Berzsenyi Dániel

Globális kihívás, regionális válaszok: kiberbiztonság Kelet-Közép-Európában[1]

A tanulmány a kiberbiztonság terminológiai kihívásainak és a kibertér trendjeinek bemutatásán túl rávilágít néhány olyan tényezőre, amelyek a kibertérből érkező kihívásokra adott regionális válaszok eredményeit befolyásolhatják Kelet-Közép-Európában. Így a visegrádi négyek kiberbiztonsági stratégiáinak értékelésével a szerző azt vizsgálja, hogy mennyire aktuálisak ezek a dokumentumok, érdemi válaszokat adnak-e a kiberbiztonsági kihívások bemutatott trendjeire, és összességében milyen intézményi környezetbe rendelik a kiberbiztonsági feladatok kezelését.

Kulcsszavak: *kiberbiztonság, információs társadalom, Kelet-Közép-Európa, nemzetbiztonság, stratégia*

Berzsenyi Dániel: Global Challenge, Regional Answers: Cybersecurity in East Central Europe

Looking beyond the terminological complexity and the overview of current cyber security trends, the study casts light upon several factors that can influence the regional answers and their results in East Central Europe. Through an examination of cyber security strategies of the Visegrad countries, the author seeks to map the institutional environment of tackling cyber security challenges, and whether the current strategies are up-to-date offering adequate answers to the introduced trends of cyber challenges.

Keywords: *cybersecurity, information society, East Central Europe, national security, strategy*

Bevezetés

Napjainkban egyre szélesebb körben ismert és elfogadott tény, hogy korunk biztonságpolitikai kihívásai között kiemelkedő szerepet töltenek be a kibertérből érkező kihívások, fenyegetések és veszélyek. Ennek legfőbb oka, hogy számuk folyamatos növekedésén túl a mindennapi életünk egyre több területén fejtenek ki egyre jelentősebb hatást, tehát a fenyegetési spektrum is dinamikusan növekszik. Miközben az információs társadalomban természetesnek vesszük, hogy a kibertérből elérhető adatok és információk folyamatosan növekednek, sokak számára kevésbé nyilvánvaló, hogy ezeknek az adatoknak és információknak a megfelelő szintű védelméről is gondoskodnunk kell. Tovább súlyosbítja a helyzetet, hogy az infokommunikációs technológia fejlődése következtében egyre több

[1] A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosító számú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

társadalmi folyamat zajlik a kibertérben, vagy annak felhasználásával, és a folyamatosan gyarapodó információkhoz egyre többféle módon és többféle eszközzel férhetünk hozzá.

Korábban egy átlagos felhasználó számára a legnagyobb problémát az jelentette, ha óvatlansága miatt számítógépe vírussal fertőződött meg, és ennek következtében kéretlen reklámüzeneteket kapott, vagy átmenetileg blokkolták hálózati hozzáférését. Idővel azonban kialakult egy olyan alapvető biztonságtudatosság, aminek köszönhetően ma már a legtöbb számítógépes felhasználó számára egyértelmű, hogy a megfelelő célszoftverekkel (víruskereső, tűzfal) jelentős mértékben csökkenteni tudja sebezhetőségét.

Az elmúlt néhány évben ugyanakkor a kiberbiztonság helyzete egyéni, nemzeti, regionális és globális szinten egyaránt gyökeresen átalakult. A jelenleg is tartó átalakulás rendkívül gyorsan és komplex módon zajlik. A kibertérben elérhető szolgáltatások dinamikus bővülése, az okoseszközök rohamos elterjedése, a gyártók felelőtlensége, a rosszindulatú felhasználók és az általuk alkalmazott módszerek körének bővülése, valamint a technológiai és tudástranszfer következtében mára egy átlagos felhasználó kitettsége a kibertérből érkező támadásoknak a sokszorosára nőtt. Napjainkban egy számítógépre telepített víruskereső és tűzfal kombinációja az alapvető biztonság szavatolásához is kevés lehet, ha emellett nem gondoskodunk adataink, kommunikációs csatornáink és okoseszközeink védelméről, nem használunk megfelelő hosszúságú és bonyolultságú jelszavakat, és nem ismerjük fel időben az emberi hiszékenységen, illetve megtévesztésen alapuló támadásokat *(social engineering)*. Az átlagos felhasználó jellemzően nincs tisztában azzal, hogy a kibertámadásoknak való kitettsége mekkora mértéket ölt – és nem is lehet reális elvárás, hogy mindenki a saját kiberbiztonsági szakembere legyen. Ugyanakkor a kiberbiztonsági tudatosság fejlesztésére és terjesztésére egyre jelentősebb igény mutatkozik, hiszen a kibertér jellemzőiből fakadóan az egyén tájékozatlansága és felelőtlen felhasználói magatartása könnyen megbéníthat egy egész szervezetet, de veszélyt jelenthet akár a nemzetbiztonságra is.

A kibertérben nincsenek államhatárok, ahol ellenőrzést lehetne folytatni, az ott zajló események gyakran a másodperc törtrésze alatt következnek be, miközben hatásuk évekig eltarthat, a folyamatok attribútumainak bizonyító erejű meghatározása pedig a legtöbb esetben rendkívül bonyolult, sokszor lehetetlen. Szintén eltér a hagyományos (offline) világunk szabályszerűségeitől, hogy a kibertérben a nemzetállamok korántsem egyeduralkodók, a társadalom megannyi szereplője megtalálható ott a multinacionális cégektől a szervezett bűnözői és aktivista csoportokon át egészen az egyéni felhasználóig. A kibertér említett jellemzői jól mutatják, hogy milyen sokszínű és bizonyos tekintetben mennyire eltérő a virtuális világ a hagyományoshoz képest.

A kibertér sajátosságait figyelembe véve a nemzetállamok a világon mindenütt próbálnak a hagyományos területekkel foglalkozó nemzetközi együttműködésekhez hasonló szövetségeket létrehozni a kibertér biztonságának szavatolása érdekében. Ezek az együttműködési kezdeményezések elsősorban az elmúlt évek kiberbiztonsági trendjeinek köszönhetők, amelyek rádöbbentették a kormányokat arra, hogy önállóan nem képesek megteremteni a kibertér biztonságos használatának alapvető feltételeit. A kibertérhez kapcsolódó nemzetközi együttműködések legtöbbször a szabályozatlanság problémájára próbálnak megoldást találni, de egyre több a kiberbűnözés elleni, határokon átnyúló összefogás, illetve

a szellemi tulajdon védelmében és a kibertérben folytatott kémkedés ellen létrehozott multinacionális együttműködés.

Magyarország több nemzetközi kiberbiztonsági kezdeményezésben is érintett, egyrészt az euroatlanti szövetségi rendszerbe való beágyazottsága, másfelől az önálló, illetve harmadik fél által indított regionális kezdeményezések révén. Utóbbiak közül kiemelkedő a 2013 májusában Ausztria és Csehország kezdeményezésére létrehozott Közép-európai Kiberbiztonsági Platform *(Central European Cyber Security Platform – CECSP),* amelynek hazánk mellett Lengyelország és Szlovákia is tagja. Azonban kérdéses, hogy a határok nélküli virtuális világban miként jelenik meg a regionalizmus, és milyen esélye lehet egy regionális együttműködésnek arra, hogy kézzelfogható eredményeket produkáljon a kiberbiztonság terén, különösen úgy, hogy az együttműködésben érintett államok alapvető terminológiája, percepciója és megközelítése eltérő képet mutat. A tanulmány célja, hogy a kiberbiztonsági terminológia kihívásainak és a kibertér trendjeinek bemutatásán túl rávilágítson néhány olyan tényezőre, amelyek a kibertérből érkező kihívásokra adott regionális válaszok eredményeit befolyásolhatják.

A kiberbiztonság terminológiai problémái

A kiberbiztonsági trendek bemutatása előtt fontos lenne, hogy az olvasó tisztában legyen az alapvető fogalmakkal, azonban számos más területhez hasonlóan a kiberbiztonságnak sincs általánosan elfogadott meghatározása. Például az Európai Unió kiberbiztonsági stratégiája szerint a „kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket. A kiberbiztonság célja a hálózatok és az infrastruktúra rendelkezésre állásának és integritásának, valamint a benne lévő információk titkosságának megőrzése."[2]

Az ENSZ mellett működő Nemzetközi Távközlési Egyesület *(International Telecommunication Union – ITU)* két meghatározása is érvényben van a kiberbiztonságra vonatkozóan. A rövidebb meghatározás szerint az adatok és rendszerek védelmét jelenti azokon a hálózatokon, amelyek az internethez kapcsolódnak. A tömör definíció helyett érdemesebb inkább az ITU hosszabb meghatározását figyelembe venni, amely szerint a kiberbiztonság olyan eszközök, politikák, biztonsági koncepciók, útmutatások, kockázatkezelési törekvések, intézkedések, képzések, legjobb gyakorlatok és technológiák együttese, amelyek alkalmasak a kibertér, illetve a kibertérben működő szervezetek és személyek tulajdonának védelmére. A meghatározás kitér arra is, hogy a szervezetek és felhasználók tulajdonának kell tekinteni minden, a kibertérrel kapcsolatban álló eszközt, infrastruktúrát, alkalmazást, szolgáltatást, telekommunikációs rendszert és az összes küldött és tárolt információt.

Az ITU meghatározása magában foglalja az információbiztonság három alapelvét: a bizalmasságot, a sértetlenséget és a rendelkezésre állást is.[3] Bizalmasságon vagy titkosságon

[2] Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér, [online], 2013, 3. o. Forrás: Európai Bizottság [2016. 05. 01.].

[3] Chad Perrin: The CIA Triad, [online], 2008. 06. 30. Forrás: TechRepublic [2016. 05. 01.].

azt értjük, hogy az információhoz csak az előírt módon és csak olyan személyek férhetnek hozzá, akiket erre feljogosítottak. A sértetlenség vagy más néven integritás nem más, mint az adat és információ eredetisége és épsége, illetve az információs rendszer hiteles és pontos állapota. Egyszerűbben fogalmazva: az adatokat és információkat csak azok módosíthatják, akik erre jogosultak, és véletlen változás nem fordulhat elő. A rendelkezésre állás szintén egy állapotot határoz meg, amely egyfelől állandóságot jelent, másfelől az adatok és információk meghatározott időben történő elérhetőségét. A rendelkezésre állást értelmezhetjük úgy is, hogy a felhasználót semmi nem akadályozza abban, hogy az adatokhoz és információkhoz hozzáférjen, amikor azokra szüksége van.

Az euroatlanti szövetségi rendszerről szólva érdemes felidézni a világ legerősebb katonai szervezeteként számon tartott NATO kiberbiztonsághoz kapcsolódó kifejezéseit. Katonai szervezet lévén, a NATO által alkalmazott terminológia alapvetően a „védelem" és a „kiber" kifejezéseket társítja, de szintén több meghatározást használnak párhuzamosan. Az egyik meghatározás szélesebb információbiztonsági környezetet foglal magába, ahol a kommunikációs és információs rendszerek biztonsága a bizalmasság, az integritás és a rendelkezésre állás megfelelő védelmének képességét jelenti. Ugyanakkor a NATO a kibervédelem kifejezésen olyan képességet ért, amellyel egy műveleti kommunikációs és információs rendszer szolgáltatásai megvédhetők a kibertérből érkező rosszindulatú tevékenységekkel szemben.[4]

Már az említett meghatározások nyomán is jól látható, hogy az egyes kiberbiztonsági definíciók között eltérés mutatkozik attól függően, hogy melyik szervezetről vagy intézményről van szó. A helyzet csak tovább bonyolódik, ha az egyes államok szintjén vizsgáljuk a kiberbiztonság meghatározását, mivel a legtöbb ország saját megfogalmazást, egyedi definíciót alkalmaz. Ezen a szinten az eltérések sokszor jelentéktelenek, de gyakran előfordulnak nagyobb különbségek is. Mivel a tanulmánynak nem célja a terminológiai hasonlóságok és eltérések részletes bemutatása, ezért az állami definíciók közül csak a magyart mutatjuk be. A 2013-ban megjelent Nemzeti Kiberbiztonsági Stratégia (NKBS) 5. pontja az alábbiak szerint definiálja a kiberbiztonság fogalmát: „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez."[5] A bemutatott meghatározások alapján jól látható, hogy a kiberbiztonság egyfelől leginkább egy állapotként írható le, amelynek három alapvető összetevője az adatok és információk bizalmassága, integritása és rendelkezésre állása, másfelől viszont egy olyan eszközrendszer, illetve képesség, amely a kibertérből eredő kockázatokat elfogadható szinten tudja tartani. Fontos megjegyezni, hogy a fizikai világhoz hasonlóan a kibertérben sem érhető el abszolút biztonság.

---

[4] Alexander Klimburg (ed.): National Cyber Security Framework Manual, [online], 2012, 8. o. Forrás: NATO CCD COE [2013. 04. 20.].

[5] 1139/2013. (III.21.) Korm. határozat, Magyarország Nemzeti Kibervédelmi Stratégiája, [online], *Magyar Közlöny,* 2013/47, 3. pont [2013. 04. 02.].

Trendek a kibertérben

Amikor kiberbiztonsági kérdésekkel foglalkozunk, gondolkodásunkat meghatározó módon formálják a kibertérben zajló folyamatok és trendek, illetve az ezeket számszerűsítő kimutatások és statisztikai adatsorok. Például egy kiberbiztonsági incidens kapcsán az egyik elsőként felmerülő kérdés, hogy hány felhasználót vagy rendszert érint az adott eset. Annak érdekében, hogy tisztában legyünk az ember alkotta virtuális világ méretével, népességével és arányaival, ajánlott az aktuális trendeket áttekinteni. Számos forrás és adatsor található arra vonatkozóan, hogy hány ember él a világon, és ebből mennyi használja manapság az internetet, ugyanakkor az egyes földrajzi és gazdasági régiók között jelentős eltérések mutatkoznak több tekintetben is.

Az egyik megbízható forrásnak számító – korábban már hivatkozott – ITU 2016 júniusában kiadott adatai szerint a világ lakosságának több mint fele továbbra sem fér hozzá a világhálóhoz. Ugyan az ITU szerint 2016 végére 3,9 milliárd főre csökken azoknak a száma, akik nem használják az internetet, regionális bontásban például Afrikában a lakosság 75%-a nem fér hozzá, miközben Európában ugyanez az arány csupán 21%. Az adatok sajátos bemutatása az ENSZ Fenntartható Fejlődési Célkitűzéseihez köthető, ha azonban megfordítjuk a megközelítést, azonnal látható, hogy 47%-os lefedettség mellett, globális szinten majdnem minden második ember hozzáféréssel rendelkezik a világhálóhoz. Európában a háztartások 84%-a csatlakozik az internethez, miközben a szélessávú mobil-előfizetések aránya meghaladja a 76%-ot.[6] A 738 millió fős európai lakosságra[7] vetítve ez több mint félmilliárd felhasználót jelent. Tovább szűkítve a vizsgálati kört, Magyarországon a rendszeres internethasználók aránya eléri a 72%-ot,[8] ami több mint 7 millió felhasználót jelent hazánkban.

Más megközelítésben érdemes elgondolkodni azon, hogy mi történik az interneten, ha egyetlen szűk perc keresztmetszetét próbáljuk megvizsgálni. Egy 2016 nyarán megjelent felmérés szerint gigantikus méreteket ölt a különböző online tartalmak generálása. A kutatási eredményeket publikáló jelentés „tartalomsokknak" nevezi a jelenséget, ugyanis a 2013-ban egy perc leforgása alatt elküldött e-mailek száma 182,9 millióról 2015-re 205,6 millióra nőtt. De hasonló adatokat mutat a legnépszerűbb internetes keresőmotor (Google) használata is, itt a 2013-as, egy perc alatt indított 2,6 millió keresés 2015-re elérte a 3,1 milliót, míg a világelső közösségi oldalon (Facebook) közzétett posztok száma 2,5 millióról 3,3 millióra nőtt. Ennél is jelentősebb a változás a legnépszerűbb közösségi videomegosztó (YouTube) oldal esetében, ahol 2013-ban egy perc alatt még csak 100 órányi videotartalmat töltöttek fel a felhasználók, 2015-ben viszont már 400 órányit. Szignifikáns a különbség az egyik népszerű azonnali üzenetküldő (WhatsApp) alkalmazás esetében is, amelynek segítségével a felhasználók 2013-ban még 11,8 millió üzenetet küldtek, 2015-ben viszont ugyanez az alkalmazás már 44,4 millió üzenetet továbbított percenként.[9] Az említett adatok

[6] ICT Facts and Figures, [online], 2016. 06. Forrás: ITU [2016. 07. 26.].
[7] World Population Prospects, [online], 2015. Forrás: UN Economic & Social Affairs [2016. 07. 26.].
[8] Rendszeres internethasználók aránya (2005–2016), [online]. Forrás: KSH [2017. 01. 20.].
[9] Robert Allen: What happens online in 60 seconds?, [online], 2017. 02. 06. Forrás: Hubspot [2017. 01. 20.].

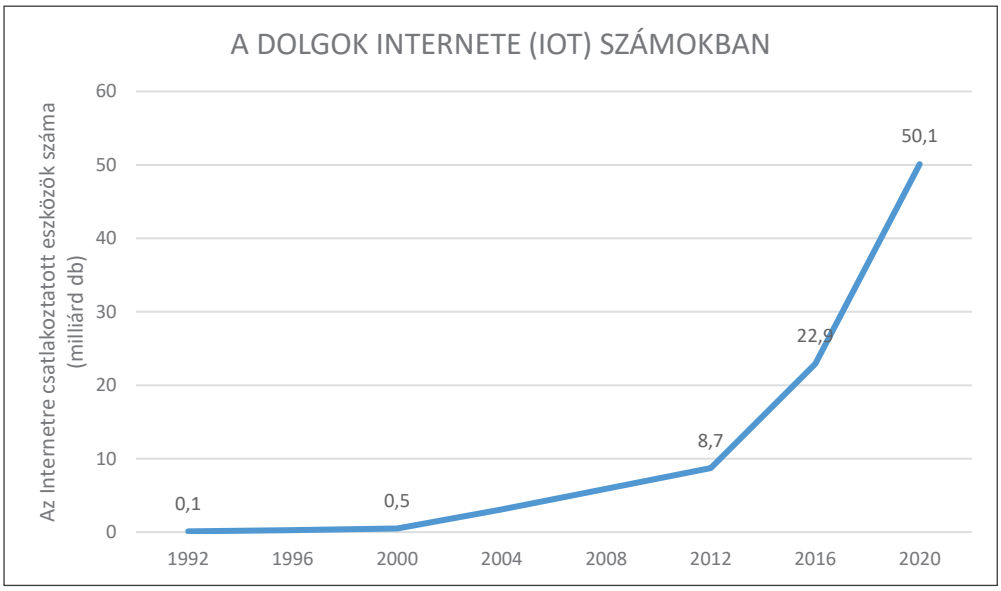
azt mutatják, hogy jelentős és folyamatos növekedés mutatkozik mind a felhasználók számában, mind pedig a felhasználás mértékében.

A kiberbiztonság jelentőségének megértéséhez további folyamatokat is feltétlenül figyelembe kell venni, amelyek közül kettőt fontos kiemelni. Korábban már szóba került, hogy a mindennapi életünk során egyre több szálon kapcsolódunk a virtuális világhoz. Míg korábban elsősorban az asztali vagy hordozható számítógépünk segítségével kommunikációra használtuk a kiberteret, később pedig pénzügyi tranzakciók lebonyolítására vagy multimédiás tartalmak fogyasztására, ma már egyre több eszközünk kapcsolódik a kibertérhez, amelyek a legkülönbözőbb funkciókon keresztül képesek digitalizálni mindennapjainkat. Gondoljunk a manapság divatos okoseszközökre (telefonok, televíziók, karórák stb.), amelyek mindegyike egy-egy újabb szálon kapcsol bennünket a kibertérhez. Az eszközök által dominált virtuális világ angol elnevezése az *Internet of Things* (IoT), vagyis a dolgok internete, és jóval túlmutat a ma elterjedt okoseszközök képességein. A dolgok internete tulajdonképpen nem más, mint hálózatba kapcsolt eszközök, járművek, épületek és egyéb ember alkotta tárgyak, amelyek a beépített elektronikának, szoftvereknek és szenzoroknak köszönhetően képesek egymással kommunikálni a hálózati kapcsolataikon keresztül. Távoli eléréssel a hálózaton keresztül érzékelhetők és irányíthatók ezek az eszközök, aminek következtében egyre inkább elmosódik a határ a fizikai és a virtuális világ között. Az ITU 2012-ben kiadott ajánlása értelmében az IoT nem más, mint az információs társadalom infrastruktúrája.[10]

Az előrejelzések alapján az IoT térnyerése következtében robbanásszerűen megnövekszik az internethez csatlakoztatott dolgok (eszközök) száma az elkövetkező néhány évben. Már most is közel 23 milliárd eszköz csatlakozik az internethez globális szinten, de ez a szám 2020-ra elérheti, sőt nagy valószínűséggel meg is haladja majd az 50 milliárdot. Ez azt jelenti, hogy a világ 7,4 milliárd lakójára vetítve már ma is minden ember három különböző eszközzel éri el az internetet.

[10] Overview of the Internet of things, [online], 2012. 06. Forrás: ITU [2016. 07. 21.].

Az internetre csatlakozó eszközök számának egyre dinamikusabb növekedése



Forrás: Project the 'Things' Behind the Internet of Things, [online]. Forrás: CompTIA [2016. 10. 04.]

Az IoT térhódítása több szempontból is megállíthatatlannak tűnik. Az internetre csatlakoztatott eszközök száma már 2008-ban meghaladta a Föld népességének számát,[11] 2017-re pedig az IoT-eszközök piaca nagyobbá válik, mint az asztali számítógépek, tabletek és telefonok piaca együtt.[12] Hamarosan olyan hétköznapi használati tárgyaink és eszközeink is kapcsolatban lesznek a kibertérrel, mint az autónk, a háztartási eszközeink (hűtő, mosógép, sütő, kávéfőző stb.), vagy akár az otthonunk teljes gépészeti, elektromos és egyéb rendszerei.

A trendekből kirajzolódó folyamatnak azonban van egy árnyoldala is, amivel ma még a kiberbiztonsági szakembereken kívül meglehetősen kevesen foglalkoznak. A legtöbb felhasználóban nem tudatosul, hogy az internetre kapcsolódó eszközök számának növekedésével együtt növekszik az a támadási felület is, amin keresztül a rosszindulatú felhasználók károkat okozhatnak. Jó példa erre a világ egyik legjelentősebb kiberbiztonsági konferenciája, a DefCon, ahol 2016-ban 21 gyártó 23 eszközében összesen 47 sérülékenységet mutattak be a résztvevők.[13]

Ugyanakkor a már jelenleg is kiterjedt támadási felület nagyságát jól szemlélteti az a 2015-ben megjelent tanulmány, amely azt vizsgálta, hogy milyen szintű Magyarország kiberbiztonsági kitettsége az internethez csatlakozó ipari folyamatirányító rendszerek tekintetében, amelyek jellemzően erőművek vezérléséért, a közüzemi szolgáltatások működésért, vagy éppen különféle gyártósorok üzemeltetéséért felelősek. A tanulmányban bemutatott, 4 és fél óra alatt elvégzett mérés eredményei szerint 6100 olyan támadási pont

[11] Dave Evans: The Internet of Things How the Next Evolution of the Internet Is Changing Everything, [online], 2011, 3. o. Forrás: CISCO [2016. 10. 04.].
[12] The Internet of Everything: 2014, [online], Forrás: Business Insider [2016. 10. 05.].
[13] Mészáros Csaba: Fenyegetések internete, [online], 2016. 12. 22. Forrás: Computerworld [2016. 12. 29.].

volt megtalálható a kibertérben, amin keresztül a hazai szolgáltatások és infrastruktúrák működése megzavarható vagy leállítható lett volna, és milliós nagyságrendűre becsülhető azoknak a sérülékenységeknek a száma, amelyek kritikus infrastruktúrákat irányító rendszerekben találhatók.[14]

A bemutatott példák és adatok a kiberbiztonsági trendeket csak nagy vonalakban ábrázolják, azonban a bevezetőben leírt dinamikus növekedést, a kibertér hódítását és a kihívások párhuzamos növekedését jól alátámasztják. Az egyre nagyobb kitettség következtében új szegmensek jönnek létre a különböző iparágakon belül, amikre jó példa az egyelőre főként nagyvállalati környezetben terjedő kiberbiztosítás. Az egyik legújabb biztosítási piac lényege, hogy a vállalatok az egyre jobban terjedő digitalizációs folyamatok következtében olyan veszélyekkel és veszteségekkel szemben is szeretnének fedezetet, amelyek a kibertérből érkeznek. A kibertámadások személyre, iparágra, nemzetre való tekintet nélkül mindenkit fenyegetnek.

Kiberbiztonsági kitekintés – Közép-Európa

A bemutatott trendeket is szem előtt tartva a társadalmi, állami és ipari rendszerek zavartalan működését elsődlegesen biztosítani hivatott nemzetállami szereplők térségünkben, Közép-Európában is reagáltak a felmerülő kihívásokra. Csehország több mint egy évtizede megkezdte a kiberbiztonsági kihívásokkal szembeni felkészülést, aminek köszönhetően 2005-ben megjelent az első nemzeti Információbiztonsági Stratégiája. Ezt követően a 2011-ben kiadott cseh Nemzeti Biztonsági Stratégia is említést tesz a kiberbiztonságról, amelyet a cseh kormány kiemelt jelentőségű területként, a regionális konfliktusokkal, a terrorizmussal és a tömegpusztító fegyverek terjedésével azonos szintű fenyegetésként kezel. Még ugyanabban az évben jelent meg a második cseh kiberbiztonsági stratégia és a kapcsolódó, négy évre szóló akcióterv, amelyeknek a legfontosabb célkitűzése a cseh infokommunikációs rendszerek védelme, illetve a bekövetkezett kibertámadásokhoz kapcsolódó kárenyhítés hatékonyságának növelése. 2015-ben a cseh kormány frissítette a kiberbiztonsági stratégiát, és 2020-ig célul tűzte ki a kiberbiztonság lehető legmagasabb szintjének elérését.[15] Az ország kiberbiztonsági szervezetrendszere szilárd alapokon nyugszik, az érintett szervezetek felelősségi területeit a stratégiák egyértelműen meghatározzák. A kialakult struktúra számos ponton hasonlít a hazai rendszerre, amire jó példa a cseh Nemzeti Kiberbiztonsági Központ, ami az egyik nemzetbiztonsági szervezet keretében működik, akárcsak Magyarország esetében a Nemzeti Kibervédelmi Intézet.

Lengyelország az elmúlt évek során számos változást léptetett életbe a kibervédelmi rendszereivel kapcsolatban, és sikerrel hajtotta végre a kiberbiztonsági stratégiában meghatározott feladatokat. A kiberbiztonság mára a lengyel nemzetbiztonsági erőfeszítések szerves részévé vált, és ezen stratégián túl több más nemzeti stratégiai dokumentum is kiemelt területként kezeli. Elsőként a 2007-ben kiadott lengyel Nemzeti Biztonsági

[14] Berzsenyi Dániel – Ványi Rajmond: Egy katonapolitikai döntés lehetséges kiberbiztonsági következményei – Az Iszlám Állam elleni magyar katonai szerepvállalás margójára, [online], *Nemzet és Biztonság,* 8. évf., 2015/3, 134–143. o.

[15] National Cyber Security Strategy of The Czech Republic for The Period from 2015 to 2020, [online]. Forrás: ENISA [2016. 02. 11.].

Stratégia tett említést a kiberbiztonsági problémákról, összekötve azokat az állam működőképességének fenntarthatóságával.[16] Öt évvel később a nemzetbiztonsági rendszerek 2011 és 2022 közötti fejlesztésére vonatkozó stratégiai dokumentum foglalkozott részletesebben a Lengyelország kibertérben történő védelmével, végül 2013-ban fogadták el az első kifejezetten kiberbiztonsági kérdésekkel foglalkozó stratégiai dokumentumot.[17] 2015-ben a lengyel Nemzetbiztonsági Iroda publikált egy részletes doktrínát, amely konkrét feladatokat határoz meg az állami intézmények számára, főként a nemzetbiztonságért felelős ügynökségek, a fegyveres erők, valamint a privát szektor és a nem kormányzati szereplők számára. Lengyelországban a kibertér biztonságáért felelős állami szervezetrendszer kiépült, a feladatok és döntéshozatali szintek megfelelően definiáltak, aminek köszönhetően a lengyel kiberbiztonság tovább is fejlődhet. Ennek a fejlődésnek a kereteit a várhatóan 2017-ben megjelenő következő generációs kiberbiztonsági stratégia fogja meghatározni.

A kiberbiztonságot a kormány lassan már egy évtizede stratégiai szintre emelte Szlovákiában is. 2008-ban fogadták el az ország első Információbiztonsági Stratégiáját, amelyet a nem minősített közigazgatási információkért felelős Pénzügyminisztérium készített el.[18] Négy évvel később jelent meg Szlovákia első Kiberbiztonsági Stratégiája[19] egy akciótervvel együtt, amit a 2009–2013 közötti időszakra egy Információbiztonsági Terv is kiegészített. Szlovákiában a kiberbiztonsági szervezetrendszer csúcsán a Pénzügyminisztérium, a Belügyminisztérium, illetve speciális esetekben a Nemzetbiztonsági Tanács áll, míg az operatív tevékenységet a Nemzetbiztonsági Hatóság látja el. A környező országok gyakorlatától némileg eltér a szlovák modell, mivel a Védelmi Minisztériumnak nincs közvetlen szerepe a kiberbiztonság kormányzati irányításában.

Magyarországon több, 2013 előtt elfogadott stratégiai dokumentum is említést tesz az információ- és kiberbiztonság jelentőségéről, így például a 2012-es Nemzeti Biztonsági Stratégia is prioritásként említi a kibertérből érkező kihívásokra való felkészülést. A 2013-ban kiadott Nemzeti Kiberbiztonsági Stratégia határozza meg nemzeti érdekként a kibertér védelmét, illetve az ország szuverenitásának biztosítását a kibertérben is.[20] A stratégia alapján az ország fontosnak tartja, hogy a NATO 5. cikkelye a kibertérből érkező támadásokra is kiterjeszthető, ami által a kollektív védelem a kibertérben is lehetővé teszi a szövetségesek együttműködését. Kormányzati szinten a kiberbiztonság irányításáért a Koordinációs Tanács felel, amelyben az összes érintett kormányzati szereplő képviselteti magát. Operatív szinten a Nemzetbiztonsági Szakszolgálat keretein belül működő Nemzeti Kibervédelmi Intézet jár el, de más társszervezetek is közreműködnek a biztonsági kihívások kezelésében.

A négy közép-európai ország röviden bemutatott kiberbiztonsági stratégiái az elmúlt évek során egyre átfogóbbá váltak, és igyekeznek azt a holisztikus szemléletmódot és megközelítést hatékonyan alkalmazni, amit a kiberbiztonság multidimenzionális jellege megkövetel. Ennek következtében a stratégiák a kiberbiztonság gazdasági, szociális, jogi,

[16] National Security Strategy of The Republic of Poland, [online], 2007. Forrás: ETH Zürich [2010. 03. 06.].
[17] Cyberspace Protection Policy of The Republic of Poland, [online], 2013. 06. 25. Forrás: ENISA [2014. 09. 23.].
[18] National Strategy for Information Security in the Slovak Republic, [online]. Forrás: ENISA [2014. 09. 22.].
[19] Cyber Security Concept of the Slovak Republic for 2015-2020, [online]. Forrás: ENISA [2016. 01. 21.].
[20] 1139/2013. (III.21.) Korm. határozat, Magyarország Nemzeti Kibervédelmi Stratégiája: *i. m.*

rendvédelmi, katonai és hírszerző aspektusaira egyaránt kitérnek, sőt egyes esetekben rugalmasabb megközelítést alkalmazva az egyéni dimenzió is kiemelésre kerül. Mindegyik ország megértette az összefüggést a kiber- és a nemzetbiztonság között, tisztában vannak vele, hogy az infokommunikációs rendszerek vagy a kritikus infrastruktúrákat üzemeltető informatikai rendszerek működésének megzavarása, illetve leállítása rendkívül súlyos nemzetbiztonsági kockázatot hordoz magában.

Jelentős különbség azonban a kiberbiztonság problémakörének megközelítésében, hogy míg a cseh, a szlovák és a magyar modell esetében főként a polgári nemzetbiztonsági szervezetek felelősek a kibertér biztonságának szavatolásáért, addig a lengyel modell az északi és balti mintákat követve a katonai struktúrákon belül koordinálja a kiberbiztonsági kihívások kezelését. A lengyel sajátosságok közül külön kiemelendő még, hogy az az egyetlen stratégia, amely a védelmi képességek mellett a támadó képességek kifejlesztését is előírja annak érdekében, hogy az ország ellenfeleit képesek legyenek elrettenteni a kibertérben. Míg Lengyelország egyértelműen meghatározza a kritikus infrastruktúrák és a kiberbiztonság közötti kapcsolatot, ami az ország működéséhez és gazdasági fejlődéséhez nélkülözhetetlen, addig a szlovák és a magyar modell inkább információbiztonsági megközelítést alkalmaz, és nem hivatkozik konkrét védelemre szoruló elemekre a kibertérben.

Összegzés

Elmondható, hogy a négy visegrádi ország kiemelten kezeli a kibertérből érkező globális kihívásokat, ugyanakkor – különböző megközelítéssel – eltérő modellek gyakorlati megvalósításával igyekeznek megteremteni a kibertér biztonságos használatának feltételeit. Bár mindegyik stratégia említést tesz a kritikus infrastruktúrák jelentőségéről és a kiberbűnözés szerepéről, a biztonsággal összefüggésben eltérő szemléletmódot alkalmaznak. Eltérések látszanak az elsődlegesen védendő elemek, a fenyegetések és kihívások rangsorolása, valamint a fenyegetések forrásainak meghatározása terén. További különbségek mutatkoznak az alkalmazott terminológia kapcsán, ami sok esetben félreértésre adhat okot az együttműködési törekvések során.

A kiberbiztonság Lengyelország által követett erősen militarizált megközelítése a cseh, a szlovák és a magyar szemléletmódtól eltér, ennek megfelelően utóbbiak stratégiai dokumentumai kevésbé pontosan fogalmaznak a nemzetbiztonsági szempontból kiemelt védelemre szoruló elemek tekintetében. Szintén ebből az eltérő megközelítésből fakad, hogy a lengyel dokumentumok a kiberbiztonsági kihívásokat veszélyesnek tartják az állam alapvető működésére, és ebből kifolyólag a kibertámadások kezelését főként a haderőre, illetve a védelmi szféra intézményeire alapozzák. Míg a lengyel megközelítés alapvetően a más államok által elkövetett kibertámadásokat tekinti elsődleges kihívásnak, addig a cseh, a szlovák és a magyar szemléletmód a kiberbiztonsági kihívások kriminalizálására fekteti a hangsúlyt. Ennek a hangsúlyeltolódásnak köszönhető, hogy a visegrádi négyek (V4) közül három országban a polgári nemzetbiztonsági szervek felelősségi területe a kiberbiztonság, és csupán kockázatként tekintenek a kibertérrel összefüggő biztonsági kérdésekre.

A kibertér globális trendjeinek tükrében a nemzeti szinten zajló kiberbiztonsági folyamatok előremutató megközelítésről tanúskodnak a V4-országok kormányai részéről, azon-

ban a szemléletmódban kirajzolódó különbségek több kérdést is felvetnek akkor, amikor egy vagy több ország a nemzeti szintű erőfeszítéseket nemzetközi szinten is alkalmazni szeretné. Végső soron az említett eltérések és hangsúlyeltolódások elvezethetnek oda, hogy a lengyel fél számára a jövőben több eredménnyel kecsegtet egy, az északi vagy balti országokkal kialakított nemzetközi együttműködés, miközben az erőforrások korlátozottsága miatt a többi kezdeményezés kevesebb figyelmet kap.

FELHASZNÁLT IRODALOM

1139/2013. (III.21.) Korm. határozat, Magyarország Nemzeti Kibervédelmi Stratégiája, [online], *Magyar Közlöny,* 2013/47, 3. pont [2013. 04. 02.]

Allen, Robert: What happens online in 60 seconds?, [online], 2017. 02. 06. Forrás: Hubspot [2017. 02. 20.]

Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér, [online], 2013, 3. o. Forrás: Európai Bizottság [2016. 05. 01.]

Berzsenyi Dániel – Ványi Rajmond: Egy katonapolitikai döntés lehetséges kiberbiztonsági következményei – Az Iszlám Állam elleni magyar katonai szerepvállalás margójára, [online], *Nemzet és Biztonság,* 8. évf., 2015/3, 134–143.

Cyber Security Concept of the Slovak Republic for 2015-2020, [online]. Forrás: ENISA [2016. 01. 21.]

Cyberspace Protection Policy of The Republic of Poland, [online], 2013. 06. 25. Forrás: ENISA [2014. 09. 23.]

Evans, Dave: The Internet of Things How the Next Evolution of the Internet Is Changing Everything, [online], 2011, 4. Forrás: CISCO [2016. 10. 04.]

ICT Facts And Figures, [online], 2016. 06. Forrás: ITU [2016. 07. 26.]

Internet of Things market to triple to $1.7 trillion by 2020: IDC, [online], 2015. 06. 02. Forrás: Reuters.com [2016. 10. 05.]

Klimburg, Alexander (ed.): National Cyber Security Framework Manual, [online], 2012, 8. o. Forrás: NATO CCD COE [2013. 04. 20.]

Mészáros Csaba: Fenyegetések internete, [online], 2016. 12. 22. Forrás: Computerworld [2016. 12. 29.]

National Cyber Security Strategy of The Czech Republic, [online]. Forrás: ENISA [2014. 12. 11.]

National Cyber Security Strategy of The Czech Republic for The Period from 2015 to 2020, [online]. Forrás: ENISA [2016. 02. 11.]

National Security Strategy of The Republic of Poland, [online], 2007. Forrás: ETH Zürich [2010. 03. 06.]

National Strategy for Information Security in the Slovak Republic, [online]. Forrás: ENISA [2014. 09. 22.]

Overview of the Internet of things, [online], 2012. 06. Forrás: ITU [2016. 07. 21.]

Perrin, Chad: The CIA Triad, [online], 2008. 06. 30. Forrás: TechRepublic [2016. 05. 01.]

Project the 'Things' Behind the Internet of Things, [online]. Forrás: CompTIA [2016. 10. 04.]

Rendszeres internethasználók aránya (2005–2016), [online]. Forrás: KSH [2017. 01. 20.]

Tumkevic, Agnija: Cybersecurity in Central Eastern Europe: From Identifying Risks To Countering Threats, [online], 2016. 12. Forrás: Baltic Journal of Political Science [2017. 05. 01.]

The Internet of Everything: 2014, [online]. Forrás: Business Insider [2016. 10. 05.]

World Population Prospects, [online], 2015. Forrás: UN Economic & Social Affairs [2016. 07. 26.]