Berzsenyi Dániel

Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése

2013 májusában Ausztria és Csehország kezdeményezésére, Lengyelországgal, Szlovákiával és Magyarországgal kiegészülve alakult meg a Közép-európai Kiberbiztonsági Platform (Central European Cyber Security Platform – CECSP). Az öt részes ország együttműködése kiterjed az információk, a legjobb gyakorlatok, valamint azoknak a különleges eljárásmódoknak a megosztására, amelyek a kibertérből érkező fenyegetésekhez, illetve konkrét (kiber)támadásokhoz köthetők. További cél a kibervédelmi kapacitások és képességek bővítése közös képzés, oktatás és gyakorlatok szervezése révén, valamint a koordinált kutatás és fejlesztés. Az együttműködés hátterében azonban olyan, a kibertér biztonságához és védelméhez kapcsolódó nemzeti értékek és érdekek sora húzódik meg, amelyek egyezés, illetve eltérés esetén is befolyásolhatják a platform hatékonyságát. A tanulmány a nemzeti kiberbiztonsági stratégiák bemutatásával, továbbá az EU- és NATO-irányelveknek való megfelelés áttekintésével, a tartalomelemzés módszereivel mutat rá azokra az analógiákra és eltérésekre, amelyek hatással lehetnek a kooperációra és a kitűzött célok elérésére.

A fejlett demokráciákban a digitális forradalom az élet minden területére kiterjed, ami egyúttal jelentős mértékű függőséget is generál. Napjainkban egyre kevésbé életképes az a társadalmi szereplő, amely nem rendelkezik elektronikus levélcímmel, nem használ bankszámlát és bankkártyát vagy éppen valamilyen helymeghatározó szolgáltatást. A digitális infrastruktúrák szerepe és jelentősége ma már vitathatatlan, rövid időn belül váltak megkérdőjelezhetetlen alkotóelemeivé az átlátható állami működésnek, a fejlődő gazdaságnak és a sikeres tudományos kutatásnak. Az információs társadalom a fejlődés motorjaként tekint az információ- és kommunikációtechnológiára (ICT[1]), miközben az önmagában is kihívást jelentő ráutaltság mellett a fejlődés és a penetráció mértéke egyre komolyabb fenyegetéseket hordoz magában.

Az ICT-rendszerekre épülő, összekapcsolt infrastruktúrák által alkotott globális virtuális tér a kibertér, amelynek rosszindulatú felhasználására számtalan lehetőség kínálkozik. A kibertérből érkező kihívások és fenyegetések folyamatos, dinamikus bővülése egyre szignifikánsabb veszélyt jelent a világ államai számára, mivel a nemzeti és nemzetközi szinten egyaránt megjelenő gazdasági károkon túl a kritikus infrastruktúrákat működte-

1 Az információ- és kommunikációtechnológia fogalma az 1980-as évek elején jelent meg, és az angolszász „information and communication technology" kifejezés alapján a rövidítése: ICT. A fogalom többféle módon is használatos, azonban jelen tanulmány keretein belül olyan átfogó kifejezésként szerepel, amely az adatok elektronikus gyűjtésére, tárolására, felhasználására és továbbítására szolgáló számítógépeket és más elektronikus rendszereket, valamint az ezekhez kapcsolódó szolgáltatásokat és alkalmazásokat jelöli.

tő ICT-rendszerek sebezhetősége miatt a létbiztonság is veszélybe kerülhet. Ugyanakkor a kibertérben elkövetett támadások és visszaélések olyan közvetlen veszélyt jelentenek a nemzeti és nemzetközi biztonságra, amivel szemben nehéz hatékony védelmet kiépíteni. Ennek oka igen egyszerű: az állami és nem állami szereplők által generált fenyegetések jellegüket tekintve sokrétűek, miközben erőteljes diverzifikáltságot mutatnak a motiváció, a kivitelezés és a célpontok tekintetében egyaránt. Tehát a szerteágazó kiberbiztonsági fenyegetések teljes spektrumát hatékonyan lefedő védelem megvalósítása még akkor is rendkívül bonyolult feladat, ha az állandó változás és fejlődés tényezőit – beleértve a rosszindulatú felhasználást is – kizárjuk.

Ebben a minden szempontból dinamikus közegben lenne szükség megfelelő, egységes válaszokra az állami és nem állami szereplők részéről egyaránt, azonban eltérő megközelítés jellemzi az állami, az üzleti és a magánszférát, ami hátráltathatja a kívánt egységes fellépés kialakítását. A különböző felfogásra és megközelítésre jó példa az Európai Hálózat- és Információbiztonsági Ügynökség *(European Network and Information Security Agency – ENISA)* 2012 decemberében kiadott, a nemzeti kiberbiztonsági stratégiákra vonatkozó gyakorlati útmutatója, amely felhívja a figyelmet, hogy gyakran még az olyan alapvető definíciók is eltérést mutatnak, mint a kiberbiztonság, de más kulcsfontosságú kifejezések használata is országonként eltér.[2]

Szövetségi ajánlások és irányelvek a nemzeti kiberbiztonsági stratégiákhoz

Európai Unió

Az Európai Unió 2004-ben döntött egy szakértői szervezet felállításáról, amely az információbiztonság területén végez specifikus technikai és tudományos feladatokat. Az ENISA[3] 2005 szeptemberében Krétán kezdte meg működését azzal a célkitűzéssel, hogy az EU-tagállamok és az üzleti szféra képességeit erősítsék a hálózat- és információbiztonsággal kapcsolatban felmerülő problémák megelőzése, kezelése és a rájuk történő reagálás terén. Az ENISA tanácsadó testületként is működik a Bizottság mellett, továbbá felkérés esetén részt vesz a jogszabályok korszerűsítését és kidolgozását megelőző technikai előkészítő munkában. A megfelelő szintű biztonság elérése érdekében az ügynökség segíti a tagállamokat, és fokozza az együttműködést az állami és a magánszektor szereplői között. Feladatai között szerepel többek között a kockázatok elemzéséhez szükséges információk gyűjtése, a tagállamok és a Bizottság tájékoztatása, a biztonsági problémák megelőzésére szolgáló közös módszerek kidolgozása, a tudatosság növeléséhez való hozzájárulás, a biztonsági szabványok kialakításának követése, továbbá saját következtetéseinek és iránymutatásainak megfogalmazása. A 10 éves fennállását ünneplő szervezet számos iránymuta-

2 Falessi, Nicole – Gavrila, Razvan – Klejnstrup, Maj Ritter – Moulinos, Konstantinos: National Cyber Security Strategies – Practical Guide on Development and Execution. *enisa.europa.eu,* 2012. 12. 19.

3 A szervezetet az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról című jogi aktus hívta életre, amelyet 2008-as és 2011-es módosítását követően 2013-ban helyezett hatályon kívül az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA).

tást, ajánlást, útmutatót és kézikönyvet adott ki, amelyek közül a nemzeti kiberbiztonsági stratégiák fejlesztésére és végrehajtására vonatkozó, 2012 decemberében elkészült gyakorlati útmutató[4] meghatározó a nemzeti kiberbiztonsági stratégiák nemzetközi beágyazottságának vizsgálatakor. Az ügynökség a létező kiberbiztonsági stratégiákat strukturális és tartalmi szempontból tanulmányozta annak érdekében, hogy meghatározhatók legyenek azok az erőfeszítések, amelyek hozzájárulnak a biztonság és rugalmasság növeléséhez. A gyakorlati útmutató az európai politikai és jogszabályi környezet ismertetését követően leír egy egyszerűsített életciklusmodellt a nemzeti kiberbiztonsági stratégiák fejlesztése, értékelése és fenntartása kapcsán. Rögzíti az egyes fázisok főbb elemeit, valamint az egyes lépésekhez kapcsolódó jó gyakorlatokat, ajánlásokat és politikákat. A kiberbiztonsági stratégiák fejlesztésére és végrehajtására vonatkozóan az alábbi 18 szempontot gyűjtötte össze az ENISA, amelyekre feltétlenül figyelmet kell fordítani:

– a vízió, az alkalmazási terület, a célok és prioritások meghatározása;
– nemzeti kockázatelemzési szemléletmód követése;
– a már létező politikák, jogszabályok és képességek áttekintése;
– átlátható kormányzati struktúra kialakítása;
– az érintett szereplők azonosítása és bevonása;
– megbízható információmegosztó mechanizmus létrehozása;
– nemzeti kiberbiztonsági veszélyhelyzeti tervek elkészítése;
– kiberbiztonsági gyakorlatok szervezése;
– alapvető biztonsági követelmények kialakítása;
– incidensek jelentését szolgáló mechanizmus létrehozása;
– felhasználói tudatosság;
– a K+F előmozdítása;
– képzési és oktatási programok erősítése;
– incidenskezelő képesség kialakítása;
– a kiberbűnözés elleni feladatok kijelölése;
– nemzetközi együttműködésben való részvétel;
– a köz- és magánszféra együttműködésének (PPP) kialakítása;
– egyensúly a biztonság és a magánszféra vonatkozásában.

Az ENISA szakemberei minden pontot részleteiben is kifejtenek, illetve minden esetben meghatározzák azokat a feladatokat és elemeket, amelyek a fenti szempontok érvényesüléséhez elengedhetetlenek. A nemzeti kiberbiztonsági stratégiák kiadását mindenkor egy értékelő mechanizmusnak kell követnie, ehhez pedig szükséges a kulcsfontosságú teljesítmény-indikátorok meghatározása. Az útmutató így összességében húsz olyan intézkedést és feladatot sorol fel a politikai döntéshozók számára, amelyek követése és végrehajtása révén a nemzeti kiberbiztonsági stratégia hatékony kormányzati eszközzé válik a kibertérből érkező kihívások kezelése és csökkentése terén.

4 Falessi, Nicole – Gavrila, Razvan et al.: i. m.

NATO

Az Észak-atlanti Szerződés Szervezetében a kiberbiztonsági kihívásokkal kapcsolatos tevékenységek egyik legfőbb letéteményese a szervezet keretein belül kialakított kibervédelmi központ, melynek terveit Észtország terjesztette elő, közvetlenül 2004-es csatlakozását követően. A NATO Kooperatív Kibervédelmi Kiválósági Központ *(NATO Cooperative Cyber Defence Centre of Excellence – NATO CCDCOE)* alapítására vonatkozó koncepciót 2006-ban hagyta jóvá a Szövetséges Erők Transzformációs Főparancsnoka, és 2007-ben indultak meg a potenciális szponzornemzetek közötti tárgyalások.[5] 2008 májusában Észtország, Németország, Olaszország, Lettország, Litvánia, Szlovákia és Spanyolország aláírta az alapításról szóló egyetértési megállapodást. A központ a kiberbiztonság területén oktatással, konzultációval, tanulságok gyűjtésével, kutatással és fejlesztéssel foglalkozik, amihez 2008. október 28-án kapott teljes akkreditációt az Észak-atlanti Tanácstól. Számos online és nyomtatott formában is elérhető kiadvány kötődik a központhoz, melyek főként a kiberkonfliktusok és kiberhadviselés etikai, illetve jogi kérdéseivel, a megfelelő kibervédelem kialakításával, technológiai témákkal, valamint a kiberbiztonsági stratégiák elkészítésével és fejlesztésével foglalkoznak. 2012 decemberében jelent meg az a nemzeti kiberbiztonsági keretrendszert bemutató kézikönyv,[6] amely részletes háttérinformációkat és elméleti kereteket biztosít a nemzeti kiberbiztonság különböző vetületeinek megértéséhez. A kézikönyv mellékletben közli a nemzeti kiberbiztonsági stratégiákra vonatkozó legfontosabb irányelvek listáját, melynek értelmében a nemzeti kiberbiztonsági stratégiáknak az alábbi elemekkel kell kezdődniük:

– a kibertér és a digitális társadalom jelentőségének igazolása;
– a fenyegetések és veszélyek meghatározása;
– a legfontosabb kifejezések és fogalmak definíciója;
– a célkitűzések deklarálása.

Az alkalmazási kör kapcsán a nemzeti kiberbiztonsági stratégiáknak ki kell térniük a kooperáció három dimenziójára: a kormányzati, a nemzeti és a nemzetközi együttműködésre. A stratégiák áttekintést kell, hogy nyújtsanak a kibertérre vonatkozó kormányzati mandátumokról. A legátfogóbb kiberbiztonsági stratégiák az alábbi területeken fogalmaznak meg politikai törekvéseket és stratégiai célokat, melyekhez szervezeteket is rendelnek:

– katonai kiberképességek;
– a kiberbűnözés elleni fellépés;
– hírszerzés és elhárítás;
– a kritikus infrastruktúra védelme és nemzeti kríziskezelés;
– kiberdiplomácia, valamint internetszabályozás és igazgatás.

A nemzeti kiberbiztonsági stratégiákra vonatkozó iránymutatás öt dilemmát azonosít, amelyekkel kapcsolatban egyértelmű és világos kompromisszumos döntések megfogalmazása elengedhetetlen. Kérdésként merül fel, hogy mi fontosabb egy kormány számára:

5 A Kooperatív Kibervédelmi Kiválósági Központ honlapja alapján a szervezetet jelenleg szponzoráló államok között van Csehország, Észtország, Franciaország, Németország, Magyarország, Olaszország, Lettország, Litvánia, Hollandia, Lengyelország, Szlovákia, Spanyolország, az Egyesült Királyság és az Amerikai Egyesült Államok.

6 Klimburg, Alexander (ed.): National Cyber Security Framework Manual. *ccdcoe.org,* 2012. december.

– a gazdaság serkentése vagy a nemzeti biztonság növelése;
– az infrastruktúra modernizálása vagy a kritikus infrastruktúra védelme;
– a közszféra vagy a magánszféra hangsúlyozása;
– az adatvédelem vagy az információk megosztása;
– a véleménynyilvánítás szabadsága vagy a politikai stabilitás?

Más stratégiákhoz mérve a nemzeti kiberbiztonsági stratégiák egyik sajátossága, hogy elkészítésük átláthatóbb, koordináltabb kormányzati folyamatot követel, mivel a kibertér nem köthető egyetlen minisztériumhoz vagy nemzethez sem. A stratégiaalkotás folyamatával kapcsolatban a központ – a teljesség igénye nélkül – az alábbi következtetésekre jutott:

– más nemzeti stratégiák másolása elutasítandó;
– a stratégiáknak kapcsolódniuk kell más nemzeti és nemzetközi stratégiákhoz;
– be kell építeni a szakpolitika frissítésére és felülvizsgálatára vonatkozó mechanizmust;
– felső- és középszintű tárcaközi koordinációs csoportokat kell biztosítani;
– szükséges a kritikus szolgáltatások és infrastruktúrák azonosítása;
– fontos a tudatosság kialakítása a politikai döntéshozókban;
– a szervezeti rugalmasságot ösztönözni kell;
– kerülendő a politikai vákuum kialakulása;
– elavult jogszabályok tervezése és elfogadása nem kívánatos;
– harcolni kell a digitális írástudatlanság ellen;
– a nemzetközi kötelezettségvállalásokat nem érdemes alá-, illetve túlbecsülni;
– az alapvető információbiztonsági követelmények integrációja szükséges.

A kézikönyv nem határoz meg egyetlen optimális keretrendszert a nemzeti kiberbiztonsági stratégiák kialakítására, mivel minden kormányzati rendszer egyedi, ezért a saját körülményekhez igazított szempontok, feltételek, hatáskörök és folyamatok érvényesülnek. Azonban a legkritikusabb kérdések meghatározhatók, és szükséges a velük kapcsolatos tudatosság növelése, valamint a megfelelő válaszok és bevált gyakorlatok terjesztése.

Nemzeti kiberbiztonsági stratégiák

Ausztria

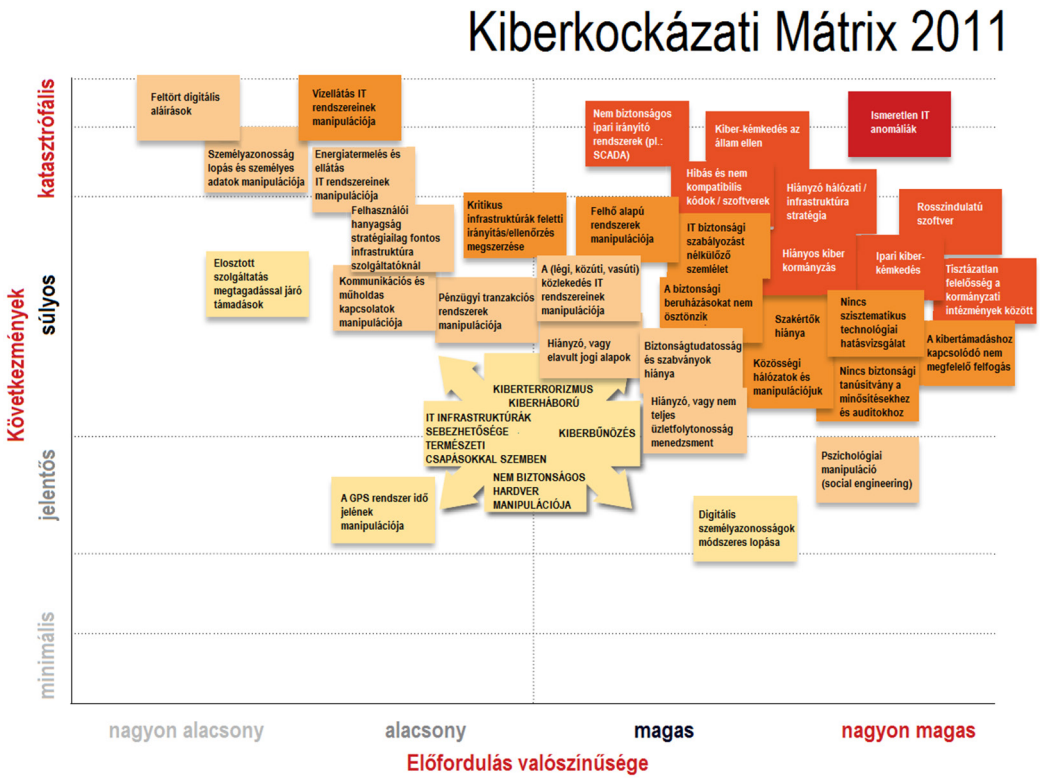
Az osztrák kiberbiztonsági stratégia[7] aktuális verziója 2013-ban jelent meg, terjedelme 23 oldal, amiből 14 oldalt tesz ki ténylegesen a stratégia, a továbbiak mellékleteket tartalmaznak (2011-es kiberkockázati mátrix, rövidítések listája, kiberbiztonsági szójegyzék). Alkotói 6 fejezetre osztották a stratégiát.

A bevezetés a digitális világgal kapcsolatos általános következtetésekkel és az internetpenetrációra vonatkozó információkkal kezdődik. A folytatás kitér a társadalmi fejlődés különböző dimenzióira, a kritikus infrastruktúrák érintettségére és azok megbízható, biztonságos működésének szükségességére. Az osztrák stratégia külön felhívja a figyelmet a kibertér és a virtuális tér szinonimaként történő használatára, majd az állami és nem állami szereplők által generált veszélyek említését követően leszögezi, hogy a kibertér fel-

7 Az Osztrák Kiberbiztonsági Stratégia kiadását az Ausztria Nemzeti ICT Biztonsági Stratégiája elnevezésű dokumentum előzte meg 2012 végén, amely kialakításában és terjedelmében is eltér a jelenlegi dokumentumtól.

használása gyakorlatilag végtelen lehetőséget jelent. A kiberbiztonság kifejezés magában foglalja a kibertér infrastruktúráinak, a kicserélt adatoknak, valamint a kiberteret használó minden személynek a biztonságát. A bevezető végül az osztrák nemzeti biztonsági stratégiát és a kritikusinfrastruktúra-védelmi programot emeli ki a kiberbiztonsági stratégia kialakítását meghatározó dokumentumokként.

A második fejezet a kibertér adta lehetőségekkel és kockázatokkal foglalkozik két alpontban. Az állami, gazdasági, tudományos és társadalmi tevékenységek szempontjából a kibertér fontos információs és kommunikációs közeg, amit konkrét használati adatok és statisztikák támasztanak alá. A kibertér a társadalmi interakciók, illetve a gazdaság és kereskedelem közegeként is értelmezhető, amit a több mint kétmilliárd internet-felhasználó, valamint az e-kereskedelem 500 milliárd dollárt meghaladó (2012) és két év alatt megduplázódó volumene igazol. A kibertér a politikai szerepvállalás és interakciók közege is, miközben felügyeleti, irányítási közegként szállítási, gazdasági, ipari és egészségügyi infrastruktúrák fenntartásában és működtetésében tölt be létfontosságú funkciókat. A rizikók és fenyegetések abból fakadnak, hogy a kibertér egyúttal a jogsértő, rosszindulatú felhasználás közege is, ahol az üzemzavaroktól a masszív támadásokig terjed az állami és nem állami szereplők nemzeti határokat is átlépő aktivitása. Az osztrák állam által érzékelt kockázatok és fenyegetések széles spektrumát a kiberkockázati mátrix mutatja be.



Kiberkockázati mátrix az osztrák kiberbiztonsági stratégiában

A stratégia harmadik fejezete Ausztria kiberbiztonsághoz fűződő alapelveit rögzíti. A dokumentum a kiberbiztonságra olyan átfogó kérdéskörként tekint, amivel az élet és a politika legtöbb területén számolni kell, ezért széles körű, integrált megközelítésre, aktív szerepvállalásra van szükség, szem előtt tartva a szolidaritás szellemét. A széleskörűség jegyében a külső és belső, valamint a civil és katonai biztonság aspektusai szorosan összefonódnak, míg az integráltság az állam, a versenyszféra, az akadémiai közeg és a civil társadalom közötti feladatmegosztást foglalja magában az alábbi tartalommal:

– politikai-stratégiai menedzsment,
– oktatás és képzés,
– kockázatelemzés,
– megelőzés és felkészültség,
– felismerés és válaszadás,
– következmények korlátozása és helyreállítás,
– kormányzati és nem kormányzati képességek és kapacitások fejlesztése.

A hangsúlyt a megelőzésre helyező proaktív kiberbiztonsági politika a kibertér globális természetéből fakadóan a szolidaritáson alapul. Ausztria, az Európai Unió és a nemzetek közösségének kiberbiztonsága szorosan összekapcsolódik, ezért intenzív kooperáción nyugvó összetartásra van szükség európai és nemzetközi szinten egyaránt. További univerzális alapelvek is alkalmazhatók (például bizalmasság, célhoz kötött felhasználás, adatvédelem stb.), de a minden esetben alkalmazandó alapelvek közé tartozik:

– a jogállamiság,
– az emberi jogok teljesülése,
– a szubszidiaritás,
– az önszabályozás és
– az arányosság elve.

A negyedik fejezet a stratégiai célkitűzések között határozza meg a biztonságos, rugalmas és megbízható kiberteret, amely az adatok integritásán túl képes garantálni azok hozzáférhetőségét, megbízhatóságát és bizalmasságát egyaránt. A biztonságos és rugalmas nemzeti ICT-infrastruktúrának az érintett minisztériumok közös erőfeszítése és a magánszektorral folytatott partnerség az alapja, amihez a kibertérben érvényesülő jog párosul. A tudatosság növelése érdekében Ausztria „kiberbiztonsági kultúrát" épít, egyúttal a digitális társadalom védelmének élharcosa és a nemzetközi kooperáció aktív szereplője kíván lenni. Az ország e-kormányzata biztonságos és folyamatos fejlesztés alatt áll, miközben az osztrák vállalkozások felelősek saját alkalmazásaik integritásáért és felhasználóik védelméért. A lakosság tudatosságának növelése szükséges, az állampolgároknak gondoskodniuk kell online tevékenységük megfelelő védelméről.

Az osztrák kiberbiztonsági stratégia ötödik, leginkább mélyreható fejezete 15 tevékenységi és intézkedési területet mutat be 7 csoportba rendezve.

Az első tevékenységi terület célja azon struktúrák és folyamatok meghatározása, amelyek az állami és magánszektor minden érintett szereplőjének bevonásával képesek biztosítani az általános koordinációt a politikai-stratégiai és operatív szinten egyaránt.

1. Ennek érdekében kormányzati kiberbiztonsági csoportot hoztak létre a szövetségi kancellária vezetésével, amely politikai-stratégiai szinten koordinálja az intézkedéseket, figyelemmel kíséri és támogatja a stratégia végrehajtását, továbbá éves kiber-

biztonsági beszámolót készít és tanácsot ad a szövetségi kormánynak. A stratégia kitér a csoport összetételére is.

2. Az operatív szintű koordináció kialakítása a meglévő struktúrákon alapul, amelyek platformként szolgálnak egy rendszeres, incidenshez kötött kiberbiztonsági összkép elkészítéséhez, ami áttekinti a kiberbiztonsági status quót a releváns információk gyűjtésével, összeállításával, értékelésével és továbbításával. A gazdasági szektor egyenrangú félként kerül bevonásra, az Operatív Koordinációs Struktúra kialakítása pedig műveleti végrehajtó szervként funkcionál válság esetén. A Belügyminisztérium által koordinált, valamint a Védelmi és Sport Minisztérium által támogatott struktúra állami oldalról a kormányzati számítógépes eseménykezelő csoportot (GovCERT), a katonai kiber-veszélyhelyzeti készenléti csoportot (MilCERT) és a Kiberbűnözési Kompetencia Központot (C 4) foglalja magába.[8] A struktúra második szintje további állami intézményeket, privát CERT-eket, valamint a gazdasági és tudományos szektor képviselőit tartalmazza.
3. Ausztriában a kiberdimenzióban zajló válságkezelés a Kormányzati Katasztrófa- és Polgári Védelemhez tartozik, ahol az állam és a kritikus infrastruktúrák üzemeltetői működnek együtt. A belbiztonság veszélybe kerülése esetén a koordinációt a Belügyminisztérium veszi át, míg a külső biztonság veszélyeztetettsége a Védelmi és Sport Minisztériumot helyezi vezető pozícióba. Szektorspecifikus és szektorokon átívelő kockázatelemzések alapján válságkezelési és üzemfolytonossági tervek készülnek, illetve rendszeresen frissítésre kerülnek, amiket kibergyakorlatok egészítenek ki.
4. A meglévő kiberstruktúrák erősítése kiterjed a GovCERT, a C 4 központ és a MilCERT fejlesztésére annak érdekében, hogy saját felelősségi területükön és hálózataikon biztosítani tudják a megfelelő képességeket és védelmet. Az Osztrák CERT Szövetség kibővítésre kerül, a CERT.at megerősítése pedig megkönnyíti az együttműködést, illetve újabb ágazati CERT-ek létrehozását.

A második tevékenységi terület célja meghatározni a kibertér állami és nem állami szereplőinek teendőit, kötelességeit és a rendelkezésükre álló erőforrásokat, valamint olyan keretrendszer kialakítása, ami az összes szereplő együttműködését lehetővé teszi.

5. Modern szabályozó keretrendszer kialakítása (átfogó elemzés készítése a kormány számára).
6. Minimumkövetelmények meghatározása („Osztrák Információbiztonsági Menedzsment Kézikönyv").
7. Éves kiberbiztonsági beszámoló készítése („Kiberbiztonság Ausztriában").

A harmadik tevékenységi terület célja az átláthatóság és a kooperáció növelése a kormányzat, a gazdaság és a társadalom között.

8 A kiberbiztonság operatív szintjén tevékenykedő, speciális szakértelemmel és eszközökkel rendelkező egységeket az angolszász terminológia Computer Emergency Response Team elnevezéssel illeti, amelynek rövidítése: CERT. A rövidítést a fenntartó kilétére utaló előtagok egészíthetik ki, így a Gov kormányzati, a Mil katonai kötődésre utal, míg a nem kormányzati és privát CERT-ek esetében gyakori a nemzetiségre vonatkozó kiegészítő tag, például CERT.at vagy Hun-CERT, de a fentiek kombinációja sem ritka (például GOV.CERT.PL). A CERT rövidítés egyre kiterjedtebb használata bizonyos esetekben az eredeti elnevezés torzulásához vezet (lásd osztrák katonai CERT: Military Cyber Emergency Readiness Team), azonban az alapvető tevékenység nem változik.

8. Az Osztrák Kiberbiztonsági Platform létrehozása elősegíti a közszféra és a magánszektor partnerségét. A platform tanácsokat ad és támogatja a Kiberbiztonsági Kormányzati Csoportot. A kritikus infrastruktúrák üzemeltetőinek bevonásával kiterjedt együttműködés valósulhat meg a partnerek között, ami a különböző szektorok szakértőinek cseréjét elősegítő program fejlesztését is magában foglalja.
9. A kis- és középvállalkozások (kkv-k) támogatása prioritási programok révén kívánja növelni az érintett szereplők tudatosságát, illetve a kkv-k igényeihez igazított információk online publikálásával és gyakorlatok szervezésével erősíti a szektor kiberbiztonságát.
10. Az érintett szereplők közötti kommunikáció optimalizálása érdekében kiberbiztonsági kommunikációs stratégia kidolgozása szükséges. Minden kormányzati weboldalt a Kiberbiztonsági Kormányzati Csoport által készített Kiber Kommunikációs Stratégia keretrendszerében hozzák létre és működtetik.

A negyedik tevékenységi terület a kritikus infrastruktúrák védelme terén hivatott pótolni és fokozni azokat a kiberbiztonsági intézkedéseket, amelyek az üzemeltetőket átfogó biztonsági architektúrák alkalmazására buzdítják.

11. A kritikus infrastruktúrák rugalmasságának tökéletesítése keretében az üzemeltetőket bevonják a kibertérben zajló nemzeti válságkezelési folyamatok mindegyikébe, a válságkommunikációt továbbfejlesztik, és kiberbiztonsági szabványokat határoznak meg. Kötelezővé válik a súlyos kiberbiztonsági incidensek jelentése, továbbá felülvizsgálják a kritikus infrastruktúrák védelmét szolgáló intézkedéseket, valamint a katasztrófa- és polgári védelem rendszerét.

Az ötödik tevékenységi terület a tudatosság növelésére és a képzések fejlesztésére vonatkozóan azt a célt tűzi ki, hogy minden célcsoport érzékenységét fokozza.

12. A kiberbiztonsági kultúra erősítése olyan tudatosságnövelő kezdeményezésekkel valósulhat meg, amelyek segítségével a különböző célcsoportok több, személyre szabott ismeretanyaghoz férnek hozzá. Ennek egyik platformjaként fog szolgálni az ICT Biztonsági Internet Portál, amelyet a Pénzügyminisztérium, a szövetségi kancellária és az A-SIT fog koordinálni, de a kiberbűnözési megelőzési programokat is továbbfejlesztik.
13. A kiberbiztonsághoz kötődő kompetenciák bevezetése szükséges az oktatás és képzés minden szintjén. Ehhez az ICT biztonsági ismereteket mélyebben kell integrálni a digitáliskompetencia-modellbe, és a pedagógusképzésre is ki kell terjeszteni. A közszféra számára is fontos a szakemberek képzése a biztonság növelése érdekében, ahogy a kritikus infrastruktúrák rendszeradminisztrátorai számára is biztosítani kell kiberbiztonsági képzéseket.

A kutatásra és fejlesztésre vonatkozó hatodik intézkedési terület célja a megfelelő technikai szakértelem biztosítása, amiben a legmodernebb kutatási és fejlesztési eredmények alkalmazása és az EU biztonsági kutatási programjaiban betöltött vezető szerep is meghatározó.

14. Az osztrák kiberbiztonsági kutatások megerősödéséhez a kiberbiztonságnak a kulcsfontosságú kutatási prioritások közé kell kerülnie nemzeti és európai uniós szinten egyaránt, továbbá Ausztriának vezető szerepet kell betöltenie a kutatási programokban.

A hetedik intézkedési terület a nemzetközi kooperációra vonatkozó célokat és lépéseket összegzi, aminek a kibertérrel kapcsolatban folytatott aktív osztrák külpolitika képezi az alapját a különböző EU-, ENSZ-, EBESZ-, Európa Tanács-, OECD- és NATO-partnerség keretében érvényre juttatott érdekek mentén.

15. Ausztria hatékony együttműködést kíván folytatni a kiberbiztonság terén Európában és világszerte, elsősorban a kiberbűnözés, az internet szabadsága és az emberi jogok védelme terén. Ehhez folytatni fogja a megkezdett munkát a NATO Partnerség a Békéért Program keretében, valamint az EBESZ bizalom- és biztonságerősítő intézkedésekre vonatkozó listájának összeállításában is aktív szerepet vállal. A kiberteret érintő külpolitikai erőfeszítéseket az Európai és Külügyminisztérium koordinálja.

A stratégia utolsó, hatodik fejezete a végrehajtásra vonatkozó rendelkezéseket tartalmazza. Ennek értelmében a Kiberbiztonsági Kormányzati Csoport a stratégia elfogadását követő három hónap során végrehajtási tervet készít, amelynek alapján koordinálja a végrehajtást. A kormányzati csoport tevékenységében érintett minisztériumok a saját működési területükre vonatkozó alsóbb szintű stratégiákat készítenek, illetve a kiberbiztonsági stratégia rájuk vonatkozó feladatainak végrehajtásáról kétévente beszámolót készítenek a szövetségi kormány részére. A végrehajtási beszámolók elkészítésének szorosan kapcsolódnia kell a kiberbiztonsági stratégia felülvizsgálatához.

Csehország

A vizsgált kiberbiztonsági stratégiák közül a 2011-ben kiadott cseh dokumentum[9] a második legrövidebb, összesen 8 oldal a terjedelme, amiből a 3 részre osztott konkrét stratégia 6 oldalt tesz ki.

A bevezetés alapján a cseh kiberbiztonsági stratégia olyan dokumentum, amely a kormányzati és nem kormányzati szereplők tudatosságnövelő erőfeszítéseiből ered, és aminek célja emelni az állami szervezetek, a kritikus infrastruktúrák, a versenyszféra és az állampolgárok kibernetikai[10] biztonságát. A cseh nemzeti biztonsági stratégia nyomán kialakított kiberbiztonsági stratégia az alapja a kibernetikai biztonság érdekében végzett jogalkotási folyamatnak, az ICT-rendszerekhez kapcsolódó politika alakításának, a szabványok és szabályok bevezetésének, az üzemeltetési és fenntartási terveknek, ajánlásoknak és más eszközöknek.

A stratégia alapvetésekkel foglalkozó első részében külön kiemelésre kerül a Stuxnet[11] vírus, amelynek létezése és a vele kapcsolatos tapasztalatok bizonyítják, hogy a létfontosságú ipari létesítmények nem immunisak a kibernetikai támadásokkal szemben, ezért az állami funkciók fenntartásához elengedhetetlen a kiberbiztonság szavatolása. Az információ- és kommunikációtechnológia modern társadalomra és gazdaságra gyakorolt ha-

9 A cseh kiberbiztonsági stratégiának két változata érhető el. Az egyik a Cseh Köztársaság Kiberbiztonsági Stratégiája a 2011–2015 közötti időszakra, amely többek között az ENISA honlapjáról is letölthető. A NATO CCDCOE honlapján elérhető dokumentum címe a Cseh Köztársaság Stratégiája a Kibernetikai Biztonság Terén 2012–2015. A cseh kormányzati CERT honlapján az utóbbi dokumentum érhető el, ezért a tanulmány ezt a stratégiát tekinti aktuálisnak.

10 A cseh kiberbiztonsági stratégia a „cyber" és „cybernetic" kifejezéseket párhuzamosan használja.

11 Az iráni nukleáris létesítmények ellen készített programra vonatkozóan lásd: Berzsenyi Dániel – Szentgáli Gergely: STUXNET: a virtuális háború hajnala. *biztonsagpolitika.hu,* 2010. 10. 07.

tásáról a cseh dokumentum azt írja, hogy a jólét és fenntartható gazdasági fejlődés egyik alapvető feltétele. Csehországban a kibertérhez kapcsolódó direkt és indirekt tevékenység stabilan nő, ezért szeretne azon fejlett országok közé tartozni, ahol a hálózatok és online szolgáltatások nemcsak biztonságosak, de rugalmasak is. Ehhez a társadalom egészének összefogása szükséges.

Az ICT-rendszerek és a tőlük függő társadalmak sebezhetők, amit fokoz a folyamatos technológiai fejlődés és a függőség mértékének növekedése. A támadásokat motiválhatja bűnözés, gazdasági haszon szerzése vagy terrorizmus, de a társadalom destabilizálására is irányulhatnak, miközben a végrehajtás szempontjából egyre összetettebbek és kifinomultabbak. A veszélyek természete, motivációja és a célpontok is állandó változást mutatnak, továbbá a támadások állami, kulturális és jogi határokat kereszteznek, aminek következtében szoros nemzetközi együttműködésre van szükség.

A stratégia alkotói a kiberbiztonság alapelveivel foglalkozó második rész elején leszögezik, hogy a kibernetikai biztonságba történő befektetés egyet jelent a jövőbe és a gazdasági növekedésbe történő befektetéssel. A kiberbiztonság információmegosztáson és koordinált tevékenységeken alapuló komplex erőfeszítések összessége katonai és civil, állami és nem állami, valamint nemzeti és nemzetközi relációban. A kibertérből érkező kihívások nem tekinthetők egyetlen területhez köthető elszigetelt problémának, ezért a kritikus infrastruktúrák működésének fenntartása, a hatékony reagálás és a digitális világ jogi védelme érdekében a társadalom egészére nézve kell elsődleges prioritásként kezelni a kiberbiztonságot.

A társadalom minden részének együttműködése és koordinált erőfeszítések mentén lehet csak növelni a kibernetikai biztonságot, és elkerülni a törekvések széttagolódását, a duplikáltságot és a kiadások növekedését. Mivel az ICT-termékek és szolgáltatások jelentős része a magánszektorból érkezik, a sikeres együttműködés elengedhetetlen feltétele a kölcsönös bizalom és információmegosztás.

Az egyéni felelősség jegyében az állam alapvető érdeke olyan ICT-biztonsági szabályozás kialakítása, amelyet a kibertér minden felhasználója elfogad és átvesz a saját rendszerének belső és külső támadásokkal szembeni védelme érdekében.

A kiberbiztonságért felelős állami szervezet a cseh Nemzeti Biztonsági Felügyelet *(National Security Authority – NSA),*[12] a tárcaközi koordinációban pedig a Kibernetikai Biztonsági Tanácsnak van kulcsszerepe. A tanács területspecifikus munkacsoportokban végzi koordinációs, tanácsadó és tervező tevékenységét.

Mivel a kiberbiztonsági törekvések csak nemzetközi beágyazottság esetén lehetnek sikeresek, a Cseh Köztársaság aktívan támogatja az EU és a NATO szerveit a nemzetközi politikák, szabványok és normák kialakításában, melyeknek nemzeti szinten történő beépítésére is nagy hangsúlyt fektet.

Az elfogadott intézkedések használhatóságát és alkalmazhatóságát kockázatelemzések biztosítják. Az intézkedéseknek az alapvető jogok tiszteletben tartásával párhuzamosan kell garantálniuk a megfelelő szintű biztonságot.

12 A cseh Nemzeti Biztonsági Felügyelet feladatköre és tevékenysége erőteljesen hasonlít a magyar Nemzeti Biztonsági Felügyelet hatáskörébe tartozó területekre.

A stratégia harmadik és egyben legfontosabb része a stratégiai célokat és a hozzájuk rendelt intézkedéseket ismerteti, amelyek alapul szolgálnak a szükséges lépéseket részleteiben tartalmazó akciótervhez.

A jogszabályi keretrendszerre vonatkozó tervet a biztonsági felügyelet készíti el, amelyben a Nemzeti Kiberbiztonsági Központ felelősségi területei is meghatározásra kerülnek. Az e-kereskedelemre és elektronikus tranzakciókra vonatkozó nemzetközi jogszabályokat, egyezményeket, trendeket és ajánlásokat rendszeres értékelést követően beépítik a cseh szabályozásba.

A Nemzeti Kibernetikai Biztonsági Központ *(National Centre for Cybernetic Security – NCCS)* a biztonsági felügyelet szervezetén belül valósul meg, és a központ részeként jön létre a kormányzati CERT. Az így létrejövő hierarchiában a központ feladata az állami szervekkel, az akadémiai intézményekkel és a gazdasági szereplőkkel való aktív együttműködés, az információk megosztása, a fenyegetések és incidensek elemzése, valamint a védelmi tevékenységekre vonatkozó ajánlások megfogalmazása. A kockázatkezelési folyamat keretében rendszeres teszteket és kibervédelmi gyakorlatokat kell folytatni.

A kritikus infrastruktúrák védelme az egyik legfontosabb prioritás, elengedhetetlen az információk kölcsönös megosztása a közszféra és magánszféra szereplői között. Alapos felmérések segítségével kell meghatározni, hogy mely területeken valósul meg maradéktalanul a biztonsági intézkedések végrehajtása, és hol van szükség további erőfeszítésekre.

A közigazgatási ICT-rendszerek kibernetikai biztonságának növelése érdekében a biztonsági szabályok és szabványok kialakítását és alkalmazását kötelezővé kell tenni és rendszeres vizsgálatokkal kell ellenőrizni. A közszféra ICT-rendszereinek felhasználóit a GovCERT.cz portálon keresztül az NCCS rendszeresen tájékoztatja az aktuális kockázatokról, valamint a szükséges biztonsági intézkedésekről és eljárásokról.

A kiberbűnözés elleni harc eredményessége érdekében az NCCS is fellép a kiberbűnözés ellen, és együttműködik a bűnüldöző szervekkel a kibernetikai támadásokkal szembeni intézkedések fejlesztése során.

A kibernetikai biztonsági tevékenységek európai szintű koordinációjában a biztonsági felügyelet döntő szerepet játszik, s az együttműködést bővíteni kell a jövőbeni tevékenységek és az újonnan felállított szervezetek irányába.

A közigazgatási ICT-rendszereknek megbízhatóaknak kell lenniük, ezért a védelmükben folyó kutatási és fejlesztési projekteket támogatni kell, továbbá technikai és alkalmazási szinten meg kell felelni a nemzetközi szabványoknak.

A kibernetikai biztonsággal kapcsolatos tudatosság növelése nem csak technikai szinten szükséges. A képzett, jól informált személyi állomány hiánya és a továbbképzés elmaradása növeli a sérülékenységet és a károkat. Az állampolgárok tudatosságának növeléséhez szükséges a médiával való együttműködés, továbbá az oktatás és képzés minden szintjén be kell építeni a kibernetikai biztonsággal kapcsolatos témákat, a tananyagot pedig rendszeresen felül kell vizsgálni és modernizálni.

A kibernetikai támadásokkal szemben megfogalmazott válaszok komplex intézkedési mechanizmust takarnak, amiket a stratégia egységes keretrendszerbe foglal. Együttműködést, aktív politikai tevékenységet és állandó felülvizsgálatot ír elő annak érdekében, hogy a Cseh Köztársaság biztosítani tudja az ICT-rendszerek megbízhatóságát a napi szintű felhasználás során.

Lengyelország

2013-ban jelent meg a lengyel kibertér védelméről szóló stratégiai dokumentum,[13] összesen 25 oldal terjedelemben, melyből 20 oldalt tesznek ki a politikai célkitűzések és a megvalósulásukhoz szükséges intézkedések. A dokumentum alapjául a kormányzat 2009–2011 közötti kibertérvédelmi programja, valamint a kormányzati domain (gov.pl) biztonsági helyzetéről készülő időszaki jelentések szolgáltak.

A hat részre tagolt stratégia elsőként a kibertérvédelmi politika hipotéziseit és a végrehajtás előfeltételeit tekinti át. Az alkotók jelzik, hogy a dokumentum az államtól a magánszemélyekig mindenkire kiterjed, illetve elhelyezik a lengyel stratégiai dokumentumok rendszerében. Nem terjed ki viszont a minősített ICT-rendszerekre és a velük kapcsolatos kiberbiztonsági feladatokra, mivel azok külön szabályozás alá esnek, és önálló védelmi mechanizmusaik vannak. Ezt követi egy rövid, a dokumentumban használt kifejezések és rövidítések definícióit tartalmazó szakasz. A stratégia célját világosan és tömören fogalmazzák meg: az állami kiberbiztonság elfogadható szintű biztosítása. A stratégiai célkitűzéseket szakértők által végzett kockázatelemzések nyomán határozzák meg, és hat további stratégia céljaira hivatkoznak, amelyekkel a kiberbiztonsági célkitűzések összhangban vannak. A stratégia hét specifikus célkitűzést nevesít:

– az állami ICT-infrastruktúrák biztonsági szintjének növelése;
– a kibertérből érkező fenyegetésekkel szembeni megelőző és harci kapacitás javítása;
– a kiberbiztonságért felelős entitások meghatározása;
– koherens kiberbiztonsági menedzsmentrendszer kialakítása;
– fenntartható koordinációs és információ-megosztó rendszer létrehozása;
– a tudatosság növelése.

A stratégia címzettjei a központi kormányzati szervek, a kormányzati háttérintézmények, a helyi, illetve járási igazgatás és az önkormányzatok szervei, valamint a minisztériumok felett álló Kormányzati Biztonsági Központ *(Government Centre for Security)*. A dokumentum ajánlásként funkcionál például a lengyel köztársasági elnök és hivatala, a lengyel parlament vagy a lengyel nemzeti bank számára, és iránymutatás a kibertér minden felhasználójának. A stratégia végrehajtásáért felelős csapatot a miniszterelnök jelöli ki, míg az elsődleges operatív szervezet a Kormányzati Számítógépes Biztonsági Incidenskezelő Csoport *(Governmental Computer Incident Response Team – CERT.GOV.PL),*[14] amely a közigazgatáson túl a civil területekért is felelős. A katonai infrastruktúra megóvását a védelmi minisztérium keretein belül létrejött, az ICT-hálózatok és -szolgáltatások biztonságért felelős központ végzi *(Departmental Centre for Security Management of ICT Networks and Services)*. A stratégia és felülvizsgálata kapcsán széles körű társadalmi egyeztetést kell folytatni.

A stratégia második része a kibertérben uralkodó állapotokkal és az onnan származó problémákkal foglalkozik. Az államnak kötelezettségei ellátásához szüksége van a kibertérre, ezért annak üzembiztos működéséről és védelméről is az államnak kell gondoskod-

13 A Lengyel Köztársaság kibertérvédelmi politikáját a közigazgatásért és digitalizálásért felelős minisztérium, valamint a belbiztonsági ügynökség készítette.

14 A lengyel CERT elnevezése, a „Computer Incident Response Team" a „CSIRT" rövidítést indokolná, amely szintén használatos a nemzetközi terminológiában. A CERT és CSIRT rövidítéseket párhuzamosan használják, lényegében azonos feladatokat és tevékenységet ellátó operatív szervezeteket jelölnek. Az ENISA szerint a CSIRT a precízebb kifejezés.

nia. A kiberteret alkotó ICT-rendszerek folyamatos működésének biztosításához minimális biztonsági követelmények meghatározása szükséges. A stratégia nyomán megvalósuló intézkedések között fontos szerepet kap a lengyel kibertérrel kapcsolatos kockázatelemzés, a segítségével azonosíthatók a források, a különböző alrendszerek és funkciók, valamint a más rendszerektől való függés.

A legfontosabb intézkedéseket a harmadik rész mutatja be prioritási sorrendben. Az elfogadható biztonsági szint elérésének kulcseleme, hogy évente január 31-ig minden kormányzati egység jelentést készít az elvégzett kockázatelemzésről, aminek a tartalmára is kitér a stratégia. Másodikként a kormányzati portálok biztonságát kell szavatolni. Ennek keretében minden közigazgatási, illetve kormányzati szervezet egyedileg elemzi a felügyelete alá tartozó portálokkal összefüggő kockázatokat és biztosítja az elvárt biztonsági szintnek való megfelelést. Az internetes portálokat üzemeltető szervezetek számára a minimális biztonsági követelményeket, elvárásokat és releváns ajánlásokat egy kormányzati munkacsoport a kormányzati CERT-központtal közösen dolgozza ki. Nem maradhat el a jogi környezet gyors és hatékony átalakítása annak érdekében, hogy a stratégiában megfogalmazott célkitűzések megvalósulhassanak, például a kiberbiztonsági képzések terén. Az eljárási és szervezeti intézkedések célja a lengyel kibertér működésének optimalizálása a legjobb gyakorlatok és szabványok bevezetésével. A stratégia ezen a ponton kitér a lengyel kibertér kormányzati menedzsmentjének egyes szervezeti elemeire (munkacsoport, CERT stb.), a közfeladatot ellátó intézmények informatikai követelményeit megfogalmazó törvényre, illetve a kibertér biztonságáért felelős vezetők és szakértők feladataira. A kiberbiztonsági oktatás, képzés és a tudatosság növelésével kapcsolatban a stratégia kiemeli, hogy az ICT-biztonsággal kapcsolatos kérdések és témák a felsőoktatás állandó elemeivé kell, hogy váljanak, és jelentős hangsúlyt kell fektetni a közigazgatásban dolgozó irodai állomány pozícióhoz, illetve kockázati szinthez kötött képzésére. A tudatosság növelésének érdekében célcsoporthoz igazított multidimenzionális társadalmi kampányt kell folytatni, hangsúlyozva a megelőzés fontosságát. A gyermekek és fiatalok körében ki kell alakítani azokat a szokásokat, amelyek védelmet nyújtanak a kibertér veszélyeivel szemben. Ezeket az ismereteket első helyen kell átadni az oktatás összes szintjén, de képezni kell a szülőket és a tanárokat is. A stratégiában foglalt intézkedések utolsó lépcsőjében a technikai dimenzió kerül előtérbe, ahol alapvető fontossággal bír a kutatási tevékenységek támogatása, a kormányzati eseménykezelő központok számának bővítése, egy korai előrejelző rendszer kifejlesztése (ARAKIS-GOV) és a megelőzést szolgáló megoldások fenntartása. Technikai oldalról további jelentőséggel bír a biztonsági szint tesztelése, a biztonsági csapatok fejlesztése és belső információs oldalak működtetése.

A dokumentum negyedik része a végrehajtás és a hozzá kapcsolódó mechanizmus részleteit mutatja be. A koordináció három szinten valósul meg, melynek csúcsát a miniszteri szint jelenti, ezt követi a CERT-ek operatív szintje, végül a harmadik szinten az egyedi ICT-rendszerekért felelős adminisztrátorok állnak. A lengyel nemzeti reagáló képesség működésének egyik alapja az információk megosztása, amihez kiforrott jogszabályi környezet és az üzleti szférával folytatott szorosabb kooperáció szükséges. Ennek a területnek az ICT-üzemeltetőkön és -szolgáltatókon kívül a másik fontos pillérét a hardver- és szoftvergyártók jelentik.

Az ötödik rész a finanszírozásról szól, aminek értelmében a hatálybalépés évében a központi büdzséből nem biztosítanak pluszforrásokat az intézkedések végrehajtásához, mivel a kitűzött célok részlegesen teljesülnek a közigazgatás jelenlegi szervezeti egységeiben. A jövőre vonatkozóan minden egyes szervezeti egységnek be kell mutatnia a kiberbiztonságra fordítandó becsült költségeit, hogy azzal a következő évi költségvetés tervezésekor számolni lehessen.

A stratégia utolsó része a hatékonyság felmérését részletezi. Meghatározza azokat az értékelési kritériumokat, amelyekhez a stratégia alkotói konkrét intézkedési példákkal is szolgálnak. A várható hatások és eredmények között szerepel a biztonság magasabb szinten történő garantálása, a támadások hatékonyságának csökkentése, valamint a szereplők kompetenciájának és tudatosságának növekedése. A stratégia részét képezik azok a folyamatok, amik a végrehajtást és a hatékonyságot értékelik. A lefektetett szabályok veszélyeztetése az információs társadalomból való kirekesztődéssel járhat, illetve akadályokat emelhet az információkhoz történő hozzáféréssel kapcsolatban.

Magyarország

A 2013-ban kiadásra került első kiberbiztonsági stratégia[15] a legkurtább a CECSP-országok hasonló témájú stratégiai dokumentumai között. Az alig 4 oldalas stratégia 11 pontban, 4 csoportba rendezve összegzi a magyar kiberbiztonsági percepciót, a célokat és a végrehajtást.

A stratégia készítői célként fogalmazzák meg a magyar kiberbiztonsági értékek és érdekek számbavételét, a kibertér biztonsági környezetének elemzését, valamint a nemzeti célok, a stratégiai irányok, feladatok és a kormányzati eszközök meghatározását. A nemzeti érdekek érvényesítését szolgáló célkitűzések mellé további két célt rendel a dokumentum. Egyrészt a szabad és biztonságos kibertér kialakítását, másrészt a nemzeti szuverenitás védelmét. Az egyéb célok között szerepel:

– a nemzetgazdaság és a társadalom szabad tevékenységének védelme és biztonságának garantálása;
– az új technológiai innovációk biztonságos adaptálása;
– a nemzetközi együttműködések kialakítása.

A stratégia elsődleges célként hivatkozik a fenyegetések és kockázatok megelőzésen alapuló kezelésére, illetve a kormányzati koordináció és eszköztár erősítésére.

A dokumentum nemzetközi beágyazottságát a vonatkozó EU- és NATO-stratégiáknak és elveknek való megfelelés biztosítja, míg nemzeti szinten az Alaptörvényben, illetve a Nemzeti Biztonsági Stratégiában foglaltak kiberbiztonsági leképezése valósul meg. A stratégia a nemzeti adatvagyon és a kapcsolódó létfontosságú rendszerek és létesítmények kiberbiztonságának dokumentuma.

Az első csoportba sorolt három pont Magyarország kiberbiztonsági környezetét hivatott bemutatni. A kibertér magyar értelmezésben globális, decentralizált, növekedő elektronikus információs rendszereket és a rajtuk keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatokat jelent. A fenyegetések jellege és a tenden-

15 A Magyarország Nemzeti Kiberbiztonsági Stratégiája című dokumentum a 1139/2013. (III. 21.) kormányhatározat mellékleteként jelent meg.

ciák kapcsán fontos a növekedés, a diverzifikáltság és a szereplők heterogenitása, valamint az információs hadviselés mint a hadviselés új formája. A stratégia kiemeli, hogy az információs és hírközlő rendszerek üzembiztonságának szabályozása nem kellően rendezett, ami önmagában is kockázatot jelent, amit fokoz az új technológiák dinamikus megjelenése. A stratégia egyik fő célja a döntéshozó szakmai és politikai figyelem, valamint a problémák kezelését biztosító képesség kialakítása. A környezetértékelés utolsó pontjaként kiberbiztonságon az alkotók politikai, jogi, gazdasági, oktatási, tudatosságnövelési és technológiai eszközök folyamatos és tervszerű alkalmazását értik, amelyek hozzájárulnak a kockázatok elfogadható szintjének biztosításához.

A dokumentum második csoportjába tartozó pontok Magyarország kiberbiztonsági értékrendjével, jövőképével és céljaival foglalkoznak. Alapvető érdek az állami szuverenitás védelme, valamint a kibertér demokratikus jogállami és biztonságos működése, ami a kormányzati, a tudományos, a gazdasági és a civil szféra szoros kooperációjával valósulhat meg. Magyarország célja az azonos értékrendek mentén megvalósuló együttműködés kialakítása más államokkal és nemzetközi szervezetekkel (EU, NATO, EBESZ, ENSZ, ET). A magyar biztonságpercepció alapján a kibertérből érkező támadások elérhetnek olyan szintet, ami szövetségesi lépéseket von maga után, ezért fontos, hogy a kiberbiztonság bekerült a NATO 5. cikkely szerinti kollektív védelem körébe. A magyar kibertérnek biztonságos és megbízható környezetként kell funkcionálnia az egyének és közösségek szabad kommunikációján keresztül megvalósuló társadalmi fejlődéshez, a hatékony és innovatív üzleti megoldások kialakításához, a jövő generációjának tanulásához, valamint az e-közigazgatás fejlesztéséhez. Mindezek érdekében megvalósítandó célnak tekinti:

– a hatékony megelőzési, észlelési, kezelési, válaszadási és helyreállítási képességek kialakítását;
– a létfontosságú rendszerek és létesítmények üzembiztos működését;
– az informatikai, hírközlési termékek és szolgáltatások nemzetközi színvonalának biztosítását;
– az oktatás, a képzés, valamint a kutatás és fejlesztés terén a legjobb nemzetközi gyakorlatok alkalmazását;
– a biztonságos kibertér kialakítása során a legjobb nemzetközi gyakorlatok alkalmazását.

A stratégia harmadik csoportjában található pontok azokat a feladatokat határozzák meg, amelyek a célok eléréshez szükségesek. Bár a kiberbiztonság helyzete szilárd, a kockázatok és fenyegetések nemzeti stratégiai kihívást jelentenek. A rendelkezésre álló eszközök és a feladatellátásban érintett területek:

– kormányzati koordináció (a Miniszterelnökség keretében összkormányzati koordináció);
– együttműködés (információcsere és az operatív együttműködés javítása);
– szakosított intézmények (specifikus szakértelemmel és hatáskörrel a CERT-ek);
– szabályozás (együttműködés a civil, gazdasági és tudományos területtel);
– nemzetközi együttműködés (aktív szerepvállalás erősítése);
– tudatosság (az élenjáró szerep fenntartása a szakmai fórumok szervezésében);
– oktatás, kutatás-fejlesztés (a kiberbiztonság integrálása az oktatásba és képzésbe);
– gyermekvédelem (minőségi online tartalom és biztonságos környezet);
– a gazdasági szereplők motivációja (közbeszerzések kiberbiztonsági követelményei).

A stratégia utolsó csoportjába kerültek azok a végrehajtáshoz rendelkezésre álló, illetve megerősítendő kormányzati eszközök, amelyek a stratégia céljainak eléréséhez szükségesek. Ezeknek a kompetenciáknak és potenciális erőforrásoknak jelentős részével már rendelkezik Magyarország, azonban ezek hatékonyabb felhasználásához szükséges egy koherens, állami és nem állami együttműködési rendszer kialakítása és fenntartása.

Szlovákia

Szlovákia Nemzeti Információbiztonsági Stratégiája[16] 2008-ban jelent meg 21 oldal terjedelemben. A dokumentum bevezető része kitér az információbiztonság alapvető szintjének meghatározására, illetve kilátásba helyezi a továbbfejlesztés lehetőségének biztosítását. A stratégia rögzíti a kiindulási pontokat, megállapítja a felelősségi területeket és kompetenciákat, továbbá célokat, prioritásokat és az ezek megvalósításához, eléréséhez szükséges lépéseket jelöl ki. A stratégia egyedi feladatokat is tartalmaz, ugyanakkor a szlovák Nemzeti Biztonsági Felügyelet *(National Security Authority – NSA)* hatáskörébe tartozó minősített információk nem képezik a stratégia részét. Az információk szivárgása és jogosulatlan felhasználása, az adatok integritásának és a személyes adatok védelmének veszélyeztetése, az ICT-rendszerek sérülése és rosszindulatú felhasználása olyan veszélyek, amelyeket el kell kerülni annak érdekében, hogy az ország megőrizze versenyképességét és hitelességét.

A második rész a dokumentumban foglaltak jelentőségét fejti ki részletesen. Elsőként az információbiztonság fontosságát hangsúlyozza, majd az összekapcsolt ICT-rendszerek által alkotott információs és kommunikációs infrastruktúrák (ICI) használatával megvalósuló, szerteágazó virtuális tevékenységet írja le. A közlekedéstől az oktatáson át a védelemig terjedő tevékenységek elengedhetetlenek az állam működésének fenntartásához, ezért biztonságuk szavatolása a működő társadalom alapfeltétele. Az állami ICI és a benne tárolt, küldött, feldolgozott információk együttesen alkotják a digitális teret, amelyet a szlovák stratégia a kibertér kifejezés szinonimájaként használ. Az információbiztonság olyan multilaterális terület, ahol az ICT-rendszerek tulajdonosai, üzemeltetői és felhasználói egyaránt érintettek. Az információbiztonság sajátossága, hogy a tudományos és technológiai fejlődésből eredő probléma, ami mára globális társadalmi kérdéssé alakult át, ezért a kezelése csak a nemzetközi perspektívák és szervezetek bevonásával lehetséges. A stratégia készítői a jogszabályi kapcsolódás bemutatásának keretében tételesen felsorolják a fontosabb kapcsolódó stratégiákat, törvényeket és rendeleteket, valamint kitérnek arra, hogy a nemzetközi egyezményekből és európai uniós szabályozásból mik kerültek átültetésre nemzeti szinten. Az információbiztonságra és a kapcsolódó kompetenciákra vonatkozó részből kiderül, hogy korábban nem létezett átfogó információbiztonsági stratégia Szlovákiában. A dokumentum az alábbi területi felosztást alkalmazva azonosítja a felelős szervezeteket:

– információs társadalom és közigazgatási információbiztonság (Információbiztonsági Bizottság);

16 A Szlovák Köztársaság Nemzeti Információbiztonsági Stratégiája a legrégebb óta érvényben levő kiberbiztonsági dokumentum a CECSP-országok között.

– minősített információk védelme (Nemzeti Biztonsági Felügyelet – NSA);
– személyes adatok védelme (Személyes Adatok Védelmének Irodája);[17]
– elektronikus kereskedelem (Gazdasági Minisztérium);
– számítógépes bűnözés (Igazságügyi Minisztérium, Belügyminisztérium);
– szerzői jog (Kulturális Minisztérium);
– szabványok és normák (Szlovák Szabványügyi Intézet, Pénzügyminisztérium, NSA);[18]
– nemzetközi együttműködés (ENISA, FESA, OECD, NATO stb.).

A minősített információkkal kapcsolatban fontos megjegyezni, hogy a hagyományos törvényhozási terminológiával szemben a stratégia nemcsak a bizalmasság kritériumát jelöli így, hanem azt a komplex védelmet is, ami biztosítja az integritást, a hitelességet és a hozzáférhetőséget. A kiberbiztonsággal foglalkozó nemzetközi szervezetek jelentős részében Szlovákia csak megfigyelő volt a stratégia készítésekor.

A harmadik rész számos pontra bontva fejti ki a stratégia részleteit, amely nemcsak a szlovák és nemzetközi dokumentumokra épít: a készítéskor felhasználták a legfejlettebb információs társadalmak, így az Egyesült Államok, az Egyesült Királyság, Németország, Finnország és Japán vonatkozó dokumentumait is. A stratégiát három szintre bontották:

– első szint: hosszú távú stratégiai célok;
– második szint: stratégiai prioritások, a stratégiai célok lebontása speciális területekre;
– harmadik szint: legfontosabb problémák és a kapcsolódó kulcsfeladatok.

Az Európai Unió stratégiájában foglaltakkal összhangban Szlovákia az alábbi hosszú távú célokat tűzte ki az információbiztonság szükséges szintjének megteremtése és fenntartása érdekében:

– megelőzés (incidensekkel szembeni védelmi, kiküszöbölési képesség);
– készenlét (incidensekre való reagálás és a hatások csökkentésének képessége);
– fenntarthatóság (megvalósítani, fenntartani, fejleszteni a szlovák kompetenciát).

A célok elérése kapcsán az állam alapvető szerepet játszik a jogi környezet megteremtésével, valamint a szervezeti, dologi és pénzügyi források biztosításával.

A stratégiai célok teljesítése közben számos problémával (kompetencia, technikai, szervezeti és finanszírozási kérdések stb.) szembesül a szlovák társadalom, ezért a dokumentum hét alapvető stratégiai prioritást definiál:

– az emberi jogok és szabadságok védelme a nemzeti információs infrastruktúrában;
– a tudatosság és kompetencia fejlesztése az információbiztonság terén;
– a biztonságos környezet megteremtése;
– az információbiztonsági menedzsment tökéletesítése;
– az állami ICI, illetve a kritikus infrastruktúrákat támogató ICI megfelelő védelme;
– nemzeti és nemzetközi kooperáció;
– a nemzeti kompetencia erősítése.

Az emberi jogok és szabadságok védelmével kapcsolatban az alkotók leszögezik, hogy a társadalom által kifejlesztett hagyományos szabályozók és védelmi mechanizmusok csak nagyon nehezen ültethetők át a digitális térbe, ezért új, megfelelően alkalmazható jogi keretrendszerre van szükség. A tudatosság és kompetencia növelése a nem megfe-

17 Office for Personal Data Protection.
18 Slovak Standards Institute – SUTN.

lelő szakértelem kiküszöböléséhez szükséges, aminek érdekében bővíteni kell az általános társadalmi ismereteket, erősíteni kell az oktatást, a szakembereknek pedig speciális követelményeknek kell megfelelniük. A biztonságos környezet kialakításában az állam a érintettek közötti kooperációhoz szükséges megfelelő kondíciók biztosításában jut szerephez. Ennek keretében szavatolja a nemzeti biztonságot, koordinálja a szlovák digitális tér védelmét, létrehozza az információbiztonság megfelelő jogi keretrendszerét, felméri a rendelkezésre álló kompetenciákat és meghatározza a felelősségi területeket, harmonizálja a szabványosítási tevékenységet, a nem minősített információkat és ICT-rendszereket biztonsági kategóriákba sorolja, alapvető információbiztonsági elvárásokat fogalmaz meg, társadalmi egyeztetés keretében bevonja a versenyszférát és a szakértőket a különböző koncepciók kidolgozásába. Az információbiztonsági menedzsment hatékonyságának növelése jelentős részben a CERT-ek feladatain és képességein múlik, ami a veszélyek figyelemmel kísérésétől az egyedi ICI-rendszerek biztonsági stratégiájának koordinálásáig terjed. A nemzeti és a kritikus infrastruktúrákat támogató ICI-k hatékony védelmének biztosítása érdekében a szlovák kormány egyes területeken már intézkedett, amire jó példa a szlovák Energiabiztonsági Stratégia információbiztonságra vonatkozó része vagy a Kritikus Infrastruktúrák Nemzeti Védelmi Programja. További lépésekre van szükség a biztonsági szabványok kötelező alkalmazására vonatkozó előírások, valamint a felmérésre, elemzésre, adaptálásra és frissítésre vonatkozó biztonsági szabályozás terén. A nemzeti és nemzetközi kooperáció tekintetében az információbiztonsági stratégia alkotói úgy vélik, hogy a helyi megoldások gyakran elégtelennek bizonyulnak, ezért a szlovák érdekek felmérését követően aktív szerepet kell vállalni a nemzetközi szervezetek tevékenységében.

Szlovákiában az információbiztonsági menedzsment struktúrája három rétegű. A kormány áll a legfelső szinten, ezt követik a központi kormányzati és tárcaközi testületek, míg a harmadik szinten az állami hatóságok különböző területekért felelős szervezeti egységei találhatók. Egy új struktúra kialakítását a jelenlegi folyamatok és kompetenciák részletekbe menő elemzésének kell megelőznie, ami alapján az optimalizálással összefüggő előterjesztés készül. A következő lépésben a számítógépes biztonsági incidenseket kezelő központot (CSIRT.SK) hoznak létre, öt éven belül átalakítják a jogszabályi, szervezeti és személyi környezetet, amihez forrást is biztosítanak. Utolsó lépésben a Nemzeti Információbiztonsági Hatóságot (NISA) hozzák létre. A strukturális átalakításokra vonatkozó erőfeszítések részleteit a 2008 végére elkészült akcióterv tartalmazza. Az információbiztonság aktuális prioritásaival kapcsolatban a stratégia alkotói kijelentik, hogy Szlovákiában kedvezőtlen a helyzet, aminek elsődleges oka az, hogy a stratégiai dokumentumokban megfogalmazott célkitűzések teljesítése gyenge, továbbá hiányzik az információbiztonsághoz és interoperabilitáshoz szükséges keretrendszerre vonatkozó állami koncepció, a jogszabályi háttér, a kompetencia, a tudatosság és még számos tényező. Szlovákia lemaradása a szabványosítás koordinálása terén jelentős, ezért ennek a területnek az erősítése kiemelten fontos. Szintén nagy jelentőséget tulajdonítanak az információbiztonsággal kapcsolatos ismeretek növelésének, amihez egy saját kategóriarendszert is felállítottak:

– általános alapvető ismeretek (minden felhasználó);
– általános IT-ismeretek (IT-specialisták, adminisztrátorok);
– specializált biztonsági ismeretek (információbiztonsági szakértők);

– alkalmazott biztonsági ismeretek (más területek ICT-biztonsághoz is értő szakértői);
– innovatív ismeretek (információbiztonsági kutató, specialista).

A nemzetközi együttműködések kapcsán a stratégia legfontosabb szempontként emeli ki, hogy azonosítani kell azokat a szervezeteket, ahol a szlovák érdekekkel összefüggő politikai folyamatok zajlanak, és megfelelően kvalifikált szakemberekre kell bízni a képviseletet. A Pénzügyminisztériumban felállított Információbiztonsági Bizottság koordinálja a nemzeti infrastruktúrák nem minősített szegmenseivel összefüggő nemzetközi tevékenységet. Az információbiztonsági oktatás és képzés rendszere szorosan kapcsolódik az ismeretek növelése kapcsán felállított kategóriákhoz. Ezen a területen is a felmérés kell, hogy az első legyen, aminek keretében megállapítható, hogy milyen ismereteket kell elsajátítaniuk az egyes kategóriákba sorolt személyeknek, továbbá az iskolai és egyéb képzési formák tekintetében meg kell határozni az információbiztonsági kapacitásokat és tartalmi lehetőségeket. Az általános információbiztonsági ismeretek oktatását már az általános iskolában be kell vezetni, míg az IT-specialisták számára élethosszig tartó tanulási modellt kell kialakítani az állami és magánszférában egyaránt.

A stratégia negyedik része a megvalósítással foglalkozik, aminek egyik legfontosabb részeként a korábban már említett akcióterv elkészítését és kormány általi elfogadását emeli ki, de további nyolc feladatot is meghatároz. Ezek között szerepel a kormányzati CSIRT. SK felállítására vonatkozó tervek elkészítése, a jogi alapok átalakítására vonatkozó elképzelések kialakítása, az információbiztonság képzési rendszerére vonatkozó fejlesztési koncepció megalkotása a megvalósíthatósági tanulmánnyal együtt. A normák és szabványok terén összesíteni kell a rendelkezésre álló információkat, és ezek alapján kell a stratégiában meghatározott tartalommal elkészíteni azt az elemzést, aminek alapján a terület átalakítható. Az egész ország információbiztonságára vonatkozóan helyzetértékelést kell készíteni, amit éves jelentéseknek kell kiegészíteniük az aktuális változásokkal. A kormánynak gondoskodnia kell módszertani dokumentumok, például egy információbiztonsági szótár kiadásáról, amelyet kétévente frissíteni kell. A megvalósításhoz kapcsolódóan határidőkre, felelősökre és konkrét összegekre lebontott költségbecslést is tartalmaz a stratégia.

A stratégia készítői az ötödik, befejező részben ismételten felhívják a figyelmet arra, hogy a dokumentum a 2008–2013 közötti időszakra készül, illetve a költségeket állami, európai uniós és privát forrásokból kívánják fedezni. A Pénzügyminisztérium által készített stratégia az akadémiai és a versenyszféra bevonásával, társadalmi egyeztetés keretében készült. Az alkotók leszögezik, hogy az információbiztonságra költött összegek megtérülése nem számszerűsíthető. A források hatékony elköltésének mérésére szolgáló egyetlen lehetőség, ha összehasonlítják az intézkedések bevezetése előtti és utáni incidensek számát és az okozott kár mértékét, bár a hatások tekintetében kénytelenek külföldi információkra alapozni.

Összehasonlítás és értékelés

A kiberbiztonsági stratégiák tartalmának ismertetéséből kitűnhet, hogy számos ponton erős hasonlóságot, sőt azonosságot mutatnak, de vannak olyan kérdések, amelyeknél komolyabb hangsúlyeltolódások érzékelhetők, néhány téma pedig nem található meg

mindegyikben. A dokumentumok elemzéséhez három forrásból gyűjtöttük össze azokat a tényezőket, amelyek alapján kialakultak az összehasonlításhoz szükséges kérdések. A vizsgálati szempontrendszer első pillérét az EU-elvárások, illetve az ENISA által megfogalmazott követelmények jelentik. A második pillér a NATO Kiberbiztonsági Kiválósági Központja által megfogalmazott feltételekből áll, míg a harmadik pillért egy 2013-ban Hollandiában készült, hasonló témájú, tíz nemzeti kiberbiztonsági stratégiát összehasonlító elemzés[19] módszertana képezi. A három pillér alapján a stratégiák összehasonlításakor az alábbi területeket vizsgálva kerestünk analógiákat és eltéréseket:

– a CECSP-országok által alkalmazott terminológiák;
– a stratégiák beágyazottsága és hatálya;
– a kiberbiztonsági környezet értékelése és a fenyegetések számbavétele;
– a célkitűzések deklarálása és prioritása;
– a végrehajtandó feladatok meghatározása,
– kockázatelemzési és -értékelési szemléletmód érvényesülése.

A CECSP-országok kiberbiztonsági stratégiáiban alkalmazott terminológia

Kézenfekvőnek tűnhet, hogy a kölcsönös megértés, a világos és egyértelmű kommunikáció, vagy éppen a félreértések elkerülése céljából az azonos területen megfogalmazott politikák és stratégiák terminológiája egyforma, és az egyes fogalmakat ugyanolyan jelentéstartalommal tölti meg minden érintett. Azonban ez koránt sincs így, az államok gyakran használnak eltérő fogalmakat különböző dokumentumaikban (jogszabályok, stratégiák, ajánlások, iránymutatások stb.), ami nemzeti és nemzetközi szinten is értelmezési problémákhoz vezethet. A nemzetközi együttműködések kapcsán feltételezhetnénk, hogy a politikai és stratégiai döntéshozók legalább akkor gondolnak az egységes terminológia alkalmazására, amikor kifejezetten egy területen vagy régióban kezdeményeznek kooperációt, de ebben az esetben is ritkán találkoznak az elvárások a valósággal.

Az öt vizsgált kiberbiztonsági stratégia közül mindössze kettő tartalmaz olyan részt, ami kifejezetten az alkalmazott terminológiával foglalkozik. Az osztrák stratégia végén található egyik függelékben majd két tucat olyan fogalom meghatározását olvashatjuk, amelyek a dokumentumban is gyakran előfordulnak. A lengyel stratégiának az elején találhatóak fogalmi definíciók, összesen tizennégy. Az osztrák stratégia leíró, magyarázó szöveg formájában mutatja be a kiberbiztonság *(cyber security)* osztrák értelmezését, míg a lengyel stratégia rövid, tömör definíciót ad a kibertér biztonságára *(cyberspace security)*. Hasonló a helyzet a kiberbűnözés vagy a kibertámadás meghatározása esetében is, és bár van néhány fogalom, amelyeket mindkét stratégia megmagyaráz, az átfedés kevés. A magyar stratégia törzsszövege ugyan tartalmaz definíciókat, de csak két pontban. A harmadik pont a kiberteret határozza meg, míg az ötödik pont részletes definíciót nyújt a kiberbiztonság fogalmának magyar értelmezéséhez. A szlovák stratégiának öt önálló melléklete van, közülük az utolsóban szerepelnek a definíciók. A cseh stratégiában egyáltalán

19 Luiijf, H. A. M. – Besseling Kim – Spoelstra, Maartje – Graaf, Partick de: Ten National Cyber Security Strategies: A Comparison, 2013.

nem találhatók fogalmi meghatározások, így magából a dokumentumból nem derül ki, hogy a kiberbiztonság helyett alkalmazott kibernetikai biztonság *(cybernetic security)* alatt pontosan mit értenek a stratégia alkotói.

A stratégiai dokumentumok alapján arra lehet következtetni, hogy az öt állam kiberbiztonság terén folytatott együttműködési törekvései érdemben egyelőre nem terjednek ki a szakterületre vonatkozó felfogás harmonizálására és a kölcsönös megértés javítására. A NATO ajánlása ellenére több stratégiából is hiányoznak a definíciók, amelyek nélkül a nemzetközi szintű harmonizáció és a közös fellépés megvalósítása nehézségekbe ütközhet.

A stratégiák beágyazottsága és hatálya

A stratégiai dokumentumok hierarchiájában a kiberbiztonsággal foglalkozókat rendszerint a nemzeti biztonsági vagy védelmi stratégiából vezetik le, és a kiberbiztonság egész társadalmat érintő jellegéből adódóan számos ágazati stratégiához kapcsolódnak. Emellett az alkotók a nemzetközi elvárásoknak és irányelveknek való megfelelésre is törekednek. A beágyazottságon túl további fontos tényező a stratégia területi, személyi, időbeli hatálya, mivel a megvalósítás, a számonkérés, az ellenőrzés és frissítés ezek hiányában problémákba ütközhet.

A CECSP-országok kiberbiztonsági stratégiáinak mindegyike figyelembe veszi az EU és NATO elvárásait, a cseh stratégia kivételével több – a nemzeti kiberbiztonsági stratégiák elkészítésére vonatkozó – rendeletet, ajánlást vagy döntést is nevesítenek. A nemzeti beágyazottság terén hasonló a helyzet, mindegyik stratégia hivatkozik a felsőbb szintű nemzeti biztonsági vagy védelmi stratégiára, illetve az ágazati stratégiákra, valamint a jogszabályi környezet bemutatása is megvalósul, bár az utóbbi mélységében jelentős eltérések vannak. Szintén különbségek tapasztalhatók a stratégiák időbeli hatályában, illetve a felülvizsgálat esedékességében. A cseh stratégia már címében is tartalmazza az időbeli érvényességet, míg a szlovák stratégiában csak utalások vannak arra, hogy az alkotók ötéves intervallumban gondolkodtak. A másik három stratégia semmilyen konkrétumot nem tartalmaz az időbeli érvényességre vonatkozóan, igaz, mindegyikben megjelenik a felülvizsgálatra vagy frissítésre utaló rendelkezés. Az érintettekre vonatkozóan egység tapasztalható, az öt stratégia mindegyike hangsúlyozza az állami és nem állami, illetve az akadémiai szféra érintettségét és felelősségét. Ugyanakkor a konkrét feladatok kapcsán az állami szerepvállalás és koordináció a domináns, elenyésző a nem állami és akadémiai szférára vonatkozó rendelkezések száma.

Az EU és a NATO által kialakított kiberbiztonsági keretrendszerek elemeit figyelembe veszi mind az öt ország, jellemző, hogy több dokumentumot is feltüntetnek, amelyekhez a kiberbiztonsági stratégia kapcsolódik. Ennek ellenére a szövetségesi ajánlások és szempontok nemzeti stratégiákba történő beépülése már vegyes képet mutat, pedig a beágyazás jelentős mértékben segíthetné a nemzetközi harmonizációt is. A rendkívül gyors technológiai fejlődés következtében a kiberbiztonsági dokumentumok felülvizsgálata fokozott gyakoriságot kívánna más ágazati stratégiákhoz képest, aminek egyszerű ösztönző eszköze lehet, ha már a dokumentum címe is tartalmazza azt az időszakot, amire a hatálya kiterjed.

A kiberbiztonsági környezet értékelése és a fenyegetések számbavétele

Az EU és a NATO dokumentumaiban egyaránt megtalálhatók a környezetértékelésre, illetve a fenyegetések és kockázatok azonosítására vonatkozó ajánlások, mivel ezek a tartalmi elemek határozzák meg a kihívások kezelésének kiindulópontját és a biztonságpercepciót. Bármilyen veszéllyel szemben történő felkészülés alapja, hogy ismerjük a veszélyt, annak mértékét, valamint a rendelkezésre álló képességeinket. Ezeknek az információknak a hiányában a célkitűzések megalapozatlanok lesznek, ami végrehajtási problémákat generálhat, végső soron pedig a biztonság csökkenéséhez vezethet.

Kiberbiztonsági környezetet és veszélyeket bemutató elemeket mind az öt stratégia tartalmaz, jellemzően a bevezető, illetve a dokumentum hátteréről, alapjairól szóló részekben. Az államok tisztában vannak azzal, hogy függenek az információs és kommunikációs rendszerektől, és ez a társadalom minden rétegére hatással van technológiai, gazdasági, szociális, kulturális, tudományos és politikai értelemben is. Kisebb eltérések itt is tapasztalhatók, de mind az öt állam a társadalom működését biztosító alapvető feltételként tekint a kibertérre és a kiberteret alkotó ICT-rendszerek üzembiztonságára. A kibertér használatából fakadó előnyök és hátrányok kéz a kézben járnak. Bár a biztonság szavatolását össztársadalmi feladatként azonosítják, az állam elsődleges koordináló szerepét és felelősségét hangsúlyozzák. Mind az öt stratégia számba veszi a kibertér szereplőit, illetve az általuk generált veszélyeket, amelyekkel szemben határokon átnyúló jellegükből fakadóan nehéz alkalmazni a társadalmak által kialakított hagyományos védelmi mechanizmusokat. A CECSP-országok jellegüktől és a technikai paraméterektől függetlenül tartanak az információs infrastruktúrák sérülésétől, ami az adatok szivárgásához, illegális megszerzéséhez, ellenőrizetlen felhasználásához, gazdasági károk okozásához, illetve súlyos esetben a létbiztonság veszélyeztetéséhez vezethet. A legtöbb dokumentumban kiemelt szerepet kap a kritikus infrastruktúrákat üzemeltető infrastruktúrák veszélyeztetettsége, valamint a kiberbűnözés és az általa generált károk növekvő mértéke.

Bármely nemzetközi együttműködésnek az alapja, hogy a kooperáló államok egységesen lássák azokat a tényezőket, amik az együttműködést létrehozzák, de legalább törekedjenek a közös szemléletmód kialakítására. A kiberbiztonság terén együttműködő közép-európai államok stratégiáiból kiderül, hogy biztonságpercepciójuk azonos, a kibertérből érkező fenyegetéseket és kihívásokat közel egyformán ítélik meg, és a biztonság jelenlegi szintjének növelését nemzetközi együttműködés hiányában nem tartják megvalósíthatónak.

A célkitűzések deklarálása és prioritása

Az öt állam biztonságpercepciójának hasonlósága alapján feltételezhető, hogy a fenyegetésekre adandó válaszok és célkitűzések is azonosak, azonban hangsúlyeltolódás akkor is elképzelhető, ha egyébként mindenben tökéletes egyetértés mutatkozik.

Az öt stratégia mindegyike meghatároz célkitűzéseket, jellemzően önálló pontokba gyűjtve. Ezeket összesítve valamennyi stratégiában megjelennek az alábbi célkitűzések:

– biztonságos környezet megteremtése a kibertér és az ICT-infrastruktúrák biztonságának, rugalmasságának fokozásával;

– a közigazgatási és kritikus infrastruktúrák tekintetében a megelőzési, észlelési, válaszadási és helyreállítási képességek javítása révén a támadások hatásainak csökkentése és az üzembiztonság növelése (például CERT-ek alapításával);
– a kiberbiztonsági tudatosság és a kompetencia össztársadalmi szintű növelése az oktatás és képzés átalakításával, fejlesztésével;
– a felelősségi területek meghatározása minden szereplőt illetően, és a jogszabályi környezet megteremtése, átalakítása az emberi jogok és szabadságok megtartásával;
– a koordináció és az információk megosztásának fokozása nemzeti és nemzetközi szinten az állami, a nem állami és az akadémiai szereplők között.

Bár a megfogalmazás és a kontextus nem minden esetben azonos, a célkitűzéseket értelmezve és a hozzájuk kapcsolt magyarázatokat tanulmányozva kiderül, hogy a fenti öt terület az, amelyek a vizsgált stratégiákban következetesen megjelennek nemzeti kiberbiztonsági célkitűzésekként. A számuk nem mérvadó, mivel több cél összevontan vagy épp szétbontva szerepel a különböző stratégiákban. A célkitűzések deklarálását az EU és a NATO ajánlásai is tartalmazzák, így ebben a tekintetben mindegyik stratégia megfelel a nemzetközi elvárásoknak. Prioritási sorrendet egyik nemzet sem állított fel a célok között.

A végrehajtandó feladatok meghatározása

A kitűzött célok elérését a stratégiák konkrét feladatok és intézkedések meghatározásával igyekeznek biztosítani. Tekintettel arra, hogy az egyes országok felkészültsége, képességei, jogi keretrendszere, szervezeti struktúrája eltérő, a megszabott feladatok és intézkedések várhatóan nem lesznek azonosak.

A cseh stratégiában a célkitűzések együtt szerepelnek az intézkedésekkel. A dokumentum készítői a jogi keretrendszert, a közigazgatási és kritikus infrastruktúrákat üzemeltető ICT-rendszerek biztonságát, a nemzeti CERT felállítását, a nemzetközi kooperációt, az állami, nem állami és akadémiai szféra együttműködését, valamint a tudatosság növelését nevesítik az intézkedések között. Mindegyik területhez 3-5 alpont tartozik, amelyek a fontosabb részletekről szólnak.

Az osztrák stratégia strukturális és folyamatirányítási, kormányzati, társadalmi, gazdasági és kormányzati együttműködési, kritikusinfrastruktúra-védelmi, tudatosságnövelési, kutatás-fejlesztési és nemzetközi együttműködési területeket jelöl ki cselekvésre. A struktúrák tekintetében kormányzati kiberbiztonsági csoport felállításáról, a műveleti szint koordinációjának megvalósításáról, válságkezelési rendszer kialakításáról és a már létező struktúrák erősítéséről rendelkeznek. Kormányzati szinten a modern jogi keretrendszer felállítására, a minimális biztonsági szabványok meghatározására és az éves kiberbiztonsági beszámoló elkészítésére vonatkozóan ad a stratégia iránymutatást. A szektorok közötti együttműködés terén gondoskodni kell egy kiberbiztonsági platform felállításáról, a kis- és középvállalatok támogatásáról, valamint egy kiberbiztonsági kommunikációs stratégia elkészítéséről. A tudatosság növelésénél a kiberbiztonsági kultúra erősítése és az oktatás-képzés minden szintjén beépülő kiberbiztonsági ismeretekre vonatkozó intézkedések jelennek meg.

A kiberbiztonság helyzetét alapvetően szilárdnak értékelő magyar stratégia a kormányzati koordináció, az együttműködés, a szakosított intézmények, a szabályozás, a

nemzetközi együttműködés, a tudatosság, az oktatás és kutatás-fejlesztés, a gyermekvédelem, valamint a gazdasági szereplők motivációja terén határoz meg feladatokat. Minden intézkedési területet és feladatot rövid, leíró jellegű szöveg egészít ki, amely az érintettek körét is meghatározza.

A szlovák stratégia a cseh dokumentumhoz hasonlóan a célkitűzésekkel együtt – stratégiai prioritások címszó alatt – taglalja a szükséges intézkedéseket. Az emberi jogok és szabadságok, a tudatosság és kompetenciabővítés, a biztonságos környezet megteremtése, az információbiztonsági menedzsment fejlesztése, a közigazgatási és kritikus infrastruktúrák védelmének biztosítása, a nemzeti és nemzetközi kooperáció és a nemzeti kompetencia erősítése terén a stratégia részletesen írja le a szükséges intézkedéseket. Az alkotók bizonyos területeket (mint például a kormányzati információbiztonsági menedzsmentet) kiemelnek, és még részletesebben, más aspektusból is bemutatják az ezek kapcsán megjelenő feladatokat.

A lengyel stratégia az egyetlen, ahol a készítők jelzik, hogy a legfontosabb intézkedések prioritási sorrendben szerepelnek. Minden feladatot megelőz a kockázatelemzés, amit évente kell elkészíteni. Ezután következnek a kormányzati és közigazgatási portálok biztonságával, a jogszabályi környezettel, majd a folyamatirányítási és szervezeti változásokkal kapcsolatos intézkedések. Utóbbi esetében a stratégia részletesen kitér a lengyel kibertér biztonságának menedzsmentjére, a szervezeti szintű biztonság megszervezésére, valamint a kiberbiztonsági döntéshozók és specialisták feladataira. Hasonlóan részletes az oktatással, képzéssel és a tudatosság növelésével kapcsolatos intézkedések leírása, amely külön kitér a kiberbiztonsági specialisták képzésével, a kiberbiztonság felsőoktatásba történő bevezetésével, a közigazgatási hivatalnokok képzésével és a társadalmi kampányok oktatási és megelőzési természetével kapcsolatos feladatokra. Az utolsó pont a technikai intézkedések területét mutatja be, kiemelve többek között a kutatási programokat, a CERT-ek bővítését, illetve egy korai előrejelző rendszer fejlesztését.

Az intézkedési területek jelentős átfedést mutatnak, ami elméletileg pozitív hatással lehet az információk és legjobb gyakorlatok megosztását célzó CECSP-együttműködésre, hiszen az érintett országokban közel azonos területeken keletkeznek a kiberbiztonság fejlesztésével kapcsolatos értékes tapasztalatok. Ugyanakkor az is látható, hogy a közös célok teljesítéséhez a stratégiák alapján más utat kell bejárnia például Ausztriának, ahol a kiberbiztonsági kultúra fejlett és már több ágazati CERT is működik, mint Szlovákiának, ahol a stratégia deklarálja, hogy a kiberbiztonság helyzete kedvezőtlen, és a központi kormányzati CERT megalakításához szükséges dologi, anyagi és humán források felméréséről épp a stratégia intézkedik elsőként. A kiberbiztonság országonként eltérő szintjéből fakadóan eltolódnak a hangsúlyok az egyes intézkedések között, aminek az együttműködésre gyakorolt hatását nehéz felmérni kizárólag a kiberbiztonsági stratégiák elemzésével.

Felmérő és ellenőrző mechanizmusok

A különböző stratégiák elkészítését rendszerint kockázatelemző és környezetértékelő folyamatok előzik meg, amelyeknek az eredményei meglehetősen fontosak a stratégia tartalmát illetően. A stratégiai intézkedéseket összefogó részekben is gyakran fordulnak elő kockázatelemzések és különböző specifikus felmérések elvégzésére vonatkozó feladatok,

továbbá a végrehajtás ellenőrzésében és a stratégia felülvizsgálata során is szerepet kapnak a különböző felmérések. A stratégiák teljes életciklusában kitüntetett szerephez jutó elemző-értékelő tevékenység biztosítja azokat az alapvető adatokat és információkat, amelyeknek a segítségével megismerhető a kiindulási helyzet, egy speciális terület paraméterei, illetve a végrehajtás eredményei és kudarcai.

Az osztrák stratégia a kormányzati koordinációval kapcsolatban írja elő éves beszámoló készítését „Kiberbiztonság Ausztriában" címmel, míg operatív szinten periodikus, incidenshez kötött helyzetértékelést vár el. Ausztriában a válságkezelési és üzemfolytonossági tervek rendszeres frissítéséhez szektorspecifikus és szektorokon átívelő kockázatelemzéseket készítenek, míg a jogi keretrendszer átalakítása kapcsán átfogó jelentést kell készíteni, amelynek felelőse a kormányzati kiberbiztonsági csoport. A csoport kétévente a stratégia végrehajtásáról is jelentést készít, együtt a stratégia felülvizsgálatával.

A magyar kiberbiztonsági stratégia alkotói nem nevesítenek önálló elemzéseket vagy környezetértékeléseket, és nem írnak elő felülvizsgálatot sem. A stratégia megfogalmazásában a célok eléréséhez, a kompetenciák és potenciális erőforrások terén szükséges eszközök jelentős részével már rendelkezik az ország, így felmérésre utaló elemek csak a kiberbiztonságért felelős kormányzati, civil, gazdasági és tudományos szervek, valamint a kritikus infrastruktúrák és vagyonelemek számbavétele kapcsán fordulnak elő.

A szlovák stratégia először a kiberbiztonsági incidensek okaival kapcsolatban hivatkozik elemzésekre, azonban csak általános jelleggel. A biztonságos környezet megteremtését illetően már meghatározza, hogy a rendelkezésre álló nemzeti kompetenciákról felmérést kell készíteni, illetve az információbiztonsági menedzsment hatékonyságát is vizsgálni és értékelni kell. A stratégia készítői további elemzési feladatokat határoznak meg a kritikus infrastruktúrák biztonsági szintjével, valamint a szlovák kiberbiztonsági képesítésekkel kapcsolatban. Az információbiztonsági struktúra átalakításának a folyamatok és kompetenciák optimalizálására vonatkozó, részletekbe menő elemzésen kell alapulnia. A szlovák szabványosítási folyamatokról áttekintés készül, amely az átalakításra vonatkozó tervek alapjául szolgál. Az oktatás és képzés fejlesztése kapcsán is felmérés és elemzés előzi meg a konkrét lépéseket. A stratégia végrehajtásáról éves rendszerességgel folyamatelemzések és feladatértékelések készülnek, amelyeket a kormánynak kell jóváhagynia, miként a szlovák kiberbiztonsági helyzetről is éves jelentésben kell tájékoztatni a kormányt.

A cseh stratégia az intézkedések alkalmassága kapcsán emeli ki, hogy kockázatelemzések elvégzésére és az eredmények felhasználására van szükség. A jogszabályi keretrendszer kapcsán Csehország rendszeresen elemzi és értékeli a nemzetközi jogszabályokat, egyezményeket, trendeket és ajánlásokat, az eredményeket pedig felhasználja a cseh kiberbiztonsági környezet fejlesztése érdekében. Operatív szinten a kormányzati CERT egyik legfontosabb feladata az incidensek azonosítása és kiértékelése, s ezek alapján rendszeresen frissített intézkedési tervek készülnek. A kritikus infrastruktúrák esetében a biztonsági előírások betartásának és végrehajtásának elemzésével azonosíthatók a megerősítésre szoruló rendszerek. Az oktatás és képzés terén szintén folyamatos elemzésre van szükség, ami a cseh felhasználók számára szükséges képesítéseket vizsgálja.

A lengyel stratégia készítői a dokumentum legelején jelzik, hogy az többek között a kormányzati CERT által összeállított, időszakos kiberbiztonsági helyzetjelentés alapján

készült. A stratégiai célkitűzések elérése érdekében megfogalmazott intézkedések és az implementáció kapcsán is kiemelik, hogy olyan, szakértők által készített kockázatelemzések alapján alakultak ki, amelyek a minimális biztonsági szabványok meghatározásakor is kiindulópontként szolgálnak. A lengyel intézkedések első helyre sorolják és kulcselemként tekintenek a kibertér működését vizsgáló kockázatelemzésre, amit az elfogadható biztonsági szint megteremtése érdekében minden év január 31-ig jelentés formájában terjesztenek az informatikáért felelős miniszter elé. A jelentés elkészítésére kötelezett szervezeti egységek körét és a jelentés tartalmát is meghatározza a stratégia. A jogi környezettel kapcsolatos intézkedések között szintén található a hatályos jogszabályok felülvizsgálatára vonatkozó rendelkezés. Végül a lengyel stratégia külön pontban foglalkozik a dokumentum hatékonyságának széles körű felmérésével és értékelésével, amihez kritériumokat és konkrét példákat is megad.

A felmérő, ellenőrző és értékelő mechanizmusok kapcsán megközelítésbeli különbségek érzékelhetők. Ausztria és Lengyelország jelentős hangsúlyt fektet a folyamatos és rendszeres elemzésekre, amelyeket mindkét állam megjelenít kiberbiztonsági stratégiájában. A szlovák stratégia kapcsán is hasonló kép rajzolódik ki, azonban a cseh dokumentum már csak specifikus területekre vonatkozóan tér ki a felmérések szerepére és szükségességére. A cseh dokumentumhoz hasonlóan a magyar stratégia sem tartalmaz ismétlődő, rendszeres felülvizsgálatra vagy ellenőrzésre vonatkozó rendelkezést és specifikus felmérést, és arra vonatkozó elemzést sem azonosít, aminek alapján a dokumentum elkészült. Ugyancsak átsiklik afelett, hogy az egyes intézkedések kialakításakor és végrehajtásakor milyen tényezőket kell számításba venni. Mindez nem jelenti azt, hogy Csehországban és Magyarországon nem működnek felülvizsgálati folyamatok, csupán azt jelzi, hogy míg a cseh stratégia alkotói csak részben, a magyar stratégia készítői egyáltalán nem vették figyelembe az EU és a NATO ajánlásait a mechanizmusok beépítésére vonatkozóan.

A közép-európai régióban beindított kiberbiztonsági együttműködési folyamat eredményei az érintett országok kiberbiztonsági stratégiáiban még nem láthatók. Egy évvel a kezdeményezés elindítását követően a tevékenység jelentős részét az operatív szinten megvalósuló közös gyakorlatok, illetve időszaki egyeztetések teszik ki, a politikai döntéshozatal felső szintjén keveset hallani a kiberbiztonsági platform működésének dinamikájáról. A stratégiákban megjelenő eltérések és analógiák több fontos kérdésre is felhívják a figyelmet. Míg a kiberbiztonsági felfogás kapcsán tapasztalható azonosságok azt mutatják, hogy az együttműködés közös alapja már létezik és meglehetősen szilárd, az azonos terminológia hiánya, a NATO- és EU-irányelvek beépülésének eltérő, többnyire alacsony szintje a kooperáció kiterjesztését és növelését determinálja. A Közép-európai Kiberbiztonsági Platform keretein belül a stratégiai, illetve a felső szintű politikai együttműködés kiterjesztése és fokozása elengedhetetlen kellék a régió kiberbiztonságának növelésére tett intézkedések sorában.