Válaszok

Kovács László:
A kiberbiztonság stratégiai megközelítése
című MTA doktori értekezéséhez

a hivatalos bírálók által megfogalmazott
kérdésekre és felvetésekre

Budapest 2020

TARTALOM

Válasz Kende György hivatalos bírálatában megfogalmazott kérdésekre és felvetésekre .. 3

Válaszok a bíráló kérdéseire 3

Válaszok a bíráló felvetéseire 7

Válasz Rajnai Zoltán hivatalos bírálatában megfogalmazott kérdésekre és felvetésekre 8

Válaszok a bíráló kérdéseire 8

Válaszok a bíráló felvetéseire 13

Válasz Munk Sándor hivatalos bírálatában megfogalmazott felvetésekre 15

A hivatalos bírálók kérdéseire és felvetéseire adott válaszaim során felhasznált források . 22

Válasz Kende György hivatalos bírálatában megfogalmazott kérdésekre és felvetésekre

Mindenek előtt tisztelettel szeretném megköszönni Kende Györgynek az MTA doktora címre benyújtott értekezésemmel kapcsolatban megfogalmazott véleményét és bírálatát!

Válaszok a bíráló kérdéseire

Bírálatában Kende György professzor úr négy kérdést tett fel, amelyekre a következőkben megfogalmazott válaszokat adom.

1. **Melyek az 1. fejezetben végzett vizsgálatokból levonható következtetések, és ezek milyen módon segítették a tudományos eredmények elérését?**

Dolgozatomnak ez a része – egy nagyon rövid, de igen fontos terminológiai felvezetést követően – azzal az alapvető problémával, illetve tudományos kérdéssel foglalkozik, hogy a digitalizáció és az infokommunikációs technológia egyre magasabb foka valóban nagyobb biztonsági kitettséget okoz-e az adott társadalomnak. A digitális technikai és technológiai függőségünket a kritikus infrastruktúrákon és a kritikus információs infrastruktúrákon keresztül mutattam be. Ezek azok a rendszerek a digitális ökoszisztémában, amelyek működése elengedhetetlen, következésképpen ezek azok a legfontosabb rendszerek, amelyek működésének biztosítása az egyik legfontosabb feladat minden fejlett digitális társadalommal rendelkező országban.

Ugyanakkor, az hogy egy adott ország mennyire fejlett digitális ökoszisztémával rendelkezik nagyon nehezen mérhető, amit tovább nehezít az, hogy ezekhez a mérésekhez sok esetben eltérő módszertant használnak. Ezért felkutattam és bemutattam olyan módszertanokat – az EU DESI, illetve az ENSZ GCI indexeit –, amelyek alkalmasnak látszanak a digitális fejlettség mérésére. Önmagában ezek a bemutatások, illetve az indexek alapján a különböző országok jellemzése a dolgozatom további fejezeteiben elvégzett vizsgálatokhoz adtak kiinduló pontokat. Ezek alapján a dolgozat későbbi részeiben az ezen országok kiberbiztonsági stratégiáinak fejlődését, illetve az azok által az indexben elért, az adott országra vonatkozó eredményeket elemeztem. Az megállapítható, hogy egy jól működő, folyamatosan fejlesztett kiberbiztonsági stratégia pozitív hatást gyakorol az adott ország digitális biztonságára, és így közvetlenül, vagy akár közvetett módon az említett indexek értékeiben is realizálható ez a változás. Erre talán az egyik legjobb példa Hollandia (de akár Észtország is ide sorolhatjuk),

ahol már a harmadik generációs kiberbiztonsági stratégia van életben, és Hollandia DESI indexen mért helyezése[1] alapján az európai élmezőnybe is tartozik.

A fejezet további részeiben azt is megvizsgáltam, hogy globálisan melyek lehetnek azok a legfontosabb stratégiai kihívások vagy veszélyek, amelyek kezelése meg kell hogy történjen egy adott országban, így annak kiberbiztonsági stratégiájának ezekre kiemelten kell fókuszálnia. Természetesen azt is megvizsgáltam, hogy ezeket a kihívásokat milyen stratégiai szintű védelmi megoldásokkal lehet hatékonyan kezelni. Az ezekből levonható következtetéseket felhasználtam a későbbiekben általam megfogalmazott nemzeti kiberbiztonsági stratégia elemeire tett javaslataimnál.

Összefoglalva mindezeket, valóban célszerű lett volna a fejezetben elvégzett vizsgálatokról készíteni egy összegzést és azokból ezen a helyen az elvégzett vizsgálatokból levont következtetéseket megadni, ugyanakkor a dolgozat későbbi részeiben megvizsgált és elemezett nemzeti kiberbiztonsági stratégiák stratégiai célitűzéseinek elemzését az ebben a fejezetben leírtak, illetve azok eredményei alapján végeztem. Azaz, mintegy iránymutatásul használtam a fejezet eredményeit a későbbi vizsgálataimhoz.

2. **Melyek a DESI (Digital Society and Economy Index), és a GCI (Global Cybersecurity Index) számításának módjai, azok értékének meghatározása milyen (matematikai) módszerekkel történik? Alkalmasak-e ezek a módszerek a 4. tudományos eredményben összefoglalt, a szerző által kidolgozott, a nemzeti kiberbiztonsági stratégia végrehajtása hatékonyságának mérésére szolgáló indikátor-rendszer mutatóinak számítására? Vagy szükségesek-e más módszerek, és ha igen, milyenek?**

A DESI az Európai Unió digitális gazdaság és társadalom indexe (Digital Economy and Society Index, DESI). Ez az index egy több elemet tartalmazó kompozit index, amelyet az Európai Bizottság évente szakértők segítségével határoz meg. A DESI öt nagy területen méri a digitális gazdaság és társadalom fejlettségét. Ez az öt terület öt indikátor csoportot jelent, amelyek a következők: összekapcsoltság, humán tőke, az internethasználat, a digitális technológiák integráltsága és a digitális közszolgáltatások. Ez az öt csoport 30 indikátort foglal magába. Egy ország DESI indexét a fő területek pontszámainak és a részterületek pontszámainak egyedi súlyozott átlagából számítják ki. Az adatok az adott ország Eurostat-nak szolgáltatott adatsoraiból származnak. Az indikátor csoportok közül az összekapcsoltság az adott ország átlagos pontszámának 25%-át, a humán tőke szintén a 25%-át, az internethasználat a 15%-át, a digitális technológiák integráltsága a 20%-át, a digitális közszolgáltatások pedig

[1] Hollandia DESI Indexen mért helyezése 2019-ben az EU tagállamok között a 3. (DESI 2019)

15%-át adják. A DESI index 0 és 1 közötti értéket vesz fel. Minél közelebb van az 1-hez az adott ország vonatkozásában az index, annál fejletten az adott ország digitális gazdasága és társadalma. (DESI 2018, idézi: Kovács 2018)

A GCI az ENSZ Nemzetközi Távközlési Egyesülete (ITU, International Telecommunication Union) által kialakított mérőszám rendszer. A magyarul Globális Kiberbiztonsági Index-nek fordítható mérőszám egy, az abban résztvevő országok által önkéntesen megadott adatokra épülő rendszer, amellyel nemzetközi téren válik lehetővé az egyes országok kiberbiztonsági helyzetének (helyeseben az adott ország kiberbiztonság iránt kifejezett elkötelezettségének) összehasonlítása. A GCI is öt pillérre épül, amelyek az adott ország kiberbiztonság területén meglévő jogi intézkedéseit, technikai intézkedéseit, szervezeti hátterét, kapacitásait, illetve az együttműködés területén meglévő tevékenységeit jelentik. Ezek a területek nagy hasonlóságot mutatnak a DESI index területeivel. A GCI a DESI-hez hasonlóan egy kompozit index, amely az 5 fő területen 25 indikátor alapján kerül kiszámításra. Az ezeken a területeken elért pontszámok súlyozott átlaga egy összpontszámot eredményez (0 és 1 között), amely így lehetőséget ad az országok kiberbiztonsági helyzetének összehasonlítására. A GCI legfontosabb célja elsősorban azonban nem csak az összehasonlítás és ennek megfelelően egy rangsor előállítása, hanem a kiberbiztonság területén megvalósuló nemzetközi együttműködés és a tudáscsere előmozdítása. (ITU 2017, idézi: Kovács 2018)

A két bemutatott módszer közül a DESI csak közvetett módon alkalmas az adott ország kiberbiztonsági szintjének a mérésére. Az index által mért területeken az azonos módszertannal összeállított adatsorok összehasonlítást is lehetővé tesznek az országok között. A DESI egy kompozit index, azaz számos olyan adat összesítését jelenti, amelyek egy-egy, a digitális ökoszisztémával kapcsolatos területen meglévő és egy adott időpillanatra érvényes adatot összegeznek. Fontos hangsúlyozni, hogy ezek az adatsorok és így a területek is csak közvetett módon kapcsolódnak a kiberbiztonsághoz. Például az elektronikus kereskedelem egyes adatait közvetve befolyásolhatják az adott ország kiberbűnözési adatai (a magasabb kiberbűnözési arány negatívan befolyásolja aez elektronikus kereskedelemhez szükséges vásárlói bizalmat).

A GCI más módszertant követve az adott ország kiberbiztonságának fejlettségét hivatott mérni, de fontos hangsúlyozni, hogy a módszertan egy összehasonlító módszerre épül. Ez azt jelenti, hogy az adott indikátort (az arra adott önkéntes nemzeti adatszolgáltatást) hasonlítják az adott régió más országainak ugyanerre az indikátorra adott válaszához. Ehhez olyan, a kiberbiztonsággal közvetlen relevanciában lévő területekről származó adatokat használnak, mint jogszabályi terület (kiberbiztonságot szabályozó nemzeti jogszabályok és a nemzetközi jogszabályok alkalmazása), technikai lépések, szervezeti háttér, képességépítés, nemzeti és

nemzetközi együttműködés. Bár ezek alapján az adatok alapján generált szintén kompozit index révén a különböző országok kiberbiztonsági helyzete összehasonlítható, mégsem ad egyértelmű utalást az adott ország nemzeti kiberbiztonsági stratégiájának, illetve az abban foglaltak hatékonyságának mérésére. Következésképpen az is kijelenthető, hogy a GCI is csak közvetve alkalmas a nemzeti kiberbiztonsági stratégiák hatékonyságának mérésére, hiszen számos más területet is magába foglal a mérőszám rendszere.

Az általam kidolgozott indikátor-rendszer mutatóinak alapján azonban az adott ország nemzeti kiberbiztonsági stratégiájának a hatékonysága válik közvetlenül mérhetővé. Ugyanakkor a fenti két módszer csak közvetett módon alkalmas a javasolt indikátor rendszer mutatóinak konkrét számítására. Ez igaz a nem számszerűsített, hanem trendekkel jellemzett mutatók (az azokban bekövetkezett változások) esetében is, de azok közvetlen kapcsolata a fenti indexek hasonló területen mért változásaival nagy korelációt mutathat. Ugyanakkor az indikátor rendszer mutatóinak nagybani meghatározásához a DESI indexel való relevanciát vettem alapul.

3. A szerző az 5. oldalon azt írja, hogy a kiberbiztonsági stratégiák többnyire statikus dokumentumok. Ugyanakkor a 200. oldalon ezt olvashatjuk: „Az általam javasolt dinamikus modell”… A stratégia - ami egy ismert definíció szerint „a cselekvések egy hosszabb távú terve egy bizonyos cél elérése érdekében” - hogyan és milyen mértékben lehet dinamikus?

A dinamizmus ebben az értelemben a nemzeti kiberbiztonsági stratégia olyan jellemzőjét jelenti, amely alapján a folyamatosan változó kibertéri környezethez, az abban megjelenő újabb és újabb technikai, vagy akár biztonságpolitikai kihívásokra[2] adható válaszok potenciális lehetőségét, illetve a fenyegetésekhez történő adaptív alkalmazkodás megvalósítható anélkül, hogy generálisan új stratégiát kellene meghatározni.

Ennek érdekében állítottam fel a nemzeti kiberbiztonsági stratégia modelljéhez szükséges végrehajtási ciklust bemutató javaslatomat. Ez négy főbb elemet foglal magába, amely mindegyike egy-egy felülvizsgálat, illetve frissítés eredményét is magába foglalja. Ugyanakkor már az első ciklus elem is változáskövetést jelent, amelyben az új veszélyek és kihívások azonosítása, majd a következő elemben az ezeknek való eredeti stratégiai célok megfelelőségének vizsgálata történik meg. Ennek megfelelően a ciklus elemek egymásra épülnek, de ez az egymásra épülés azt is feltételezi, hogy egy-egy ciklus elem inputjai olyan

[2] Ebben az értelemben a biztonságpolitikai kihívás többek között a kibertér ártó, vagy negatív szándékú olyan felhasználását jelenti, amely a biztonsági helyzet destabilizálására, lerontására vagy annak kísérletére irányul.

változók, amelyek az adott – a stratégiában szabályozott – tevékenységek és a valóság közötti relevanciát mutatják be.

Az ebben az értelemben használt stratégiai dinamizmushoz, azaz az alkalmazkodni képes stratégiához szükséges a ciklus elemek mindegyikében foglaltak objektív mérése is. Ennek érdekében dolgoztam ki a dolgozatban bemutatott indikátor-rendszert.

4. Van-e szerzőnek a bírálat egészével, vagy annak egyes részeivel kapcsolatban észrevétele?

Ezúton is nagy tisztelettel köszönöm meg Professzor Úrnak a bírálatot. Az abban foglaltakkal kapcsolatosan észrevételt nem teszek.

Válaszok a bíráló felvetéseire

Kende György professzor úr bírálatában megfogalmazott felvetések két nagy csoportra oszthatók: az első a fejezet végi következtetések hiánya, a második az 1. és a 2. fejezetben bemutatott vizsgálatokból nem megfogalmazott tudományos eredmények.

A bíráló első felvetésével maximálisan egyet kell értenem. A dolgozat szerkezete és a bemutatott vizsgálatok, az egyes fejezetkben elvégzett elemzések, illetve az azokból levont következtetések bemutatása valóban célszerű lett volna az adott fejezet végén.

A második felvetéssel kapcsolatosan, amely az 1. és 2. fejezetből levonható tudományos eredményeket jelenti, szeretném kifejezni, hogy ez valóban így van, ugyanakkor e két fejezetből levonható következtetések az én értelmezésemben a később megfogalmazott tudományos eredmények kiinduló pontjai, azaz mintegy bázisai a – reményeim szerint – gyakorlatban is használható és alkalmazható nemzeti kiberbiztonsági stratégia modelljére, illetve az abban foglaltak hatékonyságának mérésére kidolgozott mérőszámrendszernek.

Válasz Rajnai Zoltán hivatalos bírálatában megfogalmazott kérdésekre és felvetésekre

Mindenekelőtt tisztelettel szeretném megköszönni Rajnai Zoltán úrnak bírálatát, a bírálatban megfogalmazott észrevételeket és kérdéseket!

Válaszok a bíráló kérdéseire

Hivatalos bírálatában Rajnai Zoltán egy kérdést fogalmazott meg. Ugyanakkor a kérdés két egymással összefüggő rész-kérdésből áll:

Látja-e kiemelt helyét és szerepét a Közép-Európai Kiberbiztonsági Platformnak az Európai Unió kiberbiztonsági stratégiájának megvalósításában?

Ha igen, hogyan értékeli a Visegrádi országok stratégiai egyeztetésének lehetőségeit a V4 elnökségek programjaiban?

A Közép-európai Kiberbiztonsági Platformot (Central European Cyber Security Platform, CECSP) 2013-ban hozták létre a Cseh Köztársaság és az Osztrák Köztársaság kezdeményezésére. A kezdeményezést támogatta Magyarország, Lengyelország és Szlovákia is. A platform legfontosabb célja a szomszédos országok intenzív együttműködésének kialakítása a kiberbiztonság területén, amely magába foglalja az információcserét, a kiberfenyegetések és a potenciális kibertámadások területén megjelenő tudás, valamint a jógyakorlatok megosztását. (NKI 2020)

Mindezen célokkal a platform egyik legfontosabb eredménye az lehet, hogy ezen célok mentén tett kiberbiztonsági intézkedések és a közös kibertéri tevékenységek megerősítik a résztvevő országok különböző pozícióit a nemzetközi környezetben. A kibertér jellegéből adódóan – például a kibertérben nehezen értelmezhető országhatárok, globális jelleg – a platformban résztvevő országok további nagy eredménye abban mérhető, hogy európai szinten együttesen támogatják az új biztonsági kihívásokra adandó válaszok feltérképezéséhez szükséges erőfeszítéseket és így az ezen a területen is szükséges konszenzust.

A CECSP gyakorlati megvalósításában a kormányzati, nemzeti és katonai CSIRT (Computer Security Incident Response Team, Számítógép-biztonsági incidenskezelő csoport) képviselői, valamint a nemzeti kiberbiztonsági hatóságok és a nemzeti kiberbiztonsági központok képviselői vesznek közvetlenül részt. Az együttműködés közös kibervédelmi gyakorlatok formájában is megjelenik, amelyek során többek között az említett CERT-ek

(CSIRT-ek), azaz az eseménykezelő központok számára van lehetőség szimulált körülmények között a hálózatok és a rendszerek védelmére nemzetközi környezetben. (NCKB 2017)

Az Európai Unió kiberbiztonsági stratégiája *Nyílt, megbízható és biztonságos kibertér* címmel 2013-ban került elfogadásra. A stratégia az EU digitális gazdasága és társadalma számára vázol fel egy olyan jövőképet, amelyekhez szükséges stratégiai prioritásokat öt pontban foglalták össze:

- kibertámadásokkal szembeni ellenálló képesség elérése;
- a kiberbűnözés drasztikus csökkentése;
- kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (Common Security and Defence Policy, CSDP) tekintetében;
- kiberbiztonsági ipari és technológiai erőforrások kifejlesztése;
- összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Unió alapértékeinek támogatása. (Európai Unió 2013)

A fenti célok többségéhez, bár eltérő volumennel, de a kérdésben megfogalmazott CECSP nagyban hozzájárul, hiszen annak célja közvetlenül az együttműködésben rejlő kibertéri ellenállóképesség fokozása. A későbbiekben bemutatott V4-es keretben történő együttműködés pedig a kibervédelmi politikák összehangolásában, valamint az egységes közös biztonság- és védelempolitika irányába mutat.

Mindezekből következően nem túlzás azt állítani, hogy az Európai Unió kiberbiztonsági stratégiájának támogatásához a CECSP komoly mértékben járul hozzá. A platformban résztvevő öt ország egységes álláspontja egyrészt bizonyítja a résztvevők elköteleződését a nemzetközi szintéren megjeleníteni kívánt kiberbiztonság iránt, másrészt a fentiekben már említett komoly kiberdiplomáciai súlyt is képvisel. A CECSP által megfogalmazott együttműködési keret példa lehet az Európai Unió többi tagországa számára, amennyiben az elvekben megfogalmazott kiberbiztonság a különböző közös gyakorlatokon és eseménykezelési felkészüléseken is bizonyítja működőképességét.

Mindezek alátámasztására célszerű az előző négy év V4-ek elnökségi programjait, illetve az abban megjelenő kiberbiztonsági célokat elemezni, így bemutatva adni meg a választ a bírálói kérdés második felében megfogalmazottakra. A kérdés súlyát és abszolút jogosságát mi sem bizonyítja jobban, hogy minden V4-es elnökség programjában kiemelt helyet foglal el a kiberbiztonság és a kiberbiztonsági együttműködés, amelynek közvetlen alapját mind a négy V4-es ország a CECSP-ben nevezi meg.

A 2015-2016[3] cseh V4-es elnökség hivatalos programja[4] szerint a kiberbiztonság az egyik olyan terület, amelynek a Visegrádi Országok biztonsági és védelmi együttműködésében[5] kiemelt szerepet kell kapnia. Az olyan történésekkel jelzett biztonsági helyzet gyors és drámai változása, mint például az ukrajnai krízis a cseh elnökség programjára nagy kihatással volt. A biztonsági helyzet gyors és negatív változására adandó hatékony választ Csehország a közös és egységes V4-es fellépésben látta és programjában ezt is fejezte ki.

Ezzel összhangban a cseh elnökség a kiberbiztonság területén is hangsúlyozta az együttműködés fontosságát:

„A V4-ek cseh elnöksége arra törekszik, hogy elmélyítse és fokozza az együttműködést a Közép-európai Kiberbiztonsági Platformon (CECSP) keresztül. Ez magában foglalja különösen a V4-es országok álláspontjának harmonizálását a kiberbiztonság alapvető kérdéseivel kapcsolatban, ideértve a nemzetközi szervezetekben fennálló álláspontjukat, szakértői műhelyek szervezését, valamint a szabványok és a biztonságos csatornák bevezetését a CECSP-államok közötti kommunikáció részeként. A V4 folytatja a szakosodott rendőri egységek és a nemzeti 'kiválósági központok' közötti együttműködés gyakorlatát is, amely a kiberbűnözés területén folytatott kutatásra összpontosít." (V4 Cseh elnökség 2015)

A cseh elnökségi programból származó fenti idézet jól mutatja, hogy a V4 tagországok kiberbiztonsági együttműködésében fontos szerepet szánnak a CECSP-nek. Az együttműködés gyakorlati megvalósítása során az egyik kiemelt kérdés a tagországok egységes álláspontjának kialakítása. Ennek érdekében a gyakorlati megvalósítást közös szakértői műhelyek és közös

---

[3] A V4-ek elnökségi ciklusa az adott év július 1-től a következő év június 30-ig tart.

[4] A cseh elnökség programja tartalmazta és fontos V4-ek célkitűzésnek tekintette a biztonsági és védelmi együttműködés keretében az úgynevezett Visegrádi Csoport Katonai Oktatási Platformot (VIGMILEP). Ez egy olyan együttműködési keretet jelent, amely lehetővé teszi a V4 országok katonai felsőoktatási rendszereinek szinkronizálását és interoperabilitását. Ennek kidolgozásában személyesen is volt módom részt venni. Az ezzel párhuzamosan működő iMAF (International Military Academic Forum, Nemzetközi Katonai Felsőoktatási Fórum) keretében kidolgoztam azt a katonai felsőoktatás alapképzése számára egységesen alkalmazható Cyber Security (Kiberbiztonság) tantárgy leírását és szakmai tartalmát, amelyet az iMAF közössége (Ausztria, Csehország, Lengyelország és Románia) elfogadott, és amely tantárgy egységes elvek mentén lehetővé teheti a kiberbiztonság alapjainak oktatását a VIGMILEP együttműködésben is.

[5] Meg kell jegyezni, hogy a Visegrádi Országok védelmi miniszterei 2014-ben egy hosszútávú védelmi együttműködést támogató nyilatkozatot fogadtak el. A dokumentumban foglaltak alapján a V4-ek védelmi együttműködését különösen három területen fokozzák: képességfejlesztés, beszerzés és védelmi ipar; többnemzeti egyégek kialakítása és azok határokon átnyúló tevékenységének támogatása; oktatás, kiképzés és gyakorlatok. (V4 2014)

szabványok kialakításával kívánják elérni. Véleményem szerint a fentiekben megfogalmazott célok közül a legfontosabb a közös és egységes álláspont kialakítása és annak a nemzetközi közösség felé való közös képviselete. Mindezeket ki kell egészíteni a fentiekben szintén megfogalmazott közös biztonsági csatornák kialakításával is, amelyek mentén az incidenskezelésben, illetve akár – a cseh elnökségi programban szintén említett – kiberbűnözés elleni közös fellépéssel valódi előrelépés lehet a kiberbiztonság szintjének emelésének terén.

A 2016-2017 közötti időszakban lévő lengyel V4-ek elnökségi programja az Európai Unió Digitális Egységes Piaci Stratégiájával kapcsolatban az együttműködés területei között elsőként a kiberbiztonság terén szükséges közös fellépést célozta meg a következőképpen: *„…együttműködés a kiberfenyegetések elleni védelem fokozása érdekében, többek között a CSIRT együttműködés és a Közép-európai Kiberbiztonsági Platform (CECSP) révén; állandó kapcsolatok kiépítése a CECSP és a V4 között. Ezenkívül ösztönözni kell az együttműködést a különleges rendőri egységek és a nemzeti 'kiválósági központok' között, amelyek a kiberbűnözés területén végzett kutatásokra összpontosítanak."* (V4 Lengyel elnökség 2015)

A program a kiberbűnözés elleni fellépést a V4-ek rendőrségi együttműködése során külön is szorgalmazza. Ezen kívül a program meghatározza az ipar digitalizációjának fontosságát és ezzel kapcsolatosan egy olyan közös V4-es álláspont kialakítását is szorgalmazza, amely egységes európai fellépést, és így hatékonyabb érdekérvényesítést tesz lehetővé a tagországok számára. A digitalizáció területén a program mindezeken kívül célként fogalmazza meg az e-kereskedelem fejlesztését, a digitális készségek magasabb szintre emelését, valamint a digitális innováció területén megszerzett tapasztalatok cseréjét. Külön ki kell emelni, hogy a program fontosnak tartja a telekommunikációs szektor szabályozásának kérdését az Európai Unióban, amelyhez ki kell alakítani egy egységes V4-es álláspontot, így biztosítva ezen a területen is a hatékonyabb érdekérvényesítést. (V4 Lengyel elnökség 2015)

Nagyon fontosnak tartom a program azon célkitűzését, amely az e-kormányzás, illetve az e-közigazgatás területének fejlesztését célozza meg. Ez a következőket jelenti a program szerint: *„ … tapasztalatcsere a közigazgatási szervek információs és kommunikációs rendszereinek átjárhatóságának biztosításához szükséges megoldásokról, a közigazgatási rendszerek azonosításának és hitelesítésének közös mechanizmusairól és a közigazgatásban lévő e-szolgáltatások nyújtásának elfogadott modelljéről."* (V4 Lengyel elnökség 2015) Ez különösen annak tükrében nagyon előremutató célkitűzés, hogy a V4-es tagországok közül Csehország,

Magyarország és Szlovákia ezen a területen a DESI index alapján mérve mélyen az EU átlag alatt teljesít, de Lengyelország is csak a középmezőnyben helyezkedik el[6].

A cseh és a lengyel V4-es elnökség programjaiban megjelenő, a kiberbiztonság területén megfogalmazott olyan célkitűzések, mint az együttműködés, ezen belül is a CECSP platform intézményének felhasználása, valamint az egységes Visegrádi Országok nemzetközi kiberbiztonsági térben történő közös fellépése a 2017-2018-as magyar elnökség programjában is megjelenik. A magyar V4-es elnökség a következőket fogalmazta meg a CECSP-el kapcsolatban: *„[a] Közép-európai Kiberbiztonsági Platform rotációs elnökével együttműködve a magyar elnökség szakértői találkozókat, valamint közös eseményeket és képzéseket szervez az eseménykezeléssel kapcsolatban. Az elnökség konzultációkat tervez folytatni azzal a céllal is, hogy közös V4 álláspontokat alakítson ki az EU napirendjének aktuális témáiról, különös tekintettel a hálózati és információs rendszerek biztonságáról szóló irányelv végrehajtására, valamint az EU kiberbiztonsági stratégiájának felülvizsgálatára."* (V4 Magyar elnökség 2017)

Ugyanakkor a magyar elnökség szélesebb kontextusba helyezte a kiberbiztonságot, hiszen célként fogalmazta meg azt is, hogy a kritikus infrastruktúra ellenálló képességét növeljék a kibertérből származó kockázatokkal és támadásokkal szemben. Ennek érdekében közös V4-es fellépést irányzott elő a kritikus infrastruktúrákat fenyegető kibertéri kihívások és veszélyek feltárása és azok megelőzése érdekében, valamint a magyar elnökség folytatta az együttműködést a V4-országok kiberbiztonsági szervezetei és hálózati biztonsági központjai között, amelyek számára a kiberbiztonsági eseményekkel (incidensekkel) kapcsolatos információk megosztása elengedhetetlen. (V4 Magyar elnökség 2017)

A 2018-2019-es szlovák elnökség programja elemezte a Visegrádi Országok biztonsági környezetét, amelyben többek között külön alfejezetben tért ki a kiberbiztonságra, valamint az ezen a területen szükséges V4-es tevékenységekre. (V4 Szlovák elnökség 2018)

A program ezen belül a legfontosabb célkitűzést a következőképpen fogalmazta meg: *„ ... a kriptovaluták, különösen a bitcoin visszaélésével összefüggő számítógépes bűnözés elleni küzdelemben az együttműködés megerősítésére és fejlesztésére fogunk összpontosítani."*[7] (V4 Szlovák elnökség 2018)

A szlovák V4-es elnökségi program szintén kitér és nagymértékben számol a kiberbiztonság területén fontos CECSP-el. Ugyanakkor a program kitér arra, hogy bár a CECSP elnökségét

---

[6] 2016-ban a DESI index e-közigaztatás területén a V4-es országok a 28 EU tagország között elfoglalt helye a következő módon alakult: Csehország a 24. (2015-ben 25.), Magyarország a 25. (2015-ben 24.), Lengyelország a 15. (2015-ban 12.), Szlovákia pedig a 26. (2015-ben 26.) helyet foglalták el. (DESI 2016)

[7] A szlovák V4-es elnökségi program ennek a problémának az alátámasztására a kiberbűnözés által a dark neten történő kriptovaluta használatát hozza példaként, amely során szinte nyomon követhetetlenül és anonim módon olyan illegális tevékenységekkel kell számolni, mint a fegyverkereskedelem, a kábítószer-kereskedelem, a hamis dokumentumok kereskedelme és a gyermekpornográfia. (V4 Szlovák elnökség 2018)

szintén rotációs alapon látják el az abban részt vevő tagországok, az nincs harmonizálva a V4 tagországok elnökségi ciklusával. Ettől függetlenül a koordinált és harmonizált akciók, valamint az egységes V4-es fellépés az európai országok számára is jelzés értékű. Ezt támasztja alá az is, hogy Franciaország csatlakozott a CECSP által kezdeményezett különböző tevékenységek koordinációjához. (V4 Szlovák elnökség, 2018)

Összességében nagyon jól nyomon követhető, hogy a CECSP a V4-es országok programjaiban, illetve azok célkitűzéseiben nagyon komoly intézményes alapot jelent a kiberbiztonság szintjének emelése érdekében. Ehhez elsősorban a szoros együttműködés, illetve az egységes, a kiberbiztonság különböző területein megnyilvánuló egységes, Visegrádi Országok által közösen képviselt álláspont járulhat hozzá.

Ugyanakkor a V4-es elnökségi programokban foglalt, kiberbiztonságot célzó célkitűzések megvalósulásának mérése rendkívül nehéz. Közvetett módon erre lehetőséget adhatna az általam az értekezésemben javasolt mérőrendszer egységes bevezetése és alkalmazása.

Válaszok a bíráló felvetéseire

Rajnai Zoltán úr bírálatában számos olyan felvetést fogalmazott meg, amelyek megítélésem szerint nem csak a dolgozat vonatkozásában, hanem a kiberbiztonság szélesebb értelemben vett területein is nagyon fontos relevanciával bírnak.

Az első felvetés a kibertér meghatározásának kérdése. Egyetértek a bírálóval abban, hogy valóban sok definíció létezik a kibertér megfogalmazására. A dolgozatom elején megadott egy-egy definíció – bár valóban elemzések és értékelések nélkül – azt a cél szolgálták, hogy a kutatásaim során használt definíciós készletet nagyon egyértelműen lehatárolják és azt annak az értelmében jelenítsék meg az olvasó számára, ahogy azt a dolgozatomban használtam.

A következő felvetés a dolgozatban bemutatott hét kiberbiztonsági fenyegetésre és kihívásra vonatkozik. A bíráló megjegyzésében utal arra, hogy a felvázolt kihívásokat és veszélyeket célszerű lett a biztonság illetve a védelem tekintetében csoportosítani, és célszerű lett volna a gazdasági visszaélésekkel kiegészíteni. Ezzel a felvetéssel egyet kell értenem, ugyanakkor mind a gazdasági visszaéléseket, mind a bírálatban szintén említett gyermekek sérelmére elkövetett a cselekményeket a kiberbűnözés kategóriájába sorolhatónak érzem. Ezek a kibertéri tevékenységek azonban valóban olyan mértéket öltöttek az elmúlt évekre, hogy azok stratégiai jelentőségű problémát jelentenek a legtöbb országban. Ezek a kihívások és veszélyek az általam vizsgált országok nemzeti kiberbiztonsági startégiáiban a legtöbbször meg is jelennek. Ugyanakkor, ahogy a bíráló is utal rá, alapvetően a vizsgálataim katonai műszaki szempontú elemzések voltak, amelyek csak marginálisan érintik a két említett területet. Összegezve: a

felvetést elfogadom, valóban ki kell egészíteni a kibertéri stratégiai kihívásokat és veszélyeket a két felvetett területtel.

A bíráló következő felvetése a második fejezetben bemutatott különböző nemzeti kiberbiztonsági stratégiák azonosságokon alapuló összehasonlítását, és az egyes országok értékelését jelenti. Ezzel kapcsolatban meg kell jegyeznem, hogy a fejezet végén, bár valóban nem összehasonlító elemzés-módszertannal, de összesítve megjelenítettem a vizsgált országok kiberbiztonsági stratégiai céljait (2.5. alfejezet), illetve nem ebben a fejezetben, hanem a következő fejezetben (3.2. alfejezet) szintetizáltan mutattam be az egyes országok (nemzetközi szövetségek) stratégiáiból levonható következtetéseket, illetve az azokban feltárható azonosságokat. Elfogadom a bíráló megjegyzését, hogy célszerű lett volna kitérni ebben az elemzésben az adott ország stratégiai céljaira, akár annak geopolitikai helyzetének elemzésével együtt.

Válasz Munk Sándor hivatalos bírálatában megfogalmazott felvetésekre

Mindenekelőtt nagyon köszönöm Munk Sándornak az alapos és szakmailag nagyon tartalmas véleményét az MTA doktora címre benyújtott értekezésemmel kapcsolatban!

Hivatalos bírálatában Munk Sándor nem fogalmazott meg külön kérdéseket, ugyanakkor számos olyan területre rávilágít bírálatában, amelyekre jelen dokumentumban röviden reagálni szeretnék. Az ezekre a felvetésekre történő bővebb magyarázataim kiegészíthetik a dolgozatban leírtakat.

Az 1. Fejezettel kapcsolatos bírálói felvetések

„A választott kibertér fogalom indoklása elég szűkszavú, és bár a szerzőnek joga van megválasztani az általa megfelelőnek tartott definíciót, szükség lett volna annak meghatározására, hogy ennek a fogalomnak miért kiinduló pontja a stratégiai megközelítés, és be lehetett volna mutatni néhány további fogalmat, amelyekre ez kevésbé, vagy egyáltalán nem jellemző."

Dolgozatom elején a leggyakoribb fogalmak megadása, illetve az első fejezet elején a kibertér, mint definíció meghatározásakor valóban a bíráló által is felvetett dilemmába ütköztem. Megoldásként azt választottam, hogy a sok kibertéri definíció összehasonlítása helyett egy olyan meghatározást választok, amelyet már korábbi kutatásaim, illetve az azokhoz köthető publikációimban is alkalmaztam. Ennek oka elsősorban a dolgozatban is citált, Munk Sándor által is bemutatott kibertéri definíciós készlet sokszínűsége volt. Dolgozatom megírásakor ezek közül a dolgozat témájának relevanciája miatt a stratégiai szempontú meghatározást választottam ki. Természetesen célszerű lett volna rögtön a dolgozat elején a stratégiát önmagát is definiálni, hiszen ez alapvetően befolyásolja a kibertéri definíció kiválasztását. A dolgozat általam felvázolt logikai íve – kibertér meghatározása, a kibertér szerepének és annak biztonságának, majd e biztonságnak napjainkban betöltött stratégiai szerepének elemzése – miatt azonban ezt a sorrendet láttam célszerűnek.

A dolgozatban később megtett stratégia definiálása alapján az már nem csak a szűk katonai területen, hanem a tágabb értelemben vett biztonságpolitikában az államok lehetőségeinek – dolgozatom témájából adódóan alapvetően a védelmi jellegű tevékenységek – nemzetközi térben történő alkalmazását jelenti. Van azonban egy komoly probléma ebben a körben a 21. században, ez pedig az, hogy a társadalom és a gazdaság folyamatainak túlnyomó többsége a kibertéri folyamatoktól függ, illetve azokra épül. Ebből következően a stratégiának ki kell térnie arra a nem egyszerű problémakör kezelésére, amely a kibertér alapvető jellegéből, azaz például a fizikai értelemben vett határtalanságból is adódik. A korábbi stratégiai felfogások alapvetően

a fizikai térre, az abban lévő nemzetközi, gazdasági, társadalmi és ezekkel párhuzamosan a hadügyi folyamatokra adtak eligazítást. A 21. században ez alapjaiban változott meg a kibertér megjelenésével, hiszen egy eddig nem látott, fizikai értelemben csak korlátozottan megfogható dimenzióra[8] kell akár államok közötti megoldásokat is keresni, ráadásul mindezt úgy szükséges megtenni, hogy a dolgozatban is bemutatott, a kibertéri folyamatokkal szemben fenálló társadalmi és gazdasági függőség már létezik.

Mindezeknek megfelelően választottam a véleményem szerint az egyik legfontosabb stratégiai kérdést is, azaz a társadalmi és gazdasági folyamatokat is magába foglaló kibertér definíciót. A dolgozatban megfogalmazottak alapján a 2013-as hazai Nemzeti Kiberbiztonsági Stratégia által megfogalmazott kibertér fogalmat használtam egy kis kiegészítéssel, mert ez tartalmazza az általam a dolgozatban később bemutatott és elemzett kibertérrel szemben megjelenő társadalmi és gazdasági függőségre, mint stratégiailag fontos kérdésre tett utalást: *„[a] kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."* (1139/2013. [III. 21.] Korm. határozat)

A bíráló a kibervédelem meghatározását célszerűnek tartotta volna. Ezzel kapcsolatban el kell mondanom, hogy a dolgozat elején tett definíciós meghatározásoknál valóban csak a védelem fogalmát adtam meg, amely szerint a védelem olyan tevékenységeket takar, amelyek a biztonság megteremtésére és fenntartására irányulnak. Ebből következően a kibervédelem olyan tevékenységeket, illetve azok együttesét jelenti, amelyek a kiberbiztonság megteremtésére és fenntartására irányulnak. Ezek lehetnek kibertéri és kibertéren kívüli, de a kibertérre ható tevékenységek is.

Ugyanakkor ez alapján az 1.5. fejezet elején a kibervédelem meghatározása is megjelenik a dolgozatban, miszerint „*A kiberbiztonság megvalósítása érdekében szükségesek mindazok technikai, szabályozási és humán eszközök, illetve képességek megléte, amelyek a digitális ökoszisztéma, benne az infokommunikációs eszközök és rendszerek alkalmazása és működtetése során, mint védelmi megoldások tevékenységek egész sorával járulnak hozzá a biztonság kialakításához és annak fenntartásához."*

A bíráló azon felvetését, amely a hét bemutatott stratégiai szintű kibertéri fenyegetés indoklását illeti elfogadom, hiszen itt valóban nem adtam tudományos magyarázatot arra, hogy

[8] A fizikailag korlátozottan megfogható ebben az értelemben azt jelenti, hogy a kibertér alapjait létrehozó számítógép-hálózatok és egyéb hardver elemek fizikailag természetesen kézzelfoghatóak, viszont az azokon futó szoftverek által megvalósuló folyamatok már csak nehezen értelmezhetőek a fizikai térben.

miért pont ezeket a fenyegetéseket látom a legfontosabbaknak és miért ebben a formában rendszereztem ezeket.

Ezt a munkát korábbi publikációimban részben megtettem, és azok szintetizált következtetései jelennek meg a dolgozatban ebben a felsorolásban és elemzésben. A rendszerezésre nem tettem explicit magyarázatot, viszont a veszélyek és kihívások, illetve azok lehetséges következményeinél utaltam rá, hogy ezeket tartom olyan volumenű kihívásoknak, amelyek egy ország és/vagy egy szövetség esetében elérik a stratégiai jelentőséget. Bár leírva valóban nincs a dolgozatban, de ezt tekintettem a rendszerezés alapjának. Ugyanakkor elismerem, hogy ezek mellett számos olyan kibertéri kihívás is lehet, amelyek valódi stratégiai jelentőségre tesznek szert akár közvetlenül, akár egymásra gyakorolt hatásuk révén közvetett módon. Ilyen lehet például a dolgozatban említett, de részletesen nem elemzett kiberbűnözés és politikai befolyásolás egymásra hatása is.

A bíráló 3. ábrára (38. oldal) tett felvetéseivel egyetértek. Célom a citált ábra beillesztésével összességében az volt, hogy nagy vonalakban szemléltessem a kibertéri kihívások közül annak a volumenét (hatásait), amelyet kiberhadviselésnek hívunk. Úgy gondolom, hogy a kiberhadviselés, azaz egy állam, vagy államcsoport, esetleg gazdasági érdekcsoport által közvetlenül, vagy közvetett módon támogatott, stratégia szinten tervezett, összefüggő kiber- és fizikai támadások együttese hatását és következményeit tekintve is jóval túlmutat mindazon, amiket a kibertér többi veszélyforrásai esetén tapasztalhatunk.

A bíráló által a kiberbiztonsághoz kapcsolódó stratégiai feladatokkal kapcsolatos felvetésével egyetértek, valóban célszerű lett volna azok stratégiai szintű kiválasztásának szempontrendszerét megadni. Ebben a kérdésben azt a kutatásmódszertani elemet alkalmaztam, amely a hatásvizsgálatot helyezi a kutatott téma egyes kérdéseinek fókuszába. A kiberbiztonsághoz kapcsolódó stratégiai feladatok megállapítása (felsorolása) a kiberbiztonságot fenyegető kihívásokra és veszélyekre adandó (kiber)védelmi tevékenységek közül azok voltak, amelyek hatékonyan és megfelelő módon képesek eliminálni, vagy az azok kezelésére felkészülést biztosítani.

A 2. Fejezettel kapcsolatos bírálói felvetések

A bíráló offenzív kiberképességek bemutatását hiányoló felvetését elfogadom.

Az offenzív képességek megítélése folyamatosan változik, amely igaz magára a fogalomra is. Nem csak technikai, de jogi és nemzetközi jogi kérdések is gyakran a szakmai viták kereszttüzébe kerülnek, akkor, amikor az offenzív kiberképességekről van szó. Erre talán a kiberkémkedés az egyik legjobb példa, amelyről nagyon nehéz megmondani, hogy védelmi célokat, vagy támadást előkészítő célokat szolgál-e. Dolgozatomnak ebben a részében utaltam

rá, hogy az offenzív kiberműveleteket majd a kiberhadviselést bemutató résznél teszem meg. Ugyanakkor a kibertámadások, azaz az offenzív kiberműveletek nyilvánvalóan védelmi célokat is szolgálhatnak, így a kibervédelem bemutatásánál is tárgyalhatóak lettek volna, de mégis jellegükből, azaz hatásaikat tekintve, azokból adódóan véleményem szerint inkább a kiberhadviselés eszközei közé illenek. Sajnos a kiberhadviselést bemutató része a dolgozatnak terjedelmi okok miatt lényeges rövidítésen esett át a dolgozat végleges formájának szerkesztésekor, és ennek áldozatul esett az offenzív kiberképességek részletes bemutatása és elemzése is.

A bíráló stratégiai dokumentumok típusaira vonatkozó felvetésével kapcsolatban, miszerint számos ország megkülönböztet például zöld könyvet, fehér könyvet, stratégiához kapcsolódó akciótervet, egyetértek. Ugyanakkor dolgozatomban az egyszerűsítés és redukció módszerét alkalmaztam. A különböző stratégiai dokumentum típusokat, bár azok jellegüket tekintve valóban eltérnek egymástól, egy fajta dokumentumnak tekintettem. Az eltérő típusokra csak utalásokat tettem (például 127. oldal, Franciaország Fehér Könyve). Az eltérő stratégiai dokumentum típusokat céljaik, azaz az adott ország stratégiai céljainak meghatározása alapján nemzeti biztonsági stratégiai dokumentumnak, illetve nemzeti kiberbiztonsági stratégiai dokumentumnak tekintettem. Ugyanakkor kétségtelen, hogy ezen stratégiai dokumentum típusok között vannak eltérések. A Zöld Könyv általában egy adott területen az ország vagy szervezet (például az EU 2005-ben kiadott kritikus infrastruktúrák védelmére tett) elképzeléseit tartalmazza, de ezek még nem kerültek jogszabályokban rögzítésre. A Fehér Könyv számos ország, például a már említett Franciaország, vagy Szlovákia, olyan dokumentuma, amely az ország (kormány) adott területre vonatkozó legfontosabb biztonságpolitikai megállapításait és céljait nyilatkoztatja ki.[9] Úgy gondolom, hogy a stratégiai dokumentum típusok közötti különbség alapvetően történelmi hagyományokban keresendő, hiszen azok célja alapvetően az adott ország politikájának, valamint stratégiai irányainak a meghatározása az adott területen az adott ország (szövetség) számára. Ennek okán vállaltam az egyszerűsítés módszerét ebben a kérdésben.

A NATO és az EU kiberbiztonsági politikájának illetve stratégiájának összehasonlítására történő bírálói felvetéssel kapcsolatban el kell mondanom, hogy valóban sok hasonlóság van a két szervezet dokumentumaiban, ugyanakkor, ahogy a bíráló is utal rá, ezek rendkívül gyorsan

[9] Ez a megállapítás még Németország esetében is igaz. Németország Fehér Könyve, amelynek címe *Fehér Könyv Németország biztonságpolitikájáról és a Budeswehr jövőjéről* nem csak a biztonságpolitikai célokat, hanem a hadsereg jövőjét is felvázolja. (Németország 2016)

változnak, másrészt pedig eltérő a két szervezet biztonsággal kapcsolatos megközelítése. A NATO, bár alapvetően politikai szövetség, de mégis a katonai biztonság egyik legfontosabb szervezete, így céljai is alapvetően a katonai biztonság növelése irányába mutatnak. Nem vitatva, hogy ezt sok esetben az olyan területeken történő tevékenységek közvetlen vagy közvetett hatásaival is célul tűzte ki, mint például a kibervédelem. (Meg kell jegyezni, hogy ebből következően a NATO alapvetően a kibervédelem [Cyber Defence] kifejezést használja, míg az Európai Unió a kiberbiztonságot [Cyber Security] alkalmazza a hivatalos dokumentumokban is). Az Európai Unió kiberbiztonsági stratégiái alapvetően a biztonsági területek közül a gazdasági biztonság területére fókuszálnak közvetlenül, vagy közvetett módon, mint például teszi azt a hálózatok és infokommunikációs rendszerek biztonságának egységes szintre emelésével.

Ugyanakkor a NATO és az EU együttműködése elengedhetetlen a kiberbiztonság területén. Ezek mellett a bíráló által felvetett, az EU és NATO kiberbiztonsági megközelítéseire, stratégiai dokumentumaira vonatkozóan összegzett következtetés hiányára vonatkozó megállapításával kapcsolatban el kell mondanom, hogy azt egyrészt a fenti indokaim miatt nem tettem meg, másrészt azok nemzeti kiberbiztonsági stratégiákra történő hatásaiban és ráhatásaiban való értékelését szintén a 3. fejezetben megfogalmazott javaslataim szintetizáltan tartalmazzák, miután a két szervezet stratégiáiból levonható következtetéseket a 3.2. alfejezetben bemutattam.

A bíráló felvetésére miszerint a fejezetből mindhárom vizsgált területen hiányoznak az összehasonlító elemzések, hiányzik az azonosságok és különbözőségek kimutatása, utóbbiak okainak feltárása, egyetértek. Ahogy jeleztem Rajani Zoltán bírálatára adott válaszomban, ezeket a következő fejezetben szintetizálva tettem meg.

A 3. Fejezettel kapcsolatos bírálói felvetések

A bíráló által a stratégiai célok elérését időszakosan vizsgáló független szakmai testület szükségességére és összetételére vonatkozó következtetéssel kapcsolatban a következő kiegészítéseket teszem. Az általam javasolt, a stratégiai célok elérése érdekében időszakos vizsgálatokat elvégző független szakmai testületben az adott ország olyan nemzetközi tapasztalatokkal is rendelkező kiberbiztonsági szakemberei kell hogy helyet kapjanak, akik objektív módon, külső behatások és a képviselt szervezet közvetlen érdekeinek kizárásával képesek megítélni szakmailag a stratégiai célok teljesülését (hiszen nemzeti szintű stratégiáról beszélünk). A hangsúly itt az objektivitáson van, amelyeket részben a javasolt mérőszám csoportok, illetve azok kategóriái, de legalább ilyen arányban a szakértők függetlensége biztosít. Ebbe a szakértői szervezetbe képviselőt szükséges delegálnia a kiberbiztonság nemzeti

koordinációjában, vezetésében és felügyeletében szerepet játszó intézményeknek, az akadémiai szférának, valamint a kiberbiztonság piaci szereplőinek egyaránt.

A bíráló kibertámadó képességekre vonatkozó felvetését elfogadom. Ezek valóban, részben a korábban említett okok miatt hiányoznak a dolgozatból. Ugyanakkor ez az a terület, amely bár a legnagyobb változáson ment keresztül az elmúlt 2-3 évben, mégis az egyik legszenzitívebb területnek számít még ma is. Sok esetben csak általánosságban tudunk beszélni a kibertámadó képességekről, például, ahogy azt a kiberfegyverek esetében a dolgozatban tettem, de részleteiben, az alkalmazás módjainak és eljárásainak, de talán ami a legfontosabb annak nemzetközi jogszabályokkal történő harmonizációjáról már kevesebbet tudunk. A kibertámadások egyik legfontosabb kérdése azonban a dolgozatom fő filozófiai alapját is jelentő kibertéri függőségünket érinti. A kibertámadások ma nem elsősorban katonai kérdésként merülnek fel, hanem össztársadalmi problémaként, amely ráadásul a biztonság többi dimenzióját is érinti. A kritikus infrastruktúrákat, illetve a kritikus információs infrastruktúrákat érintő, látszólag kiberbűnözői céllal elkövetett (például anyagi haszonszerzésnek tűnő kiberzsarolás), de hatásait tekintve azok működésképtelenségét okozó támadások, ma lényegesebben komplexebb biztonsági problémát jelentenek, mint például a fizikai térben bekövetkező esetleges támadások (nem vitatva azok esetleges drámai hatásait).

Ezzel párhuzamosan az elrettentés célját szolgáló kibertámadó-képességnek valóságosnak és hatékonynak kell lennie. A probléma ezzel kapcsolatban az, hogy a kibertámadások elrettentési céllal a nemzeti biztonsági stratégiában és/vagy a nemzeti kiberbiztonsági stratégában történő megjelenítése önmagában nem elegendő. A hatékony elrettentésnek egy komplex, többek között a diplomáciai lépéseket, a fizikai térben megjelenő elrettentő erőket, valamint a kibertéri elrettentő erőket (például az említett offenzív kiberműveletek kilátásba helyezését) magába foglaló, eszköztárnak kell lennie. A kibertámadások esetében, legyen szó akár megelőző, akár válasz kibertámadásokról, az egyik legnagyobb probléma az attribúció, azaz a támadó megnevezése. Ez további két összetevőre, technikai és politikai attribúcióra bontható. Ezzel kapcsolatban nincs egységes nemzetközi felfogás. Vannak országok, mint például Hollandia és az Egyesült Királyság, akik alkalmazzák a nyílt attribúciót, míg vannak országok, amelyek a nyílt attributálás lehetőségével nem élnek (például Franciaország).

A bíráló stratégiai szintű kiberválságkezelési tervvel kapcsolatos felvetésére a következő kiegészítést teszem. Nincs egységes nemzetközileg elfogadott elv arra, hogy mi minősül stratégiai szintű kiberválságnak. Ugyanakkor erre talán az egyik megoldás az lehet, ha a kritikus infrastruktúra ágazatok besorolásából indulunk ki. Ennek megfelelően az lehet stratégiai kiberválság, amennyiben a stratégiai kritikus infrastruktúrákat, vagy azok egyes ágazatait éri

súlyos kibertámadás, vagy annak előkészületéről van tudomása az adott országnak. Mindezek helyett nemzetközi példákat láthatunk arra, hogy kiberválság helyett a *súlyos kibertámadások* (angol terminológiában: significant cyber attack) meghatározását használják[10]. Ennek kiberincidensekkel való közvetlen vagy közvetett hatásai azonban csak nagyon nehezen térképezhetők fel, mert a kritikus infrastruktúrák közötti intra- és interdependencia kimutatása és feltárása önmagában is komoly nehézségekbe ütközik.

Mindezek alapján tisztelettel kérem a bírálókat válaszaim elfogadására!

Budapest, 2020. 02. 28.

Kovács László
pályázó

[10] Fontosnak tartom hangsúlyozni, hogy a hazai elektronikus információbiztonsági törvényben foglalt *súlyos biztonsági esemény* meghatározása félrevezető lehet. Ez ugyanis a súlyos biztonsági eseményt a következőképpen definiálja: „*olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.”* (2013. évi L. tv.) Ez ugyanis alapvetően informatikai eseményként definiálja mindezt, ugyanakkor a súlyos biztonsági esemény más dimenzióban elkövetett támadás esetén is fennállhat.

A hivatalos bírálók kérdéseire és felvetéseire adott válaszaim során felhasznált források

1139/2013. (III. 21.) Korm. határozat Magyarország nemzeti kiberbiztonsági stratégiájáról.

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

DESI (2016): The Digital Economy and Society Index (DESI). Forrás: https://ec.europa.eu/digital-single-market/en/news/desi-2016-country-profiles (letöltve: 2020. 02. 11.)

DESI (2018): The Digital Economy and Society Index (DESI). Forrás: https://ec.europa.eu/digital-single-market/desi (letöltve: 2020. 02. 11.)

DESI (2019): The Digital Economy and Society Index (DESI). Forrás: https://ec.europa.eu/digital-single-market/en/desi (letöltve: 2020. 02. 11.)

Európai Unió (2013): Az Európai Unió Kiberbiztonsági Stratégiája: Nyílt, megbízható és biztonságos kibertér. 2013. 2. fejezet. Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/DOC/?uri=CELEX:52013JC0001&from=EN (letöltve: 2020. 02. 16.)

ITU (2017): Global Cybersecuriy Index. Forrás: https://www.itu.int/dms_pub/itu-d/opb/str/DSTR-GCI.01-2017-R1-PDF-E.pdf (letöltve: 2020. 02. 15.)

Kovács L. (2018): A kibertér védelme, Dialóg Campus, 2018.

NCKB (2017): NCKB - National Cyber Security Centre held exercise for CECSP partners. Forrás: https://www.govcert.cz/en/info/events/2532-national-cyber-security-centre-held-exercise-for-cecsp-partners/ (letöltve: 2020. 02. 22.)

Németország (2016): *Weissbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr. F*orrás: https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf (Letöltés ideje: 2020. 02. 23.)

NKI (2020): Nemzeti Kibervédelmi Intézet, Nemzetközi kapcsolatok. Forrás: https://nki.gov.hu/intezet/tartalom/nemzetkozi-kapcsolatok/ (letöltve: 2020. 02. 14.)

V4 (2014): Long Term Vision of the Visegrad Countries on Deepening Their Defence Cooperation. Forrás: http://www.visegradgroup.eu/calendar/2014-03-14-ltv (letöltve: 2020. 02. 17.)

V4 Cseh elnökség (2015): 2015-2016 Czech Presidency - V4 Trust—Program for the Czech Presidency of the Visegrad Group. Forrás:

http://www.visegradgroup.eu/documents/presidency-programs/20152016-czech (letöltve 2020. 02. 17.)

V4 Magyar elnökség (2017): 2017–2018 Hungarian Presidency. V4 Connects. Forrás: http://www.visegradgroup.eu/documents/2017-2018-hungarian/20172018-hungarian (letöltve: 2020. 02. 14.)

V4 Lengyel elnökség (2016): Program of the Polish Presidency in the Visegrad Group. July 1, 2016–June 30, 2017. Context of the Polish Presidency of the Visegrad Group (V4). Forrás: http://www.visegradgroup.eu/documents/presidency-programs/program-of-the-polish (letöltve: 2020. 02. 21.)

V4 Szlovák elnökség (2018): Dynamic Visegrad for Europe, Slovak Presidency 2018/2019 of the Visegrad Group. Forrás: http://www.visegradgroup.eu/documents/presidency-programs/slovak-v4-presidency-en (letöltve: 2020. 02. 14.)