NEMZETI KÖZSZOLGÁLATI EGYETEM

Hadtudományi Doktori Iskola

TÉZISFÜZET

Berzsenyi Dániel:

Különleges kiberműveletek

A kiber különleges műveleti képesség és kialakításának vizsgálata

című Ph.D. értekezéséhez

Témavezetők:

Prof. Dr. Szenes Zoltán ny. vezérezredes

Prof. Dr. Kovács László dandártábornok

Budapest, 2022

Tartalomjegyzék

Bevezetés 3
A kutatási probléma azonosítása 4
Kutatási célok 6
Hipotézis 7
Módszertani áttekintés 9
Az elvégzett vizsgálat tömör leírása 10
Összegzett következtetések 13
Új tudományos eredmények 16
Az értekezés kutatási és tudományos eredményeinek felhasználhatósága 17
A szerző témával kapcsolatban megjelent publikációi 18
A doktorjelölt szakmai-tudományos életrajza 20

Bevezetés

A konfliktusok egyidősek az emberiség történelmével. A különböző értékek és érdekek mentén kialakuló nézeteltérések rendezésére az emberi társadalmak az eszközök széles skáláját alakították ki, melyek között a számtalan békés módszer mellett megtalálhatók az erőszak alkalmazásának különböző formái is. A konfliktusok történetét vizsgálva kiderül, hogy az érdekelt felek és vezetőik eltérő módon igyekeztek a rendelkezésükre álló eszközrendszert alkalmazni. A napjaink nemzetközi rendszerében igénybe vett eszközökre hatást gyakorol, hogy a kétpólusú világrend felbomlásával a biztonsági kihívások, kockázatok és fenyegetések egyrészt kibővültek, másrészt olyan szereplők igyekeznek érdekeiket érvényesíteni, akik különböző kultúrkörhöz tartoznak, illetve eltérő fejlettségi szinttel, erőforrásokkal és biztonságpercepcióval rendelkeznek. Ezeknek a hatásoknak a következménye az aszimmetrikus képességek térnyerése, a hagyományos és nem hagyományos hadviselési formák kevert (hibrid) alkalmazásának terjedése, valamint az információs hadviselés, a kiberhadviselés és a kibertérben végzett hírszerző tevékenység szerepének felértékelődése. Utóbbiak az emberiség technikai fejlődésének következtében olyan képességeket és műveleteket is lefednek, amelyekkel szemben kifinomultságuk, komplexitásuk, valamint időbeli és térbeli kiterjedtségük okán egyéni és társadalmi szinten egyaránt védtelenekké válunk.

Napjaink nemzetközi rendszere több pólusú és meghatározó az összekapcsoltság, valamint a kölcsönös függőség jelensége. Emiatt az érdekek érvényesítése és a konfliktusok kezelése kizárólag hagyományos módszerekkel egyre kevésbé hatékony, különösen a háborús küszöb alatti konfliktusokban, illetve a nemzetközi kapcsolatok nyíltan fel nem vállalt tevékenységeit rejtő „szürke zónában”. A 21. század turbulens világpolitikai körülményei jelentős kihívások elé állítják a nemzetközi kapcsolatok szereplőit, elmossák a hatalmi erőviszonyokat, valamint a határokat a konfliktusok különböző szintjei között és az érdekérvényesítés eszközeinek kreatív alkalmazására ösztönöznek. A nemzeti érdekérvényesítés eszköztárában a nem hagyományos módszernek tekintett kiberműveleti képességek megítélése és stratégiai beágyazottsága eltérő. A stratégiai és technológiai téren egyaránt érettebb szereplők a kiberműveleti képességek teljes spektrumát igyekeznek lefedni, amihez különleges szemléletmódot alkalmaznak, valamint védekező (defenzív) és támadó (offenzív) komponenseket egyaránt működtetnek. A komponensek integrált alkalmazása kimutatható párhuzamot jelez olyan fenyegetések ismert paramétereivel, amikhez a

kiberbiztonsági ágazat a legjelentősebb negatív hatásokat köti és amire a tudományos kutató és szakmai elemző közösség nem, vagy csak részleges figyelmet fordított.

A kiberműveleti képességek jelentőségének vizsgálatakor tekintettel kell lenni az egyik alapvető sajátosságra, a többszöröző (multiplikáló) hatásra. Ez egyfelől tetten érhető a fizikai világban a különleges műveleti tevékenységek során is, másfelől különösen fontos a kevésbé érett, illetve korlátozott erőforrásokkal rendelkező szereplők számára. Ebből kiindulva egy sajátos modell kialakításával, specifikus kiberbiztonsági kihívások paramétereivel ötvözve vizsgálom a kiberműveleti képességekben rejlő lehetőségeket kisállami szemszögből. A kiberműveleti képességek széles skáláján belül a kutatás fókuszában azok a speciális motívumok állnak, amelyek túlmutatnak a reguláris tevékenységeken, akár csak a fizikai hadszíntereken a különleges műveleti erők alkalmazása. Módszertani szempontból a kiber különleges műveleti képességek kialakításának vizsgálatát alaposabbá és informatívabbá teszi, három aspektus elemzése és összehasonlítása: a stratégiai dokumentumok és beágyazottság, a különleges műveleti tevékenységek sajátosságai, valamint a legjelentősebb negatív hatásokat kiváltó kiberfenyegetések paraméterei. Az ezek alapján folytatott kutatással új tudományos eredményekre, valamint a nemzetközi jógyakorlatokat tartalmazó értékes háttérismeretekre tehetünk szert. Kutatásom éppen ezért kitér a kiber különleges műveleti képességek kialakításával összefüggő követelmények és mintázatok azonosítására.

A kutatási probléma azonosítása

Miközben a kiberbiztonsági incidensekhez kapcsolódó valamennyi mérőszám drasztikus növekedést mutat, a társadalom egyre szélesebb rétegei számára válnak valóban kézzelfoghatóvá a kibertérben zajló folyamatok negatív hatásai. Az akadozó szolgáltatások, a kifosztott bankszámlák, a személyazonossággal történő visszaélések, a személyes adatok titkosításán alapuló zsarolások és számos további negatív hatás már az egyén szintjén is súlyos problémákat okozhat, míg társadalmi szinten válsággá vagy nemzetbiztonsági kérdéssé fajulhat. A kiberbiztonság és -védelem területén jártas szakemberek az elmúlt időszakban növekvő számban találkoztak olyan eseményekkel, amelyek szándékos tevékenység eredményeként következtek be és társadalmi szinten is súlyos következményeket generáltak. Az ilyen események hátterében gyakran

geopolitikai feszültségekkel és törekvésekkel összefüggő érdekérvényesítési motiváció húzódik meg, ami az érintetteken túl kihívás elé állítja a 21. századi nemzetközi közösséget is.

Növekszik azoknak a nemzetközi szereplőknek a száma, amelyek felismerték a kibertérben vagy azon keresztül folytatott tevékenységek jelentőségét és időszerűségét. A kibertérben vagy azon keresztül kiváltott hatások rendkívül szerteágazók lehetnek, miközben a kibertér sajátosságai miatt korlátokba ütközik a megelőzés, a védekezés és a számonkérés is. A hadtudományi terminológiából kölcsönzött műveleti képességek kibertérre specializált szegmensének dinamikus bővülése a technológia fejlődésének és térnyerésének üteme miatt egyetlen hagyományos műveleti képességgel sem vethető össze. Mindez speciális megközelítést igényel, amely a kiber műveleti képességeket el tudja helyezni a teljes műveleti spektrumban és hatékonyan tudja alkalmazni azokat.

Nemzeti szinten az érdekek érvényesítésében és értékek védelmében közreműködő kiberműveleti képességek jellemzően a fegyveres testületeken belül kerülnek kialakításra. A hivatalos kapcsolat ugyanakkor ritkán egyértelmű, jellemzően nehezen kimutatható és szinte sosem bizonyítható, ezért elterjedt az államilag támogatott terminológia alkalmazása. A kibertér hibrid jellege és aszimmetrikus természete lehetővé teszi az alkalmazott erők és képességek multiplikálását, miközben az anonimitás fenntartása magas szinten biztosított. A kibertérben történő incidensek és az ott zajló konfliktusok, az ezek során alkalmazott módszerek és eljárások különböző aspektusokból épp úgy vizsgálhatók, mint a kinetikus hatásokkal járó fizikai térben megvalósuló incidensek és konfliktusok, azonban ez idáig nem, vagy csak korlátozottan valósult meg. Néhány állam tekintélyes előnyre tett szert ezen a téren az elmúlt évek során és mára olyan kiberműveleti képességeket birtokol, ami a saját és szövetséges rendszerek védelmén jelentős mértékben túlmutat. A speciális kiberműveleti képességekkel sebészi pontosságú kibertámadásokat tudnak végrehajtani tetszőleges célpontok ellen, amivel társadalmi, gazdasági, politikai, katonai és nemzetbiztonsági hatások érhetők el.

Ilyen hatások kiváltása a fizikai térben jellemzően a katonai különleges erők, a rendvédelmi speciális egységek, illetve nemzetbiztonsági szolgálatok erre kiképzett állományával végrehajtott műveletekkel érhető el. A fizikai térhez hasonlóan a kibertérben is azonosíthatók olyan akciók és képességek, amelyek bizonyos szempontból megfeleltethetők a különleges műveleti képességeknek. A kibertér különleges műveleti erői hasonló tevékenységet folytatnak, mint a

kinetikus térben tevékenykedő társaik, csak eltérő dimenzióban. Ugyan korlátozottan érhető el információ azzal kapcsolatban, hogy a nemzetközi rendszer egyes szereplői milyen szintű kiberműveleti képességekkel rendelkeznek, a társadalmi berendezkedésre és stabilitásra [1], a gazdasági biztonságra [2] vagy épp az energiabiztonságra [3] leselkedő legjelentősebb kiberfenyegetések között több olyan is található, amelyik államilag támogatott tevékenységre utal.

Mivel az egyik oldalon kiberműveleti képességként jelennek meg azok a tevékenységek, amik a másik oldal számára kiberfenyegetést jelentenek, időszerű a kérdés hadtudományi feldolgozása és a kiberműveletek szerepének vizsgálata a nemzetközi kapcsolatokban, a konfliktusokban, illetve a politikai és nemzeti érdekérvényesítés során. További analízis szükséges a kiberműveleti képességek speciális típusainak azonosításához, valamint az ilyen műveleteket megtervezni és végrehajtani képes egységek kialakításához.

Kutatási célok

Értekezésemben védelmi szervezeti és stratégiai nézőpontból, a nemzeti érdekérvényesítés elemeként, a nemzeti képességfejlesztés szintjén vizsgálom a kiber különleges műveleti képességek kialakítását, mint a kibertérből érkező kihívásokra adandó válaszok egyik lehetséges formáját az ezredfordulót követő időszakban. Az értekezés elkészítése során a kutatási célokat a kiber különleges műveleti képesség alapjai mentén az alábbiak szerint határoztam meg:

1. Feltárni az aktuális kiberbiztonsági és kibervédelmi stratégiai dokumentumok alapján a nyíltan felvállalt kiberműveleti képességeket és ambíció szintet Magyarország és a nemzetközileg feldolgozható stratégiai dokumentummal rendelkező szomszéd országok, illetve néhány kiválasztott kisállam és nagyhatalmi szereplő esetében. Ezek alapján következtetéseket megfogalmazni a kiberműveleti képességek megismerésének korlátjaira vonatkozóan.

[1] A társadalmi berendezkedésre és stabilitásra veszélyt jelentő kiberműveletnek tekinthető az amerikai elnökválasztásba történt 2016-os beavatkozás. Bővebben: https://www.cfr.org/cyber-operations/
[2] A gazdasági biztonságra veszélyt jelentő kiberműveletnek tekinthető a Bangladesh Bankon keresztül a nemzetközi bankközi elszámolási rendszert (SWIFT) ért 2016-os támadás. Bővebben: https://www.cfr.org/cyber-operations/
[3] Az energiabiztonságra veszélyt jelentő kiberműveletnek tekinthető az ukrán energiaszolgáltatást ért 2016-os támadás. Bővebben: https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine

2. Azonosítani azokat a kibertérből érkező fenyegetéseket, amelyekhez a legsúlyosabb ismert kiberbiztonsági incidensek köthetők és a legkifinomultabb eszközöket, módszereket és eljárásokat alkalmazva érik el a céljukat. Ez alapján meghatározni azokat a paramétereket, amelyek a védelmi szervezetek által folytatott különleges műveleti tevékenységek és a fejlett perzisztens fenyegetések kapcsán egyaránt megfigyelhetők, különös tekintettel a fedett körülmények között, kiemelkedő színvonalon, szervezetten és tervezetten, felsőbb – biztonsági, katonai, nemzetbiztonsági, politikai – érdekek mentén történő végrehajtásra.
3. Javaslatot tenni az észleléshez, felszámoláshoz és megelőzéshez szükséges, támadással arányos – megelőző és ellentámadási kapacitást is magába foglaló – kiber különleges műveleti képességek elhelyezésére a nemzeti képességfejlesztés szintjén, a nemzeti érdekérvényesítés eszköztárának elemeként, a nemzeti érdekek hatékonyabb érvényesítésének elősegítése céljából.
4. Kidolgozni a kiberműveleti és különleges műveleti képességek hasonlóságot mutató mintázatai és szabályszerűségei alapján a kiber különleges műveleti képességek kialakításának lehetőségeit és feltételrendszerét a kiberképességek teljes spektrumán, különös tekintettel az erőforrások alkalmazására.

Hipotézis

Az értekezésben a kutatási célkitűzésekkel összhangban három hipotézist és azok komponenseit vizsgáltam:

H1: A jelenlegi stratégiai környezetben az államok nyíltan nem, vagy csak részben vállalják fel azokat a kiberműveleti képességeket, amelyeknek teljes spektrumához hozzá tartozik az arányos válaszadáshoz szükséges megelőző és ellentámadási kapacitás.

H2: Az ismert fejlett perzisztens fenyegetések (Advanced Persistent Threat – APT) több jellemzője is azonosítható, amelyek hasonlóságot, illetve párhuzamot mutatnak a kinetikus tartományban alkalmazott különleges műveleti erőkkel és képességekkel.

H3: A kiberműveletek teljes spektrumát lefedő képességek megelőző és ellentámadási feladatok ellátására alkalmas elemeinek kialakítására létrehozható egy keretrendszer, amely a kinetikus különleges műveleti képességekhez mérhető speciális megközelítéssel valósítható meg.

Az első hipotézis (H1) vizsgálata biztonság- és védelempolitikai megközelítést alkalmazva azoknak a stratégiai dokumentumoknak az elemző-értékelő feltárásával és leírásával valósult meg, amelyek az értekezés készítésekor hatályosak Magyarországon és a nemzetközileg feldolgozható stratégiai dokumentummal rendelkező szomszédos államokban (Ausztria, Horvátország, Szlovákia, Szlovénia, Ukrajna), négy – a kiberbiztonsági érettség magas szintje, illetve az igazoltan fejlett kiberbiztonsági képességek megléte miatt – kiválasztott kisállamban (Izrael, Észtország, Svájc, Hollandia) és három nagyhatalmi szereplő (Kína, Amerikai Egyesült Államok, Oroszország) tekintetében. Az értekezés első hipotézishez kapcsolódó része arra a kérdésre is választ ad, hogy stratégiai szinten „Milyen szintet mutat a kibervédelmi képességek nyíltan felvállalt fejlesztésére vonatkozó ambíció a vizsgált országok és szervezetek tekintetében?”.

A második hipotézis (H2) vizsgálata a védelmi szervezetek által kialakított különleges műveleti képességek és tevékenységek, illetve a fejlett perzisztens fenyegetések kapcsán beazonosítható mintázatok és szabályszerűségek összevetésével és szakmai interjúk felhasználásával valósul meg, amelyek alapján jól láthatóvá váltak a fedett körülmények között, kiemelkedő színvonalon, szervezetten és tervezetten, felsőbb – politikai, biztonsági, katonai, nemzetbiztonsági – érdekek mentén megvalósuló végrehajtásból fakadó hasonlóságok. Az értekezés második hipotézishez kapcsolódó részei arra a kérdésre is választ adnak, hogy „A szükséges politikai felhatalmazással a nemzeti érdekek védelmében tevékenykedő APT-k felfoghatók-e a kibertér különleges műveleti erőiként?”.

A harmadik hipotézis (H3) vizsgálata a feldolgozott primer és szekunder szakértői források, valamint a szakértői interjúk nyomán kirajzolódó feltételrendszeren alapul. A feltételrendszer – a nemzeti képességfejlesztés szintjére fókuszálva – lehetőséget biztosít a kiber különleges műveleti képességek kialakításában szerepet játszó erőforrások és azok felhasználási és alkalmazási módjának beazonosítására. Az értekezés harmadik hipotézishez kapcsolódó részei arra a kérdésre is választ adnak, hogy „Milyen tartalmi elemekkel bíró keretrendszer megteremtésével valósítható meg a kiber különleges műveleti képességek sikerrel történő létrehozása és fejlesztése?”.

Módszertani áttekintés

Az értekezés jelentős mértékben deduktív módszeren alapul, ami lehetővé teszi az ezredfordulót követően a nyilvánosság számára is ismertté vált kiberbiztonsági események és folyamatok átfogó megközelítését és feldolgozását. A kutatási célok sikeres teljesítése érdekében az általános kutatási módszerek közül alkalmazásra került az analízis és a szintézis, a kritikai adaptáció, a megfigyelés, valamint kisebb arányban kvantitatív, nagyobb arányban kvalitatív, illetve komparatív módszerek. A hadtudományi kutatómunka specifikus módszerei tekintetében a kiberhírszerzési, valamint a kiberbiztonsági incidensek indikátoraival (Indicators Of Compromise – IOC) kapcsolatos tapasztalataim felhasználását és rendszerezését alkalmaztam.

Első lépésként a kiberbiztonsághoz és kibervédelemhez kapcsolódó stratégiai nézőpontok és célkitűzések értékelése érdekében elvégeztem egy átfogó szakirodalmi áttekintést, melynek során a stratégiai dokumentumokban megjelenő kiberképességekre vonatkozóan behatóan elemeztem és összevetettem a vizsgált államok ambíció szintjét. Miután a feldolgozott primer forrásokból csak korlátozottan vált szintetizálhatóvá a kitettség mértékére és a biztonság szintjére vonatkozó felfogás, jelentős mértékű szekunder forrást felhasználva elemeztem az APT-kel kapcsolatban elérhető nyílt információkat, miközben a kiberbiztonság terén érettebb állami kiberképességekkel való összefüggéseket kerestem. A folyamatelemzési módszert is tartalmazó analízis nyomán három esettanulmányt készítettem a nagyhatalmi kiberműveleti képességek és a fejlett perzisztens fenyegetések kapcsán azonosítható analógiákról. További dokumentumelemzés segítségével, átfogó megközelítést alkalmazva megvizsgáltam, értelmeztem és rendszereztem a kiberműveletek teljes spektrumát a defenzívtől az offenzív komponensekig, beleértve a nyíltan nem felvállalt ún. „szürke zónás” műveleteket. A kiberműveleti képességek meghatározása és az esettanulmányok nyomán a kutatás fókuszába beemeltem a kinetikus tartományban alkalmazott különleges műveleti erőket és képességeket, továbbá a működési körülményeik paramétereit dominancia alapú vizsgálattal összevetettem az APT-k azonosítható attribútumaival. Ezen felül a stratégiai és műveleti szempontok egységes keretrendszerben történő feldolgozásával, valamint a szabályzói háttér, a demokratikus kontroll, illetve a hatékonyság kritériumai mentén elemeztem a kiber különleges műveleti képességek kiépítésének és elhelyezésének lehetőségeit a potenciális szervezeti integrációs alternatívák bemutatásával. A kiberműveletek teljes spektrumát lefedő képességek megelőző és ellentámadó feladatok ellátására alkalmas elemeinek kialakítására

létrehozható keretrendszerhez a szakirodalmi tartalomelemzés mellett, a kvalitatív módszerek közül az irányított interjúk készítését részesítettem előnyben.

Az értekezésben felhasznált valamennyi szakirodalmat az *Irodalomjegyzék*ben tüntettem fel. Az alapvető fogalmak, meghatározások tisztázásához olyan elsősorban primer forrásokat (jogszabályok, stratégiai dokumentumok, nemzetközi szervezet szabályzata, katonai doktrína stb.) vettem alapul, amelyek az érettség, a nemzetközi elismertség vagy más jellemző okán széles körben elfogadottak. Az értekezésben tudatosan kerültem a terminológiai vitákban való elmélyülést, ezért az említett dokumentumokból közvetlenül emeltem át és alkalmaztam a definíciókat, illetve szükség esetén saját munkadefiníciót alkottam. Az értekezés sajátossága, hogy gyakran használok magyar és idegennyelvű (jellemzően angolszász) rövidítéseket, azonban ezek mindegyike megtalálható a *Rövidítések jegyzéké*ben magyarul és angolul egyaránt.

Az elvégzett vizsgálat tömör leírása

Az értekezés tíz fejezetre bontható. Az első fejezet bevezeti a kutatást, áttekinti a kutatási problémát, a célokat, hipotéziseket, valamint a kutatási módszertant és a szakirodalmat.

A második fejezet az elméleti kereteket határozza meg összesen hét alfejezetben. Elsőként a globális közös terek és a vizsgált időszak kerül bemutatásra, amit a kiberbiztonság, illetve a védelmi szervezetek 21. századi kihívásainak ismertetése követ. Mindezt a kortárs fegyveres konfliktusok és a kiberhadviselés kapcsolatának áttekintése kíséri. A két utolsó alfejezet a nemzeti képességfejlesztésbe, valamint a nemzeti érdekek, az érdekérvényesítés és a kiberműveletek közötti összefüggésekbe enged betekintést.

A harmadik fejezet a kiberműveleti képességek elemzésének első lépéseként a kiberbiztonsági stratégiai dokumentumok vizsgálatát tartalmazza, különös tekintettel a környező országok, néhány kiválasztott kisállam és három nagyhatalmi szereplő kiberképességeire. Ezt követően a fejezet a kiberműveletek teljes spektrumában megtalálható képességek feltárásával és rendszerezésével foglalkozik. A fejezet harmadik eleme a kiberműveleti képességek fejlődését bemutató esettanulmányok.

A negyedik fejezet a fejlett perzisztens fenyegetésekre (APT) koncentrál. A fejezet első része az APT-kkel kapcsolatos alapvető ismeretekre és az értelmezési keretek összpontosít. Ehhez részletesen vizsgálja az APT-k paramétereit és sajátosságait, bemutatja a kategorizálás lehetőségeit, kitér az állami támogatás részleteire, valamint a hatékonyság körülményeire és feltételeire, végül ismerteti az APT-k és tagjaik azonosításának nehézségeit. A fejezet második része tételesen elemzi és értékeli a fejlettség, a perzisztencia és a fenyegetés mértéke mentén az APT-ket és meghatározza azokat a paramétereket, amelyek alapján párhuzamok és eltérések kereshetők a kinetikus különleges műveleti erőkkel és képességekkel.

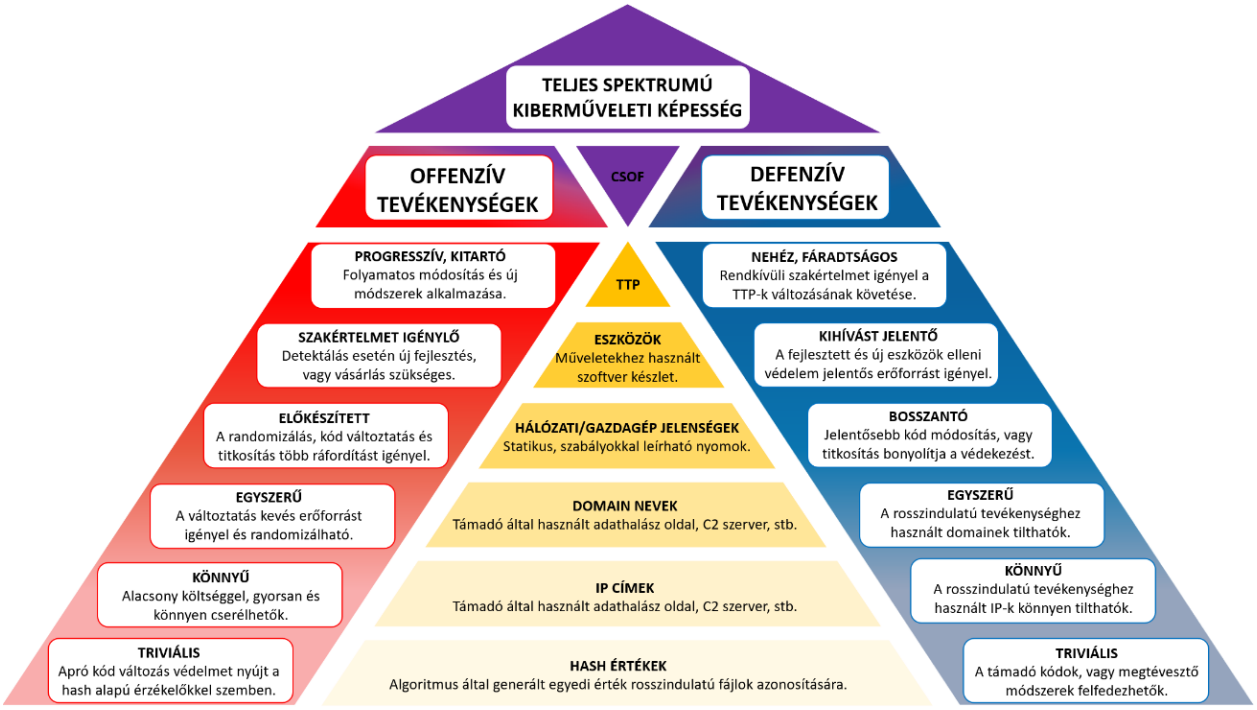
Az ötödik fejezet a védelmi szervezetek különleges műveleti képességeinek elemzésére fókuszál. Ennek keretén belül egységes keretrendszer kialakításával és alkalmazásával vizsgálja a katonai különleges műveleti erők, a rendvédelmi speciális egységek és a nemzetbiztonsági különleges képességek feladatrendszerét, valamint a működési körülményeket és jellemzőket, illetve a képzés, kiképzés és követelmények összefüggéseit. A különleges képességekkel összefüggésben a tevékenységekre leginkább jellemző paraméterek összefüggéseit és a párhuzamokat táblázat mutatja be, amibe bekerültek az APT-k azonos paraméterei a dominancia alapú összehasonlításhoz.

KÜLÖNLEGES MŰVELETI KÉPESSÉGEK	FEDETT JELLEG		JELENTŐSÉG			MŰVELETI TERÜLET		MŰVELETI CIKLUS		CÉLZOTTSÁG	ADAPTIVITÁS	SPECIÁLIS ERŐFORRÁSOK	SPECIÁLIS ELVÁRÁSOK
	FELVÁLLALT	LETAGADHATÓ	NAGY HORDEREJŰ	STRATÉGIAI	POLITIKAI	BELFÖLD	KÜLFÖLD	RÖVID	FOLYAMATOS				
KATONAI	●	●	◑	●	●	○	●	●	◑	●	●	●	●
RENDVÉDELMI	●	○	●	○	◑	●	○	●	◑	●	●	●	●
NEMZETBIZTONSÁGI	◑	●	●	●	●	●	●	◑	●	●	●	●	●
FEJLETT PERZISZTENS FENYEGETÉSEK	FEDETT JELLEG		JELENTŐSÉG			MŰVELETI TERÜLET		MŰVELETI CIKLUS		CÉLZOTTSÁG	ADAPTIVITÁS	SPECIÁLIS ERŐFORRÁSOK	SPECIÁLIS ELVÁRÁSOK
	FELVÁLLALT	LETAGADHATÓ	NAGY HORDEREJŰ	STRATÉGIAI	POLITIKAI	BELFÖLD	KÜLFÖLD	RÖVID	FOLYAMATOS				
ÁLLAMI HÁTTERŰ APT-K	○	●	●	●	●	○	●	◑	●	●	●	●	●

5. ábra: A katonai (honvédelmi), rendvédelmi és nemzetbiztonsági különleges műveleti képességek és a fejlett perzisztens fenyegetések jellemzőinek dominancia alapú vizsgálata[4]

[4] Az ábra a szerző saját munkája.

A hatodik fejezet a kiber különleges műveleti erők átfogó vizsgálatát tartalmazza hét alfejezetben. Az első alfejezet műveleti és stratégiai szempontok, valamint a különleges műveletek középtávú kihívásai alapján vizsgálja a kiber különleges műveleti erők létjogosultságát, majd a második fejezet a létrehozás és a működés hátterére koncentrál. Ebből kifolyólag külön kitér a működési keretekkel összefüggő dilemmákra, a polgári demokratikus kontroll szerepére és jelentőségére, valamint az azonnali cselekvés szükségszerűségére. A harmadik alfejezet a kiber különleges műveleti képességek szervezeti integrációjának lehetőségeit értékeli négy különböző modell segítségével. A negyedik alfejezet foglalkozik a végrehajtó állomány toborzásával és kiválasztásával, ezen belül a különböző ismeretek, készségek és képességek meghatározásával. Az ötödik alfejezetben a felkészítés és kiképzés egyes elemeinek, a szükséges infrastruktúrának, valamint a felkészítéssel szembeni elvárások nyomán bemutatásra kerül egy olyan modell, ami lehetővé teszi a kiberműveleti képességek teljes spektrumának indikátor alapú ábrázolását.



8. ábra: A teljes spektrumú kiberműveleti képességek és a kiber különleges műveleti erők modelljének sematikus ábrázolása az offenzív és defenzív tevékenységek indikátor központú skálázódása alapján.[5]

Az utolsó két alfejezet a három legfontosabb kiber különleges műveleti komponenssel, valamint a szükséges erőforrásokkal és a felmerülő kockázatokkal és kihívásokkal foglalkozik.

[5] A ábra a szerző saját szerkesztése.

A hetedik fejezet az összegzett következtetéseket, míg a kilencedik az értekezés kutatási és tudományos eredményeinek felhasználhatóságát tartalmazza. Az utolsó, tizedik fejezet két részre bontva tartalmazza a tudományos kutatásokra és a szakpolitikai lépésekre vonatkozó ajánlásokat.

Összegzett következtetések

A kiberbiztonsági stratégiák áttekintésének eredményeként arra a következtetésre jutottam, hogy az államok jellemzően nem adnak precíz információkat a kiberműveleti képességeikkel összefüggésben és a dokumentumok sok esetben nem tartalmaznak egyértelmű meghatározásokat az alkalmazott terminológiához. Ebből kifolyólag a stratégiai dokumentumok szintjén elmosódnak a határok a kibervédelem és a kiberműveletek különböző szegmensei, valamint alkalmazásuk körülményei között. Azt a következtetést vontam le, hogy a legtöbb ország esetében pusztán a kiberstratégiák alapján nehéz megállapítani, hogy ha a dokumentum említést tesz kiberműveleti képességekről, akkor pontosan milyen tevékenységek sorolhatók ide, illetve a katonai, rendvédelmi és nemzetbiztonsági szektorok közül melyik és milyen mértékben érintett. Míg a nemzetközi szervezetek esetében egyértelműen a védelmi jelleg dominál stratégiai szinten, a nagyhatalmak és a kiber szempontból fejlettebb kisállamok kapcsán előfordul az offenzív képességek nevesítése, vagy az arra való direkt utalás. A vizsgált stratégiák túlnyomó része ugyanakkor óvatos megközelítést alkalmazva, jellemzően a kiberműveleti képességek védelmi aspektusát hangsúlyozza.

A kiberműveleti tevékenységek vizsgálata rávilágított, hogy léteznek olyan keretrendszerek, amelyek alkalmazásával leírhatók a kiberműveleti képességek egyes komponensei és meghatározhatók azok a technikai, illetve etikai aspektusok, melyek segítségével a defenzív és offenzív képességek szétválasztása megoldható. A kiberműveletek különböző aspektusaink elemzésével arra a következtetésre jutottam, hogy a passzív és aktív védelem, valamint az offenzív tevékenységek többnyire néhány paraméter alapján jól szétválaszthatók, ugyanakkor sok esetben nincsenek éles határok. Ez különösen igaz a több elemből álló tevékenységek és műveletek esetében. Ilyen esetben a végeredmény egy defenzív és offenzív elemeket egyaránt tartalmazó hibrid művelet lesz, amelyben a hagyományos kibervédelmi képességek mellett speciális képességek is megjelennek. Megállapítottam, hogy a speciális vagy offenzív elemeket

korlátozottan tartalmazó kiberműveletek jellegüket tekintve, a végső cél szempontjából lehetnek defenzívek, erre vonatkozóan nincs nemzetközileg elfogadott gyakorlat, szabvány vagy szabályozás. Tulajdonképpen ez az a bizonyos szürke zóna, amire egyes stratégiák utalnak és amiben egyre több állam igyekszik hatékonyan fellépni. Ehhez kapcsolódóan az esettanulmányokból jól látható, hogy a multipoláris világ három hangsúlyos geopolitikai szereplője időben felismerte a kibertér jelentőségét és évtizedes építkezést folytat a kiberműveleti képességek terén és bár nyíltan a nemzetközi szabályozás kiterjesztését és fejlesztését szorgalmazzák, valójában a kibertér sajátosságait igyekeznek maximálisan kihasználni saját hatalmi törekvéseik és nemzeti érdekeik érvényesítésére.

Az APT-k elemzésének eredményeként megállapítottam, hogy precíz és egyértelmű célkitűzésekkel rendelkeznek, magasfokú szervezettséget mutatnak és jelentős erőforrásokhoz férnek hozzá, miközben tevékenységük időben elhúzódó, illetve ismétlődő képet mutat. Az APT-khez köthető tevékenységek jellemzően nagy horderejű, stratégiai és/vagy politikai érdekek mentén megvalósuló incidensek nyomán kerülnek nyilvánosságra. Továbbá a tevékenységekre jellemző a kifinomultság, nehezen észlelhetők és adaptív technikai megoldásokat alkalmazva képesek akár hosszú időn keresztül rejtve maradni. Az APT-k elemzése során külön is megvizsgáltam a legfontosabb jellemzőket. A fejlettség vizsgálatából kiderült, hogy az APT-k képesek olyan technológiákat felhasználni és kihasználni a tevékenységük során, amelyek speciális szakértelmet és adott esetben kiemelkedő kreativitást igényelnek. A perzisztencia vizsgálatából kiderült, hogy akár több száz napon át képes egy APT tevékenység észrevétlen maradni az áldozatok számítógépes rendszerein és hálózatain. Az APT tevékenység jellemzően visszatérő megfigyelést és adatlopást takar magasfokú reagálóképességgel (reaktivitás) kombinálva. Az APT-k elemzése során megállapítottam, hogy az általuk folytatott tevékenységek több alkalommal bizonyították, hogy képesek a virtuális és fizikai világ közötti határok átlépésével hatásokat kiváltani, ezért súlyos fenyegetést jelentenek az államok politikai-társadalmi berendezkedésére. Geopolitikai, gazdasági, biztonsági és egyéb célok mentén képesek szenzitív információkat megszerezni, manipulálni vagy akár bomlasztó hatást kiváltani, miközben a letagadhatóság olyan magas szintje érvényesül, amivel egyetlen fizikai művelet sem képes versenyezni.

Miután több paramétert meghatároztam az APT tevékenységekkel összefüggésben, amelyek külön-külön is jelentős mértékben növelni képesek a hatékonyságot, ezeket összevetettem a

védelmi szektor különleges műveleti képességeinek paramétereivel. A vizsgálat nyomán megállapítottam, hogy az egyes területek különleges és speciális képességei ágazatok szerint, a tevékenységi területnek megfelelően jól elkülöníthetők, ugyanakkor vannak átfedések, amik esetenként szoros kapcsolatra, illetve tudástranszferre utalnak. A kiber különleges műveleti erők létjogosultságának vizsgálatát a kinetikus különleges műveleti erők kihívásaival kezdtem, ami kettős képet mutat abban a tekintetben, hogy míg hazai viszonylatban egyelőre nem elképzelhető a robosztus kiberműveleti képesség különleges erők keretén belül történő kialakulása, az Egyesült Államokban aktív vita folyik arról, hogy a speciális kibermissziókban szerepet vállaló egységek a kiberműveleti vagy a különleges műveleti parancsnokság alárendeltségében jöjjenek létre. A stratégiai és műveleti szintek vizsgálatával rávilágítottam, hogy a nemzetközi rendszer állapota és a kibertér adta lehetőségek az államok egy részénél olyan viselkedési minták létrejöttét generálja, amit a nemzetközi jog szabályrendszere nem képes követni és kontrollálni, ezért az érdekek sérülése esetén jelentősen korlátozódik a válaszadáshoz alkalmazható hagyományos eszközrendszer.

Megállapítottam, hogy a kiberműveletek teljes spektrumában alkalmazható képesség kialakítása értelmezhető a nemzetközi kapcsolatok kiberdimenziójában kialakult anarchikus állapotokra történő válaszadásként, amit manapság leginkább a nagyhatalmak között zajló „kiberháború" kifejezéssel szokás leírni. Bár hadtudományi szempontból a háborús narratíva alkalmazása helytelen, a kutatás által feltárt állami, illetve állami támogatású szervezetek kiberműveleti képességei egyértelműen elérik azt a szintet, amivel bizonyos esetekben a kinetikus támadásokkal összemérhető hatásokat képesek kiváltani gyorsabban, költséghatékonyabb módon és a kibertér kínálta aszimmetria kiaknázásának maximalizálásával.

Arra vonatkozóan, hogy a kiberműveleti képességek kialakítása során milyen integrációs sémák alkalmazása kínál magasfokú hatékonyságot, egyszerű beágyazhatóságot vagy épp letagadhatóságot, több alternatívát is megvizsgáltam. A vizsgálat nyomán megállapítottam, hogy a katonai, nemzetbiztonsági, önálló félkatonai, illetve szerződéses modellek mindegyike szép számban rendelkezik előnyökkel és hátrányokkal, amelyeket minden szereplőnek mérlegelnie kell a képességek kialakítása előtt, hogy kiválaszthassa a számára leginkább kedvező megoldást. Az interjúk és a szakirodalmi vizsgálatok alapján a katonai és nemzetbiztonsági integrációval öröklődő robosztus szervezeti háttérrel és az ebből fakadó bonyolult hierarchiával és lassúsággal szemben

mindenképpen előnyösebb az önálló félkatonai vagy a szerződéses modell alkalmazása, azonban mindegyik esetben további elemzésre és értékelésre van szükség, hogy pontosabb képet lehessen alkotni az előnyökről és hátrányokról abban az adott közegben, ahol a képesség kialakításra kerül.

Új tudományos eredmények

A kiber különleges műveleti képességeket vizsgáló értekezésem az alábbi új tudományos eredményeket tartalmazza:

1. Feltártam a kiberbiztonsági stratégiák célzott, kvalitatív elemzésével a dokumentumok kiberműveleti képességekre vonatkozó részeit, **összegeztem** a kiberműveleti képességek offenzív és defenzív jellegére utaló információkat és a tapasztaltak alapján **következtetéseket fogalmaztam meg**, a valós kiberműveleti képességek és ambíció szint megismerésének korlátjaira vonatkozóan.

2. Azonosítottam a kiberbiztonsági kihívások közül a fejlett perzisztens fenyegetéseket és **igazoltam**, hogy a legsúlyosabb ismert kiberbiztonsági incidensek köthetők hozzájuk, továbbá a legkifinomultabb eszközöket, módszereket, illetve eljárásokat alkalmazva érik el a céljukat. Ez alapján **meghatároztam** a honvédelmi, rendvédelmi és nemzetbiztonsági szektorok különleges műveleti körülményei, valamint a fejlett perzisztens fenyegetések működési paraméterei közötti analógiákat, ami alapján **kidolgoztam** a kiber különleges műveleti tevékenységek egyedi feltételrendszerét.

3. Igazoltam a kiber különleges műveleti képességek létjogosultságát és a nemzeti érdekek hatékonyabb érvényesítésének elősegítésére, **javaslatot tettem** a kiber különleges műveleti képességek elhelyezésére a nemzeti képességfejlesztés szintjén, a nemzeti érdekérvényesítés eszköztárának elemeként.

4. Komparatív módon értékeltem a honvédelmi, rendvédelmi és nemzetbiztonsági ágazat különleges képességeinek, valamint a kiber különleges műveleti képességek sajátosságait, **rámutattam** azokra a paraméterekre, amelyek alapot biztosíthatnak a szervezeti integráció, a struktúra és a feltételrendszer kialakításához és **megalkottam** a teljes spektrumú kiberműveletek indikátor alapú modelljét.

Az értekezés kutatási és tudományos eredményeinek felhasználhatósága

Az elvégzett kutatás alapján elkészített értekezés eredményei az alábbi területeken használatók fel:

- Szakpolitikai területen: Az értekezés stratégiai szintű képet alkot a kiberműveleti képességfejlesztéssel összefüggő elképzelésekről és az együttműködési lehetőségek formáiról. Feltárja a kiberműveleti képességek beágyazottságát a vizsgált országok védelmi szektorainak stratégiai szintjén, valamint a kiberfenyegetésekhez kapcsolódó nemzeti percepciókat. Ehhez kapcsolódóan a kiberműveleti képességek nincsenek leírva nyílt, megismerhető forrásokban, ezért indirekt módon lehet következtetéseket levonni. Ezek nem konkrét képességekre vonatkoznak, hanem a felhasználás jellegére utalnak. Ez a jelleg meghatározó a kiberműveletek fenyegetésként, illetve képességként történő megítélésekor is. Ebből kiindulva a fejlett perzisztens fenyegetések egyúttal a kiberműveleti képességek speciális elemeként értelmezhetők és párhuzamba állíthatók a kinetikus különleges műveleti képességekkel. Ezen ismeretek elősegítik a kiber különleges műveleti képességek kialakítását, a szükséges feltételrendszer megteremtését és a kapcsolódó tervezési folyamat felgyorsítását. A kiber különleges műveleti képességeket eredményesen kialakító és alkalmazó országok eljárásainak és módszereinek ismerete növeli a szakpolitikai tervezés és döntéshozatal hatékonyságát és segíti a szükséges koordinációs tevékenységet, míg a hiányosságok azonosítása hozzájárul a hátráltató tényezők kiküszöböléséhez.
- Alkalmazott kutatásokban: Az értekezés Magyarországon eddig nem, vagy csak minimálisan kutatott területtel – a kiber különleges műveleti képességekkel – foglalkozik, így jelentős mértékben feltáró jellegű, kisebb részben pedig az elérhető nemzetközi szakirodalomra építve szintetizáló, elemző és értékelő jellegű. Kvalitatív és komparatív kutatásmódszertana – elsősorban a stratégiai vizsgálat, valamint a fejlett perzisztens fenyegetések és a különleges műveleti képességek terén – a hadtudományban újszerű, a szerző és az irányított interjúk szakértői köre által végzett kutatások és gyakorlati tapasztalatok szintetizálásának eredményét összegzi. A hasonló fókuszú és tematikájú alkalmazott kutatásokhoz mintaként szolgálhat és módszertani alapot biztosít.

- Oktatásban és kiképzésben: A kutatás során feltárt és szintetizált nemzetközi szakirodalmi források beemelése a hadtudományi, a biztonság- és védelempolitikai, valamint a kiberbiztonsági és különleges műveleti felkészítési területre olyan új ismereteket biztosít a jövő szakembereinek a védelmi szférában és azon túl, amelyekre a – kiberbiztonsági szakemberhiány okán – már rövid távon jelentős igény mutatkozhat. Az értekezés ismeretanyagának és forrásainak jelentős része csak idegen nyelven érhető el, így a magyar szakirodalomban nem szerepeltek, ezért a kapcsolódó képzési tematikák frissítéséhez felhasználhatók.

A szerző témával kapcsolatban megjelent publikációi

BERZSENYI Dániel: Kiberbiztonság. In: TÁLAS Péter Henrik – CSIKI Tamás – ETL Alex – BERZSENYI Dániel (szerk.): *A globalizált világ kihívásai*. Nemzeti Közszolgálati Egyetem, Ludovika Egyetemi Kiadó, Budapest, 2021, 341-358. o.

BERZSENYI Dániel – EDEGBEME-BELÁZ Annamária: Hungary's evolving cyber security strategy. In: MANJIKIAN Mary – ROMANIUK Scott N. (szerk.): *Routledge Companion to Global Cyber-Security Strategy*. Routledge, London, 2021, 99-110. o.

BERZSENYI Dániel: A kibertér aktuális nemzetközi biztonságpolitikai kihívásai. In: BERZSENYI Dániel – BODÓ Attila Pál – KAPITÁNY Sándor – SÁGI Gábor János – SEBŐK Viktória (szerk.): *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2017*. Dialóg Campus Kiadó, Budapest, 2017, 6-22. o.

BERZSENYI Dániel – EDEGBEME-BELÁZ Annamária: Kiberbiztonsági Stratégia 2.0: A kiberbiztonság stratégiai irányításának kérdései. *SVKK Elemzések, 2017/3*. [online], Elérhető: https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/svkk-elemzesek-2017-4-harom-evvel-az-ukrajnai-hatalomatvetel-utan-talas-p.original.pdf [2022. 07. 16.]

BERZSENYI Dániel: Globális kihívás, regionális válaszok: kiberbiztonság Kelet-Közép-Európában. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 10. évf., 2017/3. szám, 69-79. o.

BERZSENYI Dániel: A kiberbiztonság humán oldala. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 10. évf., 2017/2. szám, 54-67. o.

BERZSENYI Dániel – VÁNYI Rajmond: Egy katonapolitikai döntés lehetséges kiberbiztonsági következményei: az Iszlám Állam elleni magyar katonai szerepvállalás margójára. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 8. évf., 2015/3. szám, 134-143. o.

BERZSENYI Dániel: New dimension in V4 defense cooperation. A comparative analysis of the cybersecurity strategies of CECSP countries. Visegrad Plus – Forum for Visegrad+ Studies. 2015. 01. 18. [online] Elérhető: https://web.archive.org/web/20160611071807/http://visegradplus.org/analyse/new-dimension-v4-defense-cooperation-comparative-analysis-cybersecurity-strategies-cecsp-countries/ [2022. 07. 22.]

BERZSENYI Dániel: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 7. évf., 2014/6. szám, 110-136. o.

BERZSENYI Dániel – SZABÓ I. László: A védelmi szektor néhány elemének transzformációja. In: TÁLAS Péter Henrik – CSIKI Tamás (szerk.): *Magyar biztonságpolitika 1989-2014 - Tanulmányok*. Nemzeti Közszolgálati Egyetem, Nemzetközi Intézet, Budapest, 2014, 37-58. o.

BERZSENYI Dániel – SZENTGÁLI Gergely: STUXNET: a virtuális háború hajnala. *Biztonságpolitika: Biztonságpolitikai Szakportál*, Budapest, 2010. [online] Elérhető: http://www.biztonsagpolitika.hu/?id=16&aid=932&title=STUXNET:_a_virtu%C3%A1lis_h%C3%A1bor%C3%BA_hajnala [2022. 07. 16.]

A doktorjelölt szakmai-tudományos életrajza

Berzsenyi Dániel egyetemi tanulmányait 2005 és 2010 között a Zrínyi Miklós Nemzetvédelmi Egyetem biztonság- és védelempolitika szakán végezte. 2008-ban az Országos Tudományos Diákköri Konferencián I. helyezést ért el. Doktori tanulmányait 2014-ben kezdte meg a Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskolájában. 2016-ban Erasmus ösztöndíjjal folytathatott kutatásokat a Tallini Műszaki Egyetemen, ahol a balti államok digitális fejlettségével és kiberbiztonsági orientációjával foglalkozott. Idővel kutatási fókuszának középpontjába a kiberműveleti képességek kerültek, így doktori értekezését is ebben a témában írta. Kutatói profiljával összhangban oklevelet szerzett Tallinban *Digital Forensics Technology and Law* területen, 2018-ban letette a *Certified Information Security Manager* (CISM) vizsgát, majd *ISO 27001 Lead Auditor* képesítést szerzett. 2020-ban az Óbudai Egyetem Neumann János Informatikai Karán kiberbiztonsági szakon szerzett szakirányú oklevelet, melynek keretein belül részt vett a *White Hat Certified Defender* (WHCD) képzésen.

PhD kutatásai mellett biztonságpolitikai és kiberbiztonsági területen tevékenykedett. 2015-2016 folyamán párhuzamosan volt a Stratégiai Védelmi Kutató Intézet külső munkatársa és egy jogosultság- és hozzáférés-kezeléssel foglalkozó startup IT biztonsági tanácsadója. 2016 és 2019 között egy multinacionális pénzügyi szervezet nemzetközi kiberbiztonsági csapatában szenior kiberhírszerzési elemzőként dolgozott. 2019-ben társalapítója lett egy kiberbiztonsági tudatosság-növeléssel foglalkozó startupnak, ami mellett független kiberbiztonsági tanácsadóként és kutatóként is tevékenykedik. Magyar és angol nyelven megjelent publikációi elsősorban a kibertér stratégiai és műveleti kérdéseivel foglalkoznak. Egy angol nyelvű kiberbiztonsági tanulmánykötet társszerzője és egy magyar nyelvű biztonságpolitikai tanulmánykötet társszerkesztője. Német nyelvből felsőfokú, angol nyelvből középfokú nyelvvizsgával rendelkezik. Az angol nyelvet napi szinten aktívan használja munkája és kutatói tevékenysége során.