HADMÉRNÖK

VII. Évfolyam 4. szám - 2012. december

Szentgáli Gergely
gergely.szerntgali@gmail.com

AZ EURÓPAI UNIÓ KIBERBIZTONSÁGI TÖREKVÉSEI ÉS SZERVEZETEI I.

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. Jelen cikkben az Unió kiberbiztonsággal kapcsolatos jogi lépéseit és az Európai Digitális Menetrendet fogom elemezni. Az írás második részében (amely a következő Hadmérnökben fog megjelenni) az EU kiberbiztonságáért felelős kiemelt szervezeteit fogom bemutatni.

In the recent years, the conception of cyber security 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 my recent writing I will analyze the EU's legal steps toward cyber security, and the Digital Agenda for Europe. In the second part of the paper (which will be released in the next issue) I am presentig the EU's further bodies and actions.

Kulcsszavak: *kiberbiztonság, Digitális Menetrend, kritikus információs infrastruktúrák, Európai Unió ~ cyber security, Digital Agenda of Europe, critical information infrastructure*

BEVEZETÉS

Szinte már közhelynek számít, hogy az információs társadalmak függnek a modern kori információs eszközöktől és infrastruktúráktól. Az sem újdonság, hogy ezeknek a rendszereknek a védelme elengedhetetlen kormányzati feladat. Mindazonáltal a probléma még mindig aktuális, hiszen naponta jelennek meg új fenyegetések mind a fizikai, mind az információs dimenzióban, amelyek ezeket az infrastruktúrákat fenyegetik.

Számos állam elkezdte kidolgozni a saját stratégiáit a kiberbiztonság kérdésével kapcsolatban. Ez a folyamat az Európai Unió tagállamainál is elindult, jelenleg az alábbi államok rendelkeznek önálló stratégiával: Észtország (2008), Finnország (2008), Szlovákia (2008), Csehország (2011), Franciaország (2011), Németország (2011), Litvánia (2011), Luxembourg (2011), Hollandia (2011) és az Egyesült Királyság (2011).[1]

A döntéshozók azt is felismerték, hogy ezeknek a rendszereknek a védelme nem feltétlen kezelhető kizárólagosan az államhatárokon belül, hiszen számos infrastruktúra határokon átnyúló hálózatot alkot. Pontosan ezért szükséges, hogy a különböző nemzetközi szervezetek, az őket alkotó tagállamok biztonságának erősítése érdekében megerősítsék a saját rendszereiket, és koordinációs segítséget nyújtva elősegítsék az állami képességek kialakítását is. Ahogyan a NATO-ban, az Európai Unióban is realizálódott ez a probléma, amelyeket számtalan válasz követett.

JOGSZABÁLYOK, PROGRAMOK ÉS LÉPÉSEK EGY BIZTONSÁGOSABB UNIÓÉRT

A kibervédelem kérdésének vizsgálatakor az első számú technikai kihívás a kritikus infrastruktúrák és a hozzájuk kapcsolódó kritikus információs infrastruktúrák védelme. Az Európai Unió hangsúlyos módon 2004 óta foglalkozik a kritikus infrastruktúrák védelmével.

2004. október 20-án fogadta el a Bizottság a *„Kritikus infrastruktúrák védelme a terrorizmus elleni küzdelemben”* című közleményt,[2] illetve még ez év decemberében a Tanács jóváhagyta a Kritikus Infrastruktúrák Figyelmeztető Információs Hálózat[3] felállítását.[4]

2005. november 17-én fogadták el az uniós döntéshozók a *„Zöld Könyv a kritikus infrastruktúra védelem európai programjáról”*[5] című dokumentumot. Ehhez a programhoz igazodik a magyarországi szabályozás, a 2080/2008. (VI. 30.) kormányhatározat,azaz a *Kritikus Infrastruktúra Védelem Nemzeti Programjáról*[6] elnevezésű jogszabály. Azonban ez az uniós dokumentum azonban nem csak ezért fontos, hanem abból az okból is, hogy meghatározásra kerülnek benne a kritikus információs infrastruktúrák is, amelyek a magyar jogszabályokban még nem lelhetőek fel.

---

[1] *National Cyber Security Strategies.* http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport5-6 o. Letöltés ideje: 2012. október 1. Néhány európai állam részletesebb elemzését lásd KOVÁCS László*: Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I.* In: Hadmérnök. VII. évfolyam. 2012/2. 304-311. o.

[2] *Critical Infrastructure Protection in the Fight Against Terrorism.*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF Letöltés ideje: 2012. október 10.

[3] Critical Infrastructure Warning Infromation Network – CIWIN

[4] RÁCZ László István: *Kritikus infrastruktúra védelem hazai és nemzetközi szabályozási rendszere.* In: Hadmérnök. VII. évfolyam. 2012/2. 168. o.

[5] *Zöld Könyv a kritikus infrastruktúra védelem európai programjáról.* http://www.ivb.org.hu/documents/INNOVACIOSklub/200812ho/ZoldKonyv.pdf; Letöltés ideje: 2012. október 10.

[6] 2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. In: Határozatok Tára. 2008/31. 217-231. o.

A kritikus infrastruktúrák részét képezik a kritikus információs infrastruktúrák. Muha Lajos, a Nemzeti Közszolgálati Egyetem tanára, doktori disszertációjában az alábbi definíciót fogalmazta a kritikus információs infrastruktúrákkal kapcsolatban:

„Azon az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása, vagy megsemmisülése a kritikus infrastruktúrák működésképességét jelentősen csökkentené."[7]

Ezeknek a létesítményeknek a megléte és védelme – tekintve, hogy a kritikus infrastruktúrák részét képezik – elengedhetetlen feladat a mindennapi élet feltételeinek biztosításához, kiesésük rendkívüli károkat okozna a gazdaságban.[8] Ennek elkerülése érdekében készült el a 2009. március 30-án elfogadott *„Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása"* című dokumentum.[9] A bizottsági közlemény alaposan végigveszi a kritikus informatikai infrastruktúrákkal kapcsolatos veszélyeket, illetve mindezekhez kapcsolódóan egy cselekvési tervet is felvázol.

A dokumentum kiválóan rámutat, hogy komoly elmaradások vannak ez ügyben a tagállami szinteken, érezhető eltérések vannak mind a felkészültség, mind a szaktudás tekintetében. Ahogyan említettem, a magyar országgyűlés csupán a kritikus infrastruktúrák védelmével kapcsolatos kormányhatározatot fogadott eddig el, azonban a kritikus információs infrastruktúrák védelmével kapcsolatosan semmilyen jogszabály nem rendelkezik. Ez is egy olyan hiányosság, amit hazánknak a jövőben minél hamarabb pótolnia kell.[10]

A közlemény szintén fontosfelismerése, hogy a kritikus információs infrastruktúrák döntő többségben a magánszféra tulajdonában vannak, így a kormányzat és a magánszféra közötti kommunikáció – csak úgy, mint a kiberbiztonság számos aspektusában – létfontosságú.

Az európai irányelvhez kapcsolódó cselekvési terv eredményeiről számol be a 2011. március 31-én elfogadott, *„Eredmények és következő lépések: a globális kiberbiztonság felé"* című bizottsági közlemény.[11] Az alapvetően pozitív eredményeket tartalmazó dokumentum további számos ajánlást tesz a jövőbeni lépésekkel kapcsolatosan, kiemelve a CERT hálózat további kiépítésének szükségességét, illetve egy kiberbiztonsági vészhelyzeti terv kidolgozását 2012-ig.

A kéretlen levelek, azaz a spamek, illetve a különböző kémprogramok és kártékony szoftverek elterjedésére is reagált már az európai közösség. A spamek problematikája már

---

[7]MUHA Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. PhD értekezés. ZMNE, Budapest, 2007. 40. o.

[8]A részletes felsorolásért lásd HAIG Zsolt: Az információs társadalom információbiztonsága. In: Bolyai Szemle. XVII. évfolyam. 2008/4. 175. o.

[9]Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:HU:PDF
Letöltés ideje: 2012. október 6.

[10]Muha Lajos már megfogalmazott egy ezzel kapcsolatos javaslatot, lásd MUHA Lajos: Infokommunikációs Biztonsági Stratégia. In: Hadmérnök. IV. évfolyam. 2009/1. 214-224. o. Fontos azonban megjegyezni, hogy az Európai Digitális Menetrendben meghatározott lépéseket kivitelező Digitális Megújulás Cselekvési Terv 2010-2014 című kormánydokumentum már tartalmazza a keretek kialakítását elősegítő lépéseket. Mindezekről lásd a következő fejezetet.

[11]Eredmények és következő lépések: a globális kiberbiztonság felé
.http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:HU:PDF
Letöltés ideje: 2012. október 6.

2002-ben[12] és 2004-ben[13] is előkerült, azonban más káros tevékenységekkel kapcsolatosan 2006. november 15-én adott ki közleményt a Bizottság.[14] A közlemény nagy hangsúlyt fektet a tudatosságnövelő lépések, illetve a nemzetközi együttműködés fontosságára. Biztosítja a tagállamokat, hogy továbbra is támogatja azokat a kutatási és fejlesztési folyamatokat, amelyek segíthetnek a kártékony kibertéri jelenlét ellen. Mindezekhez kapcsolódóan megjegyzi, hogy az eddigi tapasztalatok azt mutatják, hogy szerény befektetéssel jelentős eredmény érhető el. Véleményem szerint ez a gondolat a teljes kibervédelmi törekvésekre kiterjeszthető, hiszen a kiberképességek kialakítása mind tagállami, mind nemzetközi szervezeti szinten viszonylag alacsony költségvetésű lépés, viszont a hatékonysága és a haszna mégis rendkívül nagy.

Az Európai Unió komolyan foglalkozik a fiatalok védelmével is. Ebbe a törekvésbe illeszkedik bele a *Biztonságos internet program 2009-2013* is.[15] Az Európai Parlament és a Tanács 1351/2008/EK határozata[16] alapján elindított program célja, hogy azonosítsa a gyermekekre leselkedő internetes veszélyeket, illetve harcoljon ellenük. Továbbá lehetőséget biztosít a jogellenes internetes tartalmak bejelentésére.[17]

Végül érdemes megemlíteni a formálódó európai kiberbiztonsági stratégiát. Az előzetes iránymutatást[18] olvasva elmondhatjuk, hogy az Európai Internetes Biztonsági Stratégia nevet viselő projekt nem egy tipikus kiberbiztonsági stratégia lesz, azonban számos hasonlóságot felfedezhetünk a klasszikus stratégiákat vizsgálva. Mindenesetre fontos iránymutató lesz az Unió, mint nemzetközi szervezet számára, hogy miképpen kezelje a kibertéri fenyegetéseket.

Ezen törekvések közé illeszkedik a véleményem szerinti legfontosabb dokumentum is: az Európai Digitális Menetrend.

A DIGITÁLIS MENETREND ÉS A KIBERTÁMADÁSOK

A gazdasági válság nem csak az Unió gazdasági gyengeségeire, hanem más területekkel kapcsolatos problémákra is rávilágított. Ezekre a problémákra való reagálásként került elfogadásra 2010. március 3-án az *Európa 2020 – Az intelligens, fenntartható és inkluzív fejlődés stratégiája*[19] című dokumentumot. A stratégia alapvető célja az új európai gazdasági modell kialakítása és az ehhez kapcsolódó területek fejlesztése. Ennek értelmében öt kiemelt célkitűzést határoztak meg a jogalkotók:

- *foglalkoztatás:* a 20–64 évesek foglalkoztatási rátájának 75%-ra növelése;

---

[12]2002. július 12-én fogadták el az Európai Parlament és a Tanács 2002/58/EK irányelvét, melynek 13. cikke tiltja a spamküldést. Lásd *Az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről.*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:hu:HTML Letöltés ideje: 2012. október 6.

[13]Ekkor fogadták el a 2002-es irányelvvel kapcsolatos kiegészítő lépéseket. Lásd *Measures to counter unsolicited commercial communications or 'spam'.*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0028:FIN:EN:PDF Letöltés ideje: 2012. október 6.

[14]*A kéretlen levelek, a kémprogramok és a rosszindulatú szoftverek elleni küzdelemről.*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:HU:PDF Letöltés ideje: 2012. október 6.

[15]A programnak már volt egy megelőző szakasza is*(Biztonságos internet plusz)*, ami 2005-től 2008-ig tartott.

[16]*Az Internetet és egyéb kommunikációs technológiákat használó gyermekek védelmére irányuló többéves közösségi program létrehozásáról.*
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:348:0118:0127:HU:PDF Letöltés ideje: 2012. október 6.

[17]Magyarországon is üzemel már ilyen weboldal, lásd *Biztonságos Internet.* http://www.biztonsagosinternet.hu/ Letöltés ideje: 2012. október 6.

[18]*ROADMAP: Proposal on a European Strategy for Internet Security*
http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf Letöltés ideje: 2012. október 6.

[19]*Európa 2020 – Az intelligens, fenntartható és inkluzív fejlődés stratégiája.* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:HU:PDF Letöltés ideje: 2012. október 2.

- *K+F:* a bruttó hazai termék (GDP) 3%-ának kutatásra és fejlesztésre való fordítása;
- *éghajlatváltozás/energia:* a szén-dioxid-kibocsátás 20%-kal (amennyiben lehetséges, 30%-kal) való csökkentése; a megújuló energiaforrások arányának és az energiahatékonyságnak 20–20%-kal való növelése;
- *oktatás:* az iskolából kimaradók arányának 10% alá csökkentése és a felsőoktatási oklevéllel rendelkezők arányának 40%-ra való növelése;
- *szegénység/társadalmi kirekesztés:* a szegénység által veszélyeztetett lakosok számának 20 millióval való csökkentése.[20]

A stratégia hét kiemelt kezdeményezést is előreirányoz, amelynek egyik eleme a 2010. augusztus 26-án elfogadott *Európai digitális menetrend*.[21] A menetrend fő célja egy egységes digitális piac létrehozása egy biztonságos és világos jogi keretekkel rendelkező környezetben. E cél elérése érdekében számos lépés megtételére van szükség mind uniós, mind tagállami szinten:

- 2013-ig a minimális szélessáv mindenki számára elérhető legyen;
- 2015-ig szűnjön meg a különbség a belföldi és a roaming tarifák között;
- 2015-ig a rendszeres internethasználat mutatója érje el a 75 %-ot (a jelenlegi 60 %-ról), a hátrányos helyzetűek esetében pedig a 60 %-ot;
- 2015-ig a felére kell csökkenteni azoknak a számát, akik még sosem használtak internetet.[22]

Témánk szempontjából azonban a legfontosabb az internet biztonságával kapcsolatos felismerések és a hozzájuk tartozó reakciók. Ahogyan a vonatkozó részben is olvashatjuk: *„Az európaiak nem fognak olyan technológiát felkarolni, amelyben nem bíznak – a digitális kor nem lehet egyenlősem a Nagy Testvérrel, sem az »internetes vadnyugattal«.”*[23]

A dokumentum vonatkozó része számos problémás pontra rámutat. A spam üzenetek növekvő mértéke, a banki szolgáltatások, illetve a személyes adatok egyre kifinomultabb módszerekkel való támadása ugyanúgy megjelenik, mint az államok ellen folytatott kiberhadviselés veszélye is.

A Menetrend kiválóan vázolja azokat a területeket, amelyek terén lépéseket kell tenni: gyermekpornográfia elleni harc; kritikus infrastruktúrák informatikai védelme; saját hálózatok védelme; tagállami operatív csoportok kialakításának támogatása. Magyarán a kibervédelem teljes spektrumát igyekeznek megvalósítani, ami azért is fontos, mert kezdetben az Európai Unió csupán a saját közös rendszereinek védelmét tartotta fontosnak, most azonban már egyértelművé vált, hogy a tagállamok felzárkóztatása ezen a téren elengedhetetlenül fontos a sikeres védelem kialakításához.

Minden tagállam kötelessége, hogy kidolgozza a saját cselekvési tervét, amely a Digitális Menetrendben megfogalmazottak elérését segíti. Magyarország tekintetében a 2010. december 20-án elfogadott *Digitális Megújulás Cselekvési Terv 2010-2014*[24] az iránymutató

---

[20]*Európa 2020: az Európai Unió növekedési stratégiája.* http://europa.eu/legislation_summaries/employment_and_social_policy/eu2020/em0028_hu.htm Letöltés ideje: 2012. október 2.

[21]*Az európai digitális menetrend*.(a továbbiakban: MENETREND 2010.) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF Letöltés ideje: 2012. október 2.

[22]*Miről szól a Digitális Agenda?*http://www.euvonal.hu/index.php?op=kerdesvalasz_reszletes&kerdes_valasz_id=1634 Letöltés ideje: 2012. október 2.

[23]MENETREND 2010. 18. o.

[24]*Digitális Megújulás Cselekvési Terv 2010-2014.* http://www.kormany.hu/download/6/4f/00000/Digitalis_Megujulas_Cselekvesi_Terv.pdf Letöltés ideje: 2012. október 1.

dokumentum. A program célja, hogy a magyarországi információs társadalmat mind technikai, mind gazdasági szempontból fejlessze.

Véleményem szerint a cselekvési tervnek két nagyon fontos pontja van. Az első a kritikus információs infrastruktúráknak védelmével kapcsolatosan meghatározott lépések, illetve a kapcsolódó akciók, amelyek a következőek:

- A kritikus információs infrastruktúra védelem vezetésének és a védelmi stratégia kidolgozásának kormányzati kézbe vétele, a vonatkozó EU irányelvnek megfelelően;
- Az állam vezetésével, kidolgozott módszertan alapján a nemzeti kritikus infrastruktúra, valamint az európai kritikus infrastruktúra elemek kijelölése, illetve a kijelölések folyamatos felülvizsgálata;
- A kritikus információs infrastruktúra védelmi szabályok és feladatok állami kijelölése
- Összkormányzati szinten a kritikus információs infrastruktúrák védelme területén a tudatosság növelés és az oktatás, továbbképzés.[25]

A második fontos pont a közigazgatási információs rendszerek biztonságának növelése. Mindehhez a dokumentum az alábbi akciókat kapcsolja:

- Adatszabványok, információbiztonsági követelmények kompatibilitásának megteremtése az egészségügyi informatikában;
- IT-biztonsági jogszabályok átdolgozása;
- Magas színvonalú informatikai biztonsági megoldások bevezetésének támogatása a kormányzat részére egységes szabályozás alapján.[26]

Ami a Digitális Menetrend további értékét adja az az, hogy a problémák megfogalmazásán kívül – ahogyan azt olvashattuk – válaszokat is kínál. Konkrét lépésekkel és új szervek kialakításával reagál a felmerülő fenyegetésekre, továbbá világossá teszi, hogy mely feladatok tartoznak az Unió hatáskörébe és melyek a tagállamokéba, illetve melyek azok, amelyeket közösen kell kivitelezni. Mindezekről lásd az 1. ábrát.

	Uniós szintű feladat	Tagállami feladat
Hálózat- és információbiztonsági politika végrehajtása	✓	
Kiberbűnözés elleni központ létrehozása	✓	
Globális kockázatok kezelése	✓	
Kiberbűnözést figyelő országos platformok kialakítása		✓
Jogellenes internetes tartalmak bejelentésére alkalmas pontok kialakítása		✓
Hálózatvédelmi gyakorlatok kivitelezése	✓	✓
Kritikus információs infrastruktúrák védelme	✓	✓
Számítástechnikai Sürgősségi Reagáló Egység kialakítása	✓	✓

1. ábra. Az Európai Digitális Menetrend által meghatározott fő feladatok megoszlása (Forrás: Menetrend 2010. 20-21. o.)

Ezek azok a körülmények, amiért a Digitális Menetrendet az egyik legfontosabb lépésnek tartom az EU kibervédelmének kialakításánál. Láthatóan jól átgondolt, egymásra épülő tervezet, amiből számos pontja megvalósult már. A végrehajtott lépések hatékonysága

[25] i. m. 91. o.
[26] i. m. 68. o.

természetesen csak rövid idővel később nyerhet igazolást, azonban tagadhatatlan ténnyé vált, hogy az Unió komolyan veszi ezen új típusú biztonsági kihívást.

ÖSSZEGZÉS

A fentiekben bemutattam az Európai Unió legfontosabb dokumentumait és jogi lépéseit a kiberbiztonság erősítése érdekében. Jól látható, hogy a jogi keretek kialakítása nagy erővel folyik, napjainkra már az unió szintjén a tárgyalt kérdés majdnem összes szegmense rendelkezik önálló iránymutatással. Magyarán az érzékeny területek azonosítása megtörtént. Innentől kezdve a tagállamok felelőssége, hogy a legalacsonyabb szintektől kezdve felkészüljenek a különböző incidensek kezelésére.

Érdekes trend figyelhető meg az uniós kommunikáció tekintetében, miszerint a kezdetben alapvetően ajánlás jellegűek voltak az informatikai és információbiztonság területéhez kapcsolódó intézkedések, később azonban számos lépés kötelező jellegűvé vált. Mindez természetesen üdvözölendő változás, hiszen a tagállamok közötti különbség – akár képességek, akár stratégiákat tekintetében – a közös biztonságot gyengítik.

A tanulmányom következő részében az uniós kibervédelmi szervezeteket és a lehetséges együttműködő partnereket fogom bemutatni.

Felhasznált irodalom

[1] 2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. In: Határozatok Tára. 2008/31. 217-231. o. ISSN 2063-0395

[2] A Bizottság megerősítené az informatikai támadásokkal szembeni védelmet Európában. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1239&format=HTML&aged=1&language=HU&guiLanguage=en; Letöltés ideje: 2012. október 4.

[3] Az európai digitális menetrend. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF Letöltés ideje: 2012. október 2.

[4] Critical Infrastructure Protection in the Fight Against Terrorism. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF Letöltés ideje: 2012. október 10.

[5] Digitális Megújulás Cselekvési Terv 2010-2014. http://www.kormany.hu/download/6/4f/00000/Digitalis_Megujulas_Cselekvesi_Terv.pdf; Letöltés ideje: 2012. október 1.

[6] Európa 2020 – Az intelligens, fenntartható és inkluzív fejlődés stratégiája. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:HU:PDF; Letöltés ideje: 2012. október 2.

[7] Európa 2020: az Európai Unió növekedési stratégiája. http://europa.eu/legislation_summaries/employment_and_social_policy/eu2020/em0028_hu.htm; Letöltés ideje: 2012. október 2.

[8] HAIG Zsolt: Az információs társadalom információbiztonsága. In: Bolyai Szemle. XVII. évfolyam. 2008/4. 167-180. ISSN 1416-1443

[9] KOVÁCS László: Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I. In: Hadmérnök. VII. évfolyam. 2012/2. 302-311. o. ISSN 1788-1919

[10] *Miről szól a Digitális Agenda?*
http://www.euvonal.hu/index.php?op=kerdesvalasz_reszletes&kerdes_valasz_id=1634;
Letöltés ideje: 2012. október 2.

[11] *National Cyber Security Strategies.*
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport;
Letöltés ideje: 2012. október 1.

[12] *Zöld Könyv a kritikus infrastruktúra védelem európai programjáról.*
http://www.ivb.org.hu/documents/INNOVACIOSklub/200812ho/ZoldKonyv.pdf;
Letöltés ideje: 2012. október 10.