NEMZETI KÖZSZOLGÁLATI EGYETEM

Hadtudományi Doktori Iskola

TÉZISFÜZET

Tóth Tamás:

Az IKT környezet változásainak hatásai az információgyűjtés 21. századi fejlődésére

című doktori (PhD) értekezéshez

Témavezető:
Dr. habil. Dobák Imre

Budapest, 2024.

TARTALOM

1. BEVEZETÉS

Napjainkban a biztonsági környezet dinamikus változása, a technológiák intenzív fejlődése, valamint a rendelkezésre álló információ mennyiségének folyamatos növekedése az információgyűjtő szervezetek[1] vonatkozásában szervezeti és műveleti területen egyaránt gyorsan alkalmazkodni képes, hatékony információszerző és -feldolgozó képességgel bíró szervezeteket követel meg. Tapasztalható az egyes kihívások, kockázatok, és fenyegetések, valamint a tényleges konfliktusok fokozódó hibrid, aszimmetrikus jellege, amely mára a nyílt reguláris katonai konfliktusoktól kiterjed az információs műveleteken keresztül, a terrorizmuson, a szervezettbűnözésen át, egészen a politikai, gazdasági nyomásgyakorlásig, befolyásolásig. A külső biztonsági környezet negatív irányú változásának tendenciája, valamint a digitalizáció, a technológiai környezet rohamos fejlődése átfogó biztonsági stratégiaalkotást is eredményezett mind nemzetközi, mind nemzetállami szinten.

A társadalom normál működése, a nemzeti szuverenitás biztosítása érdekében a modern államhatalom védelmi és biztonsági funkciójából adódó alkotmányos feladata az egyetemleges biztonság érvényesülésének garantálása, valamint az abban való közreműködése nemzetközi szövetségesei szintjén. A magyar állam polgárai számára alapvető jogaikat elsősorban a hon- és rendvédelmi ágazat – az értekezés szempontjából kiemelten a nemzetbiztonsági szolgálatok, igazságügyi és bűnüldöző szervek által kívánja biztosítani, indokolt esetben törvényi garanciális szabályok mellett például a jogosult szervezetek által végzett titkos információgyűjtés, valamint leplezett eszközök alkalmazása (a továbbiakban együtt értsd: titkos információgyűjtésként) által.

Az információgyűjtés szempontjából releváns adatok, információk legnagyobb hányada jelenleg valamely információ és kommunikáció technológiai (a továbbiakban: IKT[2]) eszközhöz, rendszerhez, eljáráshoz kapcsolódik. Erőteljesen zajlik az olyan diszruptív, azaz „felforgató” technológiák térnyerése, mint például a mesterséges intelligencia, az autonóm robotika, az IoT[3], a VR/AR[4], az újgenerációs hírközlő hálózatok, az űrtechnológiák fejlődése, amelyek fokozott ütemben alakítják át a biztonsági környezetet is. Így elengedhetetlen az

[1] Az értekezésben a titkos információgyűjtésre, a leplezett eszköz alkalmazására és annak végrehajtására jogosult szerveztek köre értendő.
[2] IKT: Információ és kommunikáció technológia – ICT: Information and Communication Technology
[3] IoT: Internet of Things – dolgok internete
[4] Virtual reality – virtuális valóság/ Augmented reality – kiterjesztett valóság

információgyűjtő szervezetek technikai képességeinek folyamatos fejlesztése, alkalmazkodása az aktuális és várható biztonsági, technológiai kihívások, kockázatok, veszélyek kezelése érdekében.

Néhány éve egyre több titkosított online kommunikációt biztosító „csevegőalkalmazás", mobil applikáció, azaz a hazai jogszabályi fogalomhasználat szerinti alkalmazásszolgáltatás[5] jelent meg, amelyek biztonságos kommunikációt ígértek. Ezek körében a végpont-végpont titkosítási kriptográfiai eljárás (a továbbiakban: E2EE[6]) egyre elterjedtebbé vált. A köz- és nemzetbiztonságot negatívan befolyásoló jogellenes tevékenységek – így például a nemzetközi szervezett bűnözés, a terrorizmus, az illegális fegyverkereskedelem, a nemzeti szuverenitást veszélyeztető állami és nem kormányzati törekvések – megelőzése, felderítése és elhárítása érdekében jelentős szerepe van az ezekkel összefüggő kommunikáció tartalma, kísérő- és metaadatai nemzetbiztonsági, bűnüldözési célú leplezett, jogszerű megismerésének, azaz törvényes ellenőrzésének (a továbbiakban: LI[7]).

Az értekezés tudományos vizsgálatának elsődleges tárgyát az információs társadalommal összefüggő infokommunikációs szolgáltatások körén belül a személyközi online kommunikációt megvalósító titkosított alkalmazásszolgáltatások nemzetbiztonsági célú LI tevékenysége képezi, természetesen vizsgálva a kommunikációs csatornaként alkalmazott elektronikus hírközlési, valamint az egyéb információs társadalommal összefüggő szolgáltatások kapcsolódó vetületeit, továbbá egyfajta összehasonlító jelleggel a bűnüldözési célú LI -t. A disszertációs kutatómunka fő tárgya az egyes LI módszereken belül a passzív, mély csomagátvizsgálás, azaz a DPI (Deep Packet Inspection), annak is a hírközlőhálózati oldalon megvalósuló központi monitoring alrendszer típusú formája, természetesen vizsgálva a többi LI módszer, például a szolgáltatói együttműködés vetületeit. Indokolt az LI szabályozási, és technológiai környezetének vizsgálata is, a biztonsági környezet változásainak, és a társadalmon belüli IKT trendek, tendenciák elemzése mellett.

---

[5] Az értekezés során alkalmazásszolgáltató alatt az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) 2. § m) pontja szerinti szolgáltatók körén belül a titkosított online kommunikációt biztosító szolgáltatók értendők.

[6] E2EE: End-to-End Encryption – végpont-végpont közötti titkosítás: Csak a küldő és fogadó készüléken teszi lehetővé a rejtjelezett üzenet értelmezhető formában történő visszafejtését, applikációk tekintetében azonos szolgáltatáson belül.

[7] LI: Lawful Interception – törvényes „lehallgatás", törvényes kommunikációellenőrzés. Az értekezés során az LI tágabb fogalomköre kerül alkalmazásra, azaz a tartalomellenőrzés mellett beleértendő a kommunikációra vonatkozó kísérő-, és metaadatokhoz való hozzáférés. Ezt a fajta értelmezést az IKT környezet fejlődése teszi indokolttá, hiszen a hírközlő hálózatokon, információs rendszereken ezek ellenőrzésére is lehetőség nyílik.

2. TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A nemzetbiztonsági szolgálatok tevékenységével érintett nemzeti szuverenitást sértő magatartással, terrorizmussal, egyéb kimagasló társadalomra veszélyes bűncselekményekkel összefüggésbe hozható személyek, csoportok elleni hatékony, prognosztikus szemléletű fellépés érdekében elengedhetetlen a titkos információgyűjtés komplex eszközrendszerén belül a társadalmi, technológiai, normatív kihívásokkal szemben ellenálló LI képességek fenntartása. Az EU digitális piaci és adatvédelmi stratégiai célkitűzéseinek hatására tapasztalható a lakossági célú elektronikus hírközlési, valamint az információs társadalommal összefüggő egyéb internet alapú kommunikációs szolgáltatások piacainak átalakulása, így az értekezés szempontjából elsősorban az alkalmazásszolgáltatások iránti növekvő kereslet, mely a digitalizáció, a virtualizáció, a folyamatos online jelenlét iránti szükségletek kielégítése érdekében kiemelt összetevőként azonosítható.

A diszruptív infokommunikációs termékekkel, szolgáltatásokkal kapcsolatban kialakult keresleti „dömping" egyfajta kínálati K+F+I „sokkot" okozott a 21. század IKT piacán, melynek következtében az infokommunikációs technológiák, az IKT környezet egyre dinamikusabb fejlődése tapasztalható, többek között az új adatátviteli megoldások, a kifinomultabb elektronikus információ-, kibervédelmi eljárások, valamint a normatív adatvédelmi előírások tekintetében egyaránt. A témaválasztás indoklása alapján ezen internet alapú, titkosított online kommunikációt biztosító alkalmazásszolgáltatások igénybevétele feltételezetten fokozódó ütemben azonosítható a nemzetbiztonsági szolgáltatok – és bűnüldöző szervek – tevékenységével értinett személyek, csoportok kommunikációs attitűdjében, mely tendencia egyben a piaci kereslet/kínálat szabályai szerint az „LI piacán" is feltételezetten növekedést eredményez, eredményezhet.

A témaválasztás indoklása alapján az elektronikus hírközlő hálózatokon megvalósuló személyközi kommunikáció hazai hatékony ellenőrzése tekintetében tudományosan vizsgálandó problémakörként azonosítom az IKT környezet fejlődéséből adódó kihívásokat, és azok hatásait az LI hatékonyságára, képességfejlesztésére. A szakirodalom alapján megállapítható, hogy 2015/16-ig bezárólag az alkalmazásszolgáltatások ellenőrzése állami szinten normatív, technológiai nehézségekbe ütközött. A témaválasztás indoklása alapján szükséges a témakör ezen időpontot követő tudományos alaposságú vizsgálata, mely során altémakör elsősorban az alkalmazásszolgáltatások hazai nemzetbiztonsági célú LI-je

jogszabályi és technológiai környezetének hatékonysága, így az IKT környezet fejlődésével szembeni rezilienciája[8]. Az alkalmazásszolgáltatások LI-je kapcsán indokolt a legtöbb esetben kommunikációs csatornát biztosító elektronikus mobil (telefon, internet) hírközlési szolgáltatások és azok LI-jének tudományos vizsgálata is.

Az LI hatékonysága szempontjából szükséges vizsgálni mind a hírközlő hálózatok, mind az alkalmazásszolgáltatások kriptográfiai környezetének fejlődését is. Ezen túlmenően nélkülözhetetlen a képességfejlesztési irányok meghatározásához a biztonsági környezet jellemzőinek, valamint a társadalom, azaz a felhasználók IKT szokásainak, trendjeinek vizsgálata. Megállapítható, hogy a technikai információgyűjtés, azon belüli résztevékenységként értelmezve az LI képesség hatékonyságát számos az IKT környezet folyamatos változásából, fejlődéséből adódó egymással összefüggő, igen összetett külső hatás befolyásolja direkt, indirekt módon, melyek közül a kutatómunka során a szabályozási, technológiai, társadalmi, és a biztonsági környezet vizsgálata indokolt.[9]

A kutatómunka során tudományos következtetések levonására nyílik lehetőség az IKT környezet fejlődéséből adódó többlet LI lehetőségekről és kihívásokról, melyek hozzáadott értéket képezhetnek az LI hatékonyságára irányuló képességfejlesztéshez. Annak érdekében, hogy az alkalmazásszolgáltatásokat érintő LI tevékenység hazai viszonylatban a jövőben is eredményes legyen, nélkülözhetetlen prognosztikus szemléletű következtetéseket levonni:

- a digitális IKT piac globális és hazai trendjei, tendenciái, evolúciója tekintetében;
- az IKT piac fejlődéséből adódó LI szempontú kihívásokról/többlet LI lehetőségekről;
- az LI tevékenység hazai szervezetrendszeréről, szabályozásáról, azok evolúciójáról;
- a mobilhálózatok és az alkalmazásszolgáltatások LI szempontú egyedi jellemzőiről, a tevékenységek összefüggéseiről;
- a személyközi infokommunikációs szolgáltatások körén belül a mobil hírközlési hálózatok, valamint az alkalmazásszolgáltatások elektronikus információvédelmi környezetéről, azon belül is a kriptográfiai eljárások alakulásáról;

[8] Reziliencia: Általános értelemben vett rugalmas ellenállási képesség, azaz valamely rendszernek azon reaktív képessége, amely keretében az erőteljes, megújuló, vagy akár sokkszerű külső negatív hatásokkal szemben sikeresen adaptálódjék.

[9] A részkutatási cselekmények során természetesen vizsgálat tárgyát képezik a politikai, gazdaságpolitikai környezet hatásai is elsősorban uniós szinten, azonban azok nagyrészben indirekt módon a szabályozáson keresztül érvényesülnek. Környezeti tényezők vizsgálatára nem kerül sor, tekintettel annak indokolatlanságára.

- a személyközi hírközlés normatív adatvédelmi környezetének alakulásáról;
- az alkalmazásszolgáltatásokra irányló LI tevékenységgel érintett személyek, csoportok kommunikációs szokásainak alakulásáról;
- a globalizált IKT szolgáltatások okán a nemzetbiztonsági, bűnüldözési célú LI nemzetközi, uniós együttműködésének lehetőségeiről.

3. HIPOTÉZISEK

1. A prognosztizálható IKT trendek alapján feltételezhető, hogy a GSM alapú mobil kommunikáció hagyományos LI-jével szemben a mobilinternet alapú titkosított online kommunikációt biztosító alkalmazásszolgáltatások LI igényének fokozódása várható, amelyek szolgáltatói együttműködés alapú és technikai monitoring LI módszerei is innovatív technológiai, szabályozási és szervezeti környezetet követelnek meg.

2. A jövőben a légi, világűr infrastruktúrára épülő elektronikus hírközlő hálózatok várható elterjedése, valamint az újgenerációs mobilhálózatok LI-je forradalmasíthatja az összadatforrású titkos információgyűjtés technikai képességeit az egyre heterogénebb jellegű és forrású adatforgalom okán, amennyiben az információgyűjtő szervezetek képesek technológiai szempontból kiaknázni a lehetőségeket.

3. Az alkalmazásszolgáltatások globalizációja, a nemzetközi adatvédelmi normatív és technológiai környezet fejlődése hátrányosan érintheti az azokon végbement kommunikáció LI-jének hatékonyságát, valamint azok kriptográfiai fejlődésének hatására a kommunikációellenőrzést szabályozó hatályos hazai normarendszer hatékonysága erodálódhat, e téren az LI képesség rezilienciája korlátozódhat.

4. Valószínűsíthetően a jövőben a személyközi hírközlési szolgáltatások – beleértve az alkalmazásszolgáltatásokat is – keretében végbement kommunikáció nemzetbiztonsági célú LI-jének hatékonysága érdekében nélkülözhetetlen lesz a nemzetközi, uniós együttműködés fokozása, az információcserén túl a jövő LI képességei kialakításának lehetőségét is figyelembe véve, a nemzeti szuverenitás tiszteletben tartása mellett.

4. KUTATÁSI CÉLOK

A hipotézisek igazolását tűztem ki fő célul, egyben új tudományos eredményként az LI jövőbeli hatékonyságát elősegíteni képes javaslatok megalkotásával. A definiált általános tudományos problémakörön belül elsődlegesen tudományos jelleggel vizsgálom az alkalmazásszolgáltatások hazai LI-je jogszabályi és technológiai környezetének hatékonyságát, valamint a kriptográfiai eljárások fejlődésével szembeni rezilienciáját, és az egyes nemzetbiztonsági célú LI hatékonyságnövelő intézkedések lehetőségeit, összhangban Magyarország Nemzeti Biztonsági Stratégiájának (a továbbiakban: Stratégia) átfogó célkitűzéseivel, vizsgálva az EU digitális piaci és adatvédelmi stratégiai célkitűzéseinek hatásait a témakört illetően. Ennek érdekében mind a főbb személyközi IKT trendek, tendenciák elemzésére alapozva következtetéseket vonok le a hagyományos mobil hírközlés és a mobilinternet alapú kommunikáció, valamint az ezeket érintő LI viszonyrendszerének alakulásáról, a hírközlés és a hazai LI tevékenység evolúciós folyamataik elemzésére alapozva. Összehasonlítom a mobil hírközlésre és az alkalmazásszolgáltatásokra irányuló LI tevékenység hazai normatív környezetét, majd következtetéseket vonok le azok hatékonyságáról, vizsgálva az IKT környezet fejlődéséből adódó többlet LI lehetőségeket is.

Mind a mobilhálózatok, mind az alkalmazásszolgáltatások kriptográfiai környezetének általános vizsgálatára alapozva megállapítom, hogy melyek a vizsgálat tárgyát érintő főbb kriptográfiai jellemzők, valamint, hogy ezek milyen hatékonyságkorlátozó jellemzőkkel bírnak az LI szempontjából. Következtetéseket vonok le továbbá a kriptográfiai környezet fejlődésének és a felhasználók adatkezelési attitűdjét befolyásoló egyes globális eseményeknek az alkalmazásszolgáltatások keresletváltozására gyakorolt hatásaival kapcsolatban. Az alkalmazásszolgáltatások nemzetbiztonsági célú LI-jének hazai normatív környezetét elemezve, azt összevetve az elektronikus információvédelem körében értelmezett kriptográfiai fejlődésével következtetéseket vonok le a közleményellenőrzés ellenállóképességéről, hatékonyságáról.

Az értekezés során célom kitekinteni az alkalmazásszolgáltatások jogszerűtlen célú felhasználási formáira, gyakorlati példákkal igazolva azok ellenőrzésének létjogosultságát, valamint az LI korlátozott hatékonyságának társadalomra veszélyességét. Tekintettel az elektronikus hírközlés globalizációjára az értekezés során következtetéseket vonok le az LI tevékenység egyes nemzetközi tapasztalatairól, az alkalmazásszolgáltatások értintő LI jellegű

kihívásokról, összehasonlítom a nemzetbiztonsági és a bűnüldözési célú LI-re irányuló nemzetközi együttműködések rendszerét, mely alapján értékelem a nemzetbiztonsági célú LI nemzetközi együttműködésének aktualitásait, a két tevékenységi kör viszonyrendszerét. Továbbá nemzetközi kitekintést teszek elsősorban az alkalmazásszolgáltatások LI-jével kapcsolatos kihívásokra, gyakorlatra, illetve a nemzetközi együttműködés lehetőségeire. Következtetéseket vonok le arra vonatkozóan, hogy az IKT környezet változása milyen konkrét hatásokkal bír a titkos információgyűjtésre, első sorban az LI aspektusából a stratégiaalkotás, a jogalkotás, és a tényleges LI képességek tekintetében. Az értekezés prognosztikus jellegű vizsgálatának időtávja illeszkedik az EU Digitális évtized 2030 szakpolitikai program, és a hazai Stratégia 2030-as időtávjához.

A doktori értekezés, a disszertáció fő célja a fenti elemzések, vizsgálatok során elért tudományos következtetésekre alapozva olyan gyakorlatorientált, az alkalmazott kutatásokhoz integrálható nyilvános tudományos eredmények elérése, amelyek magukban hordozzák a hazai LI képességek hatékonyságfokozásában való közreműködés lehetőségét, elsősorban jogalkotási irányok, szemléletformálás, további részkutatási irányok meghatározása által. A kutatás a feldolgozott szakirodalom rendszerző jellegű áttekintésén túl, elsődlegesen az egyes vizsgált témakörök vonatkozásában új tudományos alaposságú összefüggések feltárására, következtetések levonására hivatott. A célkitűzéseket az alábbi kutatási, vizsgálati módszerek alkalmazásával kívánom elérni, egyben a nemzetbiztonsági célú LI kutatás új tudományos módszertanának megalkotásával, és az értekezés során való alkalmazásával.

5. KUTATÁSI MÓDSZERTAN

Az értekezés során meghatározó kutatási módszerként kerülnek alkalmazásra a statisztikai adatelemzés, a trend és tendenciaelemzés, a szakmatörténeti kutatás, a jogszabályi elemzés és interpretáció, a dokumentum- és tartalomelemzés, valamint az azokon alapuló adatok és információk komplex szemléletű, egyes kvantitatív és kvalitatív szempontú elemzése, értékelése, illetve az esettanulmány jellegű feldolgozás. A szakirodalom feldolgozása, a források kritikai szemlézése során támaszkodok továbbá az elemzési munka komparatív elemzési módszerére. A kutatómunka során végig alapelvként érvényesül az észszerűség, a logika alkalmazása, az alapos és objektív „megfigyelés”, elemzés.

Az értekezés során a mobil hírközlési szolgáltatásokat és az alkalmazásszolgáltatásokat érintő egyes infokommunikációs trendekkel, tendenciákkal kapcsolatos szakirodalom feldolgozásán túl a nyíltan hozzáférhető aktuális, illetve prediktív statisztikai adatok kerülnek kvalitatív módon elemzésre és értékelésre. Kutatási kihívásként azonosítható a vizsgált tárgykört érintően a rendelkezésre álló források, statisztikai adatok megbízhatóságának, hitelességének kérdése, így azok széles körben, egymással összevetve kerülnek feldolgozásra a hiteles forráselemzés érdekében.

Vizsgálat tárgyát fogja képezni a nemzetbiztonsági – és összehasonlítási céllal a bűnüldözési – célú LI hazai normatív környezete a vonatkozó szakirodalom és jogszabályok dokumentum-, tartalomelemzés jellegű feldolgozásával, a hazai és nemzetközi, azon belül is az uniós jogforrások, a digitalizációval összefüggő uniós törekvések párhuzamos feldolgozásával. Az Emberi Jogok Európai Bíróságának (a továbbiakban: EJEB), az Európai Unió Bíróságának (a továbbiakban: EUB) és az Alkotmánybíróság ítélkezési gyakorlata is bemutatásra kerül a témához kapcsolódó egyes döntéseiknek ismertetése során. Továbbá az Európai Adatvédelmi Testület (a továbbiakban: EDPB[10]) és a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) egyes releváns döntései is feldolgozásra kerülnek az információs önrendelkezési jog korlátozását érintő jogvitákat illetően.

A hírközlést és az alkalmazásszolgáltatásokat érintő törvényes kommunikációellenőrzés hazai szervezetrendszerének, tevékenységének evolúciós vizsgálata során a fenti szempontrendszer mentén áttekintésre kerül a 21. századi hazai technológia és szabályozás fejlődése, egyfajta integrált, komplex módszertan alkalmazásával az LI-vel kapcsolatos szakmatörténeti dokumentumok, normák és jogszabályok, valamint statisztikai adatok összevetésével. Az értekezés gyakorlatorientált megközelítése érdekében esettanulmány jelleggel kerülnek feldolgozásra az alkalmazásszolgáltatások jogszerűtlen célú felhasználásával kapcsolatos nemzetközi példák, kihívások.

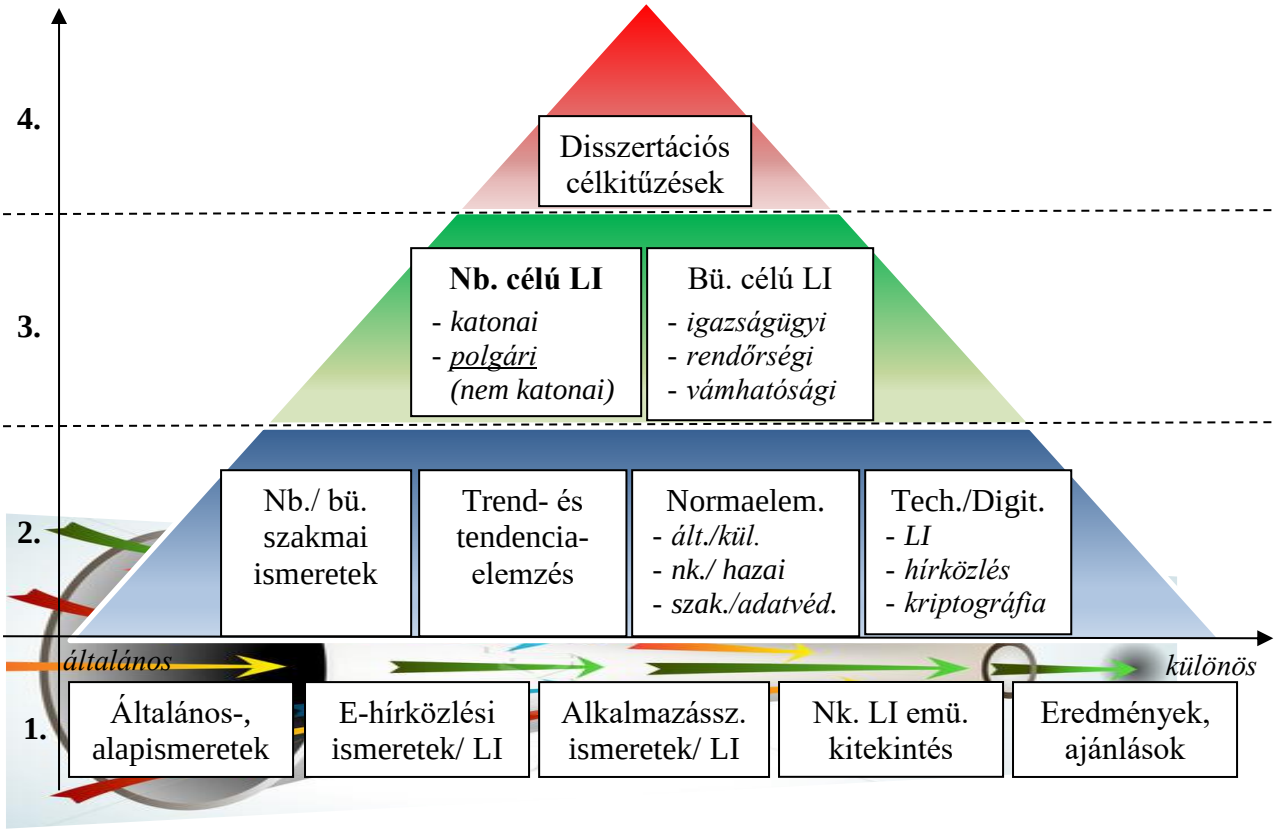
Az értekezés kutatási módszerei műszaki, technológiai elemzést, mérést nem tartalmaznak. A kutatási módszerek alkalmazása során a minősített adat védelméről szóló 2009. évi CLV. törvény szerinti minősített adat nem kerül feldolgozásra, kezelésre és nyilvánosságra hozatalra.

[10] EDPB: European Data Protection Board - Európai Adatvédelmi Testület

A témaválasztás és a kutatás aktualitása indoklásának átlagosnál hosszabb terjedelme, a tudományos probléma megfogalmazása, és a fenti módszertani leírás során láthatóvá vált a tudományos vizsgálatot igénylő igen komplex téma, amely komponensei alapján egy:

- szigorú logikai szerkezetű (általánostól halad és szűkül a különösig);
- integrált tartalmú (nemzetbiztonsági és bűnüldözési szakmai ismeretek; trend- és tendenciaelemzés; normaelemzés; technológiai és digitalizációs ismeretek);
- összefüggő tevékenységi célzat alapú (nemzetbiztonsági célzat, bűnüldözési célzat)

összetett kutatási módszertant tesz szükségessé a hipotézisek alátámasztása és az értekezés célkitűzéseinek megvalósítása érdekében. Ennek okán kidolgoztam a disszertációs kutatómunka során alkalmazott „*nemzetbiztonsági célú LI kutatás integrált interdiszciplináris tudományos módszertanát*”, melyet az alábbi – az értekezésben a 2. – ábra hivatott szemléltetni:



1. ábra: Nemzetbiztonsági célú LI kutatás integrált interdiszciplináris tudományos módszertana[11]
(Szerk.: A szerző)

[11] Rövidítések: E-hírközlési ismeretek – Elektronikus hírközlési ismeretek; Alkalmazássz. ismeretek – Alkalmazásszolgáltatási ismeretek; Nk. LI. emü. kitekintés – Nemzetközi LI együttműködési kitekintés; Nb./ bü. szakmai ismeretek – Nemzetbiztonsági és bűnüldözési szakmai ismeretek; Normaelem. – Normaelemzés; ált./kül. – általános és különös; nk./hazai – nemzetközi és hazai; szak./adatvéd. – szakági és adatvédelmi; Nb. célú LI – Nemzetbiztonsági célú LI; Bü. célú LI – Bűnüldözési célú LI.

A disszertációs kutatómunka keretében a kidolgozott kutatási módszertan alapján a szakirodalom[12] feldolgozása során, a hipotéziseknek megfelelően, az értekezés szerkezetéhez[13] illeszkedve az alfejezetekben integrált módon kerülnek elemzésre az egyes tartalmi szempontok, a tevékenység célzat alapú vizsgálatával egyetemben, melynek fő iránya a „polgári nemzetbiztonsági[14] célzat". Így vertikálisan kiteljesítve a piramis csúcsán elhelyezkedő disszertációs célkitűzéseket, horizontálisan pedig az új tudományos eredmények elérését, ajánlások megfogalmazását, végsősoron a doktori (PhD) értekezés elkészültét.

6. AZ ELVÉGZETT VIZSGÁLATOK TÖMÖR LEÍRÁSA FEJEZETENKÉNT

Az értekezés 11 fő fejezetre tagozódik, minden egyes fejezet végén elvégzésre kerül az egyes alfejezetek kutatási cselekményei alapján megállapítható részkövetkeztetések levonása. Az értekezés bevezető részében, azaz a 1. fejezetben ismertetésre kerül a témaválasztás és a kutatás aktualitásának indoklása, a tudományos probléma megfogalmazása, a hipotézisek, az értekezés célja, a kutatási módszertan, a szakirodalom áttekintése, jelen alfejezetben pedig az értekezés szerkezete, annak felépítése, és a további alfejezetek főbb tartalmának bemutatása.

Az értekezés érdemi tartalmi első része, azaz a 2. fejezet fő tárgyköre az LI garanciális, szervezetrendszeri, fogalmi és módszertani hátterének áttekintése egyfajta felvezetőként, a szükséges alapvető ismeretek tárgyalásaként, a további fejezetekben szereplő kutatási cselekmények előkészítése céljából. A fejezeten belül előkérdésként összesen 7 alfejezetben értelmezésre kerül a „nemzetbiztonsági cél" tartalma, vizsgálat tárgyát képezi az LI szabályozásának nemzetközi és hazai keretrendszere, az LI alapvető jogi és adatvédelmi garanciális hátterének áttekintése, majd az EU digitális piaci és adatvédelmi stratégiai célkitűzései hatásainak elemzése az LI aspektusából. Továbbá az LI hazai szervezetrendszerének és általános normatív háttérének ismertetése, információelméleti háttere és annak átültetése a normatív környezetbe, egyes főbb módszerei, eljárásai, a szükséges kriptográfiai alapismeretek és kihívásainak áttekintése.

[12] Lásd: Az értekezés „1.6. Szakirodalmi áttekintés" című alfejezete.
[13] Lásd: Az értekezés „1.7. Az értekezés szerkezete" című alfejezete.
[14] Értsd: A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 2. § (1) bek. szerinti polgári nemzetbiztonsági szolgálatok (Információs Hivatal, Alkotmányvédelmi Hivatal, Nemzetbiztonsági Szakszolgálat, Nemzeti Információs Központ) tevékenységi célzata.

Az értekezés érdemi tartalmi második része, azaz a 3. fejezet fő tárgyköre a mobil hírközlési ellenőrzést érintő IKT trendek, tendenciák komplex és szisztematikus elemzése a meghatározott kutatási módszertan alapján, a hipotézisek alátámasztása és az új tudományos eredmények eléréséhez szükséges részkutatómunka elvégzése érdekében. A fejezeten belül összesen 3 alfejezetben vizsgálat tárgyát képezi az elektronikus digitális mobil hírközlőhálózatok evolúciója, fejlődési trendjei, a mobilhálózatok felhasználói tendenciái, a mobilhálózatok kriptográfiai környezetének evolúciója, trendjei, kitekintve az LI szabványosításra, a hazai hírközlési kommunikációellenőrzés normatív, szervezeti, technológiai evolúciója, trendjei.

Az értekezés érdemi tartalmi harmadik része, azaz a 4. fejezet fő tárgyköre az alkalmazásszolgáltatások LI-jét érintő IKT trendek, tendenciák komplex és szisztematikus elemzése a meghatározott kutatási módszertan alapján, a hipotézisek alátámasztása és az új tudományos eredmények eléréséhez szükséges részkutatómunka elvégzése érdekében. A fejezeten belül összesen 4 alfejezetben vizsgálat tárgyát képezi az alkalmazásszolgáltatások felhasználói trendjei, az alkalmazásszolgáltatásokkal összefüggő adatvédelmi trendek, a biztonsági kihívási tendenciák és válaszintézkedések a nemzetközi térben, az alkalmazásszolgáltatások LI-jének hatályos hazai normatív, szervezeti evolúciója, trendjei.

Az értekezésnek a végkövetkeztetések levonását, összefoglalását szolgáló befejező része az 5. fejezet, amelyben az IKT környezet változásnak a titkos információgyűjtésre gyakorolt stratégiai, jogalkotási, és LI képességeket érintő hatásairól szóló komplex, a fejezetek részkövetkeztetéseit a hipotézisek mentén összefoglaló eredményei kerülnek bemutatásra. A 6. fejezetben kerülnek tételesen felsorolásra az új tudományos eredményként történő elfogadásra javasolt disszertációs kutatási eredmények. A 7. fejezet tartalmazza a kutatás eredményeinek gyakorlati felhasználhatóságára irányuló konkrét ajánlásokat, javaslatokat. Végezetül a 8. fejezetben az értekezés elkészítése, a disszertációs kutatómunka során felhasznált szakirodalom jegyzéke, a 9. fejezetben az ábrák jegyzéke, a 10. fejezetben a publikációk jegyzéke kerül szerepeltetésre, majd a 11. fejezeteben a mellékletek jegyzéke és azok csatolása történik.

7. ÖSSZEGZETT KÖVETKEZTETÉSEK

Az értekezés témaválasztásának és a kutatás aktualitásának indoklását, az azzal összefüggő tudományos problémák megfogalmazását követően, az azonosított hipotézisek mentén a kutatás céljaihoz illeszkedően kikötött „*nemzetbiztonsági célú LI kutatás integrált*

interdiszciplináris tudományos módszertanára" alapozva, a szakirodalom feldolgozását követően, az értekezés meghatározott szerkezete mentén megvalósultak az egyes kutatási cselekmények, valamint a fejezetekhez illeszkedően az elvégzett vizsgálatok tömör leírásai, a részkövetkeztetések levonásával egyetemben. Az értekezés során átfogó vizsgálat tárgyát képezte az LI garanciális, szervezetrendszeri és módszertani hátterének áttekintése, egyfajta felvezetőként, a szükséges alapvető ismeretek komplex tárgyalásaként, a további érdemi szakmai részek vizsgálatának megalapozása, előkészítése céljából. Ezt követően a mobil hírközlési LI-t érintő IKT trendek majd az információs társadalommal összefüggő alkalmazásszolgáltatási LI-t érintő IKT tendenciák komplex elemzésére került sor a meghatározott kutatási módszertan alapján, a hipotézisek igazolása érdekében. Az értekezés IKT környezet változásainak az információgyűjtés 21. századi fejlődésére gyakorolt hatásira irányuló hipotézisekkel kapcsolatos részkutatási eredményeinek összefoglaló jellegű leírását az alábbiak tartalmazzák:

Bizonyításra került az **1. hipotézis**, miszerint a prognosztizálható IKT trendek alapján a GSM alapú személyközi mobil kommunikáció hagyományos LI-jével szemben a mobilinternet alapú titkosított online kommunikációt biztosító alkalmazásszolgáltatások LI igényének fokozódása várható, amelyek szolgáltatói együttműködés alapú és technikai monitoring LI módszerei is innovatív technológiai, szabályozási és szervezeti környezetet követelnek meg. Az egyes alfejezetek kutatási cselekményei alátámasztják a hipotézist az alábbiak szerint:

- A 3.1.; 3.2.; 4.3. alfejezetek kutatási cselekményei alapján a mobil hírközlési technológiák terén kb. 10 évente tapasztalható egy generációváltás, amelyet a hálózati forgalom folyamatos heterogenizációja mellett, a lakossági fogyasztói igények, és az új IKT szolgáltatások kiszolgálása indukál. Trendelemzési kutatási módszerrel megállapításra került, hogy globális szinten kb. 2030-ra az 5G lakossági mobil-előfizetések átveszik a vezető szerepet a 4G-vel szemben, szinte teljesen kiszorítva a korábbi technológiákat (2G, 3G). Összességében a mobil-előfizetések száma folyamatosan emelkedő tendenciát mutat globális szinten, így a hálózati modernizáció mellett megállapítható a növekvő kereslet, mely tendenciák között összefüggés azonosítható az újgenerációs hálózatok többletszolgáltatási lehetőségei okán. Tendenciaelemzés során megállapításra került, hogy az újgenerációs mobilhálózatok hazai elterjedése (4G, 5G) azonos tendenciát mutat a globális és regionális trendekkel, azaz kiszorító hatással bír a korábbi technológiákra. A regionális 5G trendeket vizsgálva azonban megállapítható, hogy 2023-ban Magyarország

túlszárnyalta a közép-kelet-európai átlagot. Az alkalmazásszolgáltatások 2030/31-ig tartó piaci tendenciái alapján bizonyítottá vált azok központi szerepének további növekedése a lakossági célú kommunikációs igények kiszolgálásában, a globális piac gazdasági volumenét az előrejelzések alapján 2029 és 2031 között mintegy 1,7-szeresére növelve. Európában az előrejelzések szerint a piacvezetők a továbbiakban is a Meta szolgáltatásai (WhatsApp, Messenger), az iMessage, a Telegram, a Signal, és a Viber mellett.

- A 2.4.; 3.2.; 3.3.; 4.1.; 4.3.; 4.4. alfejezetek alapaján a Meta hatósági adatszolgáltatási attitűdjének tendenciaelemzése során megállapításra kerül a szolgáltatóhoz beérkező hatósági megkeresések globális számának exponenciális növekedése, amely a mobilinternet fogalom bővülésével azonos tendenciát mutat. Bizonyítható az internet alapú titkosított kommunikációt biztosító alkalmazásszolgáltatások bűnüldözési, nemzetbiztonsági érdeket sértő tevékenységgel való fokozódó érintettsége. A fokozódó személyes adatvédelmi előírások és a kereslet következtében az alkalmazásszolgáltatások kriptográfiai tulajdonságainak, elsősorban a központi DPI monitoring technikai LI módszer hatékonyságát kiemelten korlátozó E2EE fejlődése, egyben olyan jogellenes tevékenységek, mint a feldolgozott esettanulmányok alapján a terrorizmus, szervezett bűnözés, extrémizmus stb. számára is konspiratív lehetőséget biztosít. Sem tagállami szinten, sem az EU-t vizsgálva álláspontom alapján jelenleg nincsen hatályos hatékony bűnüldözési célú uniós jogi eszköz, és nemzetbiztonsági célú multilaterális együttműködés az USA-beli anyavállalattal és például írországi EU disztribúciós székhellyel rendelkező globális alkalmazásszolgáltatók (Meta, Apple) együttműködés alapú LI-je tekintetében.

- A 2.5.; 3.3.; 4.4. alfejezetek alapján a jogalkotó mind a hazai nemzetbiztonsági és bűnüldözési célú LI, mind a bűnüldözési célú nemzetközi LI együttműködés tekintetében a végrehajtásra az NBSZ-t jelölte ki mára, mint hazai központi LI szolgáltató szervezet, mely szolgáltatást nyújt a megrendelő nemzetbiztonsági, rendvédelmi, igazságügyi szervek számára speciális titkos információgyűjtő eszközeivel, módszereivel. Összevetve a 2015/2016-os kutatási eredményekkel, akkoriban az LI decentralizáltabb volt, akkor még nem nyerte el a mai centralizált, egy szervezetbe koncentrált formáját, amely mind jogalkalmazási egységességet, erőforrásoptimalizációt, koncentrált K+F+I tevékenységet, és ágazati szintű független szervezeti belső kontrollt is biztosít. A 2.5. alfejezetben feltárásra került, hogy az igazságügyi miniszteri és bíró engedélyhez kötött nemzetbiztonsági célú titkos információgyűjtés, így az LI számossága is átlagosan

laposabb exponenciálisan növekvő tendenciát mutat, az előrejelzések szerint előrejelezhető a nemzetbiztonsági ügyjelleg dominanciája. Az aktuális képességfejlesztési törekvéseket pedig a nyílt szakirodalom alapján alátámasztja a TIF, InfoLab, MiLab tudományos, kutatás-fejlesztési formációk létrejöttét, és azok céljai.

- A 2.5.3. részfejezet alapján az LI hagyományos rendszertani osztályozása az alkalmazásszolgáltatások kriptográfia kihívásainak az FBI által vezetett nemzetközi bűnüldözési koalícióban végrehajtott „Trójai Pajzs" akció keretében megvalósuló egyedi kezelése során a „lehallgathatatlannak" titulált ANOM alkalmazásszolgáltatás (NI-ICS) szervezett bűnözői körökben történő elterjesztésével, és ellenőrzésének konspirált technikai biztosításával kiegészült az új, innovatív „hamis zászlós" LI módszerrel.

Alátámasztásra került a **2. hipotézis**, miszerint a jövőben a légi, világűr infrastruktúrára épülő elektronikus hírközlő hálózatok várható elterjedése, valamint az újgenerációs mobilhálózatok LI-je forradalmasíthatja az összadatforrású titkos információgyűjtés technikai képességeit az egyre heterogénebb jellegű és forrású adatforgalom okán, amennyiben az információgyűjtő szervezetek képesek technológiai szempontból kiaknázni a lehetőségeket, például a kutatómunka során elméletben kidolgozott „Integrált Smart LI" (értekezésben: ISLI) koncepció keretében. . Az egyes alfejezetek kutatási cselekményei alátámasztják a hipotézist az alábbiak szerint:

- A 2.5.; 3.1.; 3.2.; 3.3.4.; 4.4. alfejezetek cselekményei során trendelemzési kutatási módszerrel megállapításra került a globális, de elsősorban európai viszonylatban az elektronikus hírközlési szolgáltatások nemzetiállami jellegének eltolódása a régiós, globalizálódó jelleg irányába, melyet alátámaszt a 6G alapú, MI támogatott, integrált VHetNet elektronikus hírközlő koncepció. Így a hírközlési LI tekintetében indokolt és szükséges a régiós prognosztikus előrejelzések figyelembevétele a hazai LI K+F+I-je és a jogalkotás szempontjából, amelyek az elkövetkező 6 éves időszakban a közép-kelet-európai régióban a lakossági célú, személyközi hírközlési kommunikációt érintően a 4G vezető szerepét vetítik előre, az 5G exponenciális erősödése, majd a 4G fokozatos kiszorítása mellett. Magyarország a 2030-ig szóló Űrstratégiájának célrendszere alapján erőteljes szerepet kíván betölteni az űripar fejlesztésében, és innovatív szolgáltatásainak hazai elterjesztésében, például a hírközlés területén, mely már aktuálisan is indokolttá teszi az LI képesség biztosítására irányuló ilyen jellegű kutatásokat, a fejlesztések előkészítését.

- A 2.7.; 3.1.; 3.2.; 3.3.; 4.4. alfejezetek részkutatási eredményei alapján a jövőben az 5G, 6G elektronikus hírközlő hálózatokon rendkívül nagy mennyiségű, és igen heterogén típusú adat fog megjelenni, például az okos város komplex digitális ökoszisztéma egyes olyan szolgáltatásai tekintetében, melyek mind a terrorizmus, illegális migráció, transznacionális szervezett bűnözés elleni tevékenység során hozzáadott értéket képezhetnek a nemzetbiztonsági, bűnüldözési célú LI számára. Optimális stratégiai kutatás-fejlesztési irányként a 3.3.2. részfejezetben bemutatott és bizonyított ISLI koncepció szerinti LI képesség kialakítását javaslom.

- A 6G alapú VHetNet műholdas hírközlési infrastruktúra előrejelzések szerinti 2030/2040 körüli elterjedése esetén legalább uniós szintű nemzetközi együttműködés keretében, a nemzeti szuverenitást tiszteletben tartó ISLI 2.0. koncepció szerinti LI képesség lehetőségének megvizsgálását javaslom. Az ISLI 2.0. képesség lehetősége kapcsán felmerül a nemzetbiztonsági tevékenység szupranacionális uniós jog alóli kivétel jellege, továbbá az egyes alkalmazásszolgáltatások kriptográfiai környezete is erőteljesen befolyásolja a koncepció hatékonyságát, így a kérdéskör további vizsgálata indokolt. A 4.4.3. részfejezetben javasolt szolgáltatói együttműködésen alapuló bűnüldözői és nemzetbiztonsági célú LI modell álláspontom alapján a kor elvárásai szerint automatizálható, elektronikus adatkapcsolat útján megvalósuló technikai LI módszerré is átkonvertálható az ISLI modell keretében. Azonban az ISLI koncepció is csak akkor tud teljes körű hatékonyságot biztosítani, ha az E2EE visszaszorítása esetén sikerül egy olyan nemzetközi standardizált kriptográfiai eljárás megalkotása, amely egyszerre biztosítja az LI eredményességét a megfelelő szintű adatvédelemmel egyetemben, így biztosítva az adatvédelem/biztonság értékduáljának kiegyensúlyozott érvényesülését.

Igazolásra került a **3. hipotézis**, miszerint az alkalmazásszolgáltatások globalizációja, a nemzetközi adatvédelmi normatív és technológiai környezet fejlődése hátrányosan érintheti az azokon végbement kommunikáció LI-jének hatékonyságát, valamint azok kriptográfiai fejlődésének hatására a kommunikációellenőrzést szabályozó hatályos hazai normarendszer hatékonysága erodálódhat, e téren az LI képesség rezilienciája korlátozódhat. Az egyes alfejezetek kutatási cselekményei alátámasztják a hipotézist az alábbiak szerint:

- A 2.7.; 4.2.; 4.3.; 4.3.; 4.4. alfejezetek kutatási cselekményei alapján a jelentősebb piacvezető alkalmazásszolgáltatók, mint például a Meta folyamatosan javítják az

alkalmazások kriptográfiai tulajdonságait a felhasználók kommunikációjának biztonságosabbá tétele valamint, marketing célból egyaránt, amely egyrészről a protokollok, algoritmusok fejlesztéséhez, másrészről az E2EE alkalmazásának általános elterjedéséhez vezetett egyfajta keresleti/kínálati öngerjesztő jelenségként. A 2014/2016-os időszakot követően napjainkra ismét egy „titkosítási verseny" kezd kialakulni az alkalmazásszolgáltatások piacán, már előre reagálva az IKT környezet fejlődésének kvantumszámítás alapú innovációjára. Bemutatásra került az alkalmazásszolgáltatásokkal kapcsolatos anonimitás kihívása, mely okán javaslatom alapján globális, de legalább is EU szinten követelményként kellene támasztani az alkalmazásszolgáltatók számára a felhasználó természetes személy regisztrációja során a mobil hívószám megadásának kötelezettségét azonosíthatósági célból. Így a jogosult rendvédelmi szervek, akár nemzetbiztonsági célú LI keretében közvetetten ugyan, de hazai viszonylatban az Eht. mögöttes szabályai alapján már jóval hatékonyabban be tudnák azonosítani az LI-vel érintett valós felhasználót.

- A 2.5.; 2.7.; 3.1.; 3.3.; 4.2.; 4.3.; 4.4. alfejezetekben elvégzett kutatási cselekmények szerint az úttörő Ekertv. 3/B. és 13/B. § szerinti szolgáltatói együttműködés alapú alkalmazásszolgáltatói LI szabályozás időtállósága kapcsán levonható következtetés, hogy az a 2.4.1. részfejezet alapján már a hatálybalépésének időpontjában is korlátozottan volt hatékony – hiszen a technológiasemlegesség elvének érvényesülnie kellett – tekintettel arra, hogy a vizsgált alkalmazásszolgáltatások ¾-e addigra már E2EE-t alkalmazott. A rendelkezések hatékonyságának aktualitását nézve megállapítható, hogy az E2EE alapértelmezettségének folyamatos terjedésével, valamint legújabban a kvantumszámításnak is ellenálló kriptográfia megjelenésével tovább korlátozódik.

- A 2.4. és 4.3. alfejezet részkutatásai alapján megállapításra került, hogy az IKT környezet fejlődéséből adódó EU-s digitalizációs stratégiai célkitűzések koherens, következetes jog- és szakpolitikai törekvést követnek a felhasználói adatvédelem, bizalom fokozását célzó normatív és technológiai információbiztonság erősítése érdekében, így elősegítve a digitális, IKT termékek és szolgáltatások elterjedését elsősorban gazdaság-, társadalompolitikai okokból. Azonban az alkalmazásszolgáltatások és az LI globális piacainak összehasonlító volumenelemzése árnyalja a fenti megállapítást, miszerint az LI piac volumene 2030-ig kb. 4-5%-a lesz az alkalmazásszolgáltatások globális piacának. Így nem zárható ki a magasabb technológiai (elsősorban kriptográfiai) K+F+I beruházási

erőforrásokkal rendelkező piacvezető „zászlóshajók” lobbitevékenysége sem a fokozódó felhasználói adatvédelmi igények marketing jellegű megalapozás érdekében, és a szabályozás szigorítása céljából, így növelve piaci részesedésüket, terjeszkedésüket, végső soron a profitjukat, a versenytársak kiszorításával egyetemben, de ez már inkább versenyjogi kérdéseket felvető következtetés. A marketing jellegű fölény pedig abban teljesedhet ki a biztonság szempontjából negatívan, miszerint az alkalmazások az E2EE kapcsán hirdetik tájékoztatójukban, hogy az erős kriptográfia által a felhasználók kommunikációs adatai „biztonságban vannak” még a szolgáltató előtt is – így ebből következtetve a kormányzati, nemzetbiztonsági, bűnüldöző szervek, hatóságok előtt.

Bizonyításra került a **4. hipotézis**, miszerint a jövőben a személyközi hírközlési szolgáltatások – beleértve az alkalmazásszolgáltatásokat is – keretében végbement kommunikáció nemzetbiztonsági célú LI-jének hatékonysága érdekében nélkülözhetetlen lesz a nemzetközi, uniós együttműködés fokozása, az információcserén túl a jövő LI képességei kialakításának lehetőségét is figyelembe véve, a nemzeti szuverenitás tiszteletben tartása mellett. Az egyes alfejezetek kutatási cselekményei alátámasztják a hipotézist az alábbiak szerint:

- A 2.1.; 2.3; 3.1.; 3.3.; 4.3. részfejezetek kutatási cselekményei, a nemzetközi kitekintés, együttműködések vizsgálata alapján az Európai Unió terrénumán a bűnüldözési célú LI-re irányuló tagállamközi együttműködéssel ellentétben, a nyilvános szakirodalom alapján a nemzetbiztonsági célú LI vonatkozásában továbbra sem tapasztalható akár csak a részleges multilaterális együttműködés normatív keretrendszerének kialakítására irányuló szervezett törekvés. Azonban álláspontom alapján a nemzetbiztonsági célú tevékenységnek, titkos információgyűjtésnek, így az LI-nek vannak a szabályozás áttöréséhez vezethető olyan vetületei, amelyek az egymással együttműködő tagállamok szuverenitására és biztonságára pozitívan hatnak. Ilyen a nemzetbiztonsági célú, de bűnüldözési érdekkörben is értelmezhető tevékenység például az Nbtv. 74. § ae) alpont szerinti nemzetbiztonsági érdek körében értelmezett terrorizmus, transznacionális szervezett bűnözés, például a fegyver-, kábítószer-, ember-, műkincskereskedelem megelőzésében, felderítésében, megakadályozásában és elhárításában való közreműködés adott nemzetbiztonsági szolgálat által. Továbbá ebbe a kategóriába sorolható az illegális migrációt, a szövetséges államok szuverenitásába beavatkozó harmadik állam és nem kormányzati szerv tevékenységét, az emberiesség elleni bűncselekményeket.

- Az értekezés komplex részkutatási eredményei szerint a hírközlési LI tevékenység már az 5G, de igazából a 6G kapcsán megjelenő VHetNet légi és világűr hírközlő infrastruktúrái már csak elhelyezkedésükből adódóan is fel fogják vetni az EU szintjén a tagállami joghatóságok kollízióját, amit a GDPR adatvédelmi oldalról prognosztikusan már igyekezett kezelni. A tagállami alkalmazandó jogok összeütközése az LI szabályozása és végrehajtása terén is jelentkezni fog. Így elengedhetetlen az uniós szintű felsőbb keretjogalkotás a jövő hatékony LI képességeinek kialakítása érdekében, például a 3.3.2 részfejezetben javasolt ISLI modell szerint. A jövő sikeres LI tevékenysége szempontjából elengedhetetlen a formális, jogi kötőerővel és hatékony kikényszeríthetőséggel bíró nemzetközi együttműködés a globális alkalmazásszolgáltatók LI terén megvalósuló jogkövető magatartásra bírása érdekében, egyben uniós jogalkotást is magával hozva, együttműködve az USA-val, például a 4.4.3. részfejezetben javasolt bűnüldözési és nemzetbiztonsági célú nemzetközi szolgáltatói együttműködés alapú LI szabályozási keret szerinti módon, mely elvi modellje alapján átkonvertálható az ISLI-be integrálható DPI monitoring technikai LI módszerré. A javasolt LI modellek hatékonyságának foka nagyban függ az E2EE-t korlátozó olyan normatív intézkedésektől, amelyek mellett azonban érvényesülni tudnak a személyes adatvédelmi törekvések, egyensúlyban tartva az adatvédelem/biztonság értékduált, de mégis felszámolva a már jelenleg is fennálló „IKT LI adatvédelmi biztonság-deficitet”.

A kutatómunka további érdemi eredményeként feltárásra és bizonyításra került, hogy a nemzetközi, uniós adatvédelmi törekvések, piaci igények hátrányosan érintik az LI tevékenység hatékonyságát az adatvédelem/biztonság értékduált vizsgálva a biztonság hátrányára egyfajta „IKT adatvédelmi biztonság-deficit”-et előidézve, az azokkal visszaélő egyes globális IKT szolgáltatók pedig kialakítottak egyfajta vitathatóan legitim kvázi „törvényességi kontrollt”, mely keretében intézményesülten magas százalékban tagadják meg az LI jogosult szerveztek nemzeti jogrendjén alapuló adatszolgáltatási megkereséseit. A 3.3.; 4.3.; 4.4. alfejezetek kutatási cselekményei alátámasztják a fenti kutatási eredményt az alábbiak szerint:

- A kutatómunka során azonosításra és alátámasztásra került az „**IKT adatvédelmi biztonság-deficit**” teória, elmélet, mely során az adatvédelem a biztonság hátrányára érvényesül az adatvédelem/biztonság értékduál egyensúlyával szemben. A 3.3.; 4.3.; 4.4. alfejezetek kutatási cselekményei alapján a fokozódó uniós adatvédelmi előírások, a kriptográfia erősödése hátrányosan érintik/ fogják érinteni az LI hatékonyságát, így a

nemzet- és közbiztonság alkotmányos közérdekek érvényesülését. Ennek oka, hogy az Unió éppen a felhasználói bizalom erősítése, a többlet fogyasztás elősegítése, így végső soron a gazdasági növekedés érdekében fogalmazza meg az IKT termékeket és szolgáltatásokat érintő fokozott adatvédelmi követelményeket. Azonban, ha ezáltal a nemzetbiztonsági, bűnüldözési célú LI korlátozottsága miatt végsősoron közvetve sérül az egyes tagállamok, így összességében az EU biztonsághoz fűződő közérdek érvényesítését célzó eszközrendszerének hatékonysága, akkor össztársadalmi szinten csökken a komplex biztonság. Mindez a vállalkozások eredményességén és a fogyasztás visszaesésén keresztül hátrányosan érheti a gazdasági növekedési törekvéseket, így az általános digitális ökoszisztéma, a digitális társadalom megteremtésének uniós szakpolitikai, stratégiai célját. Tehát az E2EE általi „túltitkosítás" közvetlen nemzetbiztonsági, bűnüldözési érdeket sérthet az LI-vel érintett célszemélyek kommunikációja ellenőrzési hatékonyságának korlátozása okán, mely jelentőségét az ENSZ Emberi Jogi Főbiztosának fellépése is jelzi. A CSAM[15] vita is mutatja az adatvédelem/biztonság kiegyensúlyozott értékduáljának adatvédelem felé történő kibillenését. A CSAM potenciális egységkovácsoló lehetőséget hordoz magában az EU politikai vezetése szintjén, egyben eddig nem látott lendülettel, ami az E2EE közbiztonsági, bűnüldözési célú korlátozását jelenti, így megnyitva a lehetőséget az „IKT adatvédelmi biztonság-deficit" visszabillentésére a biztonság javára.

- Azonosításra és bizonyításra került a globális alkalmazásszolgáltatók együttműködés alapú hatósági adatszolgáltatási megkeresések igencsak vitathatóan legitim kvázi **„törvényességi kontrollja**" és a teljesítés korlátozásának 10 éves ilyen jellegű gyakorlata, amely a nemzetbiztonsági és bűnüldözési célú LI során is érvényesül, így közvetlenül sértve a nemzetbiztonsági, bűnüldözési érdeket. A 4.3.; 4.4. alfejezetek kutatási cselekményei során megállapításra került, hogy a Meta a hatósági együttműködések keretében az egyes tagállamok jogosult hatóságai, így LI szervezetei által közvetlenül megküldött megkeresések kb. ¼-ének teljesítését megtagadja egyfajta, álláspontom szerinti vitathatóan legitim szolgáltatói „törvényességi kontroll" keretében. Ezen „intézményesült" gyakorlat sérti az egyes demokratikus államok szuverenitását, biztonsági érdekeit, hiszen az alkotmányos garanciák, a hatalmi ágak szétválasztása, a fékek és egyensúlyok érvényesülése mellett történő közhatalom gyakorlása során az állami kényszer legitim és feltétlen. A fentiek alapján elengedhetetlen a jövő sikeres LI tevékenysége szempontjából

[15] CSAM: Child Sex Abuse Regulation material – gyermek szexuális abuzálása elleni rendelet tervezet

a formális, jogi kötőerővel és hatékony kikényszeríthetőséggel bíró nemzetközi együttműködés a globális alkalmazásszolgáltatók LI terén megvalósuló jogkövető magatartásra bírása érdekében, mely terrénuma álláspontom alapján az európai országok tekintetében az EU kell, hogy legyen, egyben uniós jogalkotást is magával hozva, együttműködve az USA kormányzati szerveivel, IKT szolgáltatóival.

Egyéb kiemelt következtetések, megállapítások:

A hazai biztonsági stratégiai evolúciós elemzés során láthatóvá vált, hogy a „nemzetbiztonsági érdek", így az abból absztrahálható „nemzetbiztonsági célzat" tartalma dinamikusan, a kor elvárásai mentén változik, alakul a hagyományos területektől elmozdulva a digitális kihívások, vagy éppen a K+F+I irányába. Megállapításra és bizonyításra került, hogy az uniós jog hazai jogforrási etimológiai és tartalmi interpretálása során a „nemzetbiztonság" fogalom alkalmazása nem egységes, nem konzekvens, összemosódik a „nemzeti biztonság" az „állam biztonsága" fogalmakkal, amely pedig a normaalkalmazás során kihívásként azonosítható. Továbbá a 2.3.2. részfejezetben az Infotv. alapján ismertetésre került a nemzetbiztonsági és bűnüldözési célzat adatkezelési szempontú értelmezése.

Feltárásra és bizonyításra került az Ekertv. tárgyi hatálya szerinti alkalmazásszolgáltatásnak az Eht. tárgyi hatálya szerinti NI-ICS-sel való összefüggése az Ekertv. és az Eht., DMA, Hírközlési Kódex alapján, illetve azok funkcionális azonossága okán előállva az Ekertv. és az Eht. tárgyi hatályának összeütközése, konfliktusa. A 2.4., 2.6.; 3.3.; 4.4. alfejezetekben a kutatási cselekmények során megállapításra kerültek a fentiek. Az információs társadalommal összefüggő infokommunikációs és elektronikus hírközlési szolgáltatások szabályozásának integrált uniós jog- és szakpolitikai szemlélete végül a DMA és a Hírközlési Kódex kicsúcsosodása során 2023-ra lényegében a hatályos és alkalmazandó uniós jog tételévé vált. Így uniós és tagállami szintű jogalkotói, jogalkalmazói kötelezettségeket testesítve meg, az alkalmazásszolgáltatások körében először az Európai Bizottság 2023 végétől érvényesülő intézményi joggyakorlata körében a WhatsApp, Messenger és iMessage DMA szerinti alapvető platformszolgáltatások (NI-ICS/alkalmazásszolgáltatás) tekintetében. Az EU digitalizációs törekvései mentén a DMA és a DSA hatályának bázisán kialakult a digitális ágazat, amely beékelődött és jelentős hatást gyakorol mind az elektronikus hírközlési, mind a kiberbiztonsági ágazatra és szabályozásra (NIS2), amely jogterületek éles elhatárolása még az Unió szintjén is egy alakulóban lévő folyamat, nemhogy a tagállami jog szintjén. Az NI-ICS/

alkalmazásszolgáltatás szabályozása LI szempontjából egy kardinális kérdés, hiszen a DMA – és már a Hírközlési Kódex is – az NI-ICS tekintetében átnyúl az elektronikus hírközlési ágazati szabályozásba, amely hazai jogforrási szinten az Eht.-ben került adoptálásra, átültetésre, úgyhogy egyébként az Ekertv. tárgyi hatálya pedig továbbra is kiterjed az alkalmazásszolgáltatásra, mely jogi konfliktus azonosítása álláspontom alapján egy javasolt új tudományos eredmény is egyben.

Meghatározásra kerültek a 21. század IKT boom-jának, az IKT környezet alkalmazásszolgáltatásokkal kapcsolatos fejlődésének kiemelt nemzetbiztonsági érdekeket veszélyeztető olyan várható főbb kihívásai, mint az infokommunikációs felhasználói anonimitás lehetőségének fokozódása; az állami, az uniós és a nemzetközi jog „felett állás" státuszát gyakorló globális szolgáltatók hatósági együttműködése korlátozódásának veszélye; az E2EE-t integráló online kommunikációt biztosító alkalmazásszolgáltatások igénybevételének további terjedése a titkos információgyűjtéssel érintettek körében; valamint a kommunikációs szolgáltatásoknál az E2EE általánossá válása, és a további innovatív kriptográfiai eljárások fejlődése.

Az összegzett következtetések alapján tehát, az új „*nemzetbiztonsági célú LI kutatás integrált interdiszciplináris tudományos módszertana*" alkalmazásával teljesítésre kerültek a doktori értekezés fő célkitűzései az IKT környezet változásainak az információgyűjtés 21. századi fejlődésére gyakorolt hatásira irányuló hipotézisek igazolásán, valamint további kutatási eredményeken keresztül. A módszertan keretében elvégzett elemzések, vizsgálatok során elért tudományos következtetésekre alapozva olyan gyakorlatorientált, az alkalmazott kutatásokhoz integrálható nyilvános, a következő fejezetben taxatíve felsorolásra kerülő új javasolt tudományos eredmények kerültek elérésre, amelyek magukban hordozzák a hazai LI képességek hatékonyságfokozásában való közreműködés tényleges lehetőségét, elsősorban jogalkotási és kutatás-fejleszti irányok, szemléletformálás, további részkutatási irányok meghatározása által. Egyfajta keretet adva az értekezésnek, a témaválasztás és a kutatás aktualitásának záróindoklásként az Alaptörvény 2023. december 22-ei módosítása általános indokolás 3. pontját idézem, amely szerint az Alaptörvény az új tudományos és műszaki eredmények alkalmazásának, valamint a digitális ügyintézés állami szintű előmozdítására hivatott „*XXVI. cikkének […] kiegészítése mögött az a felismerés áll, hogy az információs és kommunikációs technológiák [IKT] fejlődése életünk gyökeres átalakulását hozza magával*."

8. ÚJ TUDOMÁNYOS EREDMÉNYEK

Disszertációs kutatómunkám során az értekezésben kidolgozott új tudományos eredményként történő elfogadását javaslom az alábbiaknak:

1. Bizonyítottam, hogy a prognosztizálható IKT trendek alapján a GSM alapú személyközi mobil kommunikáció hagyományos LI-jével szemben a mobilinternet alapú titkosított online kommunikációt biztosító alkalmazásszolgáltatások LI igényének fokozódása várható, amelyek szolgáltatói együttműködés alapú és technikai monitoring LI módszerei is innovatív technológiai, szabályozási és szervezeti környezetet követelnek meg. **[Bizonyítás: 2.4.; 2.6.; 3.1.; 3.2.; 3.3.; 4.1.; 4.3.; 4.4.]**

2. Alátámasztottam, hogy a jövőben a légi, világűr infrastruktúrára épülő elektronikus hírközlő hálózatok várható elterjedése, valamint az újgenerációs mobilhálózatok LI-je forradalmasíthatja az összadatforrású titkos információgyűjtés technikai képességeit az egyre heterogénebb jellegű és forrású adatforgalom okán, amennyiben az információgyűjtő szervezetek képesek technológiai szempontból kiaknázni a lehetőségeket, például a kutatómunka során elméletben kidolgozott „Integrált Smart LI” (az értekezésben: ISLI) koncepció keretében. **[Bizonyítás: 2.5.; 2.7.; 3.1.; 3.2.; 3.3; 4.4]**

3. Igazoltam, hogy az alkalmazásszolgáltatások globalizációja, a nemzetközi adatvédelmi normatív és technológiai környezet fejlődése hátrányosan érinti az azokon végbement kommunikáció LI-jének hatékonyságát, valamint azok kriptográfiai fejlődésének hatására a kommunikációellenőrzést szabályozó hatályos hazai normarendszer hatékonysága erodálódik, e téren az LI képesség rezilienciája korlátozott. **[Bizonyítás: 2.4.; 2.5.; 2.7.; 3.1.; 3.3.; 4.2.; 4.3.; 4.3.; 4.4.]**

4. Bizonyítottam, hogy a jövőben a személyközi hírközlési szolgáltatások – beleértve az alkalmazásszolgáltatásokat is – keretében végbement kommunikáció nemzetbiztonsági célú LI-jének hatékonysága érdekében nélkülözhetetlen lesz a nemzetközi, uniós együttműködés fokozása, az információcserén túl a jövő LI képességei kialakításának lehetőségét is figyelembe véve, a nemzeti szuverenitás tiszteletben tartása mellett. **[Bizonyítás: 2.1.; 2.3.; 2.4.; 2.6.3.; 3.1.; 3.2.; 3.3.; 4.1.; 4.2.; 4.3.; 4.4.]**

5. Feltártam és bizonyítottam, hogy a nemzetközi, uniós adatvédelmi törekvések, piaci igények hátrányosan érintik az LI tevékenység hatékonyságát az adatvédelem/biztonság értékduált vizsgálva a biztonság hátrányára egyfajta „IKT adatvédelmi biztonság-deficit”-et előidézve, az azokkal visszaélő egyes globális IKT szolgáltatók pedig kialakítottak egyfajta vitathatóan legitim kvázi „törvényességi kontrollt”, mely keretében intézményesülten magas százalékban tagadják meg az LI jogosult szervezetek nemzeti jogrendjén alapuló adatszolgáltatási megkereséseit. **[Bizonyítás: 3.3.; 4.3.; 4.4.]**

9. AJÁNLÁSOK, A KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLHATÓSÁGA

A disszertációs kutatómunka során elért eredmények gyakorlati felhasználhatósága az értekezése egyik fő célkitűzése a tényleges pozitív társadalmi hatás kiváltása érdekében. Az eredmények, következtetések álláspontom alapján valós hozzáadott értéket képezhetnek a komplex biztonsági ökoszisztéma számára, így azok gyakorlati felhasználását az alábbi ajánlások szerint javaslom mind a hazai, mind az uniós, nemzetközi jogalkotás, a nemzetbiztonsági ipari Triple Helix modell szerinti K+F+I ágazati, akadémia és egyetemi, valamint piaci szereplői számára, továbbá a felsőfokú és doktori képzések során.

Hazai, uniós és nemzetközi jogalkotás:

Javaslom a 2. hipotézis bizonyításával kapcsolatos eredmények, valamint az Eht. és Ekertv. hatályának összeütközésével kapcsolatos megállapítások felhasználását a hírközlési és online platform jogalkotás keretében. Javaslom a 1.-4. hipotézisekkel összefüggő eredmények, valamint a nemzetközi jogforrásokban megjelenő „nemzetbiztonság” fogalom eltérő hazai interpretálásával, továbbá a hatósági adatkérések vitathatóan legitim alkalmazásszolgáltatói „törvényességi kontrolljával” kapcsolatos megállapítások hasznosítását a nemzetbiztonsági és bűnüldözési célú titkos információgyűjtéssel, LI-vel kapcsolatos jogalkotás során. Javaslom a személyes adatvédelemmel kapcsolatos jogalkotás során szemlézni a 3. hipotézissel kapcsolatos megállapításokat. Javaslom a gyermekek szexuális kizsákmányolása elleni uniós jogalkotás keretében a 3.-4. hipotézisek eredményeinek hasznosítását, mely hazai vetületű aktualitását, és a magyar álláspont fokozottabb érvényesíthetőségét a 2024 második féléves Magyarország általi EU Tanács soros elnöksége még inkább elősegíthet.

Ágazati nemzetbiztonsági ipari K+F+I:

Javaslom az 1-4. hipotézis bizonyítása, vizsgálata során feltárt eredmények hasznosítását a nemzetbiztonság elméleti kutatások, továbbá az LI gyakorlati kutatás-fejlesztés, a kettős felhasználási lehetőségek vizsgálata során. Ezen eredményeket különösen figyelmébe ajánlom a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal felügyeletében működő InfoLab, MiLab, illetve a KNBSZ IKK keretében zajló alkalmazott kutatások számára. Továbbá a TIF keretében folyó polgári nemzetbiztonsági tudományos munka, alapkutatások számára.

Akadémiai és egyetemi nemzetbiztonsági ipari K+F+I:

A HUN-REN figyelmébe ajánlom az 1-3. hipotézisek vizsgálata keretében elért eredmények hírközlési, online platform kutatás során történő hasznosítását. Az NKE figyelemébe ajánlom a formális had- és rendészettudományi doktori, azon belül is nemzetbiztonsági kutatási céllal az 1. és 3. hipotézisekkel összefüggő eredmények falhasználását. A BME figyelmébe ajánlom szintén az 1. és 3. hipotézisek hasznosítását, különösen a CrysyLab keretében zajló kriptográfiával, kibervédelemmel kapcsolatos alkalmazott kutatások számára. A Pázmány Péter Katolikus Egyetem (a továbbiakban: PPKE), valamint a Pécsi Tudományegyetem (a továbbiakban: PTE) állam- és jogtudományi doktori, valamint felsőfokú képzései során figyelembe ajánlom az 1. és 4. hipotézisekkel, a „nemzetbiztonság" fogalom eltérő hazai interpretálásával, továbbá az alkalmazásszolgáltatói „törvényességi kontrollal" kapcsolatos megállapítások jogtudományi hasznosítását, akár új kutatási irányok meghatározása céljából.

Piaci nemzetbiztonsági ipari K+F+I:

Javaslom az 1.-4. hipotézisek vizsgálata során feltárt eredmények, megállapítások hasznosítását olyan kutatási területeken, mint a MI, az autonóm rendszerek, és a diszruptív IKT technológiák, elsősorban az ipari K+F technikai támogatása, valamint a nemzeti innovációs platformokhoz való hozzájárulás érdekében. Javaslom az eredmények hazánkban és a régióban rendelkezésre álló mélyreható szakértelem kiaknázásával, a jövőbeni védelmi képességeknek, így a komplex védelmi innovációs ökoszisztémának a kettős felhasználású termékek és szolgáltatások fejlesztése során történő felhasználását. Javaslom az eredmények hasznosítását például az európai információs műveletekkel foglalkozó kettős felhasználási célú K+F projektek keretében, az EU tagállamai közös biztonságának növelése, az európai védelmi piac integrációjának és hatékonyságának fokozása céljából.

Oktatás, képzés:

Figyelembe ajánlom az értekezés következtetéseinek, kutatási eredményeinek általános hasznosítását az NKE számára a nemzetbiztonsági elméleti oktatás, a BME számára a kibervédelem és nemzetbiztosági technológiák gyakorlati kapcsolódásaival kapcsolatos képzés, valamint a PPKE, PTE számára nemzetbiztonsági, hírközlési jogi képzés során. Továbbá aktualitás, időszerűség, szükségesség esetén javaslom a nemzetbiztonsági célú LI tevékenység jogállami garanciális feltételeinek való magas szintű megfelelése alátámasztásának lakossági tájékoztatási célú, tudományos megalapozottságú edukációs, kommunikációs felhasználását.

10. AZ ÉRTEKEZÉS BENYÚJTÓJÁNAK A TÉMAKÖRBŐL KÉSZÜLT PUBLIKÁCIÓS JEGYZÉKE

1. DOBÁK Imre – TÓTH Tamás (2023). A külső környezet és tendenciák nyomon követésének szükségessége a stratégiaalkotás tükrében. In DOBÁK Imre – RESPERGER István (szerk.): *Stratégiák, stratégiai gondolkodás, nemzetbiztonság*. Budapest: Ludovika Egyetemi Kiadó. 33–50. ISBN: 978-963-531-85-1-3
2. TÓTH Tamás (2023): Actualities of certain security aspects of cryptography with regard to information societies. *National Security Review*, 9(1), 107-118. ISSN 2416-3732
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2023_1_NSR.pdf#page=107
3. TÓTH Tamás (2022): Magyarország Nemzeti Biztonsági Stratégiájának nemzetbiztonsági aspektusú elemzése. *Szakmai Szemle*, 20(3), 69-99. ISSN 1785-1181
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_3_szam.pdf
4. TÓTH Tamás (2022): Az információgyűjtés új típusú kihívásai a mobil hírközlési hálózatok technológiai fejlődésének aspektusából. In SZELEI Ildikó (szerk.): *A hadtudomány aktuális kérdései napjainkban II*. Budapest: Ludovika Egyetemi Kiadó. 105-122. ISBN: 978-963-531-61-6-8
   Online: https://webshop.ludovika.hu/termek/konyvek/hadtudomany/a-hadtudomany-aktualis-kerdesei-napjainkban-ii/

5. TÓTH Tamás (2022): Magyarország nemzeti biztonsági stratégiai evolúciója, annak aktualitásai és főbb nemzetbiztonsági vetületei. *Szakmai Szemle*, 20(2), 58-73. ISSN 1785-1181
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_szam.pdf#page=58.

6. DOBÁK Imre – TÓTH Tamás (2022): Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle*, 69(2), 195-212. ISSN 2677-1632
   Online: https://ojs.mtak.hu/index.php/belugyiszemle/article/view/5345/4209

7. TÓTH Tamás (2020): A mobilhálózatok technológiai fejlődéstörténete: Az analóg hangátviteltől az 5G-hálózatokig. *Nemzetbiztonsági Szemle*, 7(4), 44-60. ISSN 2064-3756
   Online: https://doi.org/10.1007/s11276-015-1165-z

8. TÓTH Tamás (2020): Az információgyűjtő szervezetek technikai képességeire ható külső közvetett tényezők. *Felderítő Szemle*, 19(2), 43-57. ISSN 1588-242X
   Online: https://www.knbsz.gov.hu/hu/letoltes/fsz/2020-2.pdf#page=43

9. TÓTH Tamás (2020): Az egyes social engeneering módszerek elhatárolása és rendszerezése. *Szakmai Szemle*, 18(1), 87-110. ISSN 1785-1181
   Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2020_1_szam.pdf#page=87

10. TÓTH Tamás (2020): New challenges of recruiting personnel for the national security services in light of the information society. *Belügyi Szemle*, 68(2 – Special Issue), 125-139. ISSN 2677-1632
    Online: http://doi.org/10.38146/BSZ.SPEC.2020.2.9

11. TÓTH Tamás (2019). A Nemzetbiztonsági Szakszolgálat felvételi eljárási rendszere. *Belügyi Szemle*, 57(1), 53-67. ISSN 2677-1632
    Online: http://doi.org/10.38146/BSZ.2019.1.4

12. TÓTH Tamás (2019): General description of social engineering and its place in information warfare. *National Security Review*, 5(1), 42-55. ISSN 2416-3732
    Online: https://doi.org/10.38146/BSZ.SPEC.2020.2.9

13. TÓTH Tamás (2019): Az Európai Unió tervezett kiberbiztonsági tanúsítási keretrendszerének bemutatása *Szakmai Szemle*, 17(1), 97-115. ISSN 1785-1181
    Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2019_1_szam.pdf

14. TÓTH Tamás (2019): A digitális alapú, integritás centrikus közszolgálati szervezetek személyi integritását sértő tényezőinek kialakulása, valamint kihívásaik az információs társadalom tükrében. *Rendvédelem*, 8(1), 50–132.ISSN 2560-2349
Online:https://epa.oszk.hu/03300/03353/00014/pdf/EPA03353_rendvedelem_2019_1_050-132.pdf

15. TÓTH Tamás (2018): A NATO Kibervédelmi Kiválósági Központ bemutatása. *Nemzetbiztonsági Szemle*, 6(4), 48–62. ISSN 2064-3756
Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1485/804

16. TÓTH Tamás (2018): Humán kockázatok a kritikus információs infrastruktúrában. *Rendvédelem*, 7(1), 149–176. ISSN 2560-2349
Online:https://epa.oszk.hu/03300/03353/00012/pdf/EPA03353_rendvedelem_2018_1_150-177.pdf

17. TÓTH Tamás (2018). Az üzleti információszerzés új kihívásai a szervezett bűnözés XXI. századi paradigmaváltásának következtében. *Szakmai Szemle*, (1), 102–122. ISSN 1785-1181
Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2018_1_szam.pdf

11. AZ ÉRTEKEZÉS BENYÚJTÓJÁNAK SZAKMAI-TUDOMÁNYOS ÉLETRAJZA

Tóth Tamás 2014-től tölt be tiszthelyettesi, tiszti, majd vezetői beosztásokat kezdetben a Pest Vármegyei Rendőrfőkapitányság, majd a Nemzetbiztonsági Szakszolgálat állományában. 2015-ben szerzett rendőr-tiszthelyettes szakképesítést, majd 2017-ben az NKE RTK-n rendészeti igazgatás-szervezőként főiskolai végzettséget, 2019-ben az NKE HHK-n okleveles nemzetbiztonsági szakértői egyetemi végzettséget. Folytatta tanulmányait és 2020-ban az NKE KTI-n elektronikus információbiztonsági szakirányú vezetői szakképesítést, 2023-ban az NKE ÁNTK-n okleveles kiberbiztonsági szakértői egyetemi végzettséget kapott, 2024-ben a PPKE JÁK-n okleveles jogász egyetemi végzettség megszerzése várható. Angol és spanyol idegennyelvekből rendelkezik komplex középfokú nyelvismerettel.

Tagja a Magyar Hadtudományi Társaság Nemzetbiztonsági Szakosztályának, a Magyar Rendészettudományi Társaság Polgári Nemzetbiztonsági Tagozatának, a Hírközlési és Informatikai Tudományos Egyesület Információbiztonsági Szakosztályának, ellátta a Belügyi

Tudományos Tanács Mesterséges Intelligencia Munkacsoportjának titkári feladatait, továbbá részt vett az NKE Nemzetbiztonsági Szakkollégium munkájában. A Belügyminisztérium közigazgatási államtitkára kétszer adományozott számára elismerő oklevelet a Belügyi Tudományos Tanács által kiírt tudományos pályázatokra benyújtott pályaművei elismeréséül.

Kutatási témájában eddig összesen 15 hazai lektorált tudományos mértékadó folyóirat cikket publikált melyekből 3 idegennyelvű, továbbá 2 könyvfejezetet, és 3 absztraktot is jegyez. Rendszeres előadója a polgári nemzetbiztonsági szféra zárt szakmai-tudományos konferenciáinak, továbbá pályázatával részt vett a XXXIII. Országos Tudományos Diákköri Konferencia Had- és Rendészettudományi Szekcióján. Kutatási témájához kapcsolódóan óraadóként is részt vesz az NKE tevékenységében, az NKE Nemzetbiztonsági MSc/BSc képzésein diplomamunka témavezetői, szakdolgozat bírálói feladatokat is ellát. Aktív résztvevője a nemzetbiztonsági és a tudományos szféra együttműködésének.