A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon

Berki Gábor[1]

Absztrakt:

Magyarország világszinten is az elsők között van a kibervédelem szabályozásának kérdésében. A Magyar Kormány 2013 márciusában kormányhatározatot fogadott el Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. A stratégia megfogalmazott célja, a kibertér biztonsági környezetének elemzése alapján azon nemzeti célok, stratégiai irányok, feladatok és átfogó kormányzati eszközök meghatározása, amelyek alapján hazánk érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is. A tanulmány célja, hogy bemutassa a hazai kibervédelem fejlődését, jogszabályi környezetét, jelenlegi struktúráját és a fejlesztés lehetséges irányait.

Kulcsszavak: kibertér, kiberfenyegetések, kibervédelem, információbiztonság

Abstract:

Hungary belongs to the leading states in the field of cybersecurity regulation. In March 2013, the Hungarian Government adopted a government resolution on the National Cyber Security Strategy of Hungary. Based on an analysis of cyberspace security environments, the declared aim of the strategy is the definition of national goals, strategic directions, tasks and comprehensive government tools that allow our country to enforce its national interests in the Hungarian cyberspace as part of the global cyberspace. The purpose of this study is to show the development of domestic cyber protection, its legal environment, its current structure and the possible directions of future development.

Keywords: cyberspace, cybertreaths, cyberdefence, informationsecurity

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorjelölt,
e-mail: berki.gabor@uni-nke.hu, ORCID azonosító: 0000-0002-9531-4074

Bevezetés

Napjainkra a társadalmak informatikai rendszerektől való függése olyan mértékben megnövekedett, hogy nemcsak a pénzügyi szektor, a közigazgatás, az egészségügy, hanem az átlagemberek mindennapjai is elképzelhetetlenek számítógépek nélkül. Használjuk őket az iskolában, a munkahelyeken, utazás közben és otthonainkban. Kikapcsolódásként a világhálón keresünk szórakozást. Ezt bizonyítja az az adat is, mely szerint 2017. december végén a föld lakosságának 54,4 százaléka, közel 4,2 milliárd ember használt Internetet (ezen belül Európa lakosságának 85,2 százaléka és Észak-Amerika lakosságának 95 százaléka)[2].

Ezek az eszközök, rendszerek nagyban megkönnyítik a mindennapi életet, munkafolyamatokat automatizálnak, gördülékenyebbé teszik a hivatali ügyintézéseket, szabadabb, gyorsabb kommunikációt biztosítanak mindenki számára. Nem szabad ugyanakkor megfelejtkeznünk azokról a kockázatokról sem, amelyek ezen eszközök használata során felmerülhetnek. A sajtóban nap mind nap hallani lehet különböző kibertámadásokról, az időről időre felbukkanó és rengeteg problémát okozó zsarolóvírusokról, a feltört kormányzati és katonai rendszerekről, kiberkémek általa ellopott titkokról, kiberbűnözők jóvoltából kiürített bankszámlákról vagy elveszett kriptovalutákról[3].

A világon már mindenhol felismerték a kiberbiztonság fontosságát, a legtöbb helyen már született törvényi szabályozás ezekről a kérdésekről, stratégiák láttak és látnak napvilágok a teendőkről. Kampányokat szerveznek, hogy felhívják a figyelmet a kiberbiztonság fontosságára. Legjobb példa erre az Európai Kiberbiztonsági Hónap, amelyet az Európai Hálózatbiztonsági Ügynökség szervez minden év októberében. A rendezvénysorozat célja a kiberbiztonsági tudatosság növelése, valamint a kibertérben megjelenő fenyegetések széles körben történő megismertetése. A Kiberbiztonsági Hónap keretében képzések, tudatosító előadások és konferenciák kerülnek megszervezésre az egész Európai Unióban. A Nemzeti Közszolgálati Egyetem is csatlakozott a kampányhoz, ennek kapcsán számos programot szervezett a témában. De nem csak az Európai Unióban, hanem szerte a világban kormányzati szervek és a piaci szereplők is komoly erőfeszítéseket tesznek a kibervédelem területén. E tanulmány célja, hogy bemutassa a kibervédelem fejlődését Magyarországon, a korai lépésektől a törvényi szabályozáson át a napjainkra kialakult struktúrákig. Első lépésben azonban tisztáznunk kell né-

[2] Internet World Stats https://www.internetworldstats.com/stats.htm (letöltve: 2018.08.01)

[3] A kriptovaluta olyan digitális eszköz, mely csereeszközként vagy manapság fizetőeszközként is funkcionál. Titkosítást használ a tranzakciók biztonságossága érdekében. A kriptovaluták a digitális valuták egy részhalmazát képviselik, de besorolhatók az alternatív valuták vagy a virtuális valuták csoportjába is. Például Bitcoin, Ethereum.

hány alapfogalmat, mint például, hogy mit is értünk kibertér alatt, illetve, hogy milyen fenyegetések érhetik innen a felhasználókat.

A kibertér fogalma

A kibertér fogalmát William Gibson tudományos-fantasztikus szerző alkotta meg 1984-es Neurománc című regényében. Úgy írta le, mint egy számítógép-hálózatok által teremtett világot, tele mesterséges intelligens lényekkel és felhasználók milliárdjaival. A Enciklopédia Britannica megfogalmazása szerint *„a kibertér egy alaktalan, vélhetően „virtuális" világ, amely számítógépek, internet-képes eszközök, szerverek, routerek és az internet-infrastruktúra egyéb elemeinek összekapcsolása révén jön létre."*[4] Hétköznapi megfogalmazásban számítógépek, számítógép-hálózatok, az ezeket összekötő kommunikációs csatornák, az itt futó alkalmazások és az itt tárolt adatok alkotta virtuális világ összefoglaló neveként hivatkozhatunk rá. Nagyon sok kutató, szervezet próbálta már meghatározni a kiberteret, ennek megfelelően nagyon sok definíció is született rá. Az Egyesült Államok Védelmi Minisztériuma által kiadott és 2016 februárjában pontosított katonai terminológiai szótárában meghatározottak szerint a kibertér *„Az információs környezet egy globális tartománya, amely tartalmazza az informatikai infrastruktúrák, a bennük tárolt adatok egymással összefüggő hálózatát, beleértve az internetet, a távközlési hálózatokat, a számítógép rendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket"*[5].

Hazánkban a kibertér hivatalos megfogalmazására a 2013-ban megjelent, a Magyarország Nemzeti Kiberbiztonsági Stratégiája nevet viselő 1139/2013. számú kormányhatározatban került sor. Eszerint „a *kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint, ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett."*

A fenti meghatározásokból leszűrhető, hogy a kibertér az összekapcsolt elektronikus információs rendszerek és hálózatok összessége. Így a hálózatba nem kötött, önálló számítógépek nem részei a kibertérnek. Ha az összekapcsolás módját tekintjük, amely nemcsak vezetékes lehet, hanem vezeték nélküli is, a

[4] Jennifer BUSSELL: Cyberspace - Enciklopedia Britannica (letöltve: 2018.08.01)

[5] Department of Defense Dictionary of Military and Associated Terms http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-07-25-091749-087 p.59 (Letöltés ideje: 2018.08 01.)

kibertér részének kell tekintenünk az elektromágneses spektrumot is, amelyen keresztül a kommunikáció történik. A vezeték nélküli kommunikáció legközismertebb formája a Wi-Fi, amely már szinte mindenhol elérhető, de ide kell sorolnunk a mobilhálózatokon keresztül igénybe vehető adatforgalmat is.

A kibertérből érkező fenyegetések

Ez a fejezet megvizsgálja, hogy milyen fenyegetések érkezhetnek a kibertérből. Alapvetően a támadások az informatikai rendszereken tárolt és kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása ellen irányulhatnak. Az adatok bizalmasságán azt értjük, hogy azt csak az arra jogosultak és csak a jogosultsági szintjüknek megfelelő mértékben ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. A sértetlenség az adat azon tulajdonsága, mely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyezik, nem történt benne illetéktelen változtatás. Ebbe beleértjük a hitelességét is, hogy a megfelelő forrásból származik-e. A rendelkezésre állás arra vonatkozik, hogy az adatot az arra jogosultak a szükséges helyen és időben elérhessék, használhassák. A rendszerelemek rendelkezésre állása pedig a rendeltetésszerű használat lehetőségét jelentik.[6]

Ha megvizsgáljuk a támadások indítékait, csoportosíthatjuk a támadók körét, akiknek a szándékai, rendelkezésre álló erőforrásai és szaktudásuk nagymértékben eltérő lehet. A szakirodalmakban a fenyegetések többféle csoportosításával is találkozhatunk, jelen tanulmány a szerző által legfontosabbnak tartott fenyegetéseket vizsgálja meg.

Ezek a következők:

- kiberbűnözés;
- kiberkémkedés;
- hacktivizmus;
- kiberterrorizmus;
- kiberhadviselés.

Kiberbűnözés:
A szerző meghatározása szerint a kiberbűnözés számítógépek és számítógépes rendszerek segítségével, vagy számítógépek és hálózatok kárára elkövetett bűncselekmények gyűjtőfogalma. Motivációjáról az esetek többségében bátran kijelenthetjük, hogy az az anyagi haszonszerzés.

[6] MUHA Lajos, KRASZNAY Csaba: Az elektronikus információs rendszerek biztonságának menedzselése Budapest, NKE, 2014., ISBN:978-615-5491-65-8 p.10

2001. november 23-án, Budapesten 30 ország írta alá a Számítástechnikai Bűnözés Elleni Egyezményt, melyben részletesen leírták az ilyen típusú bűncselekményeket, az államok jogharmonizációjához szükséges lépéseket és az együttműködés kereteit. Három fő részre osztották a számítógépes bűncselekményeket.

1. *A számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények*
   Ide tartozik például a jogtalan belépés, az adatok vagy rendszerek sért lensége elleni cselekmények, vagy az eszközökkel történő visszaélés.
2. *Számítástechnikai bűncselekmények*
   Ez alatt a számítógépes hamisítás és a csalás fogalmának kifejtésére került sor.
3. *A számítástechnikai adatok tartalmával kapcsolatos bűncselekmények*
   Ez a passzus a gyermekpornográfiával szembeni eredményesebb fellépést lehetővé tévő intézkedéseket tartalmazza.[7]

A szükséges intézkedéseket már minden ország megtette és beiktatta jogrendszerébe a megfelelő paragrafusokat, így könnyebbé vált a fellépés ezekkel a bűncselekményekkel szemben. A sikeres harc azonban így sem egyszerű, hisz ezen bűncselekmények jellemzői közé tartozik a gyorsaság és a nemzetköziség, amely nagyon megnehezíti a felderítést. Ahogy az internetpenetráció növekszik a világban, úgy nő a kiberbűncselekmények száma és az általa okozott anyagi kár is.

A kiber bűncselekmények egy része napjainkra kampányjelleget öltött, a bűnözők zsarolóvírusok terjesztésével próbálnak operálni, adathalász kísérleteket indítanak, egyre nagyobb számban és egyre kifinomultabb módszerekkel. 2017 májusában például kiterjedt zsarolóvírus kampány indult világszerte. A rosszindulatú kód, amely WannaCry néven vált közismerté, pár óra alatt gépek tízezreit fertőzte meg és titkosította a rajtuk található fájlokat. Komoly fennakadásokat okozott világszerte, például a brit kórházakban is, ahol tömegesen kellett műtéteket elhalasztani a használhatatlanná tett gépek miatt. A titkosítást csak egy bizonyos összeg átutalása esetén lettek volna hajlandóak feloldani a támadók. Nincs adat arra vonatkozóan, hogy hány áldozat fizetett és hogy ők megkapták-e a feloldó kódokat.

Hazánkban is egyre elterjedtebb a bankok, közüzemi szolgáltatók nevében küldött hamis e-mailek, amelyek különböző biztonsági frissítések elvégzésére vagy újonnan érkezett számlák befizetésére ösztönzik a felhasználókat, természetesen az e-mailben megadott link használatával.[8] Ezek a linkek hamisított, ám

[7] Számítástechnikai Bűnözés Elleni Egyezmény
http://www.jogiforum.hu/publikaciok/50 (Letöltés ideje: 2018.08 05.)

[8] BOLCSÓ Dániel: Vigyázzon, csalók a Díjnet nevében akarnak adatokat lopni

a bankok vagy cégek oldalával szinte megegyező formájú oldalakra mutatnak, ahol a belépési adatokat kívánják megszerezni. Ezek az adathalász támadások szerencsére még felismerhetőek a helytelen magyarsággal íródott levelek alapján, de ne legyenek illúzióink, a bűnözők, ezen a téren is fejlődni fognak. A kiber bűnözők elleni harc egyik alapvető eleme a tájékoztatás, a képzés, a felhasználói tudatosság növelése.

Kiberkémkedés:
A kémkedés vélhetően egyidős az emberiséggel. Nem csak a katonai titkok megszerzése jelent előnyt az ellenséggel szemben, hanem az ipari, pénzügyi, diplomáciai információk is az esetleges vetélytársakkal szemben. Az számítástechnikai eszközök elterjedése és az internet kialakulása kifejezetten hasznos volt a kémek számára, hiszen egy jó felkészült támadó képes akár a világ másik végén lévő informatikai rendszerbe is behatolni és onnan adatokat letölteni. Az Egyesült Államok kiberbiztonsággal foglalkozó hatóságai 2002-től észleltek olyan informatikai behatolás sorozatokat, amelyek a katonai, a kormányzati és a vállalati szektor informatikai hálózatait érintette. A vizsgálatok szerint Kínához köthető hackerek hosszú időn keresztül precízen megtervezett és kivitelezett támadásokon keresztül 10-20 terrabájtnyi anyagot töltöttek le a megtámadott rendszerekről. Az akcióban, amely a Titan Rain nevet kapta, érintett volt a NASA, a Lockheed Martin és a Pentagon is.[9]

2012 nyarának végén jelent meg egy új, kifejezetten kémkedésre kifejlesztett rosszindulatú program. A Gauss névre keresztelt kód elsősorban banki és egyéb hozzáférési adatokat gyűjtött a fertőzött rendszerből, majd továbbította azokat a C&C[10] szerverek felé. Egy biztonsági cég szerint a Gauss elsősorban Libanonban, Izraelben és a Palesztin területeken volt aktív, de az Egyesült Államokból is jelentettek fertőzést.[11]

2018 márciusában a Kaspersky Lab kutatói egy olyan kiberkémkedésre használt rosszindulatú programot azonosítottak, mely főleg a Közel-Keleten és Afrikában működött 2012-től 2018. februárig. A Slingshot-nak elnevezett kód feltört routereken keresztül támadta és fertőzte áldozatait, átvéve a kontrollt azok eszközei felett. A kutatók szerint számos egyedi és új technikát használtak a készítők

https://index.hu/tech/hoax/2018/06/07/vigyazzon_csalok_a_dijnet_neveben_akarnak_adatokat_lopni/ (Letöltés ideje: 2018.09.15.)

[9] KOVÁCS László: Információs hadviselés kínai módra
Nemzet és biztonság II. évfolyam 7. szám. Budapest, 2009. pp.: 35-44

[10] Command and Control - Irányító és vezérlő szerver

[11] CERT: Újabb taggal bővült a Stuxnet „család”
http://tech.cert-hungary.hu/tech-blog/120810/ujabb-taggal-bovult-a-stuxnet-csalad (Letöltés ideje: 2018.08.05.)

az ellopott adatok összesítésére. Ügyeltek a rejtőzködőképesség fejlesztésére és a kommunikáció elfedésére is.[12]

A fenti kiragadott példák is jelzik, a kiberkémkedés milyen jelentős problémává vált mind az üzleti, mind a kormányzati szektorban. Akárcsak a kiberbűnözés megelőzésében, itt is a felhasználói tudatosság fejlesztése az egyik legfontosabb feladat.

Hacktivizmus:

A hacktivizmus jelenségét is fontosnak tartom megemlíteni a kibertérből érkező fenyegetések sorában. A szó a hacker és az aktivista szavakból alakult ki. Leghírhedtebb képviselőjük az Anonymous csoport. Ez a laza szerveződésű internetes közösség vélt, vagy valós sérelmek megtorlásául vagy egyszerűen valamely ügyet felkarolva indít támadásokat internetes tartalmak, cégek, kormányzatok ellen.

Fő módszere a weboldalakat automatikus lekérdezésekkel megbénító túlterheléses támadás, amire magasztos hangnemben megfogalmazott webes szórólapjain toborozza a résztvevőket, rendszerint nem csak a 4chanon, hanem más csevegő szobákban és fórumokon is. A szaknyelven dosolásnak[13] nevezett támadásokban való részvételhez nem is kell más, csak pár ingyenesen letölthető szoftver, amelyek beszerzéséhez, használatához a felhasználók rendszerint már a szórólapokon megkapják a szükséges instrukciókat. Emlékezetes támadást indítottak a szcientológiai egyház ellen 2008-ban. Tiltakozásul az egyház által véleményük szerint elkövetett csalások, illetve az egyház által állítólag végzett agymosások miatt, kiterjedt támadásba kezdtek ellenük. A szolgáltatásmegtagadásos támadásokon kívül, amellyel elérhetetlenné tették az egyház honlapját, nyilvánosságra hoztak több száz iratot és dokumentumot, amelyeket számítógépes betörések útján szereztek.[14] Saját meghatározásuk alapján tiltakoznak és felléphetnek minden olyan jelenség ellen, amely a szólásszabadságot és az Internet szabadságát veszélyeztetik.

A legnagyobb visszhangot kiváltó támadássorozatuk a Wikileaks támogatását megakadályozó amerikai intézkedések miatt következett be. Mint az ismeretes, 2010-ben a Wikileaks több ezer titkos amerikai diplomáciai és katonai iratot jelentetett meg az Interneten a szólásszabadság jegyében. Ez komoly diplomáciai feszültséget és még komolyabb biztonsági problémákat okozott, elsősorban az amerikai hadsereg műveleti területein. Az amerikai kormány erős politikai nyo-

[12] Alexey Shulmin, Sergey Yunakovsky, Vasily Berdnikov, Andrey Dolgushev: The Slingshot APT FAQ
https://securelist.com/apt-slingshot/84312/ (Letöltés ideje: 2018.08.05.)

[13] DOS - Denial of Service – szolgáltatás-megtagadással járó támadás

[14] NEMES Dániel: Hackerek a szcientológia ellen
http://pcworld.hu/kozelet/hackerek-a-szcientologia-ellen-20080128.html
(Letöltés ideje: 2018.08.08.)

mást fejtett ki az oldal ellehetetlenítésére, többek között a finanszírozásával kapcsolatban. A PayPal, a Visa vagy a MasterCard e nyomás hatására nem engedélyezte a Wikileaks számláira történő utalásokat. Ennek hatására hirdette meg az Anonymous a fenti pénzintézetek elleni támadássorozatát, amelyben sikerült is kisebb fennakadásokat okozni az említett szolgáltatók rendszereiben. Ezekért a támadásokért 2013-ban 13 embert el is ítélt egy amerikai szövetségi bíróság.[15] 2015-ben a párizsi Charlie Hebdo szerkesztőségét ért támadás, majd a novemberi 129 emberéletet követelő merénylet után háborút hirdettek az Iszlám Állam ellen is.[16] Feltörték a terrorszervezet több szerverét, hozzájuk köthető Twitter és Facebook fiókokat és adataikat nyilvánosságra hozták.

Hosszan lehetne még sorolni a csoport által elkövetett támadásokat, a világ szerzői jogvédő hivatalaitól az arab tavasz támogatásán át a világméretű pedofilhálózat feltöréséig.

Céljaik néhány esetben támogathatók ugyan, de a módszereik veszélyesek és egyértelműen törvénytelenek. Nincsenek nevesített vezetőik, szervezetük decentralizált és tagjaik a világ minden részén megtalálhatók. Az, hogy milyen célpontot támadnak sikeresen, attól is függ, hogy mennyi támogatót tudnak megnyerni maguknak.

Nagyon sokszor elhangzik politikusok vagy éppen újságírók szájából, hogy az Anonymous csoport tagjai kiberterroristák. A szerző ezzel a véleménnyel nem ért egyet, álláspontja szerint a hacktivizmust nem lehet összemosni a terrorizmussal, hisz sem a pánikkeltés, sem az erre alkalmas erőszak nem tartozik az eszköztárukba.

Kiberterrorizmus:

A terrorizmus napjaink egyik központi problémája világszerte. Míg a 70-es évek terrorcselekményei elszigetelt jelenségek voltak és csupán néhány országot érintettek, mára már világméretűvé vált a fenyegetettség, gondoljunk csak az Iszlám Állam vagy a Boko Haram rémtetteire.

A terroristacsoportok is kihasználják a korszerű technológiák adta lehetőségeket, melyek segítségével gyorsabban, hatékonyabban tudják a számukra fontos információt megszerezni, illetve azokat célközönségük irányába eljuttatni. Ha az információtechnológia terrorista célú alkalmazását vizsgáljuk, akkor több terület is kiemelhető.

[15] Nate RAWLINGS: Anonymous Hackers Plead Guilty to PayPal Cyber Attack http://techland.time.com/2013/12/09/anonymous-hackers-plead-guilty-to-paypal-cyber-attack/ (Letöltés ideje: 2018.08.08.)

[16] Anna DUBUIS: Anonymous declares war on Islamic State after Paris attacks in chilling video: 'We will hunt you down' http://www.mirror.co.uk/news/world-news/anonymous-declares-war-islamic-state-6839030 (Letöltés ideje: 2018.08.08.)

Mivel a hagyományos vezetékes és mobil telefonok könnyen lehallgathatók a hatóságok által, ezért az Internet nyújtotta kommunikáció nagyon népszerű a terrorista szervezetekben. A sok helyről letölthető és könnyen kezelhető titkosító programok segítségével kódolhatják az üzeneteiket, így nehezítve meg a felderítésüket. Az utóbbi időben előszeretettel használják a különböző játékkonzolok játékainak azon funkcióit is, amelyek segítségével a játékosok kommunikálhatnak egymással.

Az információszerzés igen lényeges a terrorszervezetek számára és az internet adta lehetőségeket ki is használják. Ha beírjuk a Google keresőjébe a „How to make a bomb?" kérdést 244 000 000 találatot kapunk 0,36 másodperc alatt. Itt számtalan videót is találhatunk, amelyek lépésről-lépésre mutatják be a bombakészítés módszereit. De a terrorakciók szervezéséhez jó szolgálatot tehet például a Google Maps, melynek segítségével fel lehet térképezni akár egy potenciális támadás környezetét is. Számos épület 3D-s látványképei és alaprajzai is megtalálhatók a neten. A lehetőségek széles tárházát támasztja alá egy al-Kaida kézikönyv, ami szerint nyilvános forrásokból, többnyire az internetről a szükséges információk 80%-a megszerezhető.[17]

Az Internet nagyon lényeges eszköz a terroristáknak az eszméik, szervezeteik és tevékenységük bemutatására, hiszen a hagyományos médiákat nem használhatják propaganda célokra. Ezért saját web oldalakat üzemeltetnek itt számolva be tetteikről, céljaikról. Mindig hangsúlyozzák, hogy az ellenségeik hajthatatlansága miatt, céljaik elérésére nincs más lehetőségük, mint az erőszak. Saját magukat szabadságharcosnak állítják be és így próbálnak szimpátiát ébreszteni maguk és az ügyük iránt. A könnyen befolyásolgató embereket akár terrorcselekmények elkövetésére is ösztönözhetik az ilyen oldalak. A propaganda másik célja a félelemkeltés, a pszichológiai hadviselés. A legjobb példa erre az Iszlám Állam, amely professzionális szintre fejlesztette ezt a tevékenységet. Nap-nap után töltötték fel a különböző videomegosztó helyekre a hatásosan megvágott, HD minőségben felvett videóikat, elrabolt emberek lefejezéséről, elfogott katonák tömeges kivégzésekről. Ezekkel a felvételekkel nemcsak a keresztény világnak üzentek, hanem az ellenük harcoló muszlimoknak is. A módszer működött is, hisz katonai sikereiket nem egyszer az iraki vagy a szír hadsereg megfutamodásának köszönhették.

A terrorista szervezetek működésük finanszírozásához is felhasználják az Internetet, weboldalaikon, fórumokon gyűjtenek adományokat. Figyelemmel kísérik a közösségi oldalakat is, ahol azokat a felhasználókat, akik pozitívan nyilatkoznak hozzászólásaiban róluk, e-mailben keresik meg, hogy támogatást kérjenek tőlük. Természetesen nem terrorcselekmények támogatását kérik az olva-

[17] Timothy L. THOMAS: Al Qaeda and the Internet: The Danger of "Cyberplanning" http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/03spring/thomas.pdf (Letöltés ideje: 2018.08.08.)

sóktól, hanem árvaházakét, gyermekekét, amely sok esetben hatásos érvelésnek bizonyul.[18]

Biztosak lehetünk benne, ha egy terrorszervezetnek lenne lehetősége létfontosságú rendszerelemek elleni kibertámadásra, amellyel emberéleteket is veszélyeztetne, habozás nélkül megtennék. Szerencsére azonban még nincsenek birtokában annak a tudásnak, mely ilyen támadás kivitelezéséhez szükséges. Már törtek be rendszerekbe, loptak el adatokat, módosítottak honlapokat, de komolyabb támadást még nem sikerült véghezvinniük. Az nyilvánvaló, hogy ha egy hagyományos terrortámadást össze tudnának vonni egy kibertámadással, amely egymással összefügg, komoly károkat okoznának.

Kiberhadviselés:
A hagyományos fegyverekkel végrehajtott támadások kibertámadásokkal való ötvözése már a kiberhadviselés témaköréhez tartozik. A szerző véleménye szerint kiberhadviselésről abban az esetben beszélhetünk, ha egy ország egy másik ország számítógépes hálózatai, létfontosságú rendszerelemei ellen indít támadást informatikai és fizikai eszközökkel saját nevében vagy egy harmadik fél bevonásával. E harmadik fél lehet állam, valamilyen szervezet vagy csoport. Ezt azonban az elmúlt évek támadásaiban még egyszer sem sikerült bizonyítani, hiszen minden hírbe hozott ország határozottan tagadta a vádakat. Legjobb példa erre az Észtországot 2007-ben ért kiterjedt, több héten át tartó kibertámadás, mely egy szovjet hősi emlékmű eltávolítása nyomán keletkező konfliktus folyománya volt. A célpontok kiválasztása, a támadások összehangoltsága, precíz kivitelezése és hatékonysága arra mutatott, hogy e támadások hátterében szervezett erők állnak. Néhány esetben szakértők megállapították, hogy a támadások orosz szerverektől indultak, amit az orosz hatóságok természetesen tagadtak. Ugyanakkor a megtámadott szerverek jellegéből adódóan nyilvánvaló, hogy a támadások célja egyértelműen a balti állam kritikus információs infrastruktúrájának bénítása volt.[19]

Kibervédelem Magyarországon

Hazánkban már nagyon korán felismerték a szakemberek a információbiztonság fontosságát, így az első szabályzó már 1994-ben napvilágot látott. Ez volt a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságának 8. sz. ajánlása, egy informatikai biztonsági módszertani kézikönyv, amely egy tájékoztató volt az informatikai biztonság megteremtésének legfontosabb elemeiről. Ennek célja az

[18] HAIG Zsolt.: Internet terrorizmus
Nemzetvédelmi Egyetemi Közlemények, XI. évfolyam, 2. szám Budapest, 2007. pp.: 81-93.
[19] HAIG Zsolt, KOVÁCS László: Fenyegetések a cybertérből
Nemzet és biztonság I. évfolyam, 5. szám. Budapest, 2008. pp.: 61-69

volt, hogy a szervezetek felkészülhessenek az informatikai biztonsági koncepciójának kialakítására. A kézikönyv tartalmazott egy kockázatelemzési módszertant is.

1996-ban jelent meg a MeH ITB 12. sz. ajánlása, amely az informatikai rendszerek biztonsági követelményeit tartalmazta. Ezek nem csak logikai védelem előírásait jelentette, hanem részletes követelményeket és védelmi intézkedéseket is az informatikai biztonság adminisztratív és a fizikai védelem területeire, valamint a szervezeti, személyi és fizikai biztonság kérdéseire is.[20]

Sajnos azonban ezeket az elveket – néhány kivételtől eltekintve - nem sikerült a gyakorlatban megvalósítani, ugyanis az ajánlásokat nem tették kötelezővé. 2013-ban a kormány elfogadta Magyarország nemzeti kiberbiztonsági stratégiáját, amelyben rögzítették, hogy a megelőzésre épülő hatékony védelmi intézkedések útján elsődleges cél a kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése, az ehhez szükséges kormányzati koordináció és eszköztár erősítése.

Ezzel összhangban elfogadták a 2013. évi L. törvényt (továbbiakban: Ibtv.), amely, állami és önkormányzati szervek elektronikus információbiztonságáról szól. Ezzel hivatalosan is, törvénybe foglaltan kimondatott:

„A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.

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 a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.” [21]

A törvény rendelkezett az állami és önkormányzati szervezeteknél az elektronikus információs rendszer biztonságáért felelős személy kinevezéséről, aki felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. A törvényi megfelelés a következő feladatokat rótta az érintettekre:

- Elektronikus információs rendszerek biztonsági osztályba sorolása kockázatelemzés alapján
- Szervezet biztonsági szintbe sorolása

[20] Az informatikai biztonság kézikönyve
Verlag Dashöfer Ltd. Budapest, 2004. ISBN 9639313122 p.3.2.5

[21] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300050.tv
(Letöltés ideje: 2018.08.11.)

- Cselekvési terv a biztonsági osztály meghatározásánál megállapított hiányosságok megszüntetésére.

A törvény szerint a szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról. Itt kell megjegyezni, hogy a törvény az az állami és önkormányzati szervezetekre kötelező, a civil szférára nem.

A biztonsági osztályba és biztonsági szintbe sorolás követelményeit először a 77/2013. (XII. 19.) NFM rendelet szabályozta részletesen, amelyet 2015-ben a 41/2015. (VII. 15.) BM rendelet váltott fel. A szervezeteknek az ebben a rendeletben előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell megvalósítaniuk, amelyek támogatják:

- a megelőzést és a korai figyelmeztetést,
- az észlelést,
- a reagálást,
- a biztonsági események kezelését.

Az Ibtv.-hez kapcsolódva a 233/2013. (VI. 30.) Korm. rendelet rendelkezett az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről, amelyet szintén 2015-ben a 185/2015. (VII. 13.) Korm. rendelet váltott fel.

- Az addig a Puskás Tivadar Közalapítvány által üzemeltetett CERT-Hungary feladatait 2013. július 1-től a Nemzetbiztonsági Szakszolgálat égisze alatt a Kormányzati Eseménykezelő Központ (GovCERT) vette át. Feladatai a következők lettek:
- Nonstop (0/24 órás) ügyeleti rendszer működtetése.
- Hálózatbiztonsági szolgáltatásokat nyújtása a támogatott közigazgatási és kritikus információs infrastruktúrákat üzemeltető szervek részére.
- Mint az országon belüli koordinációs szervezet, az internetet támadási csatornaként felhasználó incidensek kezelését és elhárításának koordinálásának ellátása.
- A felismert és publikált szoftver sérülékenységek közzététele. A szoftver sérülékenységek kockázatértékelés után, magyar nyelven, a honlapján történő publikálása, illetve jelentések és hírlevelek formájában a partnerek értesítése.
- A Központ szolgáltatások (preventív információ-megosztás és operatív incidens-kezelés) a kormányzati szervezetek és önkormányzatok részére történő nyújtása.

- A magyar társadalom felkészítése az internet minél tudatosabb és biztonságosabb használatára, amelynek keretében oktatási anyagokat dolgoz ki, tréningeket tart, felvilágosító, szemléletformáló kampányokat szervez.[22]

Megalakításra került a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (továbbiakban: LRLIBEK) a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságán. Az LRLIBEK feladatait a 185/2015. (VII. 13.) Korm. rendelet, valamint a 187/2015. (VII.13.) Korm. rendelet szabályozza, amelyek szerint fő feladatai:

- Ellátja a nemzeti létfontosságú rendszerelemként azonosított informatikai rendszerek és hírközlő hálózatok felé irányuló, a globális kibertérből érkező beavatkozások elhárításának koordinálását,
- Rendszeres tájékoztatást ad a nemzeti létfontosságú rendszerelemként azonosított informatikai rendszerek és hírközlő hálózatok felé a felismert és publikált sérülékenységekről,
- Más hálózatbiztonsági szervezettől átvett információk és adatok alapján, a nemzeti létfontosságú rendszerelemet érintő, a globális kibertérből érkező beavatkozást, és az internet-forgalomba való beavatkozásra utaló jeleket kiértékeli, és folyamatos ügyeleti rendszerén keresztül értesíti a létfontosságú rendszerelem üzemeltetőjét, valamint az érintett hálózatbiztonsági és létfontosságú elektronikus információs rendszer és létesítmény üzemeltetőjét,
- A megelőzés érdekében a szükséges technikai beavatkozásokat elvégzi, és a Belügyminisztérium és szervei érintett informatikai munkatársai részére képzéseket szervez, tart.[23]

Az állami és önkormányzati szervezetek elektronikus információs rendszerei hatósági felügyeletét a 187/2015. (VII.13.) Korm. rendelet szerint a Nemzeti Elektronikus Infromációbiztonsági Hatóság végzi.

Az operatív szintű szervek mellett stratégiai szintű szervezetek is létrejöttek, amelyek közül a Nemzeti Kiberbiztonsági Koordinációs Tanácsot (továbbiakban: Tanács) érdemes kiemelni. A Tanács a kormány javaslattevő, véleményező szerve lett és összehangolta a védelmi tevékenységeket. A Tanács munkáját az általa felkért gazdasági, tudományos és civil szféra felsővezetőiből álló Kiberbiztonsági

[22] Kormányzati Eseménykezelő Központ honlapja
http://www.cert-hungary.hu/node/1 (Letöltés ideje: 2018.08.11.)

[23] BM OKF honlapja
http://www.katasztrofavedelem.hu/index2.php?pageid=lrl_ibek (Letöltés ideje: 2018.08.11.)

Fórum segítette, amely a Tanács munkáját véleményező és javaslattevő szervként támogatta.

A Tanács koordinációs tevékenységét, valamint döntéseinek végrehajtását ágazati és funkcionális kiberbiztonsági munkacsoportok segítik.

Ezzel a struktúrával Magyarország a kibervédelem tekintetében a világ élvonalába került. 2013 márciusában a kormány elfogadta Magyarország Nemzeti Kiberbiztonsági Stratégiáját (1139/2013. (III.21.) Korm. határozat), melyben rögzítette, hogy a megelőzésre épülő hatékony védelmi intézkedések útján elsődleges cél a kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése, az ehhez szükséges kormányzati koordináció és eszköztár erősítése.

2015-ben az Országgyűlés az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról szóló 2015. évi CXXX. törvény elfogadásával módosította az információbiztonsági törvényt. Az információbiztonsági törvény felülvizsgálatával párhuzamosan a Kormány, valamint a Belügyminisztérium elvégezte a végrehajtási rendeletek felülvizsgálatát is. Ezek alapján a fent már említett 77/2013. és 233/2013. rendeletek hatályon kívül kerültek. Az átalakítás a szervezeti struktúrát is érintette. A 2014-es kormányzati átalakítás eredményeként már a korábbiakban a Belügyminisztériumhoz került a Nemzeti Biztonsági Felügyelet és a Nemzeti Elektronikus Információbiztonsági Hatóság is.

Az információbiztonsági törvény és annak végrehajtási rendeleteinek módosításával a Nemzeti Biztonsági Felügyelet sérülékenységvizsgálati szakhatósági feladatköre megszűnt, azt a Nemzetbiztonsági Szakszolgálat vette át.[24]

2015. október 1-jétől megalakult a Kormányzati Eseménykezelő Központot (GovCERT-Hungary), a Nemzeti Elektronikus Információbiztonsági Hatóságot és az E-biztonsági Intelligencia Központot (NBF-CDMA) egységes keretben magába foglaló, koordináltabb, hatékonyabb feladat-végrehajtást és információáramlást lehetővé tevő Nemzeti Kibervédelmi Intézet. Ezen intézkedésnek köszönhetően a Nemzeti Kibervédelmi Intézet az elektronikus információs rendszerek teljes információbiztonsági életciklusára vonatkozóan feladatkörrel rendelkezik, és nyomon tudja követni és segíteni tudja annak alakulását, a tervezési szakaszt, a szabályozást az ellenőrzést, valamint az incidenskezelést egyaránt. A Nemzeti Kibervédelmi Intézeten belül három szervezeti egység különül el a tevékenységüknek megfelelően, a Nemzeti Elektronikus Információbiztonsági Hatóság, a

[24] MISÁK István: Módosult információbiztonsági előírások http://www.jogiforum.hu/hirek/34135 (Letöltés ideje: 2018.08.11.)

Kormányzati Eseménykezelő Központ incidenskezelési szakterülete, valamint a Biztonságirányítási és Sérülékenység vizsgálati terület.[25]

Miután megjelent a Nemzeti Kiberbiztonsági Stratégia, 2013 szeptemberében kiadásra került a Magyar Honvédség Kibervédelmi Szakmai Koncepciója is. A dokumentum összhangban van a Nemzeti Katonai Stratégiával és a NATO Stratégiai Koncepciójában elfogadott kibervédelmi alapelvekkel. Kimondja, amit a NATO csak a 2016-ban, a varsói csúcstalálkozón deklarált, hogy a kibertér egyenrangúvá vált a hagyományos hadszínterekkel, amelyben különböző típusú felderítő, támadó vagy védelmi műveletek folyhatnak. Kijelöli azokat a létfontosságú rendszerelemeket, amelyek nélkülözhetetlenek a honvédelmi feladatok ellátásához. Meghatározott egy három lépcsős menetrendet a Magyar Honvédség Kibervédelmi Képességének kialakítására. A három lépcső a kezdeti, alap és a teljes képességeket fedi le. Többek között célként tűzi ki a létfontosságú információs rendszerelemek védelmét, sebezhetőségeinek csökkentését, az esetleges károk mielőbbi felszámolását. Fontos helyen említi a kutatás-fejlesztés erősítését és az oktatási feladatok fontosságát.[26] 2017. IV. 28-án jelent meg a honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól szóló 15/2017. számú HM utasítás. Ez leírja a Katonai nemzetbiztonsági Szolgálat alárendeltségében dolgozó Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ feladatait, a honvédelmi célú elektronikus információs rendszerek biztonsági felügyelete során ellátandó hatósági feladatokra, az eseménykezelésre és a sérülékenységvizsgálatra vonatkozó közös szabályait.[27]

Következtetések

A fentiek alapján elmondható, hogy hazánkban a kibervédelem jól szabályozott, megfelelő törvényi háttérrel és szervezetrendszerrel rendelkezik. Ez azonban nem jelenti azt, hogy ne lenne szükség további fejlesztésekre és minden rendben

[25] Nemzeti Kibervédelmi Intézet honlapja
http://nbsz.hu/?mid=42 (Letöltés ideje: 2018.08.11.)

[26] HAIG Zsolt: Információ, társadalom, biztonság
NKE, Budapest 2015. ISBN 978-615-5527-08-1 p.250-251

[27] 15/2017. (IV. 28.) HM utasítása honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17U0015.HM&timeshift=fffffff4&txtreferer=00000001.TXT (Letöltés ideje: 2018.08.11.)

lenne. A kiberbiztonság mindenki ügye kell, hogy legyen, nemcsak azoké, akiket erre a törvény kötelez. Minél szélesebb körben kell elvégezni a tudatosítást, minél több emberhez kell eljuttatni a kibervédelemmel kapcsolatos információkat. Fejleszteni kell a nemzetközi együttműködést, az oktatást, a fiatalok körében a biztonságos, értékteremtő és tudatos internethasználatot, fejleszteni az intézményrendszert, ösztönözni a kiberbiztonsággal kapcsolatos kutatás-fejlesztést, hatékonyabbá kell tenni a kiberbűnözés elleni fellépést és végül, de nem utolsó sorban meg kell teremteni a megelőző védelmet szolgáló specifikus elhárító- és támadóképességet, létre kell hozni ennek szabályozási és szervezeti kereteit, amely elősegíti a biztonság fenntartását.

Felhasznált irodalom

- p. 59. (Letöltés ideje: 2018.08 01.)
- BOLCSÓ Dániel: Vigyázzon, csalók a Díjnet nevében akarnak adatokat lopni https://index.hu/tech/hoax/2018/06/07/vigyazzon_csalok_a_dijnet_nevében_akarnak_adatokat_lopni/ (Letöltés ideje: 2018.09.15.)
- Jennifer BUSSELL: Cyberspace - Enciklopedia Britannica http://www.britannica.com/topic/cyberspace (Letöltés ideje: 2018.08.01.)
- Anna DUBUIS: Anonymous declares war on Islamic State after Paris attacks in chilling video: 'We will hunt you down' http://www.mirror.co.uk/news/world-news/anonymous-declares-war-islamic-state-6839030
- HAIG Zsolt.: Internet terrorizmus Nemzetvédelmi Egyetemi Közlemények, XI. évfolyam, 2. szám Budapest, 2007. pp.: 81-93.
- HAIG Zsolt: Információ, társadalom, biztonság NKE, Budapest 2015. ISBN 978-615-5527-08-1 p.250-251
- HAIG Zsolt, Kovács László: Fenyegetések a cybertérből Nemzet és biztonság I. évfolyam, 5. szám. Budapest, 2008. pp.: 61-69
- KOVÁCS László: Információs hadviselés kínai módra Nemzet és biztonság II. évfolyam 7. szám. Budapest, 2009. pp.: 35-44
- MISÁK István: Módosult információbiztonsági előírások http://www.jogiforum.hu/hirek/34135 (Letöltés ideje: 2018.08.11.)
- MUHA Lajos, Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése Budapest, NKE, 2014., ISBN:978-615-5491-65-8 p.10
- NEMES Dániel: Hackerek a szcientológia ellen http://pcworld.hu/kozelet/hackerek-a-szcientologia-ellen-20080128.html (Letöltés ideje: 2018.08.08.)
- Nate RAWLINGS: Anonymous Hackers Plead Guilty to PayPal Cyber Attack http://techland.time.com/2013/12/09/anonymous-hackers-plead-guilty-to-paypal-cyber-attack/ (Letöltés ideje: 2018.08.08.)

- Alexey SHULMIN, Sergey YUNAKOVSKY, Vasily BERDNIKOV, Andrey DOLGUSHEV: The Slingshot APT FAQ https://securelist.com/apt-slingshot/84312/ (Letöltés ideje: 2018.08.05.)
- Timothy L. THOMAS: Al Qaeda and the Internet: The Danger of "Cyberplanning" http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/03spring/thomas.pdf (Letöltés ideje: 2018.08.08.)
- BM OKF honlapja http://www.katasztrofavedelem.hu/index2.php?pageid=lrl_ibek (Letöltés ideje: 2018.08.11.)
- CERT: Újabb taggal bővült a Stuxnet „család" http://tech.cert-hungary.hu/tech-blog/120810/ujabb-taggal-bovult-a-stuxnet-csalad (Letöltés ideje: 2018.08.05.)
- Internet World Stats http://www.internetworldstats.com/stats.htm (Letöltés ideje: 2018.08.19.)
- Department of Defense Dictionary of Military and Associated Terms http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-07-25-091749-087
- Az informatikai biztonság kézikönyve Verlag Dashöfer Ltd. Budapest, 2004. ISBN 9639313122 p.3.2.5
- Kormányzati Eseménykezelő Központ honlapja http://www.cert-hungary.hu/node/1 (Letöltés ideje: 2018.08.11.)
- Nemzeti Kibervédelmi Intézet honlapja http://nbsz.hu/?mid=42 (Letöltés ideje: 2018.08.11.)
- Számítástechnikai Bűnözés Elleni Egyezmény http://www.jogiforum.hu/publikaciok/50 (Letöltés ideje: 2018.08 05.)
- 15/2017. (IV. 28.) HM utasítása honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17U0015.HM&timeshift=fffffff4&txtreferer=00000001.TXT (Letöltés ideje: 2018.08.11.)
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300050.tv (Letöltés ideje: 2018.08.11.)