012. szeptember 25.
[23] Tell-all telephone, Zeit Online, http://www.zeit.de/datenschutz/malte-spitz-data-retention , Leöltés ideje: 2012. október 7.
[24] Barna József: Európában kikapcsolja az arcfelismerést a Facebook, IT Cafe, 2012. szeptember 24., http://itcafe.hu/hir/facebook_europa_arcfelismeres_tag_suggestions.html
Letöltés ideje: 2012. szeptember 27.
[25] Kémkedhet utánunk a kamerás telefon, Index, 2012. október 1., http://index.hu/tech/2012/10/01/kemkedhet_utanunk_a_kameras_telefon/ , Letöltés ideje: 2012. október 1.
[26] Symantec: Norton Cybercrime Report-2012, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
Letöltés ideje: 2012. október 4.
[27] Konrad: Pukkadjatok meg, Onlinemarketing blog, 2011. december 12., http://onlinemarketing.blog.hu/2011/12/11/pukkadjatok_meg
Letöltés ideje: 2012. október 7.
[28] Online and social media division, Office of The Chief of Public Affairs:*U.S. Army Social Media Handbook*, 1500 Pentagon, Washington DC, 2011. január, http://fbmonitor.com/social_media_handbook.pdf
Letöltés ideje: 2012. szeptember 29.

[29] Marton Péter: Hírszerzési trükkök: iraki gerillák vs. Apache helikopterek, Kprax blog, 2012. március 16., http://kprax.blog.hu/2012/03/16/hirszerzesi_trukkok_iraki_gerillak_vs_apache_helikopterek , Letöltés ideje: 2012. szeptember 28.
[30] Dan Dieterle: Surviving a Public Infrastructure or Energy Grid Attack, Infosec Island, 2012. szeptember 28., http://www.infosecisland.com/blogview/22108-Surviving-a-Public-Infrastructure-or-Energy-Grid-Attack.html
Letöltés ideje: 2012. szeptember 28.,
[31] Nate Anderson: Who Was That Masked Man?, Foreign Policy, 2012. január 31. http://www.foreignpolicy.com/articles/2012/01/31/who_was_that_masked_man
Letöltés ideje: 2012. szeptember 29.
[32] Hancu: Az internet legyőzte a SOPA-t, Index, 2012. január 16., http://index.hu/tech/2012/01/16/az_internet_legyozte_a_sopa-t/
Letöltés ideje: 2012. október 2.
[33] Varga Gergely: A nato új, lisszaboni stratégiai koncepciója. Nemzet és Biztonság 2010 december.
[34] Sztrenák György: Lisszaboni csúcstalálkozó.
[35] Csiki Tamás: A NATO védelmi minisztereinek brüsszeli találkozója. Nemzet és Biztonság 2011 július.
[36]. Defending the networks The NATO policy on Cyber Defence http://www.nato.int/cps/en/natolive/official_texts_68828.htm#cyber (2012. október 12.)
[37] Cserháti András: A Stuxnet vírus és az iráni atomprogram. Nukleon 2011. március
[38]http://tech.cert-hungary.hu/tech-blog/120810/ujabb-taggal-bovult-a-stuxnet-csalad
(2012. október 10.)

Feldolgozott jogszabályok

2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
Magyarország Nemzeti Biztonsági Stratégiája
http://www.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf