Prof. Dr. Rajnai Zoltán PhD
Magyarország kiberkoordinátora

# Hivatalos bírálat

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

Az MTA Doktori Tanácsa felkérésére elvégeztem Prof. Dr. Kovács László ***"A kiberbiztonság stratégiai megközelítése"*** című doktori Dsc értekezésének bírálatát, amelyet az MTA Doktori szabályzata, az MTA IX. osztály és a Hadtudományi Bizottság követelményrendszere alapján készítettem el. Megállapításaimat az alábbiakban foglalom össze.

***Az értekezésekkel szembeni követelmények teljesülése:***
Prof. Dr. Kovács László eredeti, önálló tudományos teljesítményének igazolására alkalmas értekezést nyújtott be. Terjedelmét tekintve megfelel a követelményeknek, a 270 oldal tartalmi részből, összegzett következtetésekből és új tudományos eredményekből összeállított dolgozat formai és tartalmi szempontból is teljesíti a követelményeket.

**Témaválasztás, a téma aktualitása**
Az Európai Unió az elmúlt években stratégiai szintű döntéseket hozott az Uniót érintő kiberbiztonság erősítésében. Elfogadta a tagországokra nézve kötelező érvényű „Hálózatbiztonsági irányelveket” (NIS direktíva), megalkotta az EU kiberbiztonsági stratégiáját, és a hazai jogrendben megkezdődött a stratégiai szintű gondolkodásmód kialakítása.
A kibertér védelme, az online tér mindennapi használata, a kiberbűnözés terjedése arra készteti a döntéshozókat, hogy minél szélesebb körben törekedjenek a problémák feltárására, keressenek megoldásokat a biztonságos tér használatára.
A szerző a kiberteret mint mindennapi alkalmazandó környezetet értékeli, a benne zajló műveletekkel, amelyeket nemcsak pozitív értelemben kell és lehet értelmezni. A virtuális teret átszövi a technológiai fejlődés, elegendő, ha csak a mobiltelefonok, a mobil internet világára gondolunk; ma már az ötödik generációs hálózatok működtetéséről beszélhetünk néhány évtizednyi evolúció „termékeként”.
És ez a virtuális tér nemcsak a pozitív hatású alkalmazásokra kész, hanem a károkozó, szándékos sérüléseket, hátrányokat, befolyásokat is okozni képes, nem ritkán kormányzati „szponzorációval”, és nem riadnak vissza kormányzati, állami vagy akár kritikus infrastruktúrákat romboló tevékenységektől sem.

A jelölt tudományos problémafelvetésével egyetértek, ami szerint a stratégiák többnyire statikusak, míg a kibertérre jellemző dinamizmus csak kis mértékben képes megjelenni a szabályzás rendszerében.
Elfogadom azt a problémafelvetést is, hogy az egyes országok nemzeti szinten csak korlátozott hatású elveket és szervezeti hátteret képesek megalkotni.

Megítélésem szerint a jelölt jól határolta körül kutatási célkitűzéseit, jónak tartom, hogy felvállalta egy kiberstratégiai modell megalkotását, és ennek érdekében elemzi a nemzetközi szervezetek, a nemzetközi szövetségek, a nagyhatalmak kibertér-beli tevékenységeit, következtetéseket von le.

A mérőrendszer elvi alapjainak és indikátorainak meghatározása alapján a stratégia mérhetővé tétele eddig nem kutatott területek közé tartozik.

Összesítve tehát a jelölt egy rendkívül aktuális, stratégiai területen eddig kevésbé kutatott témát vizsgál, eredményei elméleti és gyakorlati szinten is alkalmazhatóak.

**Tartalmi értékelés:**
Az értekezés tartalmi részét a szerző három fejezetben foglalta össze. A fejezetek logikus sorrendben követik egymást. A második fejezet, még ha méretében nagyobb terjedelmű is a másik két fejezettel összehasonlítva, fontos része a kifejtésnek, hiszen több ország stratégiáját veszi górcső alá

Az ***első fejezet***ben vizsgált kibertér, kiberbiztonság fogalomrendszerének értelmezése, a napjainkban betöltött szerep vizsgálata meghatározza, segíti a dolgozat közös értelmezését. Ugyanakkor meg kívánom jegyezni, hogy a kibertér fogalmi meghatározására számtalan „definíció" található, amennyiben a szerző egy értekezésben használt kifejezésrendszert akarna használni, úgy érdemes lett volna a definíciók értékelése, vagy azokból egy konzekvens meghatározás generálása.

Fontosnak tartom, hogy a stratégiák értékelését megelőzően a jelölt a kibertérben jelentkező stratégiai kihívásokat és veszélyeket bemutatja. A hét kiberbiztonsági fenyegetés és kihívás véleményem szerint keveredik a biztonság és a védelem között. A kibervédelem területei közé sorolnám a kiberhadviselést és a kiberfegyverek elterjedését, míg a másik öt kategória kiegészíthető lenne a nemzeti stratégia által is deklarált kibertér biztonságos alkalmazása érdekében meghatározható kiberbűnözés egyes válfajaival, vagy a gyermekvédelem témakörével is.

Ezt az alfejezetet szűkszavúnak érzem, a stratégiai gondolkodás szempontjából és a stratégiaalkotásból adódóan hiányérzetem volt a fejezet olvasásakor.
Nem leltem fel a gazdasági visszaélésekre utalást sem, holott a régiónkban az elmúlt öt-hat évben megtízszereződött az online térben elkövetett, informatikai eszközökkel és rendszerekkel végrehajtott anyagi haszonszerzésből elkövetett műveletek száma.

Ugyanakkor elfogadom, hogy a jelölt katonai műszaki-hadtudományi területű értelmezését adja a kihívásoknak és a veszélyeknek, ha ez megjelent volna szöveges tartalomban is, úgy a bíráló könnyebb helyzetben lenne a bírálat elkészítésekor.

A szerző által megjelölt alátámasztó források korrektek, frissek, mutatják a pályázó kutatási eredményességét, alkalmazhatóságát.

Összefoglalva az első fejezet megalapozza az értekezés további fejezeteit, elsősorban a közös értelmezést segíti elő. A fejezetben leírtakkal alapvetően egyetértek, elfogadom a digitális ökoszisztéma kialakulására, a létfontosságú infrastruktúrák kiemelt védelmére, létező mérési módszerek alkalmazhatóságára vonatkozó következtetéseket. Ez a fejezet alapvetően a jelölt gondolkodás és felfogásmódjának értelmezését adja új tudományos eredmények nélkül, de az e fejezetben rögzítettek nélkül nehezen értelmezhető lett volna a másik két fejezet.
A jelölt állításaiban megfogalmazottakkal egyetértek, ugyanakkor a stratégiai veszélyek, kihívások bemutatása, értékelése véleményem szerint elnagyoltra sikerült.

A ***második fejezet*** taglalja a kiberbiztonság stratégiai megjelenését. Itt ismerteti álláspontját a stratégiák kapcsolatrendszerében, bemutatja a nagyhatalmak (USA, Kína, Oroszország) stratégiai koncepcióit. Ez a rész alapvetően leíró jellegű, a személyes következtetések mélyebb bemutatását, értékelését hiányolom. A következő alfejezetben (2.3) az EU és a NATO stratégiai felfogását mutatja be, elsősorban a feldolgozott irodalom alapján.
A számomra legérdekesebb rész ebben a fejezetben a 2.4 alfejezet, ahol tíz ország kiberbiztonsági stratégiáit elemzi a jelölt. Ebben bemutatja a stratégiák fő célkitűzéseit, összegzi azok fő összetevőit. Sikeres és jó értékelési rendszerben mutatja be a stratégiákat.

Ugyanakkor a szövetségi-közösségi rendszerek bemutatása területén hiányolom a (bár közös stratégiával nem rendelkező) Közép-Európai Kiberbiztonsági Platform (V4 országok+Ausztria) stratégiai törekvéseit.

Egyetértek azon felvetésekkel, hogy az egyes országok más-és más módon értékelik a kiberbiztonság stratégiai megközelítését, ezek a nemzeti érdekekből és értékekből is következhetnek.

Sikeres lehetett volna a fejezetben egy azonosságokon alapuló összehasonlítás, ami bemutatja, hogy az egyes országok értékelése milyen alapon nyugszik, komolyabb értékelési rendszerrel bemutatni az egyes országok stratégiai érdekeit, és elemzésekkel alátámasztja azokat. A fejezet a jelölt által is deklaráltan nem tartalmaz új tudományos eredményeket, viszont jelentős irodalomfeldolgozáson alapul, ez a dolgozat (és a jelölt) nagy érdeme.

A ***harmadik fejezet*** a nemzeti kiberbiztonsági stratégia modellje témakörben roppant érdekes, előre mutató és új tudományos eredményeket is tartalmaz. Itt található meg a jelölt összegző, lényeglátó képessége, a kreatív értékelés és modellalkotás is, ami elvezet az új eredményekhez.

A szerző bemutatja a nemzeti kiberbiztonsági stratégiák kialakítására és felépítésére utaló elért eredményeket, bemutatja a modellalkotás lehetőségét, majd a kiberbiztonsági stratégiák elemzéséből levont következtetések követik a gondolatmenetet.

A nemzeti kiberbiztonsági stratégia életciklusára vonatkozó javaslatok előremutatóak, helyesek és új tudományos eredmények között is megállják helyüket.

Hasznosnak ítélem meg a stratégiai szintű kiberválság kezelési terv fontosságára, összetételére vonatkozó megállapításokat, jól mutatja a jelölt álláspontját, hozzáértését, eltökéltségét és következetességét a témában.

A kiberbiztonsági stratégia mérési rendszerére vonatkozó javaslatait megalapozottnak tartom, azok helyesek és jók. Hasznosnak és alkalmazhatónak tartom az indikátorrendszer kimunkálását, új tudományos eredményként elfogadom és ajánlani tudom.

Összefoglalva ez a fejezet a dolgozat nagyon értékes, új tudományos eredményeket tartalmazó része, amelyik jól mutatja a jelölt mély kutatási eredményeit, kutatói affinitását.

Hiányolom (mint mindegyik fejezetnél) a fejezet végi összefoglalót, jól segítené az ismerethalmaz rendszerezését.

***Formai észrevételek:***
A jelölt a dolgozatot formailag az MTA Doktori Szabályzata és a IX. Osztály DSc Ügyrendjében foglaltaknak megfelelően készítette el. Formailag jól szerkesztett, arányos, ábrái megfelelőek, bár egyes esetekben nyomtatásban nehezen olvashatók (pl.: 5. ábra).

Forráskezelése szabályos, hivatkozásai, lábjegyzetei tartalmazzák a szükséges bibliográfiai adatokat, azok visszakövethetők. Az értekezés nyelvezete magyaros, kellően szakmai, tudományos igényességgel elkészített értekezés.

Megállapítom, hogy az értekezés kellően alátámasztottan új tudományos eredményeket tartalmaz, a szerző által megjelölt eredményeket elfogadom.

Úgy ítélem meg, hogy Kovács László kutatási eredményei gazdagítják a katonai műszaki és a hadtudományokat, dolgozata hiánypótló . Az értekezés nyilvános vitára, védési eljárásra javaslom

***Sikeres vita után az MTA doktori cím odaítélését javaslom!***

**Kérdésem a jelölthöz:**
- 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?

Budapest, 2020. február 10.

Prof. Dr. Rajnai Zoltán PhD
Magyarország kiberkoordinátora

Prof. Dr. Rajnai Zoltán PhD
Magyarország kiberkoordinátora

# Hivatalos bírálat

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

Az MTA Doktori Tanácsa felkérésére elvégeztem Prof. Dr. Kovács László ***"A kiberbiztonság stratégiai megközelítése"*** című doktori Dsc értekezésének bírálatát, amelyet az MTA Doktori szabályzata, az MTA IX. osztály és a Hadtudományi Bizottság követelményrendszere alapján készítettem el. Megállapításaimat az alábbiakban foglalom össze.

***Az értekezésekkel szembeni követelmények teljesülése:***
Prof. Dr. Kovács László eredeti, önálló tudományos teljesítményének igazolására alkalmas értekezést nyújtott be. Terjedelmét tekintve megfelel a követelményeknek, a 270 oldal tartalmi részből, összegzett következtetésekből és új tudományos eredményekből összeállított dolgozat formai és tartalmi szempontból is teljesíti a követelményeket.

**Témaválasztás, a téma aktualitása**
Az Európai Unió az elmúlt években stratégiai szintű döntéseket hozott az Uniót érintő kiberbiztonság erősítésében. Elfogadta a tagországokra nézve kötelező érvényű „Hálózatbiztonsági irányelveket” (NIS direktíva), megalkotta az EU kiberbiztonsági stratégiáját, és a hazai jogrendben megkezdődött a stratégiai szintű gondolkodásmód kialakítása.
A kibertér védelme, az online tér mindennapi használata, a kiberbűnözés terjedése arra készteti a döntéshozókat, hogy minél szélesebb körben törekedjenek a problémák feltárására, keressenek megoldásokat a biztonságos tér használatára.
A szerző a kiberteret mint mindennapi alkalmazandó környezetet értékeli, a benne zajló műveletekkel, amelyeket nemcsak pozitív értelemben kell és lehet értelmezni. A virtuális teret átszövi a technológiai fejlődés, elegendő, ha csak a mobiltelefonok, a mobil internet világára gondolunk; ma már az ötödik generációs hálózatok működtetéséről beszélhetünk néhány évtizednyi evolúció „termékeként”.
És ez a virtuális tér nemcsak a pozitív hatású alkalmazásokra kész, hanem a károkozó, szándékos sérüléseket, hátrányokat, befolyásokat is okozni képes, nem ritkán kormányzati „szponzorációval”, és nem riadnak vissza kormányzati, állami vagy akár kritikus infrastruktúrákat romboló tevékenységektől sem.

A jelölt tudományos problémafelvetésével egyetértek, ami szerint a stratégiák többnyire statikusak, míg a kibertérre jellemző dinamizmus csak kis mértékben képes megjelenni a szabályzás rendszerében.
Elfogadom azt a problémafelvetést is, hogy az egyes országok nemzeti szinten csak korlátozott hatású elveket és szervezeti hátteret képesek megalkotni.

Megítélésem szerint a jelölt jól határolta körül kutatási célkitűzéseit, jónak tartom, hogy felvállalta egy kiberstratégiai modell megalkotását, és ennek érdekében elemzi a nemzetközi szervezetek, a nemzetközi szövetségek, a nagyhatalmak kibertér-beli tevékenységeit, következtetéseket von le.

A mérőrendszer elvi alapjainak és indikátorainak meghatározása alapján a stratégia mérhetővé tétele eddig nem kutatott területek közé tartozik.

Összesítve tehát a jelölt egy rendkívül aktuális, stratégiai területen eddig kevésbé kutatott témát vizsgál, eredményei elméleti és gyakorlati szinten is alkalmazhatóak.

**Tartalmi értékelés:**
Az értekezés tartalmi részét a szerző három fejezetben foglalta össze. A fejezetek logikus sorrendben követik egymást. A második fejezet, még ha méretében nagyobb terjedelmű is a másik két fejezettel összehasonlítva, fontos része a kifejtésnek, hiszen több ország stratégiáját veszi górcső alá

Az ***első fejezet***ben vizsgált kibertér, kiberbiztonság fogalomrendszerének értelmezése, a napjainkban betöltött szerep vizsgálata meghatározza, segíti a dolgozat közös értelmezését. Ugyanakkor meg kívánom jegyezni, hogy a kibertér fogalmi meghatározására számtalan „definíció" található, amennyiben a szerző egy értekezésben használt kifejezésrendszert akarna használni, úgy érdemes lett volna a definíciók értékelése, vagy azokból egy konzekvens meghatározás generálása.

Fontosnak tartom, hogy a stratégiák értékelését megelőzően a jelölt a kibertérben jelentkező stratégiai kihívásokat és veszélyeket bemutatja. A hét kiberbiztonsági fenyegetés és kihívás véleményem szerint keveredik a biztonság és a védelem között. A kibervédelem területei közé sorolnám a kiberhadviselést és a kiberfegyverek elterjedését, míg a másik öt kategória kiegészíthető lenne a nemzeti stratégia által is deklarált kibertér biztonságos alkalmazása érdekében meghatározható kiberbűnözés egyes válfajaival, vagy a gyermekvédelem témakörével is.

Ezt az alfejezetet szűkszavúnak érzem, a stratégiai gondolkodás szempontjából és a stratégiaalkotásból adódóan hiányérzetem volt a fejezet olvasásakor.
Nem leltem fel a gazdasági visszaélésekre utalást sem, holott a régiónkban az elmúlt öt-hat évben megtízszereződött az online térben elkövetett, informatikai eszközökkel és rendszerekkel végrehajtott anyagi haszonszerzésből elkövetett műveletek száma.

Ugyanakkor elfogadom, hogy a jelölt katonai műszaki-hadtudományi területű értelmezését adja a kihívásoknak és a veszélyeknek, ha ez megjelent volna szöveges tartalomban is, úgy a bíráló könnyebb helyzetben lenne a bírálat elkészítésekor.

A szerző által megjelölt alátámasztó források korrektek, frissek, mutatják a pályázó kutatási eredményességét, alkalmazhatóságát.

Összefoglalva az első fejezet megalapozza az értekezés további fejezeteit, elsősorban a közös értelmezést segíti elő. A fejezetben leírtakkal alapvetően egyetértek, elfogadom a digitális ökoszisztéma kialakulására, a létfontosságú infrastruktúrák kiemelt védelmére, létező mérési módszerek alkalmazhatóságára vonatkozó következtetéseket. Ez a fejezet alapvetően a jelölt gondolkodás és felfogásmódjának értelmezését adja új tudományos eredmények nélkül, de az e fejezetben rögzítettek nélkül nehezen értelmezhető lett volna a másik két fejezet.
A jelölt állításaiban megfogalmazottakkal egyetértek, ugyanakkor a stratégiai veszélyek, kihívások bemutatása, értékelése véleményem szerint elnagyoltra sikerült.

A ***második fejezet*** taglalja a kiberbiztonság stratégiai megjelenését. Itt ismerteti álláspontját a stratégiák kapcsolatrendszerében, bemutatja a nagyhatalmak (USA, Kína, Oroszország) stratégiai koncepcióit. Ez a rész alapvetően leíró jellegű, a személyes következtetések mélyebb bemutatását, értékelését hiányolom. A következő alfejezetben (2.3) az EU és a NATO stratégiai felfogását mutatja be, elsősorban a feldolgozott irodalom alapján.
A számomra legérdekesebb rész ebben a fejezetben a 2.4 alfejezet, ahol tíz ország kiberbiztonsági stratégiáit elemzi a jelölt. Ebben bemutatja a stratégiák fő célkitűzéseit, összegzi azok fő összetevőit. Sikeres és jó értékelési rendszerben mutatja be a stratégiákat.

Ugyanakkor a szövetségi-közösségi rendszerek bemutatása területén hiányolom a (bár közös stratégiával nem rendelkező) Közép-Európai Kiberbiztonsági Platform (V4 országok+Ausztria) stratégiai törekvéseit.

Egyetértek azon felvetésekkel, hogy az egyes országok más-és más módon értékelik a kiberbiztonság stratégiai megközelítését, ezek a nemzeti érdekekből és értékekből is következhetnek.

Sikeres lehetett volna a fejezetben egy azonosságokon alapuló összehasonlítás, ami bemutatja, hogy az egyes országok értékelése milyen alapon nyugszik, komolyabb értékelési rendszerrel bemutatni az egyes országok stratégiai érdekeit, és elemzésekkel alátámasztja azokat. A fejezet a jelölt által is deklaráltan nem tartalmaz új tudományos eredményeket, viszont jelentős irodalomfeldolgozáson alapul, ez a dolgozat (és a jelölt) nagy érdeme.

A ***harmadik fejezet*** a nemzeti kiberbiztonsági stratégia modellje témakörben roppant érdekes, előre mutató és új tudományos eredményeket is tartalmaz. Itt található meg a jelölt összegző, lényeglátó képessége, a kreatív értékelés és modellalkotás is, ami elvezet az új eredményekhez.

A szerző bemutatja a nemzeti kiberbiztonsági stratégiák kialakítására és felépítésére utaló elért eredményeket, bemutatja a modellalkotás lehetőségét, majd a kiberbiztonsági stratégiák elemzéséből levont következtetések követik a gondolatmenetet.

A nemzeti kiberbiztonsági stratégia életciklusára vonatkozó javaslatok előremutatóak, helyesek és új tudományos eredmények között is megállják helyüket.

Hasznosnak ítélem meg a stratégiai szintű kiberválság kezelési terv fontosságára, összetételére vonatkozó megállapításokat, jól mutatja a jelölt álláspontját, hozzáértését, eltökéltségét és következetességét a témában.

A kiberbiztonsági stratégia mérési rendszerére vonatkozó javaslatait megalapozottnak tartom, azok helyesek és jók. Hasznosnak és alkalmazhatónak tartom az indikátorrendszer kimunkálását, új tudományos eredményként elfogadom és ajánlani tudom.

Összefoglalva ez a fejezet a dolgozat nagyon értékes, új tudományos eredményeket tartalmazó része, amelyik jól mutatja a jelölt mély kutatási eredményeit, kutatói affinitását.

Hiányolom (mint mindegyik fejezetnél) a fejezet végi összefoglalót, jól segítené az ismerethalmaz rendszerezését.

***Formai észrevételek:***
A jelölt a dolgozatot formailag az MTA Doktori Szabályzata és a IX. Osztály DSc Ügyrendjében foglaltaknak megfelelően készítette el. Formailag jól szerkesztett, arányos, ábrái megfelelőek, bár egyes esetekben nyomtatásban nehezen olvashatók (pl.: 5. ábra).

Forráskezelése szabályos, hivatkozásai, lábjegyzetei tartalmazzák a szükséges bibliográfiai adatokat, azok visszakövethetők. Az értekezés nyelvezete magyaros, kellően szakmai, tudományos igényességgel elkészített értekezés.

Megállapítom, hogy az értekezés kellően alátámasztottan új tudományos eredményeket tartalmaz, a szerző által megjelölt eredményeket elfogadom.

Úgy ítélem meg, hogy Kovács László kutatási eredményei gazdagítják a katonai műszaki és a hadtudományokat, dolgozata hiánypótló . Az értekezés nyilvános vitára, védési eljárásra javaslom

***Sikeres vita után az MTA doktori cím odaítélését javaslom!***

**Kérdésem a jelölthöz:**
- 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?

Budapest, 2020. február 10.

Prof. Dr. Rajnai Zoltán PhD
Magyarország kiberkoordinátora