Prof. Dr. Munk Sándor DSc

Hivatalos bírálat Kovács László: "A kiberbiztonság stratégiai megközelítése" című MTA doktori (DSc) értekezéséről

Az MTA Doktori Tanácsa felkérésére elvégeztem Kovács László "A kiberbiztonság stratégiai megközelítése" című doktori munkájának bírálatát és véleményemet az alábbiakban foglalom össze.

Az értekezés témaválasztása, célkitűzések

A jelölt által választott téma aktualitása megítélésem szerint megkérdőjelezhetetlen. A kibertér, a kibertérben végbemenő események, műveletek, valamint a kiberbiztonság napjainkban jelentős szerepet kapnak mind a legkülönbözőbb szakterületek tudományos vizsgálataiban, mind a köznapi beszédben. A fejlett információtechnológia eredményeként kialakuló hálózatokra épülő kibertér egy olyan szolgáltatási, virtuális működési, sőt "élet"környezetté vált, amely mindenki számára érzékelhető virtuális térként, világként megélhető környezetet alkot. Ebben a "térben" szereplők tevékenykednek, folyamatok zajlanak, események történnek, amelyek pozitív hatással, vagy negatív (káros, vagy akár pusztító erejű) következményekkel vannak a "hagyományos" világ szereplőinek életére, tevékenységére.

A szerző kutatási célkitűzésének meghatározó jellemzője a kiberbiztonság stratégiai szintű megközelítése, alapvető eleme egy kiberbiztonsági stratégia modell megalkotása. Ezt meggyőző módon indokolja annak a tudományos problémának a megfogalmazásával, hogy napjaink regionális, szövetségi, és nemzeti kiberbiztonsági stratégiái nem egységes elvi alapra épülnek, pedig érvényülésük – a kibertér határokat nem ismerő jellege miatt – csak egymással összhangban, az érintett szereplők együttműködésével lehetséges.

A szakirodalomban ismereteim szerint még nem került sor a kiberbiztonsági stratégiák monografikus jellegű feldolgozására, a velük szemben támasztott általános követelmények, közös jellemzőik, általános felépítésük és tartalmi elemeik, életciklusuk elemzésére, meghatározására. E tekintetben a szerző munkája hiánypótló jelentőségű, a kérdéskör kutatásának értékes össze-

tevője lehet. A kutatási eredmények hiányával, de legalábbis szűkösségével egyetértő véleményem mellett szívesen láttam volna az értekezésben valahol (talán az 1. fejezet végén) egy önálló pontot az ezekkel a kérdésekkel foglalkozó szakirodalom ismertetésére, vagy ennek hiánya, a nem vizsgált témakörök markánsabb bemutatására.

Az alapvető kutatási célhoz (kiberbiztonsági stratégia modelljének megalkotása) a szerző által megfogalmazott részcélok jól illeszkednek: egyrészt világosabbá teszik, részletezik az alapvető cél megvalósításának útját, módszereit, és meghatározzák az azt kiegészítő, támogató célokat. Pontos és indokolt a kutatási terület lehatárolása is.

Tartalmi értékelés

Az értekezés 277 oldalon, három érdemi fejezetben, összegzett következtetésekben és az új tudományos eredményekben mutatja be a jelölt által az adott témakörben végrehajtott tudományos kutatás részleteit és eredményeit.

Az **első fejezet** 42 oldalban a kibertér és a kiberbiztonság fogalmi alapjait, napjainkban betöltött szerepük értékelését, valamint a kibertérben jelentkező stratégiai kihívásokat és veszélyeket, valamint a kapcsolódó stratégiai feladatokat tartalmazza.

A *kibertér és a kiberbiztonság alapvető fogalmainak* szerző általi értelmezése röviden kerül bemutatásra. 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.

A kiberbiztonság fogalmának rögzítésével sincs alapvető szakmai ellenvetésem, azonban a hozzá fűzött magyarázatban ellentmondás van a következő két megállapítás között: "a kiberbiztonságot olyan tevékenységek sorozataként kell vizsgálnunk, amelyek …", és "a kiberbiztonság azt az állapotot jelenti, amelyben …". A pont egészének tükrében az előbbit jelentős problémát nem okozó megfogalmazásbeli pontatlanságnak tartom. Ehhez kapcsolódóan helyesnek tartom a szerző azon álláspontját, amely a kiberbiztonságot egy elérendő, fenntartandó állapotnak tekinti, azonban szükséges lett volna ebben a pontban értelmezni, meghatározni a kibervédelem fogalmát is, amely a kiberbiztonság (mint állapot) megteremtésére és fenntartására irányuló tevékenységek összessége. Ez a kifejezés ugyanis az értekezés további részében még sok esetben szerepel, és fontos szerepet is játszik.

A *kibertér és a kiberbiztonság napjainkban betöltött szerepének* bemutatása megalapozott, szakmailag helyes. A szerző megfelelő hivatkozásokkal alátámasztott módon tárgyalja a következő három kérdést:

- a függőség növekedése az informatikai szolgáltatásoktól;
- az állami, társadalmi, gazdasági igények kielégítésének alapvető feltételrendszerét képező kritikus információs infrastruktúrák szoros, és egyre bővülő kapcsolata a kiberbiztonsággal;
- a digitalizáció társadalomra gyakorolt hatásai – a tárgyalt téma szempontjából mint a kibertér "hasznosításának" – mérésére, illetve a kiberbiztonság állapotának mérésére alkalmas indexek (DESI, GCI) célja, tartalma, alakulásuk.

A *kibertérben jelentkező stratégiai kihívások és veszélyek* vizsgálata az értekezés alapvető kutatási célkitűzéséhez igazodik. A szerző a szakirodalomban (többek között saját publikációiban) már feltárt kibertéri fenyegetéseket tárgyalja stratégiai keretbe helyezve. Ennek részeként hét fenyegetést azonosít, amelyek bemutatása önmagában szakszerű. Ezzel kapcsolatban azonban vannak hiányérzeteim.

Hiányzik annak indoklása, hogy miért ez a hét fenyegetés jelenik meg stratégiai szinten, és van-e olyan kibertéri fenyegetés, amelynek nincs stratégiai jelentősége. Ehhez szükséges lett volna a kibertéri fenyegetések szakirodalmi háttérre alapozott rövid, teljeskörű bemutatása, és a stratégiai jelentőségűnek minősítés szempontjainak meghatározása.

Hiányolom annak bemutatását is, hogy a hét fenyegetés jellege különböző, köztük összefüggések állnak fent. Kiberfegyvereket értelemszerűen használ a kiberhadviselés, de a hacktivisták is használhatják ezeket (amire a szerző is ad példát). A politikai befolyásolás eszköze nyilvánvalóan lehet kiberhadviselés részét képező kiberművelet. Összességében úgy érzem, hogy a kibertéri fenyegetések, ezen belül a stratégiai szintű fenyegetések rendszerezése nem eléggé kimunkált.

Végül a 3. ábra (38. oldal) nem megfelelően támogatja a szövegkörnyezet mondanivalóját. Egyrészt nincs összhangban azzal (a politikai befolyásolás és a kiberfegyverek helyett az IKT technológia hibáját tartalmazza), ami lehet indokolt, de ez az indoklás hiányzik. Másrészt az ábrából – legalábbis nekem – nem világos a tengelyek értelmezése. Ez lehet kétértékű (pld. nem fizikai, vagy fizikai), vagy háromértékű (nem fizikai, nem fizikai és fizikai együtt, fizikai). Valószínűleg szerencsésebb lett volna egy négy mezőre osztott ábrázolás, amelyben egyes fenye-

getések egy vagy több mezőre is kiterjednének. Nem világos az sem, hogy a fenyegetések vízszintes elhelyezkedésében látható eltéréseknek van-e jelentősége, és ha igen, akkor pld. az IKT technológia hibája miért kevésbé fizikai, mint a kritikus infrastruktúra támadása.

A *kiberbiztonsághoz kapcsolódó stratégiai feladatok* esetében a szerző úgy fogalmaz, hogy "a stratégiai szintű tevékenységek közül emelek ki néhányat a teljesség igénye nélkül". Az e pontban foglaltakkal – elfogadva, hogy a szerző ezeket az értekezés későbbi részében, a stratégiák elemzése során vizsgálja részletesebben – hasonló hiányérzetem van, mint a stratégiai fenyegetések esetében. A felsorolt öt kibervédelmi feladat szakszerű bemutatása mellett itt is hiányzik annak bemutatása, hogy milyen szempontok alapján történt a stratégiai szintű feladatok kiválasztása, milyen körből, és legalább felsorolás szinten meg kellett volna adni, mely feladatok vannak még, és azok miért nem minősülnek stratégiai szintűnek.

A 44. lábjegyzethez (49. oldal) szereplő magyarázattal ellentétben nem értek egyet azzal, hogy az offenzív jellegű – a kiberbiztonság kialakítását és fenntartását szolgáló – kibervédelmi tevékenységek kimaradtak a felsorolásból. Ezekről a szerző is azt írja, hogy "a védelem teljessé tétele érdekében szükség van". Ezek hiányában a stratégiai szintű feladatok bemutatása nem teljes. Az ehhez kapcsolódó kérdések a későbbiekben már egységes formában nem jelennek meg.

Összességében a fejezet jó alapozása az értekezés következő két fejezetének, amely a szerző által megfogalmazott új tudományos eredményt nem tartalmaz. A fejezetben foglaltak összegzése az Összegzett következtetések fejezetben szerepel. Az abban foglaltakkal alapvetően egyetértek. Teljes egészében elfogadom a szerzőnek a digitális ökoszisztéma kialakulására, ennek biztonsága alapvető fontosságára, ezen belül a kritikus infrastruktúrák védelmének kiemelt helyére, a digitális techonológia társadalmi hatásaira, valamint e hatások létező mérési módszereinek kiberbiztonsági szintet jellemző közvetett módon történő alkalmazhatóságára vonatkozó következtetéseit.

A fejezet értékes részét képezi a stratégiai szemlélet alkalmazása, érvényesítése a kibertéri fenyegetések, illetve védelmi megoldások számbavétele, bemutatása során. Emellett a korábbiakban már megfogalmazottak alapján gyengébbnek ítélem a stratégiai szintű fenyegetések, és védelmi tevékenységek meghatározásának teljességét, indoklását, és a stratégiai szintűnek minősítés kritériumainak meghatározását. Az összegzett következtetésekben megfogalmazottak közül a fejezetben (indoklással, adatokkal, hivatkozásokkal) bővebben megalapozott lehetett volna az állami támogatású kibertámadások egyre növekvő száma, illetve a fejezetben foglaltak

nem támasztják alá, hogy a kiberelrettentést a szerző azonosította, mint a védelem egyik megoldását.

ꕥ

A **második fejezet** a tartalmi fejezetek mintegy 60%-át magában foglaló 128 oldal terjedelmével az értekezés alapvető részét képezi, a nemzeti biztonság és a kiberbiztonság stratégiai összefüggéseit, a nagyhatalmak kibertérrel fennálló viszonyát, majd a kibertérhez kapcsolódó Európai Uniós, NATO, illetve nemzeti megközelítéseket, stratégiákat tárgyalja.

A *nemzeti biztonság és a kiberbiztonság stratégiai összefüggéseinek bemutatása* a stratégia fogalmának rövid, példák alapján történő értelmezésével indul, majd ismertetésre kerül az állami stratégiai dokumentumok rendszere, és ezek egymással fennálló viszonyai. A stratégia, mint azt a frissen kiadott új Hadtudományi Lexikon is tartalmazza, több értelmezést takar. Ezek közül a szerző választása nem eléggé markáns, azonban ez a központi kutatási cél szempontjából nem jelent érdemi problémát.

Szükségesnek láttam volna viszont a stratégiai dokumentum fogalmának meghatározását, értelmezését, mert ez az értekezés kulcsfogalma. Ezen kívül a nemzeti biztonsági stratégia és az ágazati (közte kiberbiztonsági) stratégiák mellett hasznos lett volna röviden bemutatni más stratégiai dokumentum típusokat is (pld. zöld könyv, fehér könyv, stratégiához kapcsolódó akcióterv), mert ilyenekre az értekezés maga is hivatkozik.

A fejezet ezt követően a *három nagyhatalom kibertérhez, kiberbiztonsághoz kapcsolódó viszonyát* ismerteti, elemzi. A 2.2 pontban bemutatott nemzeti álláspontok, stratégiai dokumentumok rendszerezett, értékelt információi megalapozottak, teljeskörűek, tudományos értéket hordoznak. Pozitívumként értékelem a kínai és orosz nézetek részletesebb bemutatását, vizsgálatát. mivel a szakirodalom általában többet, és részletesebben foglalkozik az Egyesült Államokhoz kapcsolódó információk feldolgozásával.

Ami tovább növelhette volna ezen rész értékét, az a három megközelítés összevetése, az azonosságok és különbözőségek kimutatása, illetve ez utóbbiak okainak meghatározása. Mindez megítélésem szerint erőteljesebben alapozta volna meg az általános kiberbiztonsági stratégia modell megalkotását. A tudományos probléma megfogalmazásában a szerző is hangsúlyozta, hogy a kiberbiztonsági stratégiák esetében egy nemzetközi konszenzussal létrejövő közös elvi modellre van szükség.

A nagyhatalmak után *az Európai Unió és NATO kibertérhez kapcsolódó stratégiáinak bemutatása, elemzése* Magyarország uniós, és a Magyar Honvédség szövetségi tagsága miatt

meghatározó jelentőségű. Ebben a részben a szerző egyenszilárd módon, tartalmilag és módszertanilag korrekt módon ismerteti a kiberbiztonsághoz kapcsolódó stratégiai elképzeléseket, dokumentumokat, és ezek fejlődését, változásait. Helyesen emeli ki a 2016-ban megjelent új EU kül- és biztonságpolitika, valamint a 2016-os NATO csúcstalálkozón a kibertér műveleti dimenziónak minősítése szerepét.

Ebben a részben is értéknövelőnek tartottam volna az Európai Unió és a NATO kiberbiztonsághoz kapcsolódó megközelítéseinek, álláspontjainak, stratégiai dokumentumainak összehasonlító elemzését, az eltérések indokainak feltárását. Az EU és a NATO szerepmegosztása, együttműködése folyamatos fejlődésen megy keresztül, amelynek egyik legutóbbi dokumentuma a 2018. júliusi Együttes nyilatkozat az EU-NATO együttműködésről. Eszerint az együttműködés öt fókuszterületének egyike éppen a kiberbiztonság.

A *nemzeti kiberbiztonsági elképzelések, stratégiák vizsgálata* tíz európai országra terjed ki. A szerző a vizsgálandó országokat alapos, és logikus indoklás alapján választotta ki, amelynek alapvető szempontjait már a bevezetésben, a kutatás lehatárolásában meghatározta, a választás részletesebb indokait pedig a 2.4 pont elején rögzítette. A vizsgálat egységes módszertan alapján történt. A szerző elsőként az adott állam nemzeti biztonsági stratégiáját (Magyarország esetében a nemzeti katonai stratégiát is), majd nemzeti kiberbiztonsági stratégiáját elemezte. Ez a pont az értekezés egyik különösen értékes része.

A fejezetet a vizsgált országok egyes kibertéri jellemzőit és kiberbiztonsági stratégiai céljait egységes űrlap formájában *összegző kimutatások* zárják. Az országonkénti adatok nem kerülnek együttesen, egymás mellett kimutatásra, így az egyes jellemzők összehasonlítása, általános, vagy egyedi jellege szemléletesen nem jelenik meg. A kiberbiztonsági stratégiai célok esetében az összevetés érdekében célszerű lett volna az egyedi megfogalmazásoknak a kutatási cél által meghatározott kategóriákba sorolása. Ez is alapját képezhette volna az általános jellemzők kimutatásának.

Összességében a fejezet – bár a szerző által megfogalmazott új tudományos eredményt ez sem tartalmaz – az értekezés alapvető részét, a tudományos eredmények szilárd alapját képezi. A fejezetben foglaltak összegzése az Összegzett következtetések fejezetben szerepel. A három nagyhatalomra vonatkozóan a szerző következtetésével (nemzeti biztonságuk alapvető összetevőjeként tekintenek a kibertérre és annak biztonságára, kibertéri képességeikre a nemzetközi biztonsági, gazdasági és politikai viszonyrendszerben is számítanak) egyetértek, ez azonban – bár a tartalom alátámasztja – a fejezet szövegében nem kerül markánsan megfogalmazásra, iga-

zolásra. Az EU és NATO kiberbiztonsági megközelítéseire, stratégiai dokumentumaira vonatkozóan összegzett következtetés nem kerül megfogalmazásra, amit hiányolok. Egyetértek az egyes európai országokra vonatkozó következtetéssel is (eltérő módon közelítik meg a kibertér biztonságát, de a stratégiai megközelítésben azonosíthatóak hasonló elemek), azonban a fejezetben ez sem kerül megfogalmazásra, igazolásra. Ezen észrevételeim megerősítik azon korábbi megjegyzéseimet, hogy a fejezetből mindhárom vizsgált területen hiányoznak az összehasonlító elemzések, hiányzik az azonosságok és különbözőségek kimutatása, utóbbiak okainak feltárása.

ꕥ

A 44 oldalas ***harmadik fejezet*** tárgya a nemzeti kiberbiztonsági stratégia modellje, amelyhez a stratégia végrehajtását leíró akcióterv felépítésére, illetve a végrehajtás hatékonyságát mérő indikátor-rendszer elvi alapjaira vonatkozó javaslat kapcsolódik. Ebben a fejezetben realizálódnak a szerző által megfogalmazott új tudományos eredmények.

A fejezet elsőként *a nemzeti kiberbiztonsági stratégiák kialakítására és felépítésére vonatkozó eddigi eredményeket* ismerteti. Az EU Hálózat- és Információbiztonsági Ügynökség (ENISA) által javasolt felépítés, a Nemzetközi Távközlési Egyesület (ITU) referenciamodellje, és a NATO Kiberbiztonsági Kiválósági Központ (CCDCOE) keretrendszere az értekezés tárgyához illeszkedő tartalommal és mélységben, szakszerűen kerül bemutatásra.

Ezt szerzőnek *a megvizsgált kiberbiztonsági stratégiák elemzéséből levont következtetései* követik. Elsőként az Európai Uniós és NATO, majd a nemzeti stratégiákból önállóan levont következtetések kerülnek megfogalmazásra. Ezeket a szerző megítélésem szerint jól választotta ki, és öntötte formába, megalapozottak, tárgyszerűek, a második fejezetben foglaltakra épülnek. Ezt a hasonlóan jó minőségű szintetizált következtetések követik, amelyben kiemelt szerepet játszik a stratégia legfontosabb elemeinek felsorolása. Ennek értékét javította volna a vizsgált 15 kiberbiztonsági stratégiában történő előfordulásuk (arányuk) megadása, illetve a listába be nem került, de egy, vagy több stratégiában szereplő elem megadása. Mindez megvalósítható lett volna egy szemléletességet biztosító táblázat formájában.

A pont végén szereplő, a stratégiai célok elérését időszakosan vizsgáló független szakmai testület szükségességére és összetételére vonatkozó következtetést jelenlegi formájában nem látom kellően megalapozottnak. Erre vonatkozó megállapításokat az értekezés korábbi részeiben – talán saját hibámból, de – nem találtam.

A 3.3 pont első része *a nemzeti kiberbiztonsági stratégia modelljére tett javaslatot* tartalmazza, amely a szerző 1. tudományos eredménye. Ez az utolsó pontban szereplő értékelési rendszer kivételével megegyezik a korábban megfogalmazott szintetizált következtetésekkel. Ez utóbbi azonban indoklás nélkül jelenik meg a javaslatban, az értekezés korábbi részeiben ehhez kapcsolódó markáns utalást, következtetést nem találtam. A kérdéskörhöz egyedül a korábban általam szintén nem kellően megalapozottnak minősített független szakmai vizsgáló testület kapcsolódik.

A stratégia általános elemei mellett a szerző célszerűnek látja megjeleníteni a hadsereg szerepét az ország kibervédelmében, és felsorolja az ehhez kapcsolódó, a stratégiában szerepeltetendő kérdéseket. Ehhez kapcsolódóan fogalmazza meg azt a véleményét, hogy a kiberbiztonsághoz kapcsolódóan szükség van kibertámadási képességekre is. Ezekkel a megállapításokkal magam teljes mértékben egyetértek, azonban megítélésem szerint a kérdéskör nem kellően kidolgozott.

A kiberbiztonság kialakítására és fenntartására irányuló kibertámadási képességekre vonatkozó javaslat az értekezés korábbi részeiben nincs megalapozva, ehhez kapcsolódó hivatkozások, elemzések, megállapítások nem szerepelnek. Hiányoznak az elrettentést szolgáló támadó képességekre, valamint a védelmi célú megelőző támadó képességekre vonatkozó kutatási részeredmények.

A 3.3 pont második része *a nemzeti kiberbiztonsági stratégia életciklusára vonatkozó javaslatot* tartalmazza, amely a szerző 2. tudományos eredménye. A bemutatott életciklus modell megalapozott, illeszkedik a stratégiák életciklusára vonatkozó tudományos eredményekhez (bár ezekre hivatkozásokat nem tartalmaz), és a kiberbiztonsági stratégiákra vonatkozó korszerű, az értekezésben is ismertetett eddigi eredményekhez. Az életciklus fázisok és azok javasolt tevékenységeinek meghatározása logikus, teljeskörű, összehangolt. A megfogalmazottak levezethetőek az értekezés korábbi részeiben foglaltakból.

Egyetértek a stratégiai szintű kiberválságkezelési terv szükségességére, jellegére, tartalmára vonatkozó megállapítással is. Ennek vizsgálati mélységét azonban nem tartom elég mélynek. Megítélésem szerint részletesebben kellene elemezni, hogy mi minősül stratégiai szintű kiberválságnak, sőt meg kellene határozni magának a kiberválságnak a fogalmi alapjait is, kapcsolatrendszerét a kiberbiztonsági eseményekkel (incidensekkel).

A 3.4 pont *a kiberbiztonsági stratégia végrehajtását vezérlő akcióterv felépítésére vonatkozó javaslatot* tartalmazza, amely a szerző 3. tudományos eredménye. A javaslatban foglaltakkal kapcsolatban elvi ellenvetésem nincs, azonban a megfogalmazott követelmények, az akcióterv javasolt elemei túl általánosak, érdemi tudományos eredményt nem tartalmaznak. A javaslat az értekezés korábbi részeiben lényegében nincs megalapozva. Tulajdonképpen a pontban foglaltak, és a 10. ábra tartalma a kiberbiztonsági jelző törlése, vagy bármely más szakterülettel történő felcserélése esetén is érvényesek lennének.

A fejezet utolsó pontja *a kiberbiztonsági stratégia végrehajtási szintjének mérési rendszerére vonatkozó javaslatot* tartalmazza, amely a szerző 4. tudományos eredménye. Teljes egészében egyetértek a szerzőnek az indikátorokra (mutatókra) épülő mérési rendszer szükségességére, rendeltetésére vonatkozó megállapításával. Ez egyébként levezethető a stratégiai tervezés szakirodalmának eredményeiből is. Megalapozottnak tartom az indikátor-rendszer célterületeire vonatkozó javaslatot is, amely összhangban van a kiberbiztonsági stratégia felépítésére vonatkozó javaslattal. A javaslatnak kiemelten értékes része a konkrét indikátorok meghatározása.

Összességében a fejezet eredményesen zárja az értekezés tartalmi részét. A szerző a kiberbiztonsági stratégiákra vonatkozó eddigi eredmények bemutatását, valamint a 2. fejezetben foglalt elemzésekből levont következtetések megfogalmazását követően javaslatot tesz a kiberbiztonsági stratégiák általános felépítésére (modelljére), életciklusára, a végrehajtását támogató akcióterv általános felépítésére, valamint megvalósulásának mérési (indikátor) rendszerére. Az akciótervre vonatkozó résztől eltekintve a javaslatok megítélésem szerint megalapozottak, indokoltak, szakszerűek.

Formai értékelés

Az értekezés megfelel a doktori munkával szemben támasztott követelményeknek. Rendelkezik mindazokkal a formai elemekkel, összetevőkkel, amelyeket az MTA Doktori Szabályzata, a tartalom, és a tudományos kutatás szabályai megkövetelnek. Az értekezést záró rövidítések jegyzéke, illusztrációk jegyzéke, táblázatok jegyzéke és irodalomjegyzék nélküli mintegy 11 ívnyi terjedelme megfelel a IX. Gazdaság- és Jogtudományok Osztálya DSc Ügyrendjében foglaltaknak (minimum 8, maximum 16 szerzői ív).

A forráskezelés korrekt, a hivatkozások, lábjegyzetek megfelelnek a tudományos publikálás követelményeinek. A feldolgozott irodalom széleskörű, a 227 dokumentum, publikáció megítélésem szerint tartalmazza az értekezés témája szempontjából releváns anyagokat.

Az értekezés ábrái, táblázatai jól segítik a mondanivaló megértését, növelik szemléletességét. Az ábrák egy kivételével jól szerkesztettek, áttekinthetőek, a 3. ábra értelmezése azonban számomra nem világos. Egy helyen – a 2.5 pont végén, a kiberbiztonsági stratégiák jellemzőinek együttes megjelenítése esetében – a szerző nem élt a táblázatos szemléltetés lehetőségével.

Az értekezés nyelvezete helyesírási, stilisztikai és esztétikai szempontból jó szintű, szakszerű, könnyen érhető. A használt terminológia pontos. Az értekezés tudományos stílusa színvonalas, jó minőségű. Hiányosságnak egyedül a fejezeteket záró összegzések elmaradását tartom.

Összegzés

Összességében az értekezés elsősorban a hadtudomány, de néhány más tudományág szempontjából is rendkívül aktuális témát, a kiberbiztonság stratégiai tervezésének kérdéseit, a kiberbiztonsági stratégiák általános követelményeit, jellemzőit, és az ehhez kapcsolódó feladatokat dolgozza fel a teljesség igényével. Meghatározó jellemzője a szakirodalomban gyakrabban alkalmazott technikai megközelítés helyett a stratégiai szemlélet alkalmazása. A munka hiteles adatokat tartalmaz, a szerző korábbi kutatásaira épül, azokat új eredményekkel bővíti.

A szerző értekezésének zárásaként négy, egymással összefüggő, egymásra épülő új tudományos eredményt fogalmaz meg. Ezek közül az 1., 2. és 4. – a kiberbiztonsági stratégia modelljére, életciklusára, és a végrehajtásának hatékonyságát mérő indikátor-rendszerre vonatkozó – eredményt elfogadom. A 3. eredményt azonban az értekezésben foglalt tartalommal nem tartom érdemi új tudományos eredménynek, megalapozottnak, nem fogadom el.

Mindezek alapján úgy ítélem meg, hogy Kovács László a PhD értekezésének megszerzését követő kutatási tevékenységével jelentős új eredményekkel gyarapította a hadtudományt. Értekezése alkalmas a nyilvános vitára, így az értekezést ***védési eljárásra javaslom,*** valamint a vita sikeres lefolytatása után a doktori munka elfogadását és ***az MTA doktori cím odaítélését javaslom***.

Budapest, 2020. január 18.

(Dr. Munk Sándor)
professor emeritus
az MTA doktora