HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Szentgáli Gergely
gergely.szentgali@gmail.com

AZ EURÓPAI UNIÓ KIBERBIZTONSÁGI TÖREKVÉSEI ÉS SZERVEZETEI II.

Absztrakt

Napjainkra a kiberbiztonság kérdése az első számú biztonságpolitikai kihívások között szerepel. Az információs társadalmak biztonságát meghatározó informatikai környezet és a hozzá kapcsolódó kihívások minden államot arra sarkallnak, hogy építsék ki a megfelelő védelmi szerveket és alkossák meg a szükséges jogszabályokat. Ezt a felelősséget az Európai Unió is felismerte és megkezdte a felkészülést ezen új típusú biztonsági kihívás kezelésére. Írásom első részében bemutattam az Unió jogi lépéseit, illetve a Digitális Menetrendet és az ahhoz kapcsolódó feladatszabást. Jelen tanulmányomban az uniós kiberbiztonsági szervezeteket és a lehetséges partnereket fogom megvizsgálni.

In the recent years, the conception of cybersecurity developed into a critical security policy matter. Security challenges associated with the informatical environment, which are determining the security of informational societies, are reinforcing states to create their own enforcement agencies and to materialise the requisite legal measures. The European Union has acknowledged this sort of responsibility, and it began to prepare the management of new forms of security challenges. In the first part of my paperI presented the EU's legal steps as well as the Digital Agenda for Europe and the tasking linked to it. In the current writing I am trying to examine the EU's cybersecurity organizations and its possible partners.

Kulcsszavak: *kiberbiztonság, Számítástechnikai bűnözés elleni küzdelem európai uniós központja,Európai Unió, NATO ~ ENISA,European Cybercrime Centre, cybercrime, NATO*

BEVEZETÉS

Tanulmányom első részében[1] az Európai Unió kiberbiztonsággal kapcsolatos jogi lépéseivel és különböző stratégiáival foglalkoztam.Bemutattam a vizsgált kérdéshez tartozó jogi kereteket és stratégiákat. Bár sok esetben ezek csupán ajánlás jellegűek, de kétségtelenül fontos lépések. Tanulmányom második és egyben záró részében azt fogom megvizsgálni, hogy melyek azok a szervek, amelyek az uniós kiberbiztonságot garantálják, illetve kik azok a partnerek, akik jelentősen hozzájárulnak az európai biztonság ezen szegmensének erősítéséhez.E kapcsolatok és összefüggések feltárása, illetve a figyelem felhívása az esetleges hiányosságokra, kulcskérdés a hatékony és közös védelem kiépítésének tárgyalásakor.

Európai Hálózat- és Információbiztonsági Ügynökség

Minden szervezet felépítésében komoly szerep jut az informatikai kiszolgáló rendszerek védelme érdekében létrehozott szerveknek. Az Unió esetében ez a szerv az Európai Parlament és az Európai Tanács 460/2004/EK rendelete által létrehozott Európai Hálózat- és Információbiztonsági Ügynökség,[2] amely jogilag 2004. március 10-én jött létre.

Az Ügynökség rendkívül széles feladatkörrel bír. Elsődleges feladata az Unió központi informatikai rendszerének felügyelete és védelmének támogatása, illetve a kiberbiztonság erősítése különböző válságmenedzselési feladatok ellátásával; a Bizottságnak adott tanácsokkal és a tagállamok számára nyújtott segítséggel egyaránt. Célja továbbá, hogy erősítse az együttműködést a különálló szervek és tagállamok között, illetve mint kapcsolatfenntartó szerv is működik az Unión kívül kibervédelmi szervezetekkel.

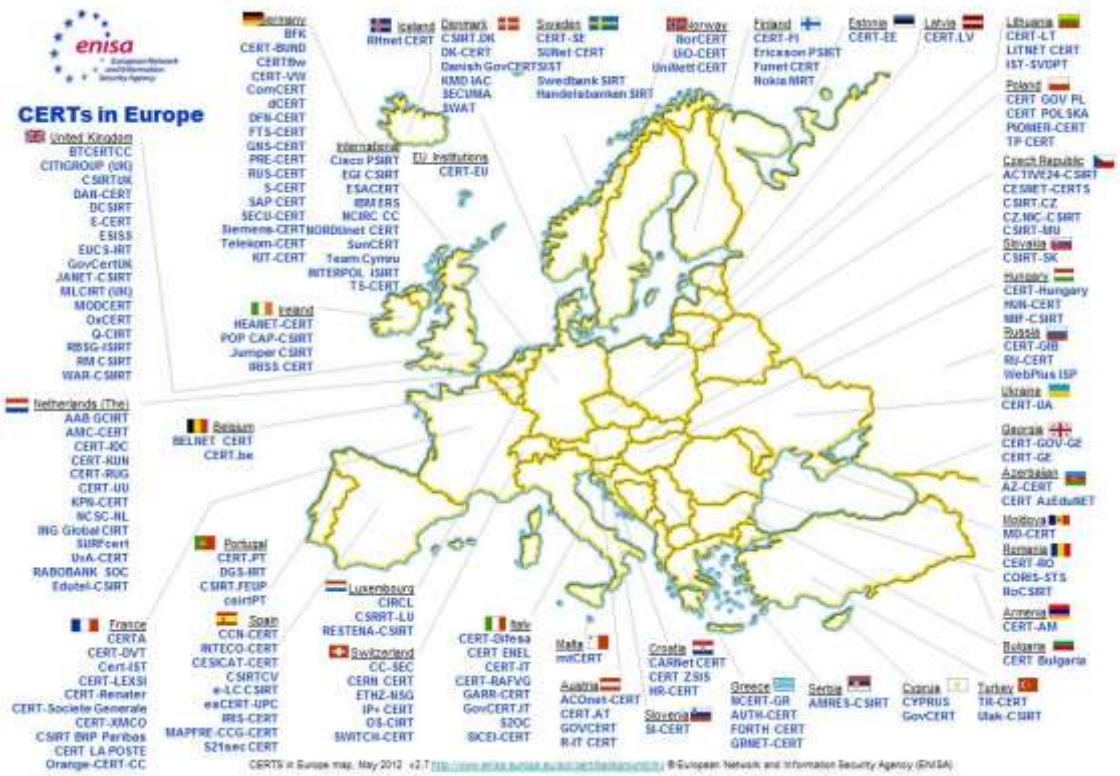
Az Ügynökség egy önállóan működő európai ügynökség, azonban nagyban támaszkodik a tőle függetlenül működő Computer EmergencyResponseTeam-ek (CERT), magyarul a Számítástechnikai Sürgősségi Reagáló Egységek munkájára. A CERT koncepció 1988-ban jelent meg a Carnegie Mellon Egyetemen, az Egyesült Államokban, melynek az volt a lényege, hogy egy szakértőkből álló csoportot hoztak létre, melynek feladata a nemzeti hálózatok felügyelete és valós idejű védelme. A CERT-ek nincsenek alárendelve az Ügynökségnek, azonban együttműködnek vele. Magyarán az Ügynökség jelen esetben koordinációs segítséggel erősíti az európai kibervédelmet.

Számos esetben a CERT mellett/helyett az államok Computer SecurityIncidentsResponse Team-et (CSIRT), azaz Számítógépes Biztonsági Incidensekre Reagáló Csoportot tartanak fenn. Ezek a csoportok alapvetően csupán a nevükben különböznek az előbb említettektől, feladatukat és hatáskörüket tekintve azonban ugyanazok.

Sok esetben ezek a szervek látják el a nemzeti kibervédelmi felügyeletet, ez nagyban jellemző azon uniós tagállamokra is. Az európai megoszlásról lásd az 1. ábrát.

[1] SZENTGÁLI Gergely: *Az Európai Unió kiberbiztonsági törekvései és szervezetei I.*In: Hadmérnök. VII. évfolyam. 2012/4. 172-179. o.

[2] European Network and InformationSecurityAgency (ENISA)



1. ábra. Az európai CERT hálózat
(Forrás: http://www.enisa.europa.eu/activities/cert/background/inv/files/certs-in-europe-map/at_download/fullReport)

Magyarországon három CERT működik jelenleg: HUN-CERT SZTAKI, NIIF-CSIRT és a CERT-Hungary. Ezek közül a CERT-Hungary, azaz a Nemzeti Hálózatbiztonsági Központ az a kormányzati szerv, amely ellátja a nemzeti infrastruktúrák védelmét.

Ezek az egységek a kibervédelem zászlóshajói, nem egy esetben tettek már kiváló szolgálatot az államoknak, többek között Magyarországnak is. Velük kapcsolatosan valóban elmondható, hogy óriási hangsúly van az együttműködésen. Pontosan ez adja meg erejüket, hiszen az önálló műveletek kivitelezése mellett kiválóan képesek – számos esetben az Ügynökség koordinációs segítségével – uniós szinten is együtt dolgozni.[3] Mindezekhez kapcsolódóan üdvözölendő hír, hogy 2012. szeptember 11-én létrehozták az Unió ezen kiemelt szervét, az EU-CERT-et.[4]

A CERT/CSIRT szervek közötti európai és regionális együttműködést hivatott támogatni a TF-CSIRT szakmai platform, ami a hatékony információáramlás biztosításával kívánja fokozni ezen szervek hatékonyságát. Hasonló fórum az európai kormányokhoz kapcsolódó CERT/CSIRT szervek informális fóruma az ECG,[5] ami hasonló szerepkörrel bír, mint a már taglalt platformok.

A nemzetközi együttműködéselősegítése érdekében alakult meg a több mint 180 szervezetet tömörítő FIRST fórum. A cél a technikai eszközök, információk, eljárások és legjobb gyakorlatok megosztása, illetve új CERT/CSIRT szervezet létrehozásának

[3]CERT cooperation and itsfurtherfacilitationbyrelevantstakeholders.ENISA Report. 2006. 12. 01. 18-41. o.
[4]Sikeres kísérleti projekt hatására nőtt az uniós intézmények kiberbiztonsága. Sajtóközlemény. IP/12/949. Brüsszel, 2012. szeptember 12.
[5]European GovernmentCERTsgroup

elősegítése. A nemzetközi fórum a teljes skálát lefedi: tagjai között egyaránt megtalálhatjuk a kormányzati, vállalati és akadémiai incidenskezelő szervezeteket is.[6]

Véleményem szerint a sikeres felkészülés egyik legjobb eszköze a különböző kibervédelmi gyakorlatok kivitelezése. Az élesben lezajlott támadások könnyen rámutatnak a rendszerek sérülékenységeire, illetve a védelmi képesség hatékonysága is napvilágra kerül – mindez egy biztonságos környezetben. Ezt az Ügynökség is felismerte, és alapvetően NATO minta alapján, elsőként 2010-ben szervezte meg a *Cyber Europe 2010* gyakorlatot. Az esemény során a kritikus információs infrastruktúrák kerültek fókuszba, illetve az, hogy a tagállamok hogyan tudnak együttműködni egy komoly kibertámadás-sorozat alatt.

A gyakorlat hasznát és sikerét figyelembe véve, 2012. október 4-én került megrendezésre a *Cyber Europe 2012*, több mint 300 szakértő részvételével. A többek között Magyarország részvétel lezajlott hálózatbiztonsági gyakorlaton első ízben vettek részt bankok és internetszolgáltatók. Mindezen új szereplők részvétele tovább segíti a komplex kibervédelem kialakítását. A gyakorlat három célt tűzött ki maga elé:

1. Az európai hatóságok közötti együttműködés mechanizmusainak, eljárásainak ésinformációáramlásának tesztelése a hatékonyság és a méretgazdaságosság szempontjából.
2. Az európai köz- és magánszektorbeli szereplők közötti együttműködés vizsgálata.
3. A nagyszabású európai kiberbiztonsági incidensek kezelésére alkalmas hatékonyabbmódszerek kidolgozása a meglévő hiányosságok és kihívások azonosítása révén.[7]

A lezajlott gyakorlatot valamennyi résztvevője hasznosnak és sikeresnek ítélte meg.

További hasznos lépésnek tartom a különböző biztonságtudat erősítő programokat. Az Ügynökség alapfeladatai között is helyet kapó figyelem felkeltő események nagyban hozzájárulnak a hatékonyabb kiberbiztonság eléréséhez. Ezek közé illeszkedik az európai kiberbiztonsági hónap is, amely 2012 októberében kapott helyet. A program célja az volt, hogy EU-szerte felhívja a figyelmet a kiberbiztonság fontosságára, illetve a tudatos internet felhasználásra. A különböző szakmai programok mellett, egy komplett internetes kampány is folyt az események támogatása érdekében.

Összegezve a fent leírtakat, az Ügynökség rendkívül komplex feladatokat lát el.Fontos, hogy a feladatkörök jól elkülöníthetőek legyenek, megszűntetve ezzel a párhuzamos erőfeszítéseket. Gondolok itt például arra, hogy nem feltétlenülszükséges, hogy a kiberbűnözésre is összpontosítson komoly energiát, hiszen arra már megvannak a kijelölt szervek.

Tény, hogy az Ügynökség léte elengedhetetlen az Unió biztonsága tekintetében, tekintve, hogy a közvetlen védelem mellett jelentős szerepe van a biztonságfelfogás formálásában is. Ez pedig az egyik legfontosabb eleme a kibervédelem kérdésének, hiszen biztonsági rést legtöbbször a felelőtlen felhasználó jelent. Pontosan ezért továbbra is meg kell szervezni a tudatosságformáló programokat, illetve az ehhez kapcsolódó tagállami tanácsadást.

Érdemes lenne minden évben megszervezni a már taglalt kibervédelmi gyakorlatokat – valószínűsíthetően ez a trend fog megvalósulni –, de nem csak uniós szinten, hanem tagállami szinten is, annak érdekében, hogy világosan láthatóvá váljon, hogy milyen szinten állnak a nemzeti kiberképességek. Hangsúlyoznunk kell, hogy nincsenek azonos szinten a tagállamok, és ez sok esetben a közös munka akadálya is lehet. Ennek a megoldásában lehet kiváló partner az Ügynökség, aki tagállami szinten nyújtana támogatást a képességek kialakításához.

---

[6]HAIG Zsolt: *Az információbiztonság szabályzói és szervezeti keretei.*In: Hadmérnök. Robothadviselés 7. tudományos szakmai konferencia különszám. 2007. november 7.
http://hadmernok.hu/kulonszamok/robothadviseles7/haig_rw7.pdf Letöltés ideje: 2013. február 22.

[7]*Cyber Europe 2012. Főbb következtetések és ajánlások.* ENISA, 2012. december. 4. o.

Mind az együttműködés, mind a kibervédelmi gyakorlatok hasznosságát felismerve, 2010-ben az uniós döntéshozók megerősítették az Ügynökséget, elfogadva az új információs rendszerek elleni támadásokról szóló irányelvet.[8] Ennek értelmében 2017-ig meghosszabbították az Ügynökség megbízatását.

SZÁMÍTÁSTECHNIKAI BŰNÖZÉS ELLENI KÜZDELEM EURÓPAI UNIÓS KÖZPONTJA

A kiberbűnözés fogalmának meghatározása nehéz feladat. A nemzetközi trendeket figyelve elmondhatjuk, hogy – hasonlóan a terrorizmus fogalmához – a törekvések inkább a fogalom tartalmának a meghatározására fókuszálnak egy egységesített definíció létrehozása helyett. Ebből kiindulva megállapíthatjuk, hogy a kiberbűnözés főbb kategóriái a következőek: számítógépes hálózatok és rendszerek feltörése és adatok lopása; hamis identitások használata pénzszerzés céljából; adathalászat; gyermekpornográfia, illetve szerzői jogi bűncselekmények.[9] Ezt erősíti meg a kriminológia is, ami hasonlóan jelöli meg a csúcstechnológiai bűnözés típusait: számítógépes hálózatok feltörése; ipari kémkedés; szoftverkalózkodás; gyermekpornográfia; elektronikus levélbombák; jelszószimatolók (keyloggerek) és hitelkártyacsalás.[10]

A kiberbűnözés veszélyének komolyságát az is mutatja, hogy a Symantec, informatikai biztonsággal foglalkozó cég 2012-es jelentése szerint a számítógépes bűnözés évente megközelítően 110 milliárd dollár veszteséget okoz az államoknak és az egyéni felhasználóknak.[11] Tovább nehezíti a kiberbűnözés elleni harcot, hogy az elkövetők spektruma rendkívül széles: a jól képzett hackerektől kezdve, terroristákon át, az egyszerű felhasználó is kiberbűnözővé válhat, az interneten terjedő elkövetési módszerek megismerésének segítségével.[12]

Az egyre kifinomultabb módszerek és az egyre növekvő esetek száma az Európai Uniót is arra ösztönözték, hogy létrehozzon egy önálló szervet, ami fókuszáltan a kiberbűnözés problematikájával foglalkozik. 2012. március 28-án történt meg ez a lépés: az Európai Rendőrségi Hivatal[13] szervezetén belül megalapították a Számítástechnikai Bűnözés Elleni Küzdelem Európai Uniós Központját,[14] amely 2013. január elsejére érte el teljes műveleti képességét. A szervezet jogelődje a három munkacsoporttal (gyermekek szexuális kizsákmányolása, bankkártyacsalás és kiberbűnözés) rendelkező Csúcstechnológiai Bűnözés Elleni Központ[15] volt.[16]

---

[8] A Bizottság megerősítené az informatikai támadásokkal szembeni védelmet Európában. Sajtóközlemény. IP/10/1239. Brüsszel, 2010. szeptember 30.

[9] SCHREIER, Fred – WEEKES, Barbara – WINKLER, Theodor H.:CyberSecurity: The RoadAhead. DCAF Horizon 2015 WorkingPaperNo. 4. DCAF, 2012. 9-11. o.

[10] ADLER,Freda – MUELLER, Gerhard O. W. – LAUFER, William S.:Kriminológia. Osiris Kiadó, Budapest, 2005. 403-405. o.

[11] 2012 Norton CybercrimeReport. http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf Letöltés ideje: 2013. február 10.vö. Gragido, WILL – Pirc, JOHN: Cybercrime and Espionage. An Analysis of SubversiveMultivectorThreats. Elsevier, 2011. 9-10. o.

[12] SZEGEDINÉ LENGYEL Piroska: Számítógépes bűnözés avagy fiatalok a cyber-térben.In: Hadmérnök. V. évfolyam. 2012/2. 371-373. o.

[13] European Police Office (Europol)

[14] European Cybercrime Centre (EC3)

[15] HighTechCrime Centre

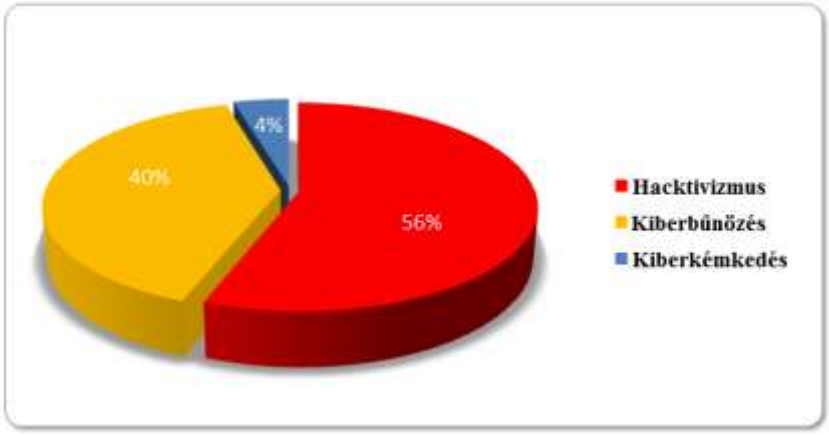
[16] TÓTH Tamás: *Az Europol tevékenysége II. (2010-2012).* http://www.biztonsagpolitika.hu/?id=16&aid=1264&title=az-europol-tevekenysege-ii-2010-2012- Letöltés ideje: 2013. február 11.

Az új Központ megalapításának előzménye a *Stockholmi Program*[17] egyik fontos eleme, a 2010. március 26-án elfogadott, *Az Európai Unió belső biztonsági stratégiája* című dokumentum. Bár a számítógépes biztonság kérdése már a 2008-ban elfogadott *Európai Biztonsági Stratégiában* is megjelent,[18] a kiberbűnözés jelensége, mint hangsúlyos belső probléma itt tűnt fel elsőként.[19] Azonban a Központtal kapcsolatos teendők végül nem a stratégiában, hanem az annak végrehajtásáért felelős akciótervben realizálódtak.[20]

A Központ feladata elsősorban a kiberbűnözés elleni harc koordinálása, különös hangsúlyt fektetve a nagy nyereséggel járó bűnözés elleni tevékenységre. A további feladatok között megtaláljuk még a személyazonosság-lopás elleni küzdelmet; az elektronikus bankszolgáltatásokat érintő bűncselekmények elleni harcot; a gyermekek szexuális kizsákmányolása elleni harcot, illetve az Európai Unió kritikus infrastruktúráinak és informatikai rendszereinek korlátozott védelmét.[21]

A koordinálási feladatokhoz kapcsolódóan a Központ kiemelt feladata, hogy figyelmeztesse a tagállamokat az esetleges fenyegetettségekre. Szintén lényeges lépés az online szervezett bűnözői csoportok felkutatásának és azonosításának támogatása, ezt erősítve a Központ tagállami szinten is képes segítséget nyújtani konkrét nyomozásokhoz.

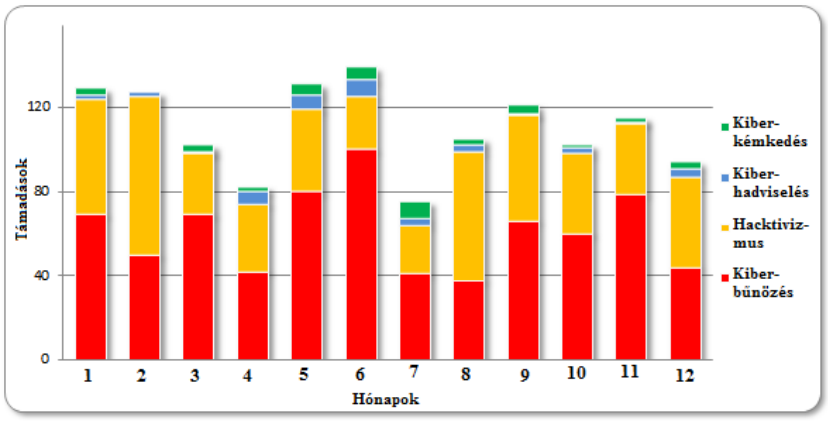
Erre a munkára pedig egyre nagyobb szükség van, tekintve, hogy a számítógépes bűncselekmények száma napról-napra növekszik. Paolo Passeri, a Lastline IT biztonsági cég munkatársa, minden hónapban statisztikát készít az elmúlt hónap globális, reflektorfénybe kerültkibertámadásairól.[22]A legfrissebb havi eloszlásért lásd a 2. ábrát.



2. ábra. 2013januárjában elkövetett kibertámadások motivációs háttere
(Forrás: http://paulsparrows.files.wordpress.com/2013/02/motivations-january-2013.png)

Érdemes megvizsgálnunk a már említett kutató 2012-re vonatkozó egyesített statisztikáját (3. ábra) is. Az általa készített diagramokat figyelembe véve elmondhatjuk, hogy a kiberbűnözés az egyik legjelentősebb eleme a rosszindulatú kibertéri jelenlétnek.

[17]Az Európai Tanács tájékoztatása.A Stockholmi Program – A Polgárokat Szolgáló Védő, Nyitott és Biztonságos Európa. 2010. 5. 4. (2010/C 115/01)
[18]Európai Biztonsági Stratégia. Biztonságosabb Európa egy jobb világban. Luxembourg, 2009. 13-14. o.
[19]Az Európai Unió belső biztonsági stratégiája. Az európai biztonsági modell felé. Luxembourg, 2010. 14. o.
[20]The EU InternalSecurityStrategyin Action: Fivestepstowards a more secure Europe. Press release. MEMO/10/598. Brussels, 22 November 2010.
[21]A számítástechnikai bűnözés elleni küzdelem európai uniós központja az internetes bűnözők elleni küzdelem és az e-fogyasztók védelme érdekében. Sajtóközlemény. IP/12/317. Brüsszel, 2012. március 28.
[22]PASSERI, Paolo: 2012 CyberAttacksStatistics.http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/ Letöltés ideje: 2013. január 22.



3. ábra. A 2012-es év egyesített statisztikája
(Forrás: http://paulsparrows.files.wordpress.com/2012/06/2012-attack-distribution.png)

Magyarországon a Nemzeti Nyomozó Iroda alárendeltségébe tartozó Csúcstechnológiai Bűnözés Elleni Osztálya foglalkozik a leghangsúlyosabb módon a kiberbűnözés problémájával. Hazánk és a kiberbűnözés témája már szerepelt közös platformon, tekintve, hogy 2011. november 23-ánBudapesten írták alá a *Számítástechnikai Bűnözésről Szóló Egyezményt*,[23] ami az első jelentős európai szintű lépés volt a kiberbűnözés elleni harcban.

A politikai vezetés komoly eredményeket vár az újonnan felállított Központtól. Remélhetően a központi koordinálásban partnerek lesznek a tagállamok is, ezzel is segítve a felderítések hatékonyságát. Fontos szerep jut a magánszférának is, hiszen a magánkézben lévő IT biztonsági cégek mindig is partnerei voltak a kormányzati szerveknek a kiberbiztonság kérdésében. Mindezeken túl fontos lenne, hogy a nem kiberbiztonsággal foglalkozó magánvállalatok is felismerjék a kiberbűnözés fenyegetésének súlyát és kellőképpen vegyék figyelembe az ezzel kapcsolatos ajánlásokat, mert egy valami biztos: a Központ csak akkor lehet sikeres, hogyha az érintett államok és azok állampolgárai igyekeznek felelősségteljes és biztonságtudatos internet felhasználóvá válni.

EGYÜTTMKÖDŐ PARTNEREK

A kollektív és kooperatív biztonság garantálásának alapfeltétele, hogy az adott szövetség tagjai megfelelő garanciákkal rendelkezzenek egymás irányába, és hatékony módon tudjanak együttműködni egymással. Azonban rendkívül fontos, hogy a szervezet a saját keretein kívül is keressen partnereket, szövetségeseket. Az uniós kiberbiztonság kérdésének vizsgálatakor az egyik legkézenfekvőbb partner a NATO.

Az Európai Unió és a NATO között számos területen van együttműködés, a legfontosabb biztonságpolitikai folyamatok összehangolása már 2001-ben elindult. A katonai műveletek terén történő együttműködés 2003-ban vette kezdetét, tekintve, hogy ekkor indult az Európai Unió első, CONCORDIA elnevezésű válságkezelő missziója, ahol az uniós erők nagyban támaszkodtak a NATO támogatására.[24]

Kiberbiztonság tekintetében fontos állomás volt a 2011. november 19-én és 20-án lezajlott lisszaboni csúcstalálkozó, ahol a tagállamok elfogadták a NATO új Stratégiai Koncepcióját.[25]

---

[23] *Számítástechnikai bűnözésről szóló egyezmény.* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Hungarian.pdf Letöltés ideje: 2013. január 22.

[24] HORVÁTH Gábor: *NATO and EU: Cooperationorcompetition?*In: Academic and Applied Research in Military Science. VI. évfolyam. 2007/3. 480. o.

[25] *Aktív Szerepvállalás, Modern Védelem. Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és*

Mind a Koncepcióban, mind a csúcstalálkozó során kiemelték a NATO és az Európai Unió stratégiai együttműködésének fontosságát. Mindkét fél részéről egyezség született arról, hogy a hagyományosnak mondható együttműködéseken (terrorizmus, non-proliferáció stb.) túl, a kiberbiztonság területén is szorosabbra fűzi kapcsolatát a két szervezet.[26]

Az együttműködés fontossága a továbbiakban sem veszített súlyából, a 2012. május 20-án és 21-én lezajlott chicagói csúcstalálkozón szintén kiemelt partnerként beszéltek az Európai Unióról. Herman Van Rompuy, az Európai Tanács elnöke is részt vett a csúcstalálkozón, beszédében elmondta: az Unió továbbra is párbeszédet folytata kiberbiztonság kérdésében a NATO-val, ezzel is erősítve a térség biztonságát.[27]

Tekintve, hogy számos NATO tagállam egyben EU tagállam is, a párhuzamos kibervédelmi törekvések sok esetben gyengítik egymást, ezért is lenne szükség a folyamatos szinkronizálására. Elsősorban közös gyakorlatok megszervezése, a megszerzett tapasztalatok megosztása, illetve különböző konferenciákalkotják az együttműködés főbb pólusait. Ezt erősítette meg Iklódy Gábor is, a NATO új típusú biztonsági kihívásokkal foglalkozó főtitkár-helyettese, a Microsoft által szervezett kiberbiztonsági konferencián elmondott beszédében.[28] Hozzátette, hogy egy nagyobb támadás esetén növelné a hatékonyságot a közös fellépés, továbbá a rendszerek közös védelmét sem tartja kizártnak a jövőben.

A kiberbiztonsággal kapcsolatosegyüttműködési kérdésekben az Unió tekintetében az *Európai Hálózat- és Információbiztonsági Ügynökség, még a NATO tekintetében a Kooperatív Kibervédelmi Kiválósági Központ*[29] *a kiemelten felelős szerv.*

A Központ több ország kooperációjával jött létre: Észtország, Németország, Olaszország, Litvánia, Lettország, Szlovákia, Spanyolország voltak az alapító tagok, 2010-ben Magyarország is csatlakozott a Központhoz, 2011 novemberében pedig az Amerikai Egyesült Államok és Lengyelország vált támogató taggá.Aszervezet nem a NATO kibernetikai támadóerejét jeleníti meg, hanem mint kutatási és oktatási központ kíván működni. Kétségtelen, hogy kiváló kapcsolati pont lehet a NATO tekintetében. Továbbá figyelembe véve a már említett tagállami átfedéseket, logikus és a világgazdasági folyamatokat figyelve pedig szükségszerű lenne az együttműködés szorosabbá tétele.

Véleményem szerint a közös védelem kialakítása lenne az egyik legfontosabb és egyben az egyik legköltséghatékonyabb lépés. Tekintve, hogy mindkét szervezet azonos értékeket vall, ezért nem látom akadályát annak, hogy ilyen komoly szinteken is megvalósuljon a feladatok megosztása. A jövőben elképzelhetően ez lesz a legnagyobb feladat a két szervezet kibervédelmi együttműködésének tekintetében.

Másik kiemelt partner az Amerikai Egyesült Államok. Annak ellenére, hogy az USA tagja a NATO-nak, az Unió és Amerika között önállóan is kialakításra kerültek kiberbiztonsági kapcsolatok. Ebbe az együttműködésbe tartozik a *CyberAtlantic 2011*gyakorlat is. A hangsúly a transzatlanti együttműködésen volt, azaz azt vizsgálta, hogy egy esetleges támadás esetén az amerikai szervek hogyan tudnak segítséget nyújtani európai partnereiknek, illetve mindez fordítva hogyan valósulhat meg. A transzatlanti kiberbiztonsági kapcsolatok 2011-ben kaptak

---

*Biztonságról.*http://www.biztonsagpolitika.hu/documents/1291766875_NATO_Strat_Koncepcio_2010_hun_BSZK.pdf Letöltés ideje: 2013. február 10.

[26]*NATO-EU: a strategicpartnership*. http://www.nato.int/cps/en/natolive/topics_49217.htm Letöltés ideje: 2013. február 11.

[27]*Statement of thePresident of the European Council, Herman Van Rompuy, atthe Chicago NATO Summit.* Press release.EUCO 105/12. Chicago,20 May 2012.

[28]HALE, Julian: *NATO OfficialHighlightsAreasfor EU-NATO CyberCooperation.* http://www.defensenews.com/article/20120531/DEFREG01/305310005/NATO-Official-Highlights-Areas-EU-NATO-Cyber-Cooperation Letöltés ideje: 2013. január 25.

[29]NATO CooperativeCyberDefence Centre of Excellence (CCD CoE)

nagy lendületet, amikor létrehoztak egy közös munkacsoportot, amely alapvető informatikai biztonsági kérdésekkel, illetve a kiberbűnözéssel foglalkozik.[30]

Tény, hogy a kiberbiztonság tekintetében élen járnak az amerikaiak, tapasztalataikat pedig szívesen megosztják szövetségeseikkel. Sajnálatos módon a kártékony programokra és a különböző behatolásokra sok esetben csak reagálni lehet, kevesebb alkalommal lehet megelőzni azokat. Többek között ezért lenne fontos az együttműködést a munkacsoport szintjénél egy komolyabb dimenzióban megvalósítani.

KÖVETKEZTETÉSEK

A fent leírtak alapján elmondható, hogy az Európai Unió komolyan veszi a kiberbiztonság kérdését. Bár a fent leírt dokumentumok és szervezetek nem fedik le az összes lépést, amit az Unió tett polgárai védelmének érdekében, kétségtelenül jól példázzák az erőfeszítéseket.

Jól jelzi a folyamat dinamikáját, hogy még az előző cikkemben csupán tervként bemutatott kiberbiztonsági stratégia mára már valósággá vált: 2013. február másodikán bemutatták az Európai Unió kiberbiztonsági stratégiáját.[31]

Az új stratégia öt prioritást emel ki:

- a kibertámadásokkal szembeni ellenálló képesség megteremtése;
- a számítástechnikai bűnözés drasztikus visszaszorítása;
- a kibervédelmi politika kidolgozása és a közös biztonság- és védelempolitikát (KBVP) érintő képességek fejlesztése;
- a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtése;
- az Európai Unió által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése.[32]

A dokumentum elemzése egy külön tanulmányt érne meg, az mindenesetre most is megállapítható, hogy rendkívül átfogó intézkedések gyűjteménye, kiemelt tekintettel a kiberbűnözés problematikájára, amely uniós tekintetben a legkomolyabb kiberbiztonsági kihívásnak számít. Továbbá a stratégia számos válaszlépést is tartalmaz a fellépő fenyegetések kezelésére. Ezen akció időtartalma azonban az esetek többségében hosszabbtávú politikai cselekvést igényel, így a stratégia helytállóságát később lehet csak lehet reálisan megítélni.

A bemutatottak alapján jól látható, hogy a jogszabályi környezet kiépítése megtörtént, 2013-ra a szükséges szervezetek is elérték a teljes műveleti képességüket. Magyarán a mostani év lesz az első éles főpróbája az európai kibervédelmnek. Az együttműködés iránti igény is jól látható, azonban véleményem szerint sok esetben szétaprózódáshoz vezethet a sokszoros átfedés. A CERT/CSIRT szervek esetén is jól látható, hogy több európai és nemzetközi fórumon kell összehangolniuk tevékenységüket, mindezeket az elsődleges nemzeti igényekhez igazítva. Véleményem szerint érdemes lenne csúcsszerveket/fórumokat létrehozni ennek érdekében, megszüntetve a számos, sok esetben párhuzamos (néha egymást kioltó) törekéveseket.

A kiberbiztonságot erősítő folyamatok azonban kétségtelenül elindultak, így remélhetjük, hogy az uniós szintű együttműködés eredményeképpen mindannyian egy biztonságosabbá váló Európa polgárai lehetünk.

---

[30]Cybersecurity: EU and US strengthentransatlanticcooperationinface of mountingglobalcyber-security and cyber-crimethreats. Press release. MEMO/11/246. Brussels, 14 April 2011.

[31]JointCommunicationtothe European Parliament, theCouncil, the European Economic and SocialCommittee and theCommittee of Regions. CybersecurityStrategy of the European Union: An Open, Safe and SecureCyberspace. 7.2.2013. JOIN(2013) 1 final.

[32]Uniós kiberbiztonsági terv a nyílt internet, valamint az online szabadság és lehetőségek védelmére. Sajtóközlemény. IP/13/94. Brüsszel, 2013. február 7.

Felhasznált irodalom

[1] *2012 Norton CybercrimeReport.* http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf Letöltés ideje: 2013. február 10.

[2] *A Bizottság megerősítené az informatikai támadásokkal szembeni védelmet Európában.* Sajtóközlemény. IP/10/1239. Brüsszel, 2010. szeptember 30.

[3] *A számítástechnikai bűnözés elleni küzdelem európai uniós központja az internetes bűnözők elleni küzdelem és az e-fogyasztók védelme érdekében.* Sajtóközlemény. IP/12/317. Brüsszel, 2012. március 28.

[4] ADLER,Freda – MUELLER, Gerhard O. W. – LAUFER, William S.:*Kriminológia.* Osiris Kiadó, Budapest, 2005. ISBN 963-389-793-9

[5] *Aktív Szerepvállalás, Modern Védelem. Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságról.*http://www.biztonsagpolitika.hu/documents/1291766875_NATO_Strat_Koncepcio_2010_hun_BSZK.pdf Letöltés ideje: 2013. február 10.

[6] *Az Európai Tanács tájékoztatása.A Stockholmi Program – A Polgárokat Szolgáló Védő, Nyitott és Biztonságos Európa.* 2010. 5. 4. (2010/C 115/01)

[7] *Az Európai Unió belső biztonsági stratégiája. Az európai biztonsági modell felé.* Luxembourg, 2010. ISBN 978-92-824-2685-2

[8] *CERT cooperation and itsfurtherfacilitationbyrelevantstakeholders.* ENISA Report. 2006. 12. 01.

[9] *Cyber Europe 2012. Főbb következtetések és ajánlások.* ENISA, 2012. december.

[10] *Cybersecurity: EU and US strengthentransatlanticcooperationinface of mountingglobalcyber-security and cyber-crimethreats.* Press release. MEMO/11/246. Brussels, 14 April 2011.

[11] *Európai Biztonsági Stratégia. Biztonságosabb Európa egy jobb világban.* Luxembourg, 2009. ISBN 978-92-824-2427-8

[12] Gragido, WILL – Pirc, JOHN: *Cybercrime and Espionage. An Analysis of SubversiveMultivectorThreats.* Elsevier, 2011. ISBN 978-1-59749-613-1

[13] HAIG Zsolt: *Az információbiztonság szabályzói és szervezeti keretei.*In: Hadmérnök. Robothadviselés 7. tudományos szakmai konferencia különszám. 2007. november 7. http://hadmernok.hu/kulonszamok/robothadviseles7/haig_rw7.pdf
Letöltés ideje: 2013. február 22.

[14] HALE, Julian: *NATO OfficialHighlightsAreasfor EU-NATO CyberCooperation.* http://www.defensenews.com/article/20120531/DEFREG01/305310005/NATO-Official-Highlights-Areas-EU-NATO-Cyber-Cooperation
Letöltés ideje: 2013. január 25.

[15] HORVÁTH Gábor: *NATO and EU: Cooperationorcompetition?*In: Academic and Applied Research in Military Science. VI. évfolyam. 2007/3. 479-489. o. ISSN 1588-8789

[16] *JointCommunicationtothe European Parliament, theCouncil, the European Economic and SocialCommittee and theCommittee of Regions. CybersecurityStrategy of the European Union: An Open, Safe and SecureCyberspace.* 7.2.2013. JOIN(2013) 1 final.

[17] *NATO-EU: a strategicpartnership*. http://www.nato.int/cps/en/natolive/topics_49217.htm Letöltés ideje: 2013. február 11.

[18] PASSERI, Paolo: *2012 CyberAttacksStatistics*.http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/ Letöltés ideje: 2013. január 22.

[19] SCHREIER, Fred – WEEKES, Barbara – WINKLER, Theodor H.:*CyberSecurity: The RoadAhead*. DCAF Horizon 2015 WorkingPaperNo. 4. DCAF, 2012.

[20] *Sikeres kísérleti projekt hatására nőtt az uniós intézmények kiberbiztonsága.* Sajtóközlemény. IP/12/949. Brüsszel, 2012. szeptember 12.

[21] *Statement of thePresident of the European Council, Herman Van Rompuy, atthe Chicago NATO Summit.* Press release.EUCO 105/12. Chicago,20 May 2012.

[22] *Számítástechnikai bűnözésről szóló egyezmény.* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Hungarian.pdf Letöltés ideje: 2013. január 22.

[23] SZEGEDINÉ LENGYEL Piroska: *Számítógépes bűnözés avagy fiatalok a cyber-térben.*In: Hadmérnök. V. évfolyam. 2012/2. 366-379. o. ISSN 1788-1919

[24] *The EU InternalSecurityStrategyin Action: Fivestepstowards a more secure Europe.* Press release. MEMO/10/598. Brussels, 22 November 2010.

[25] TÓTH Tamás: *Az Europol tevékenysége II. (2010-2012).* http://www.biztonsagpolitika.hu/?id=16&aid=1264&title=az-europol-tevekenysege-ii-2010-2012- Letöltés ideje: 2013. február 11. ISSN 2062-4379

[26] *Uniós kiberbiztonsági terv a nyílt internet, valamint az online szabadság és lehetőségek védelmére.* Sajtóközlemény. IP/13/94. Brüsszel, 2013. február 7.