HADMÉRNÖK

VII. Évfolyam 2. szám - 2012. június

Kovács László
kovacs.laszlo@uni-nke.hu

EURÓPAI ORSZÁGOK KIBERBIZTONSÁGI POLITIKÁINAK ÉS STRATÉGIÁINAK ÖSSZEHASONLÍTÓ ELEMZÉSE I.

Absztrakt

Az európai országok nemzeti szinten próbálnak választ adni arra a problémára, amely a kibertér egyre kiterjedtebb fontosságából és az ezzel összefüggő veszélyekből ered. Az európai országok kiberbiztonsági stratégiáinak elemzésekor láthatjuk, hogy számos ország az információs társadalom és annak biztonsági vetületei, más országok pedig a kritikus információs infrastruktúrák és azok biztonsági kérdései felől közelítik meg a kérdést. Jelen írás néhány nagy európai, és néhány Magyarországhoz hasonló méretű ország kiberbiztonsági stratégiáját és politikáját tekinti át, mindamellett, hogy az Európai Unió és a NATO ilyen irányú irányelveit és dokumentumait is bemutatja.

The European countries try to answer to the problems, which are stems from the associated risks of the cyberspace and its importance at national level. Analyzes of the cyber security strategies of European countries show that many countries' approach based on the information society and its security aspects, in other countries focuses on critical information infrastructures and its security issues. This present paper analyses some of the major European countries cyber security strategy and policy, as well some Hungary similar-sized countries strategy. In addition the European Union's and NATO's cyber policies and cyber security documents will also present.

Kulcsszavak: *kiberbiztonság, kritikus információs infrastruktúra, biztonság ~ cyber security, critical information infrastructure, security*

BEVEZETÉS

Az ma már nemcsak a hivatásszerűen ezzel foglalkozók számára, hanem a mindennapi emberek számára is világos tény, hogy fejlett nyugati társadalmunk nem nélkülözheti az információs technológiákra épülő infrastruktúrákat.

Ezeknek az infrastruktúráknak a biztonsága, amelyek a mindennapi közműszolgáltatásoktól kezdődően, a gazdasági életen át a közigazgatásig, vagy akár a mindennapjaink legapróbb részletéig mindenhol ott vannak, elsőrendű fontosságot élvez. Ennek oka nagyon egyszerű: ha nem működnek ezek a rendszereink, akkor nem működik a társadalom sem.[1]

A kihívás tehát hatalmas, fejlett nyugati világunk nem létezhet az információtechnológia, illetve az ezekere a technológiákra épülő infrastruktúrák nélkül.

Stratégiai szinten a probléma kezelése országonként eltérő. Számos ország az információs társadalom építése és fejlesztése, más országok az információs inftasruktúrák oldaláról közelítik meg a kérdést. Utóbbi megoldási mód esetében az információs infrastruktúrák több országra, régióra vagy akár több kontinensre is kiterjedő interdependenciája azt is feltételezi, hogy ez a nemzeti szinten végzett és megvalósított védelem koordinált és az érintett felek (országok) között egyeztetett módon történik. Ugyanakkor azt is ki kell jelenteni, hogy minden stratégia csak akkor lehet hatékony, ha az további rész-startégiákra bontható, így például az információbiztonságra vonatkozóan, annak komplex megközelítését kell elvégezni, azaz a személyi, fizikai, dokumentum- és elektronikus információvédelem területeire egyaránt figyelmet kell fordítani. [1]

Mindezeknek megfelelően érdemes megvizsgálni, hogy melyik ország milyen kiindulópontot használt fel az információs kor kihívásainak kezelése, az arra való kormányzati illetve társadalmi felkészülés elindításakor.

Jelen írás néhány nagy európai, és néhány Magyarországhoz hasonló méretű ország kiberbiztonsági stratégiáját és politikáját tekinti át, mindamellett, hogy a NATO ilyen irányú irányelveit és dokumentumait is bemutatja.

NEMZETI CYBER STRATÉGIÁK

A fentiekben megfogalmazottak alapján – jelen írás terjedelmi korlátai miatt – vázlatosan bemutatásra és elemzésre kerül néhány ország, valamint a NATO cyber-teret érintő startégiája. A nemzeti, illetve kormányzati szintű cyber stratégiák – a korábban kifejtett okok miatt, országonként eltérő módon – a biztonságot, az információs társadalom fejlődését illetve zavartalan működését, illetve a kritikus információs infrastruktúrák védelmét külön-külön, vagy akár egyszerre is tárgyalják, illetve ezeket célozzák meg. Az ismertetésre kerülő nemzeti szintű cyber stratégiák alapvetően az Európai Hálózat- és Információbiztonsági Ügynükség (ENISA – European Network and Security Agency)[2] országértékeléseinek felhasználásával készültek.

---

[1] Természetesen az információs korszak és az ebben megjelent IT eszközök és eljárások előtt is működött a társadalom. Ugyanakkor napjainkban talán a gazdaság és az ipar a legjobb példái annak, hogy IT eszközök, rendszerek, illetve az ezekre alapozott eljárások nélkül nem lehet versenyképes és nem lehet fejlődő a gazdaság. Ma igaz az, ami a posztindusztriális társadalom előtti korokra nem feltétlenül volt igaz: a fejlődés, és így maga a társadalom működése alapvetően az információra, annak feldolgozására, tárolására, szétosztására és felhasználására épül. E folyamat vagy folyamatok azonban alapvetően feltételezik azt, hogy megfelelő információs (infokommunikációs) eszközök állnak rendelkezésre, amelyek keresztül, illetve amelyek támogatásával az említett folyamatok elvégezhetőek.

[2] Az ENISA fő tevékenysége arra koncentrál, hogy az EU-ban a hálózat- és információbiztonság megfelelően magas szintű legyen. Ennek érdekében az ügynökség szaktanácsokkal segíti a tagállamok különböző hatóságait, valamint az uniós intézményeket a hálózat- és információbiztonság különböző kérdéseiben. Az ENISA fórumot

MAGYARORSZÁG

2012 óriási – mondhatni áttörő – változást hozott Magyarországon is azzal, hogy a Nemzeti Biztonsági Stratégiába kiemelt helyen kerül be, mint veszélyforrás a cyber kihívások jelentette veszély.

Az új Nemzeti Biztonsági Stratégia a következőképpen fogalmaz:

„*Kiberbiztonság. Az állam és a társadalom működése – a gazdaság, a közigazgatás, vagy a védelmi szféra mellett számos más területen is – mind meghatározóbb módon a számítástechnikára épül. Egyre sürgetőbb és összetettebb kihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatok, valamint a kapcsolódó kritikus infrastruktúra fizikai és virtuális terében. Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem-állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését. E támadások eredetét és motivációját gyakran nehéz felderíteni. A kibertérben világszerte növekvő mértékben jelentkező nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmi vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kell állnia.*

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

b) A nemzeti kritikus információs infrastruktúra védelmének erősítése mellett szövetségeseinkkel és

EU-partnereinkkel együtt arra törekszünk, hogy az információs rendszerek biztonsága erősödjön, valamint részt vegyünk a megfelelő szintű kibervédelem kialakításában." [2]

Hazánkban az ezredforduló környékén alapvetően az információs társadalom építése, majd ennek fejlesztése volt az a stratégiai irány, amelyet a kormány fő célkitűzésnek tekintett a kibertér tekintetében. 2001-ben került kiadásra a Nemzeti Információs Társadalom Stratégia, amely alapvetően hét részben – Infrastruktúra-fejlesztési Program, Gazdaságpolitikai Program, Kultúra Program, Oktatási Program, Társadalompolitikai Program, Elektronikus Kormányzati Program, Önkormányzati Program – határozta meg azokat az alapvető célkitűzéseket, amelyek hazánkban az információs társadalom építéséhez elengedhetetlenek.[3] [3] Ezt a stratégiát 2003-ban – újabb stratégia követte, amely a Magyar Információs Társadalom Stratégia néven került kiadásra. E stratégia célja, hogy Magyarországon tudásalapú gazdaságot létrehozva, az információs társadalom fejlesztésével az egyén és a közösség életminőségének és életkörülményének javítását lehessen elérni. [4]

2010-ben jelent meg a harmadik olyan hazai startégia, amely az információs társadalom kialakítását, építését és fejlesztését célozta meg. A Digitális megújulás cselekvési terv 2010-2014 címet viselő dokumentum összhangban van az Európai Unió célkitűzéseivel és annak infokommunikációs programjaival. A stratégia alcíme Az infokommunikációs ágazat cselekvési terve a társadalom és a gazdaság megújulásáért, amely tükrözi az információs társadalom építésének és fejlesztésének érdekében szükséges kormányzati, gazdasági és össztársadalmi feladatokat. [5]

---

biztosít ahhoz, hogy az érintettek megoszthassák egymással bevált módszereiket, továbbá elősegíti a kapcsolatépítést az uniós intézmények, a tagállami hatóságok és a vállalkozások között. [6]

[3] E stratégia nem tartalmazott olyan akciótervet, amely felmérte volna azokat a veszélyeket, amelyek az információs társadalom kiépítése – illetve kialakulása esetén –, annak működése során jelentkezhetnek. [7]

Természetesen hazánkban is született a technikai oldal, azaz a kritikus infrastrukturák védelmére irányuló kormányzati elgondolás. Ez a 2080/2008. (VI.30.) Korm. határozat A Kritikus Infrastruktúra Védelem Nemzeti Programról címet viseli. Ebben határoztaban célozta meg a magyar kormány a teendőket és a felkészülsé alapvető teendőit a kritikus infrastruktúrák védelmének területén. Ez a dokumentum, illetve kormányhatározat már tartalmaz utalásokat és némi kategorizálást a kritikus információs infrastruktúrák vonatkozásában, ugyanakkor a fogalom meghatározása, azaz, hogy mit tekintünk kritikus információs infrastruktúrának, annak részletes felsorolása, osztályozása, valamint a védelem konkrét feladatainak leírása mindezidáig hivatalosan, kormányzati szinten nem történt meg. [8]

Jelenleg törvényalkotási szakaszban van a Kritikus infrastruktúrákról szóló törvény, és előkészítési fázisban van az az Információbiztonsági törvény, amely hasznos kiinduló alapja lehet a kritikus információs infrastruktúrák hazai védelmének.

SZLOVÁKIA [9]

2009 októberében a szlovák kormány elfogadta az új Információs Társadalom Stratégia 2009-2013 című dokumentumot. E stratégiai dokumentum – címének megfelelően – a Szlovák Köztársaság aktualizált információs társadalom stratégiáját rögzíti.

Az új stratégia felváltotta az eredeti Információs Társadalom Stratégiát és cselekvési tervet. Ennek oka elsősorban az volt, hogy az előző startégia megjelenése (2004) óta eltelt időben olyan új kihívások és trendek jelentek meg, amelyekre már a régi stratégia nem tudott megfelelő és adekvát válaszokat adni.

Az új stratégia lefedi az addig rész-startégiák által kezelt területeket, ugyanakkor a korábban a rész-stratégiák által meghatározott területeket nem szabályozza részletesen.

Az átdolgozott stratégia meghatározza azokat a legfontosabb fejlesztési területeket és prioritásokat, amelyek a Szlovák Köztársaság információs társadalmának építése során elengedhetetlenek. Ezek a következők:

- szélessávú hozzáférés növelése;
- információbiztonsági szabványok kidolgozása;
- e-kormányzat és e-egészségügy fejlesztése;
- digitális írástudás fejlesztése, eoktatás kialakítása;
- az energia fogyasztás csökkentése és az energia hatékonyság növelése.

Meg kell még említeni Szlovákia Nemzeti Informatikai Biztonsági sratégiáját, amelyet a szlovák kormány 2008 augusztusában fogadott el. Ez a dokumentum három szintet tartalmaz. Az első szint leírja a hosszú távú információbiztonsági stratégiai célokat Szlovákia számára. A második szint a stratégiai prioritásokra összpontosít, a harmadik szint pedig feltárja a legfontosabb problémákat, valamint meghatározza az ezek kezelésével kapcsolatos feladatokat. A dokumentum nagyon világosan szétválasztja a hatásköröket, meghatározza a prioritásokat és a megteendő intézkedéseket. A dokumentum a nem minősített információk védelméhez szükséges feladatokat is meghatározza, azaz ajánlásokat tesz az információ szivárgás, a jogosulatlan információ felhasználás és az adatok integritásának megsértése elkerülése érdekében.

2010 óta tart a Cyberbiztonsági Törvény előkészítése, amelyet a Szlovák Pénzügyminsztérium jegyez, és amely törvény alapvetően a közigazgatás különböző ágazataiban használt információs rendszerek működését hivatott majd szabályozni.

CSEHORSZÁG [10]

A Cseh Köztársaság új nemzeti biztonsági kutatási stratégiáját, amelyet a Belügyminisztérium dolgozott ki 2008-ban hagyta jóvá a cseh kormány. A stratégia középpontjában olyan prioritások felállítása került, amely a kiválóságot, a legjobb gyakorlatok elterjesztését és alkalmazását, valamint a beruházások racionalizálását célozta meg. Három fő területen határozott meg prioritásokat:

- a polgárok biztonsága (beleértve a terrorizmus elleni tevékenységet, a szervezett bűnözést, a polgári védelmet, a környezeti biztonságot, stb.);
- a létfontosságú infrastruktúrákat (beleértve az energia-, víz-, élelmiszer-, a közlekedés, banki és pénzügyi, az IKT szektorokat, stb);
- válságkezelés (beleértve a korai figyelmeztetést és a felkészülést).

A stratégia meghatározott horizontális prioritásokat is:

- incidens előrejelzés és speciális forgatókönyvek kidolgozása;
- készenlét (tudatosítása);
- innováció;
- felhasználók és eszközök azonosítása;
- koordináció az EU-val.

Mindezeken túl 2011 januárjában elfogadásra került a Digitális Cseh Köztársaság stratégiai dokumentum, amely alapvetően a nagy sebességű hálózati hozzáférés fejlesztését volt hivatott rendezni. E dokumentumban a fő prioritásként és fő célként jelenik meg a Cseh Köztársaság polgárainak és a vállalatainak nagy sebességű internet kapcsolatának kialakítása, valamint az, hogy mindenkinek legyen lehetősége az elektronikus kommunikációs technológiák használatára. A folyamat és a stratégia végrehajtásának, valamint a nyílt platformok cseréjének, és a legjobb gyakorlatok regionális és helyi szinten történő bevezetése és végrehajtása ellenőrzésére az Ipari és Kereskedelmi Minisztérium elindította a www.digitalnicesko.cz információs portált. Ezen a portálon közzéteszik a legfontosabb híreket, jogszabályokat, valamint az ajánlott technológiai megoldásokat. A stratégia előirányozza a pénzügyi források hatékony felhasználását pl. az Európai Beruházási Bank, a Vidékfejlesztési Alap és a strukturális alapok vonatkozásában.

2011-ben készült el és került kiadásra a Cseh Köztársaság Cyber biztonsági stratégiája a 2011-2015 közötti időszakra, amely alapvetően a Cseh Köztársaság Nemzetbiztonsági Stratégiájára alapul. A stratégia fő célja, hogy a Cseh Köztársaság területén a számítógépes biztonság megszilárduljon, és létrejöjjön egy hiteles információs társadalom szilárd jogi alapokon. A dokumentum elkötelezett a biztonságos információ továbbítás és feldolgozás felé, valamint annak – az élet valamennyi területén történő –, szabad és biztonságos megosztása mellett.

A következő stratégiai célok kerültek megfogalmazásra a dokumentumban:

- jogszabályi háttér kidolgozása;
- a közigazgatás és a kritikus infrastruktúrák cyber biztonságának erősítése;
- nemzeti CERT[4] ügynökség megalapítása;
- nemzetközi együttműködés fokozása;
- együttműködés erősítése az állam, a magánszektor és az akadémiai szektorok között;
- a cyber biztonság tudatosságának növelése.

[4] CERT: Computer Emergency Response Team, számítógépes vészhelyzeti reagáló csoport.

LENGYELORSZÁG [11]

Lengyelországban 2010-ben kezdődött meg a Kormányzati számítógépes biztonság 2011-2016 cselekvési terv kidolgozása (Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016, RPOC).

Az RPOC meghatározza a nemzeti információbiztonságban szerepet játszó minden szereplő feladatait és felelősségi körét, valamint az elérendő célokat a 2011 és 2016 közötti időszakban.

Lengyelországban a CERT közösség kulcsfontosságú szerepet játszik a kialakítandó cyber stratégia megalkotásában. A CERT GOV.PL csapat működési keretein belül létrehozott Belső Biztonsági Ügynökség (ABW) aktív szerepet tölt be a kormányzati CERT feladatainak megvalósulása során. Együttműködve a CERT Polskával, amely a legrégebbi nemzeti CERT, state-of-the-art korai előrejelző rendszert, az ARAKIS-GOV-ot működtetik annak érdekében, hogy valamennyi kormányzati hálózat vonatkozásában a malware-ekkel és más új biztonsági fenyegetésekkel szemben a védelmet biztosítani tudják.

A legnagyobb távközlési szolgáltatók Lengyelországban együttműködnek a kormánnyal különböző fórumok fenntartásában, amely fórumok a visszaélésekről, a közös kezdeményezésekről adnak számot, valamint együttműködési felületete biztosítanak a közös incidens kezeléshez.

2007-ben kezdődött meg a Lengyelország információs társadalom fejlesztési stratégia 2013-ig dokumentum kidolgozása. Ez a stratégiai dokumentum előirányozza egy olyan társadalom kialakítását, ahol az állampolgárok és a vállalkozások tudatosan használják az IKT nyújtotta lehetőségeket a gazdasági, társadalmi és kulturális fejlődés érdekében. Ennek hatékony támogatásával egy korszerű és felhasználóbarát közigazgatás léterhozása a cél.

Lengyelország információs társadalom stratégiája választ kíván adni a sajátos lengyel kihívásokra, ugyanakkor összhangba kívánja hozni mindezt az európai kezdeményezésre létrejött Európai digitális menetrenddel.

A stratégia a következő attribútumokat határozza meg Lengyelország információs társadalmának kialakításához:

- hozzáférhetőség, biztonság bizalom: hozzáférés biztosítása a megbízható információkhoz vagy biztonságos szolgáltatásokhoz, amelyek elengedhetetlenek a polgárok és a vállalkozások számára;
- a nyitottság és a sokszínűség: nincs preferencia az információhoz való hozzáférés, különösen a lakosság tájékoztatásának kérdésében;
- egyetemesség és elfogadhatóság: erőfeszítéseket kell tenni annak biztosítása érdekében, hogy aktívan részt vegyen minél több szereplő az információs társadalom kiépítésében, amely alapján az a lehető legnagyobb mértékben megvalósítható, és az információs társadalom termékei és szolgáltatásai minél szélesebb körben hozzáférhetővé váljanak;
- kommunikáció és interoperabilitás: az információ keresésése és hozzáférése a biztonságos, gyors és egyszerű legyen.

CYBER STRATÉGIA A NATO-BAN

A NATO a 2007-es észt incidens óta kiemelt területként kezeli a cyber kérdést. Az nagyon hamar világossá vált és számos NATO hivatalnok hangúlyozta is, hogy a területem központi koordináció és központi irányítói szerep szükséges.

Szintén többször kinyilatkoztatott tény a NATO-ban, hogy az eltérő technikai fejlettségű országok, vagy akár az egyes országokon belüli eltérő fejlettségű régiók, eltérő módon kezelik

a biztonságot is, így a cyber biztonságot is. Ennek megfelelően nem azonos szintű biztonságot valósítanak meg, amely hatalmas kockázatot jelent. Az úgynevezett digitális szakadék, amely az eltérő technikai és társadalmi (oktatási, gazdasági, stb.) fejlettségből eredeztethető megoldandó problémaként jelenik meg.

A NATO 2010-es lisszaboni csúcstalálkozója után a Szövetség Stratégiai Koncepciójában[5] is szerepelteti, hogy az egyre kifinomultabb számítógépes támadások miatt a Szövetség információs és kommunikációs rendszerek védelme az egyik legsűrgősebb feladat. *„A kibertámadások egyre gyakoribbá, szervezettebbé és a kormányok, vállalkozások, gazdaságok és potenciálisan a közlekedési és ellátási hálózatok valamint más kritikus infrastruktúrák számára is egyre nagyobb károkat okozóvá válnak. Elérhetik azt a küszöböt, ami már a nemzeti és euro-atlanti prosperitást, biztonságot és stabilitást veszélyezteti. Külföldi haderők és titkosszolgálatok, szervezett bűnözők, terrorista és/vagy szélsőséges csoportok egyaránt lehetnek egy ilyen támadás végrehajtói. „* [12]

2011. június 8-án a NATO védelmi miniszterek jóváhagyták a NATO újredefiniált cybervédelmi politikáját. E politika világos jövőképet határoz meg a cyber védelem területén az egész szövetség vonatkozásában, valamint egy kapcsolódó cselekvési terv végrehajtásáról is rendelkezik. 2011 októberében a miniszterek elfogadták e cselekvési terv részleteit is.

2012 februárjában, egy 58 millió eurós szerződés került megkötésre, amely a NATO Cyber incidens kezelési képesség (NATO Cyber Incident Response Capability - NCIRC) 2012 év végéig történő teljes kiépítését teszi lehetővé. Mindezekkel párhuzamosan a Szövetség egy úgynevezett Cyber fenyegetetés előrejelző központot (Cyber Threat Awareness Cell) is létrehozott annak érdekében, hogy fokozza a hírszerzési információk megosztását valamint a reális helyzetismeretet. [13]

Mindezekkel összhangban van a 2012-es chicagói csúcs után kiadott hivatalos állásfoglalás szerint: *„A számítógépes támadások továbbra is jelentősen növekedni fognak mind azok számát, mind azok kifinomultság és a komplexitását tekintve. Megerősítjük a lisszaboni csúcstalálkozón tett számítógépes védelmi kötelezettségvállalásainkat. Lisszabon után tavaly a NATO elfogadta a Cyber Védelmi Koncepció című politikát és cselekvési tervet, amely most kerül végrehajtásra. Építve a NATO meglévő képességeire, a NATO Számítógép Vészhelyzeti Incidenskezelő Képesség (NATO Computer Incident Response Capability - NCIRC) Teljes Műveleti Képessége (Full Operational Capability - FOC), beleértve a legtöbb helyszínt és a felhasználót, kialakításra kerül 2012 végéig. Vállaljuk, hogy biztosítjuk a forrásokat és véghezvisszük a szükséges reformokat ahhoz, hogy minden NATO alá tartozó szerv központosított számítógépes védelemben részesüljön, annak érdekében, hogy a fokozott számítógépes védelmi képességekkel megvédjük a kollektív NATO értékeket.*

Tovább integráljuk a számítógépes védelmi intézkedéseket a Szövetség struktúrájában és folyamataiban, valamint minden egyes tagországában, és továbbra is elkötelezettek vagyunk mindazon nemzeti cybervédelmi képességek ügyében, amelyek erősítik az együttműködést és a kölcsönös átjárhatóságot a Szövetségen belül, többek között a NATO védelmi tervezési folyamatokban. Továbbra is fejleszteni fogjuk azokat a képességeinket, amelyekkel képesek vagyunk a megelőzésére, a felderítésére, a védelemre, és a számítógépes támadások következményeinek felszámolására. Arra törekszünk, hogy párbeszédet folytassunk a partner nemzetekkel, a nemzetközi szervezetekkel, többek között az EU-val, az Európa Tanáccsal, az ENSZ-el és az EBESZ-el, abból a célból, hogy a számítógépes biztonsági fenyegetésekkel kapcsolatban javítani lehessen a közös biztonságot és a konkrét együttműködést. Teljes mértékben kihasználjuk az észtországi Cybervédelmi Kiválósági Központ (Cooperative Cyber Defence Centre of Excellence – CCDCOE) által kínált szakértelmet." [14]

[5] A NATO 2010-es új stratégiai koncepciója: Aktív Szerepvállalás, Modern Védelem Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról.

Ugyanezen csúcsértekezlet után került kiadásra a Védelmi Képességek: A NATO Erők 2020-ban (Summit Declaration on Defence Capabilities: Toward NATO Forces 2020) dokumentum, amely a cyberbiztonságot szintén előtérbe helyezi. [15]

1. sz. táblázat.
A különböző országok cyber biztonsági stratégiáinak áttekintése

Ország / Nemzetközi szervezet	Stratégia címe	Fő terület	Koordináció
MAGYARORSZÁG	2080/2008 kormányhatározat	Kritikus infrastruktúrák védelme	nincs központi kormányzati koordináció
SZLOVÁKIA	Information Society Strategy for 2009-2013 (2009) National Strategy for Information Security (2009) The National Strategy for Information Safety of Slovakia (2008)	Információs társadalom, információbiztonság	nincs központi kormányzati koordináció (vezető: Belügyminisztérium)
CSEHORSZÁG	Digitális Cseh Köztársaság A Cseh Köztársaság cyber biztonsági stratégiája 2011 – 2015 között	Információs társadalom, információbiztonság	Interdepartmental Coordination Board for Cyber Security (vezető: Belügyminisztérium)
LENGYELORSZÁG	Lengyelország információs társadalom fejlesztési stratégia 2013	Információs társadalom, információbiztonság	nincs központi koordináció (vezető: Védelmi Minisztérium és Belügyminisztérium)
NATO	Stratégiai Koncepció NATO Cybervédelmi Politika	Cybervédelem	Koordináció: NATO főtitkár helyettes Iklódy Gábor (Assistant Secretary General for Emergency Security Challenges)

ÖSSZEGZÉS

Összességében a néhány ország, illetve a NATO cyber védelmi dokumentumainak, stratégiáinak, illetve politikáinak áttekintéséből a következő megállapítások szűrhetők le:

- a stratégiák eltérőek: csak néhány helyen jelenik meg a konkrét cyber defense stratégia;
- az információs társadalom kiépítése és fejlesztése kiemelt feladatként jelentkezik számos ország esetében;
- a cyber védelmi stratégiák (amennyiben van ilyen) nem mindenhol épül a nemzetbiztonsági stratégiára;
- minden országban a cyber bűnözés elleni fellépés kiemelt feladat;
- néhány országban a kritikus információs infrastruktúrák védelme jelenik meg stratégiai szinten;
- központi (kormányzati) koordinált védelem nincs minden országban, így hazánkban sem jelenik ez meg;
- legjellemzőbb az informatikai incidens kezelés, majd az erre épülő együttműködés.

FELHASZNÁLT IRODALOM

[1] Póserné Oláh Valéria: A szervezeti informatikai biztonság. in: Hadmérnök, 2007/4. http://hadmernok.hu/archivum/2007/4/2007_4_poserne.html

[2] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról

[3] Nemzeti Információs Társadalom Stratégia. 2001.

[4] Magyar Információs Társadalom Stratégia, 2003.

[5] Digitális Megújulás Cselekvési Terv 2010-2014. Nemzeti Fejlesztési Minisztérium, 2010

[6] Ügynökségek és decentralizált szervek. ENISA. http://europa.eu/agencies/regulatory_agencies_bodies/policy_agencies/enisa/index_hu.htm

[7] Ványa László (szerk), Haig Zsolt, Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Tanulmány a TÁMOP 4.2.2/B-10/1-2010-0001 Tudományos képzés műhelyeinek támogatása Kockázatok és válaszok a tehetséggondozásban (KOVÁSZ) projekt támogatásával, NKE, Budapest, 2012.

[8] KOVÁCS László: Az információs terrorizmus elleni tevékenység kormányzati feladatai. HADMÉRNÖK 2008:(2) pp. 138-148. (2008)

[9] Enisa country reports – Slovakia. http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Slovakia.pdf

[10] Enisa country reports – Czech Republic http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/CzechRepublic.pdf

[11] Enisa country reports – Poland
http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Poland.pdf

[12] NATO stratégiai koncepciója 2010 a Biztonságpolitikai szakkollégium fordításában:
http://www.biztonsagpolitika.hu/documents/1291766875_NATO_Strat_Koncepcio_2010_hun_BSZK.pdf

[13] NATO and cyber defence, http://www.nato.int/cps/en/natolive/topics_78170.htm?]

[14] http://www.nato.int/cps/en/SID-D95FAE1D-99C8ECE1/natolive/official_texts_87593.htm

[15] http://www.nato.int/cps/en/natolive/official_texts_87594.htm

Jelen publikáció a Magyar Tudományos Akadémia
Bolyai János Kutatási Ösztöndíjának támogatásával valósult meg.