HADTUDOMÁNYI SZEMLE
12. évfolyam (2019) 4. szám 27–34. • DOI: 10.32563/hsz.2019.4.3

Hronyecz Erika[1]

A Visegrádi Csoport szerepvállalása a kiberbiztonság területén

Engagement of the Visegrád Group in the Field of Cyber Security

Absztrakt

A Visegrádi Együttműködés fő célja, hogy az Európai Uniót érintő kérdésekben lehetőség szerint közös álláspontot alakítsanak ki és képviseljenek a hatékonyabb fellépés és érdekérvényesítés tekintetében, hiszen a négy ország önmagában a lakosságszámot, a gazdasági, illetve a katonai erőt tekintve nem képvisel számottevő súlyt az EU többi tagállamához viszonyítva. Az együttes fellépéssel viszont komolyabb politikai jelentőséggel bírnak, nagyobb ráhatással tudnak lenni az Európai Unión belül az őket érintő kérdéseket és intézkedéseket illetően. A Visegrádi Csoport számos területen törekszik a régión belüli helyét és szerepét erősíteni az egyéb szakterületeken történő összefogással, ide tartozik a kiberbiztonság is.

Kulcsszavak: *Visegrádi Csoport, kiberbiztonság, regionális együttműködés, regionális biztonság*

Abstract

The main objective of the Visegrád Cooperation is to develop common positions on issues affecting the European Union in terms of more effective action and advocacy, since the four countries alone do not represent a significant population, economic or military strength compared to other EU member states. However, acting together is of greater political importance, with greater influence within the European Union

[1] Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, doktorandusz – National University of Public Service, Doctoral School of Military Sciences, PhD student, e-mail: hronyecz.erika@gmail.com, ORCID: https://orcid.org/0000-0003-2002-8521

on issues and measures affecting them. The Visegrád Group strives to strengthen its position within the region and strengthen its role in cooperation with other areas of expertise, including cyber defence.

Keywords: *Visegrád Group, cyber security, regional cooperation, regional security*

Bevezetés

Lengyelország, Csehszlovákia és Magyarország vezetői 1991. február 15-én Visegrádon aláírták azt a nyilatkozatot, amellyel létrejött a Visegrádi Együttműködés. A Visegrádi Csoport országait több olyan tényező és egységes cél kötötte össze – a földrajzi kapcsolatok, a történelmi tradíciók, az euroatlanti biztonsági rendszer, az euroatlanti szervezetekhez való társulás –, amelyek erősítették az együttműködés létrejöttét és további funkcionalitását. A deklaráció céljai között szerepelt az előző rendszer maradványainak felszámolása, a demokrácia védelme és ezek mellett a részt vevő országok gyors és gördülékeny csatlakozásának elősegítése az euroatlanti szervezetekhez.

A múltat tekintve a legnyilvánvalóbb és leglogikusabb irány a jövőt illetően a Nyugat felé történő politikai és gazdasági orientáció volt. 1993-ban Csehszlovákia felbomlásával négytagúvá vált a Visegrádi Együttműködés. Az 1990-es évek közepén stagnálni látszott a Visegrádi Négyek aktivitása, de az évtized végétől ismét komolyabb intenzitás jellemezte a négy ország együttműködését, hiszen az ezredforduló küszöbén felgyorsultak a nemzetközi események is az Észak-atlanti Szerződés Szervezetéhez (a továbbiakban: NATO) és az Európai Unióhoz (a továbbiakban: EU) való csatlakozásuk miatt. 2004. május 1-jétől mind a négy állam már tagja volt a NATO-nak és az Európai Uniónak egyaránt, elérve ezzel legfontosabb politikai céljukat mind állami, mind regionális szinten, az euroatlanti integrációt.

Az együttműködés új dimenziója

Az elért sikerek után 2004. május 12-én a négy ország – Cseh Köztársaság, Szlovák Köztársaság, Lengyel Köztársaság és a Magyar Köztársaság – miniszterelnökei a Kroměříž városában zajló V4-es csúcstalálkozón egy új nyilatkozatot fogadtak el, ami felváltotta a csoport létrehozásáról szóló 1991-es dokumentumot. A V4-ek képviselői bejelentették, hogy elérték a korábban megfogalmazott célkitűzéseiket és kinyilvánították, hogy immár a NATO és az EU tagjaiként is eltökéltek az együttműködés folytatásában és elmélyítésében. Erőfeszítéseiket és célkitűzéseiket továbbra is a közép-európai régió identitását erősítő regionális tevékenységekre és kezdeményezésekre összpontosítják, a megvalósítás folyamatát pedig konkrét projekteken alapuló rugalmas és nyitott jellegű kooperáció keretében tervezik véghezvinni. A Visegrádi Csoport országai határozottan elkötelezettek abban, hogy közösen járuljanak hozzá az EU közös céljainak teljesítéséhez és az európai integráció sikeres folytatásához, tudásuk és tapasztalataik megosztásával segítsék az EU-ba csatlakozni kívánó országokat. Készek arra is, hogy a közös érdekű területeken a szélesebb régió országaival, más európai regionális csoportokkal, valamint harmadik országokkal és nemzetközi szervezetekkel is

együttműködjenek. A Visegrádi Együttműködés elsődleges célja, hogy az Európai Uniót érintő kérdésekben lehetőség szerint közös álláspontot alakítsanak ki és képviseljenek a hatékonyabb fellépés és érdekérvényesítés tekintetében, hiszen a négy ország önmagában a lakosságszámot, a gazdasági, illetve a katonai erőt tekintve nem képvisel számottevő súlyt az EU többi tagállamához viszonyítva. Az együttes fellépéssel viszont komolyabb politikai jelentőséggel bírnak, nagyobb ráhatással tudnak lenni az Európai Unión belül az őket érintő kérdéseket és intézkedéseket illetően.

A Visegrádi Csoport miniszterelnökei mély meggyőződésüket fejezték ki azzal kapcsolatban, hogy a tagországok közös igyekezetükkel és munkájukkal hozzájárulnak egy újraegyesített, demokratikus és virágzó Európa építéséhez. Az együttműködés területeit az alábbi pontokban fogalmazták meg:

- kultúra;
- oktatás, ifjúsági cserék, tudomány;
- a Visegrádi Együttműködés civil dimenzióinak megerősítése a Nemzetközi Visegrádi Alapban és annak struktúráiban;
- határokon átnyúló együttműködés;
- infrastruktúra;
- környezet;
- terrorizmus, a szervezett bűnözés és az illegális migráció elleni küzdelem;
- schengeni együttműködés;
- katasztrófavédelem;
- eszmecsere a munka- és a szociálpolitika területén folytatott lehetséges együttműködésről;
- tapasztalatcsere a külföldi fejlesztési támogatási politikáról;
- hadiipar.[2]

A 2000-es évek közepétől globális szinten új típusú, biztonságot fenyegető kihívások jelentek meg, úgymint terrorizmus, ember- és kábítószer-kereskedelem, szervezett bűnözés, kibertérbeli bűnözés, amelyekkel a tagországok is szembesülni kényszerültek. A fent említett új típusú biztonsági kihívások megelőzése és ellensúlyozása komoly feladat elé állítja a nemzeteket. Biztonságpolitikai szempontból a V4-országok esetében egységesen kiemelt szereppel bír a kiberbiztonság kérdése. A kritikus információs infrastruktúra védelmére a 2000-es évek végétől egyre több figyelem összpontosult, hiszen ezek a rendszerek több szempontból és számos módon könnyen sebezhetővé válhatnak, és a sérülékenységeken keresztül egy teljes ország, sőt akár egy egész régió is támadható gazdasági, pénzügyi, közigazgatási szektorokon át egészen a védelmi szféráig. Az adott területen működő rendszerek hosszabb vagy rövidebb ideig, részlegesen vagy akár teljes egészében működésképtelenné válhatnak egy célzott támadás

[2] The Kroměříž Declaration – Declaration of Prime Ministers of the Czech Republic, the Republic of Hungary, the Republic of Poland and the Slovak Republic on cooperation of the Visegrad Group countries after their accession to the European Union, 12 May 2004, www.visegradgroup.eu/2004/declaration-of-prime (Letöltve: 2019. 04. 02.)

esetén.[3] A kiberbiztonság területe globális szinten állandó fejlesztés alatt áll – állandóan újradefiniálja magát és határait.[4]

A tagországok infokommunikációs fejlettsége nagymértékben meghatározza a kibervédelemre irányuló tevékenységének hatásfokát. A magasfokú biztonság elérésének egyik mérőeleme lehet a fejlett infokommunikációs eszközök, rendszerek alkalmazása. Az ENSZ infokommunikációs technológiákkal foglalkozó szervezete a Nemzetközi Távközlési Egyesület (ITU: International Telecommunication Union) feladata a távközlési ágazat összehangolása globális szinten, a távközlési szolgáltatások használatának elősegítése érdekében. Az ITU évenként elvégzi az országok infokommunikációs technológia (IKT) fejlesztésére irányuló méréseit, amelyet a honlapján közread. A méréseket 11 indikátor figyelembevételével végzi el, majd az IDI (ICT Development Index) elnevezésű referenciaértékben összesíti azokat. Az IDI indikátorai az alábbiakból tevődnek össze:

- az IKT-fejlesztések szintje és alakulása, valamint az országok ezirányú tapasztalatai egymáshoz viszonyítva;
- az IKT-fejlesztések a fejlett és fejlődő országokban;
- az államok közötti különbségek az IKT-fejlesztés szintjei tekintetében (digitális szakadék);
- az információs és kommunikációs technológiák fejlesztési potenciálja és annak mértéke, hogy az országok milyen mértékben használhatják fel őket a növekedés és a fejlődés javítása érdekében a rendelkezésre álló képességek és készségek összefüggésében.[5]

A 2009 óta elérhető adatok megmutatják, hogy az országok milyen fejlettségi szintet értek el. Az 1. táblázat összehasonlításképpen a V4-tagállamok és Ausztria adatait mutatja be a 2016. évi és a 2017. évi adatok alapján, amelyekből leolvasható, hogy a négy plusz egy országból Ausztria, Lengyelország és Magyarország tudott felmutatni előrelépést, Csehország és Szlovákia az összesített adatok alapján hátrébb csúszott az előző évhez képest.

[3] Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, *Nemzet és Biztonság,* 10 (2017/1) 3–16.

[4] Strengthening the Eastern Frontier, http://europeum.org/data/articles/v4-security-strengthening-the-eastern-frontier-of-the-v4.pdf (Letöltve: 2019. 05. 30.)

[5] The ICT Development Index (IDI): conceptual framework and methodology, www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx (Letöltve: 2019. 05. 26.)

1. táblázat: *A V4-tagállamok és Ausztria IKT-fejlettsége 2016-ban és 2017-ben*

ORSZÁG	IDI		HELYEZÉS	
	2016	2017	2016	2017
Csehország	7,06	7,16	39	43
Lengyelország	6,73	6,89	50	49
Magyarország	6,74	6,93	49	48
Szlovákia	6,84	7,06	46	47
Ausztria	7,7	8,02	24	21

Forrás: ITC Development Index 2017. www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017byregion-tab alapján szerkesztette a szerző (Letöltve: 2019. 05. 30.)

Közép-európai Kiberbiztonsági Platform – kibervédelmi együttműködés a V4-ek keretén belül

A Visegrádi Csoport országainál a hasonló földrajzi, történelmi, kulturális és politikai környezetből kifolyólag számos területen hasonló problémák is merülnek fel, amelyek lassíthatják az általános fejlődést. E problémák mennyiségét, mélységét, illetve az általuk generált negatív következményeket csökkenthetik a térségen belüli együttműködés erősítésével. A V4-országok felismerték, hogy szükségszerű a regionális kooperáció a kibervédelem területén is, hiszen e terület biztonsága komoly hatással van a biztonság többi – katonai, politikai, gazdasági, társadalmi és környezeti – szektorára is.

Előzetes egyeztetéseket követően Csehország, Lengyelország, Szlovákia, Magyarország és Ausztria részvételével 2013-ban megalakult a Közép-európai Kiberbiztonsági Platform (Central European Cyber Security Platform – a továbbiakban: CECSP), az első hivatalos ülésre 2013. május 27–29. között került sor Prágában. A V4-országokból a kormányzati és nem kormányzati eseménykezelő központok (CERT: Computer Emergency Response Team), Ausztria részéről a katonai eseménykezelő központ (MilCERT) meghívott képviselői megtárgyalták az adott időszakban aktuális kiberbiztonsági helyzetüket, különös tekintettel a vonatkozó jogi háttérre, a technikai képességekre és gyakorlatokra. A CECSP célja – mint a Visegrádi Csoporton belüli együttműködés döntő többségének – a közép-európai régió biztonságának erősítése, a platform esetében a kibervédelem területére vonatkoztatva. A CECSP egyfajta koordinációs testületként hivatott működni, az államok közötti bizalomra és információmegosztásra épül, és feladatául a kiberbiztonság regionális szintű fokozását tűzték ki. A CECSP a Cseh Köztársaság által kidolgozott deklaráción alapul, amelyet 2013-ban alá is írtak az érintett országok.[6] A CECSP-n belüli részvétel önkéntes

[6] Packa, Roman – Ulmanova, Martina: CECSP: Towards effective collaboration on cyber security in Central Europe, *Cyber Security Review*, Winter 2014/15, 12–16.

alapon működik, így az államok közötti bizalom döntő fontossággal bír. A képviselők csak abban az esetben képesek az információmegosztásra, ha megbízható környezet áll fenn. Hogy melyik ország tölti be az adott évben az elnöki szerepet, azt az országok neveinek ábécés sorrendje szabja meg. Azt is meghatározták, hogy az elnökségi tagok a platformon évente legalább kétszer részt vesznek, magasabb szinten pedig évente egyszer. A találkozókat az éppen aktuális elnöki szerepet betöltő ország szervezi. Lefektették továbbá, hogy az adott országok CERT-jeinek legalább háromévente közös kiberbiztonsági gyakorlatot kell lebonyolítani. A CECSP-együttműködésnek számos célkitűzése van, amelyeket a deklaráció részletesen megfogalmaz. A tagállamok legfontosabb vállalásai a következők:

- erősítik képességeiket;
- rendszeresen megosztják az információkat, a legjobb és leghatékonyabb gyakorlatokat;
- közös képzés, oktatás és gyakorlatok szervezését;
- biztonságos kommunikációs csatornák tervezését és megvalósítását;
- nemzetközi fórumok előtt az egyéni álláspontok összehangolását;
- egységes definiálásra és besorolási rendszerre való törekvés az érzékeny adatokat illetően;
- koordinált kutatás és fejlesztés;
- gyakorlati munkacsoportok létrehozása.

Hosszú távú célok közé sorolható a kibervédelmi tudatosság növelése és a kockázatkezelés módszereinek harmonizálása regionális szinten. A kiberbiztonság területén a V4 országai természetesen aktív résztvevői az egyéb kiemelt szereppel bíró nemzetközi együttműködéseknek, úgymint NATO, EU, EBESZ, ENSZ, és fontos kiemelni, hogy a CECSP-országok kiberbiztonsági stratégiáinak mindegyike figyelembe is veszi az EU és a NATO elvárásait.[7]

A CECSP eddig elért eredményei

A CECSP keretén belül a kezdeti időszakban igen magas aktivitást mutattak a tagországok. A megalapítást követő találkozókon a részt vevő államok ismertették a kibervédelemmel kapcsolatos szabályozási rendjüket, aktuális helyzetüket, a szakterület kihívásainak kezelésére kialakított nemzeti álláspontjukat, illetve megvitatták a regionális együttműködés gyakorlati aspektusait.

Az első közös kibervédelmi gyakorlatot – aminek házigazdája Magyarország volt – 2014. június 23-án rendezték meg. A gyakorlaton a CECSP-országok különböző szintű kormányzati és katonai szervezeteinek képviselői vettek részt, aktív játékos vagy megfigyelői szerepkörökben. A gyakorlatot számos munkacsoportülés előzte meg, amelyeken a technikai hibaelhárításért, behatárolásért felelős szervezetek képviselői is részt vettek, ezzel is biztosítva, hogy a megoldandó feladatok a valós életben

[7] Berzsenyi Dániel: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése, *Nemzet és Biztonság,* 7 (2014/6) 131–136.

előforduló kihívásokat mutassanak. A gyakorlat során a rendezők olyan technikai jellegű, haktivistacsoportok tevékenységét magába foglaló, kormányzati és katonai oldalak tartalmának megváltoztatására irányuló támadássorozatot modelleztek, amely alkalmas volt a belső eljárásrendek tesztelésére, a várható reakcióidők modellezésére, az esetlegesen meghozandó kiegészítő intézkedések elemzésére.[8] Az államok közötti együttműködés hajlandóságát és egyben hatékonyságát először ezen a gyakorlaton lehetett lemérni. Az esemény a tapasztalatokat és eredményeket illetően sikeresnek volt mondható.

2016. május 23–24. között Brnoban is tartottak egy gyakorlatot, amelyet a Cybernetic Proving Groundban rendeztek meg a Masaryk Egyetem részét képező Institute of Computer Science (ICS) területén. Az esemény zárt, speciálisan módosított technikai környezetben, szimuláció formájában zajlott, amely jellegénél fogva lehetővé teszi az ilyen technikákat és manipulációt olyan tartalommal felruházni, amelyek komoly veszélyt jelentenek egy nyitott hálózaton. A külföldi résztvevőknek egyedülálló esélyük volt arra, hogy megvédjék az adott hálózatot a számítógépes támadások ellen. A játékosok a meghívott országok kormányzati vagy nemzeti CERT-csapatai, szakértői voltak. A kis csapatokra osztott résztvevők hat órán át tartó kibertámadásokkal szembesültek, és mind az alapvető, mind a kifinomultabb eseményeket kezelniük kellett. A játékosok technikai készségeit tesztelték, és hangsúlyt fektettek az egymás közötti, illetve más szervekkel, szervezetekkel történő információcsere fontosságára. Céljuk és feladatuk nemcsak a támadásokra és a technikai problémákra való reagálás volt, hanem a média szerepvállalásának, jelenlétének kezelése is komolyabb odafigyelést igényelt a gyakorlatban résztvevő személyektől, csapatoktól. A média jelenlétének köszönhetően megnövekedett stresszkörnyezetben dolgozhattak, éppúgy, mint a valós világ kiberbiztonsági válsága esetében. A gyakorlat alapja egy olyan forgatókönyv volt, amely tükrözte a valós világban tapasztalható eseményeket és tanulságokat.[9]

Összességében megállapítható, hogy bár a tagok komoly figyelmet fordítottak egy bizalommal és elkötelezettséggel jellemezhető környezet kialakítására, az utóbbi két évben mégis érezhető több állam részéről az információmegosztás aktivitásának csökkenése, ami egyértelműen visszaveti a hatékony és fokozottabb ütemű feladatellátást, ennek következményeként az együttműködés eredményességét.

Következtetések

Napjainkban a biztonság dimenziói minden részelemének kezelése nemzetközi szinten egyértelműen kooperatív jellegű hozzáállást, összefogást és munkát igényel. A kiberbiztonság területét tekintve sok esetben már az is kihívás, hogy két ország egyezségre jusson adott kérdéseket, illetve megállapodásokat illetően, több szereplő esetén ez többszörösen nehezebb próbatételnek bizonyul. Minden állam egyéni felelőssége, hogy olyan stratégiát dolgozzon ki az információs infrastruktúra védelme érdekében,

[8] Draveczki-Ury Ádám: Szoros együttműködés a kibertérben, 2014, https://honvedelem.hu/cikk/szoros-egyuttmukodes-a-kiberterben/ (Letöltve: 2019. 12. 18.)

[9] National Cyber Security Centre held exercise for CECSP partners, 2017, www.govcert.cz/en/info/events/2532-national-cyber-security-centre-held-exercise-for-cecsp-partners/ (Letöltve: 2019. 05. 30.)

amelyre alapozva képes megelőzni, illetve ellensúlyozni a szektort érintő fenyegetéseket mind napjainkban, mind az elkövetkezendő évekre vonatkozóan. Viszont az is tény, hogy a kibertámadások sokszor országhatárokon átnyúló jellegéből adódóan az egyes államok nem képesek önállóan kezelni az ilyen típusú fenyegetéseket, a hatékony és legjobb megoldás alkalmazását illetően szükségszerű a nemzetközi szintű együttműködés. Ennek alapja azonban a megfelelő szintű bizalom, ez kulcsfontosságú tényező a közép-európai kibertér regionális szintű biztosításához.

A tanulmány az Emberi Erőforrások Minisztériuma ÚNKP-18-3-IV-NKE-77 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

Felhasznált irodalom

Berzsenyi Dániel: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése, *Nemzet és Biztonság,* 7 (2014/6) 110–136.

Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, *Nemzet és Biztonság,* 10 (2017/1) 3–16.

Packa, Roman – Ulmanova, Martina: CECSP: Towards effective collaboration on cyber security in Central Europe, *Cyber Security Review,* Winter 2014/15, 12–16.

Internetes források

Draveczki-Ury Ádám: Szoros együttműködés a kibertérben, https://honvedelem.hu/cikk/szoros-egyuttmukodes-a-kiberterben/ (Letöltve: 2019. 12. 18.)

ICT Development Index 2017, www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017-byregion-tab (Letöltve: 2019. 05. 30.)

The ICT Development Index (IDI): conceptual framework and methodology, 2017, www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx (Letöltve: 2019. 05. 26.)

The Kroměříž Declaration – Declaration of Prime Ministers of the Czech Republic, the Republic of Hungary, the Republic of Poland and the Slovak Republic on cooperation of the Visegrad Group countries after their accession to the European Union, 12 May 2004, www.visegradgroup.eu/2004/declaration-of-prime (Letöltve: 2019. 04. 02.)

National Cyber Security Centre held exercise for CECSP partners, 2017, www.govcert.cz/en/info/events/2532-national-cyber-security-centre-held-exercise-for-cecsp-partners/ (Letöltve: 2019. 05. 30.)

Strengthening the Eastern Frontier, http://europeum.org/data/articles/v4-security-strengthening-the-eastern-frontier-of-the-v4.pdf (Letöltve: 2019. 05. 30)