sciendo

Műszaki Tudományos Közlemények vol. 11. (2019) 89–92.
https://doi.org/10.33895/mtk-2019.11.18
https://eda.eme.ro/handle/10598/31213
Angol nyelven: https://doi.org/10.33894/mtk-2019.11.18

EME MTSZ MTK

AZ EBESZ ÉS A V4-EK SZEREPE ÉS JELENTŐSÉGE A KIBERBIZTONSÁG TERÜLETÉN

THE ROLE AND IMPORTANCE OF THE OSCE AND THE V4 IN CYBERSECURITY

Hronyecz Erika

Nemzeti Közszolgálati Egyetem, Budapest, Magyarország, hronyecz.erika@gmail.com

Abstract

From the mid-2000s new types of security challenges have emerged at global level. Their prevention, management and recovery, given their characteristics, is serious challenge for the countries. The cyber security challenges require special attention and close interaction both at national and international levels. In this paper the author presents the highlights of OSCE and V4 cooperation on cyber defense.

Keywords*: cybersecurity, V4, OSCE, Central European Cyber Security, regional cooperation.*

Összefoglalás

A 2000-es évek közepétől globális szinten olyan új típusú biztonsági kihívások jelentek meg, melyek megelőzése, kezelése és helyreállítása jellemzőiknél fogva komoly feladat elé állították az országokat. A kiberbiztonsági kihívások kiemelt figyelmet, szoros interakciót követelnek meg nemcsak nemzeti, hanem nemzetközi szinten is. Jelen tanulmányban a szerző az EBESZ és a V4-ek kibervédelemre vonatkozó együttműködési tevékenységének kiemelt pontjait mutatja be.

Kulcsszavak*: kiberbiztonság, V4-ek, EBESZ, Közép-európai Kiberbiztonsági Platform, regionális együttműködés.*

1. Bevezetés

A kiberbiztonság a fejlett társadalmak, a modern világ egyik legfontosabb kihívása. A kibertérben megjelenő kihívások és veszélyek száma és gyakorisága állandó készenlétre kényszerít minden olyan nemzeti és nemzetközi szervezetet, melyek feladata és célja az ilyen típusú események megakadályozása, illetve kezelése.

A biztonság korábbi értelmezése alapján öt szektort különböztettünk meg: katonai szektor, politikai szektor, gazdasági szektor, társadalmi szektor és környezeti szektor. A 2010-es évektől azonban a fent említett öt szektor mellett erőteljesen körvonalazódott és megjelent az informatikai szektor is, mely gyors ütemben kibontakozó terület a biztonsági tanulmányok keretén belül.[1]

A kiberbiztonsági eseményekre jellemző, hogy kiszámíthatatlanok, gyakoriak, nagyon rövid időn belül alakulnak ki és gyakran országhatárokon átnyúló, egyszerre több országot érintő kiterjedéssel bírnak. Mindezt figyelembe véve kiemelkedő szerepe van a nemzetközi szintű összefogásnak. Kiberbiztonság területén általában két állam közötti megállapodás is rendkívül komplikált kihívás tud lenni az eltérő nemzeti érdekek, értékek és célok tekintetében, ezt alapul véve regionális szinten ez többszörösen nehéznek bizonyul.

2. Az EBESZ szerepvállalása a kiberbiztonság tekintetében

Az elmúlt másfél évtizedben az új típusú biztonsági kihívások hatására az EBESZ is felismerte, hogy alkalmazkodnia kell az új biztonsági környe-

zet okozta elvárásokhoz. Az Európai Biztonsági és Együttműködési Szervezet nagy múlttal rendelkező, 57 európai, észak-amerikai és közép-ázsiai részt vevő államból és 11 partnerállamból álló páneurópai biztonsági szervezet. Az EBESZ a biztonságot átfogó és kooperatív módon értelmezi és kezeli, ami abban nyilvánul meg, hogy a biztonság minden területével, szektorával egységesen foglalkozik és mind az 57 részes állama egyenlő jogokkal rendelkezik. A Szervezet legfontosabb rendeltetése az európai biztonság és stabilitás megőrzése, a korai előrejelzés, a konfliktuske-zelés, a válságkezelés és a válságok megoldását követő helyreállítási folyamatok rendezése, lebonyolítása. Az EBESZ folyamatosan alkalmazkodik az új biztonsági környezet okozta elvárásokhoz és felvette a küzdelmet az új típusú fenyegetések ellen, úgy mint terrorizmus, ember-és kábítószer kereskedelem, szervezett bűnözés, kibertérbeli bűnözés.

Az EBESZ Állandó Tanács hogy fokozza az egyéni és kollektív erőfeszítéseket az információs és kommunikációs technológiák (Information and Communications Technologies - ICTs) átfogó kezelése érdekében, 2012. április 29-én a 1039. számú döntése alapján létrehozta a kiberügyekkel foglalkozó informális munkacsoportot (Informal Working Group – IWG). A munkacsoport feladatául kiberbiztonsági bizalomépítő intézkedések (Confidence Building Measures – CBMs) kidolgozását határozták meg az államközi együttműködés, átláthatóság, kiszámíthatóság és stabilitás érdekében, illetve az IKT-k használatából eredő félreértések, eszkalációk és konflikutsok kockázatának csökkentése céljával. Az összesen 16 CBM-et tartalmazó 1202-es döntés alapján összegezve a következő feladatokat vállalták a részt vevő országok:

- önkéntesen megosztják egymással nemzeti álláspontjukat a nemzeti és transznacionális fenyegetések különböző aspektusairól és az IKT-k használatáról.
- önként elősegítik a kompetens nemzeti szervezeteik közötti együttműködést és információcserét az IKT-k vonatkozásában
- önkéntes alapon konzultációkat tartanak az IKT-k használata kapcsán felmerülő félreértésekből adódó politikai és katonai feszültségek csökkentésének céljából
- önként megosztják a nyílt, interoperábilis, biztonságos és megbízható internet biztosításának céljából meghozott intézkedéseiket
- az EBESZ-t párbeszédek lefolytatására, jó gyakorlatok megosztására, az IKT-k biztonságára vonatkozó kapacitásnövelés megvitatására. és egyes támadásokra adott hatékony válaszlépések megosztására alkalmas platformként kezelik és alkalmazzák
- olyan nemzeti szabályozásokat hoznak létre, melyek lehetővé teszik a kompetens hatóságok – kiemelten a bűnüldöző szervek - közötti kétoldalú együttműködéseket
- önként megosztják a nemzeti stratégiáikat, irányelveiket és programjaikat, beleértve együttműködésüket a köz- és a magánszférával, illetve az IKT-k biztonságát és alkalmazását
- kijelölnek egy kapcsolattartó pontot, megosztják a nemzeti struktúra egyes elemeihez tartozó kapcsolattartási adatokat, melyeket egy esetleges incidens alkalmával használnak és ezen adatokat évente frissítik
- a közös terminológia hiányából adódó esetleges félreértések elkerülése végett egy magyarázatokkal és definíciókkal ellátott listát készítenek az IKT-k használatára és biztonságára vonatkozó terminológiákról
- a CBM-ekkel kapcsolatos kommunikáció megkönnyítése érdekében EBESZ platformok és mechanizmusok felhasználásával önkéntes alapon folytatnak eszmecserét
- a kijelölt tagállami szakértők szintjén évente legalább 3 alkalommal találkoznak az IWG keretein belül a bizalomerősítő intézkedések tárgyalását, megvalósítását és továbbfejlesztését illetően
- workshopok, szemináriumok, kerekasztal beszélgetések szervezése és megtartása által támogatják az információmegosztást és az államok közötti információ cserét
- elősegítik, hogy tisztviselőik és szakértőik védett, engedélyezett csatornákon keresztül kommunikáljanak a lehetséges félreértések, konfliktusok és eszkalációk megelőzése és csökkentése érdekében
- népszerűsítik a köz- és magánszféra közötti együttműködéseket
- elősegítik a regionális és kistérségi együttműködés kiépítését a kritikus infrastruktúrák biztonságáért felelős hatóságok között
- ösztönzik a felelős információmegosztást az IKT-k biztonságát és használatát érintő sérülékenységekre vonatkozóan, hiszen minden ilyen jellegű tájékoztatás és kommunikáció elősegíti az EBESZ-t érintő régión belüli együttműködéseket.[2]

A munkacsoport az EBESZ elnöksége által évente kinevezett elnök vezetése alatt működik és törekszik az EBESZ által elfogadott bizalomerősítő

intézkedések végrehajtására vonatkozó javaslatok kidolgozását vállaló országok munkáinak elemzésével hatékony és alkalmazható eredményeket felmutatni.

3. V4-ek és a Közép-európai Kiberbiztonsági Platform

A visegrádi együttműködés – a középkori történelmi előzményekre építve – 1991. február 15-én jött létre Visegrádon akkor még három ország – Csehszlovákia, Lengyelország és Magyarország – részvételével. A deklaráció céljai között szerepelt a kommunista blokk maradványainak eltüntetése Közép-Európában, a demokrácia védelme és a tagországok gyors és gördülékeny csatlakozásának elősegítése az euroatlanti közösséghez. Miután a sikeres integrációs folyamat befejeződött, újabb célkitűzések fogalmazódtak meg a V4-ek körében, hiszen a 2000-es évek derekától globális szinten új típusú, biztonságot fenyegető kihívásokkal kellett szembesülni a tagországoknak.[3]

A közép-európai országok a fent említett megváltozott biztonsági kihívások hatására a 2010-es évek elején kezdtek foglalkozni intenzívebben a kibervédelmmel. Létrehozták saját kibervédelmi stratégiájukat, emellett szükségét érezték egy Unión belüli egyfajta regionális összefogásra is ezen a területen. Megkezdték együttműködési rendszerük kialakítását. 2013-ban Ausztria és Csehország kezdeményezésére Magyarország, Szlovákia és Lengyelország csatlakozásával létrehozták a Közép-európai Kiberbiztonsági Platformot (Central European Cyber Security Platform – CECSP), melynek céljául a kiberbiztonság regionális szintű fokozását tűzték ki. Ennek megvalósítására az alábbi 5 kiemelt pontban megfogalmazottakat irányozták elő:

- Információ, know-how és a legjobb, leghatékonyabb gyakorlatok bemutatása: a kiberfenyegetésekkel szembeni ellenálló képesség javítása és a felkészültség előmozdítása érdekében a tagállamok elkötelezték magukat, hogy erősítik képességeiket és rendszeresen megosszák az információkat és a legjobb gyakorlatokat a kiberbiztonság területén, illetve a közös képzés, oktatás és gyakorlatok szervezése is részét képezi megállapodásnak.
- Biztonságos kommunikációs csatornák tervezése és megvalósítása: a jövőbeni, az aktuális illetve a már megoldott kiberfenyegetésekhez kapcsolódó adatok, információk biztonságos továbbítása érdekében a tagállamok törekednek olyan információs csatornákat kialakítani, melyekhez illetéktelenek nem képesek hozzáférni és azokat lehallgatni.
- Definiálás és megegyezés besorolási rendszerre vonatkozóan: az információ megosztás érdekében a tagállamoknak meg kell állapodni egy besorolási rendszerben az érzékeny adatokra vonatkozóan. Ajánlott olyan előírásokat megfogalmazni és lefektetni, melyek alkalmazásával könnyebbé válik az adott kiberbiztonsági incidens megértése, elemzése.
- Az egyéni álláspontok összehangolása nemzetközi fórumok előtt: a nyilatkozat szerint a résztvevőknek minden nagyobb nemzetközi szintű megbeszélés – úgymint EU, NATO, UN, OSCE és ENISA - előtt konzultálniuk kell a nemzeti álláspontjukat illetően a regionálisan átnyúló megközelítések harmonizálásának érdekében.
- Gyakorlati munkacsoportok létrehozása: speciális témák megvitatásának céljából lehetőség van alkalmi munkacsoportok létrehozására. A minimum két tagállam részvételével működő munkacsoportok jellege attól függ, hogy milyen céllal, milyen alapon hozták létre (műszaki, irányítási, műveleti, politikai). Közös ügyek, közös témák vonatkozhatnak szabványosításra és adott aktuális fejlesztésekre, hardver és szoftver hitelesítésre és beszerzésre, határokon átívelő együttműködésre stb.

A Közép-európai Kiberbiztonsági Platform tevékenysége és eredményessége a 2013-ban történt megalakulása óta a fenti irányelveket tekintve leginkább csak a kölcsönös tapasztalatcseréről és közös gyakorlatok megszervezéséről szólt. Ennek oka az eltérő stratégiákban, a külpolitikai hangsúlyeltolódásokban, illetve az információk és tapasztalatok megosztási hajlandóságának csökkenésében keresendő. Míg Magyarország 2013-ban az Európai Unió tagállamai között is szinte elsőként alkotta meg nemzeti kibervédelmi stratégiáját, napjainkra már Csehország és Lengyelország vette át az innovatívabb és kezdeményezőbb szerepet. [4] Mindent összevetve van remény a visegrádi négyek kibervédelmének összehangolására, azonban ezen cél eléréséig még hosszú út áll az érintett államok előtt a bizalom kiépítésével és a különböző érdekek közti kompromisszumok megteremtésével párhuzamosan.[5]

4. Következtetések

A nemzeti és a regionális kiberbiztonsági érdekek és célok eléréséhez szükséges a térségen belüli szoros együttműködés javítása, a hatékony és gyors információcsere. A kiberbiztonsági ki-

hívások, fenyegetések elleni hathatós fellépés elengedhetetlenné teszi az államok kollektív, összehangolt munkáját. Elsődleges cél természetesen a megelőzés, de legalább olyan fontos maga a kiberbiztonsági eseményekre és válsághelyzetekre való gyors és hatékony reagálás, konfliktuskezelés, illetve a helyreállítás folyamata is. Az adott országok nemzeti érdekeinek védelme és előtérbe helyezése sokszor komoly akadályt képez a nemzetközi együttműködések során, hosszabb-rövidebb ideg tartó stagnálást előidézve az adott kooperáció tevékenységében, céljainak elérésében. Az EBESZ és a V4-ek esetében is van és lesz is rá precedens, hogy a fent említett okok visszább vetik a kooperáció lendületét, viszont ezt tudomásul véve azzal is tisztában vannak, hogy napjainkat és a jövőt tekintve is a határokon átnyúló új típusú biztonsági kihívások kezelésére és megoldására nélkülözhetetlen a nemzetközi szintű regionális összefogás.

Köszönetnyilvánítás

„Az Emberi Erőforrások Minisztériuma ÚNKP-18-3-IV-NKE-77 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült”

Szakirodalmi hivatkozások

[1] Gazdag F., Remek É.: A biztonsági tanulmányok alapjai. Dialóg Campus Kiadó, Budapest, 2018.

[2] Decision No.1202 OSCE Confidence-building measures toreduce the risks of conflict stemming from the use of information and communication technologies https://www.osce.org/pc/227281?download=true (letöltve: 2019. február 27.).

[3] V4 connects, *Hungarian presidency 2017/2018 of the Visegrad Group* http://v4.gov.hu/a-visegradi-egyuttmukodesrol (letöltve: 2019. február 27.).

[4] Rajnai Z., Fregán B.: *Új alapokon a magyarországi kibervédelmi stratégia*. In: A XXII. Fiatal műszakiak tudományos ülésszak előadásai. Proceedings of the 22th international scientific conference of youngth engineers, Kolozsvár/Cluj, Románia, Műszaki Tudományos Közlemények 7. (2017) 351–354. https://eda.eme.ro/handle/10598/29842

[5] Antal József Tudásközpont, *Kutatás- Kutatói Blog* http://www.ajtk.hu/kutatoi-blog/219/a-visegradi-negyek-helyzete-a-kibervedelem-tekintetében-/ (letöltve: 2019. február 26.).